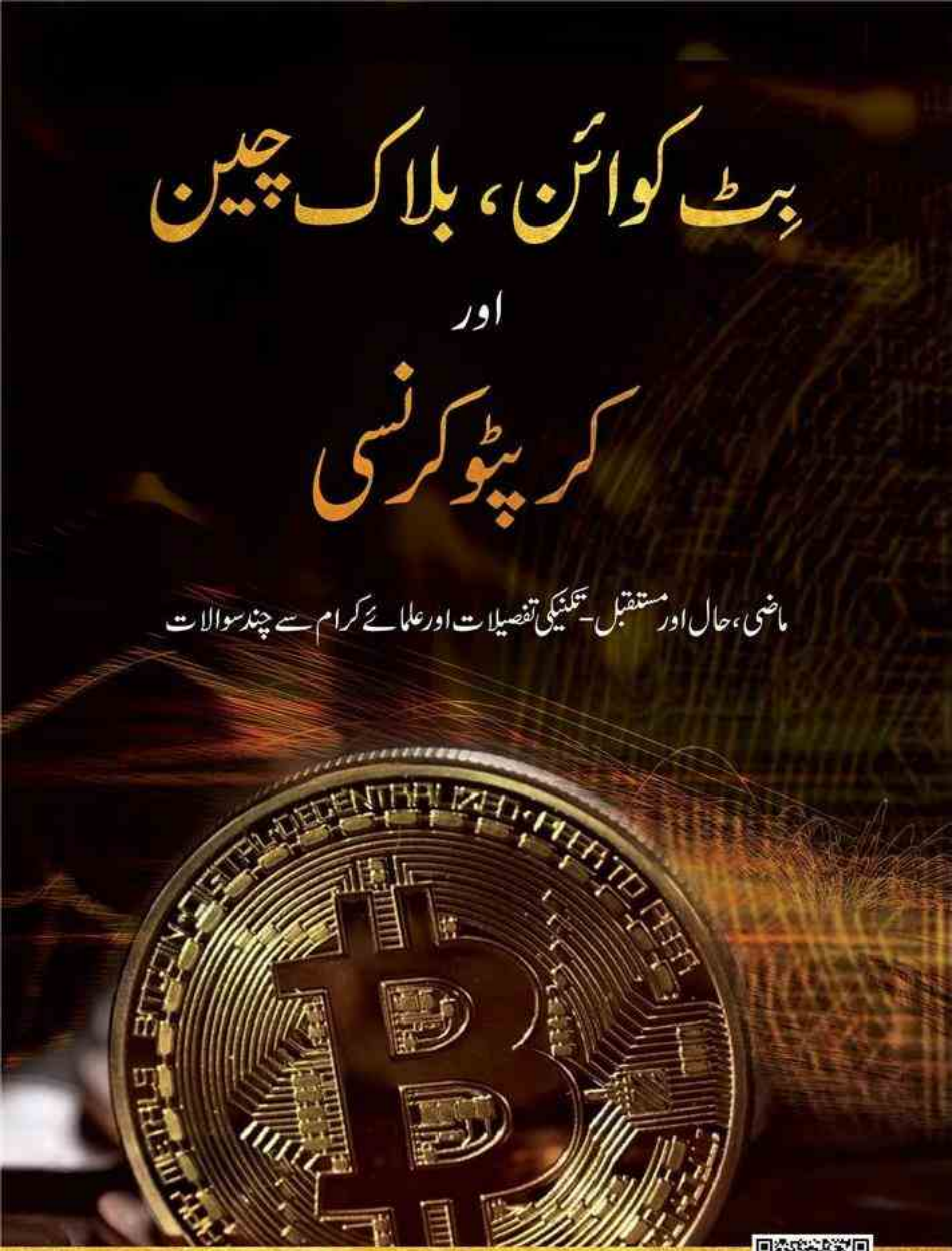
بِٹ کوائن، بلاک چین

اور

کرپٹو کرنسی

ماضی، حال اور مستقبل۔ تکنیکی تفصیلات اور علمائے کرام سے چند سوالات



ذیشان الحسن عثمانی

ساقی ارباب ذوق

PDF BOOK COMPANY

مدد، مشاورت، تجاویز اور شکایات :

Muhammad Husnain Siyalvi
0305-6406067
Sidrah Tahir
0334-0120123
Muhammad Saqib Riyaz
0344-7227224

بِٹ کوائن، بلاک چین
اور کرپٹو کرنسی

ماضی حال اور مستقبل۔ تکنیکی تفصیلات اور علمائے کرام سے چند سوالات

ذیشان الحسن عثمانی

گفتگو پبلیکیشنز

جملہ حقوق بحق ناشر محفوظ

عنوان کتاب: بِٹ کوائن، بلاک چین اور کرپٹو کرنسی

مصنف: ذیشان الحسن عثمانی

سن اشاعت: اپریل2018ء

اہتمام: گفتگو پبلیکیشنز، اسلام آباد

قیمت: 800روپے

پاکستان میں پرنٹ آن ڈیمانڈ(POD)فراہم کرنے والا منفرد ادارہ

اپنی کتاب چھپوانے کیلئے رابطہ کیجئے

ملنے کا پتا:

گفتگو پبلیکیشنز، اسلام آباد، پاکستان

فون:990 4455 340 92+| ای میل:info@gufhtugu.com

ویب سائٹ:www.gufhtugu.com

ISBN: 978-969-7758-12-8

انتساب!

بابا سائیں کے نام جنھوں نے امید دلائی کہ میں بڑا آدمی بن سکتا ہوں

اور

امی کے نام جنھیں یقین تھا کہ میں ہوں

(اللہ سبحانہ وتعالیٰ دونوں کی مغفرت فرمائے۔ آمین!)

ستاری ارباب ذوق
0305 6406067
PDF Book Company

فہرست عنوانات

نمبر شمار	عنوان	صفحہ نمبر
1	عرض مصنف	07
2	شکریہ	09
3	یہ کتاب کیوں پڑھیں؟	11
4	پیسے کی کہانی	15
5	بلاک چین کا تعارف	65
6	بلاک چین— تکنیکی ماہیت اور تعریف	79
7	ستوشی ناکاموتو اور اس کا پیپر	85
8	بِٹ کوائن	113
9	بین الاقوامی ممالک میں بِٹ کوائن کی قانونی حیثیت	121
10	متبادل کرنسی(Alternative Coins)	153
11	ایتھریم(Ethereum)مائننگ	173
12	ایتھریم(Ethereum)پر قرطاسِ ابیض	183
13	کنسنسیز الگورتھمز(Consensus (Algorithms	257
14	ICO	269
15	علمائے کرام سے چند سوالات	275
16	فتاویٰ	283

عرضِ مصنّف

زن، زر، زمین اور ان کے قصے بچپن سے سنتے آئے تھے مگر کیا معلوم تھا کہ ایک دن یہ زر (پیسہ Money) اپنے کام کی فیلڈ میں سب کچھ تبدیل کر کے رکھ دے گا۔ بٹ کوائن اور بلاک چین کی یہ کتاب میری زندگی کی مشکل ترین کتابوں میں سے ایک ہے۔ قریباً تیس ہزار سال کی پیسے کی کہانی کو چند صفحات میں منتقل کرنا بڑا ہی کٹھن ثابت ہوا۔ نہ جائے ماندن نہ پائے رفتن کے مصداق سوائے لکھنے کے اور کوئی چارہ نہیں۔

یہ کتاب کوئی سہ رخی تلوار ہے۔ اپنی بات سمجھا نہ پایا تو حرام و کفر کے فتوے لگیں گے، خاموش رہوں تو مولانا عبدالحق یاد آتے ہیں اور لکھوں تو ڈر اس بات کا کہ یہ نفس اور عقل کہیں جہنم میں نہ دھکیل دے۔

اللہ سے دعا ہے کہ میری بات آپ کو سمجھ میں آجائے، اس کتاب کے ذریعے جواز یا عدم جواز، کچھ بھی ہو، ہم بحیثیت مسلمان اور قوم کوئی ایک فیصلہ کر لیں اور آپ کی تجاویز و رہنمائی سے میرے جیسوں کا کچھ بھلا ہو جائے۔

نئی ایجادات اور ٹیکنالوجی کے ساتھ مسلمانوں کی روش پچھلے کوئی چار سو سالوں سے خاصی معاندانہ رہی ہے۔ کوئی سو سال پہلے دہلی میں کاغذی نوٹ، اس کے استعمال اور شرعی حکم پر اجلاس ہوا۔ مولانا عبدالحق حقانی بھی مدعو تھے۔ اب وہ بار بار کہتے کہ بھائی کھانا کھلا دو، منتظمین سیخ پا ہو گئے کہ مولوی صاحب یہاں ہم امت کے مال، زکوۃ، نصاب، عشر کا حساب کر رہے ہیں چودہ سو سال سے چلے آئے درہم و دینار کے "اسلامی ورثہ" کی حفاظت کر رہے ہیں اور آپ کو کھانے کی پڑی ہے، تو وہ کہنے لگے کہ جو چاہے کر لو، کاغذی نوٹ آ کے رہے گا اور آپ کے

حرام کی نعروں سے کچھ نہیں ہوگا۔ سو سال گزر گئے، اب کون ہے جو کاغذی نوٹ اور اس کے ساتھ ہونے والے لین دین کو حرام کہے۔

جہاز میں سفر کفار کی مشین پر سفر کرنا ٹھہرا، پھر لاوڈ سپیکر اور پھر کاغذ کا پرنٹنگ پریس۔ امت دو سو سالوں میں تصویر کے جائز اور ناجائز ہونے پر ہی متفق نہ ہو سکی۔

اب یہی حال بے چاری کرپٹو کرنسی کا ہے۔ میری بات کس نے سننی ہے۔ مگر جب تاریخ حرام کے دعووں (فتوی لکھتے ڈر لگتا ہے اس کی سند اللہ تک جاتی ہے) کا ذکر کرے تو مولوی عبدالحق کی سنت بھی زندہ رہنی چاہیے۔ آپ سے تو کھانا کھلانے کی درخواست بھی فضول ہے۔ آپ بس یہ کتاب پڑھ لیں۔

ایک گزارش اور کہ اسے صرف دس سال کے لئے سنبھال کر رکھ لیں۔ وقت ساری سلوٹوں پر استری خود ہی پھیر دیتا ہے۔

آپ کی تجویز، تنقید اور آرا کا منتظر

ذیشان الحسن عثمانی

11 اپریل، 2018ء

ویلنئس، لتھونیا

شکریہ!

سب سے پہلے اللہ رب العزت کا شکریہ کہ جس نے یہ کتاب لکھنے کی توفیق دی

کتاب لکھنا اور اسے لکھنے سے پہلے موجودہ مواخذ کو پڑھنا ایک وقت طلب کام ہے۔ بڑی حق تلفی ہو گی اگر ان احباب کا شکریہ ادا نہ کروں جنھوں نے کسی نہ کسی طرح اس کتاب کی تحریک اور ترتیب میں مدد کی۔

مفتی سعید خان صاحب کا شکریہ جنھوں نے پہلے باب کو غور سے پڑھا اور کئی جگہ رہنمائی فرمائی۔ اِس موضوع پر ان کے ساتھ ہونے والی متعدّد نشستوں سے اِس کتاب کے خیال کو تحریک ملی۔

دارالعلوم کراچی کے مفتی عیسیٰ اِبراھیم اور مفتی شاکر جھکورا صاحب کا شکریہ کہ اُن سے سیکھنے کا موقع ملا، اور اس بات کا احساس ہوا کہ کتاب عوام النّاس اور خصوصاً علمائے کرام کے لئے کس درجہ ضروری ہے۔ جناب طاہر فاروقی صاحب کا شکریہ جنھوں نے خصوصی وقت دے کر مدد فرمائی۔

جامعۃ الرشید کے مفتی اویس پراچہ صاحب کا ممنون ہوں جو اِس موضوع پر تحقیقی مقالہ لکھ رہے ہیں۔ کرپٹو کرنسی کے مشکل مضامین کو عام فہم زبان میں بیان کرنے کی قدرت ان کا خاصہ ہے۔

Consensys کے جوزف لیوبن جو کہ اِیتھریم کے معاون موجّد بھی ہیں کا خصوصی ممنون ہوں کہ ان کے ساتھ طویل نشستوں میں مارکل ٹری اور اِسمارٹ کانٹریکٹ کو سمجھنے کا موقع ملا

نوبل اِنعام یافتہ سائنسدان ملٹن فریڈمین کے پوتے اور ماہر معاشیات پاٹری فریڈمین کا شکریہ جنھوں نے اقوام عالم پر اقتصادی پالیسیز اور ایک نئی معاشی دنیا کے وجود پر راہنمائی فرمائی

ڈاکٹر ڈینئیل کرک کا شکریہ جنھوں نے زر کی تاریخ پر بھرپور راہنمائی کی

ڈاکٹر اسد زمان کا شکریہ جنھوں نے دولت کی پیدائش کے نظریے کو سمجھایا

ایکسپریس اخبار کے علیم احمد اور ٹیلی نار کی ثناء رشید کا شکریہ جنھوں نے ستوشی ناکا موتو اور اِیتھیریم وائٹ پیپر کے ترجمے میں میری مدد کی۔

میرے انٹرنز کا شکریہ جنھوں نے بلا مبالغہ سینکڑوں ریسرچ پیپرز اور ویب سائٹ کھنگال کے مجھے میرے مطلب کی تفصیلات مہیا کیں۔ شمس العارفین، مہک نرمین اور خواجہ حسین

اپنے پبلیشر، گفتگو پبلی کیشنز اور محمّد اُسامہ کا تہہ دل سے مشکور ہوں جو ہر بار میری کتابیں چھاپ کر رِسک لیتے ہیں کہ ان کی رقم ڈوب جائے گی

میرے بیوی/بچوں کا شکریہ جن کے وقت میں سے وقت نکال کر، میں اس کتاب پر کام کرتا رہا

اور آپ سب قارئین کا بھی شکریہ، کہ لکھنا کس کام کا، اگر آپ پڑھیں نہیں

یہ کتاب کیوں پڑھیں؟

میرے خیال میں یہ کتاب ہر پاکستانی کو پڑھنی چاہئے۔ اِس کا دیباچہ لکھنے کی بجائے اگر میں 115 سال پُرانا دیباچہ علامہ اقبال کی کتاب 'علم الا قتصاد' سے کاپی پیسٹ کر دوں تو بھی کافی رہے گا۔ جہاں ہم 115 سال پہلے کھڑے تھے، وہیں آج ہیں۔

بلاک چین اور کرپٹو کرنسی پر کئے جانے والے زیادہ تر اعتراضات کی وجہ کم علمی ہے۔ دنیائے معاشیات میں صرف وہ چیز نئی ہے جو آپ نے پڑھی نہیں، ورنہ نوعِ انسانی نے ہر چیز کسی نہ کسی رنگ میں ضرور دیکھ رکھی ہے۔

مثال کے طور پر ایک اعتراض یہ کیا جاتا ہے کہ بِٹ کوائن پر بجلی بہت لگتی ہے۔ پہلی بات تو یہ کہ بٹ کوائن کے علاوہ بھی کرپٹو کرنسیز موجود ہیں، جو مختلف Consensus (اِتفاق رائے) کے الگورتھمز استعمال کرتی ہے اور ان پر اِتنی بجلی صرف نہیں ہوتی، برسٹ کوائن (Burst Coin) پروف آف کیپے سٹی (Proof Of Capacity) پر چلتا ہے اور بہت کم بجلی استعمال کرتا ہے۔

ہم پورا معاشی نظام بنانا چاہ رہے ہیں۔ آپ اس کا موازنہ بینکوں، ڈیٹا سینٹرز، 24 گھنٹے چلنے والی ATM مشینز اور مالیاتی اِداروں میں کام کرنے والوں کی آمد و رفت کے ذرائع اور ان سے پیدا ہونے والے کاربن فُٹ پرنٹ سے کریں تو آپ کو کرپٹو کرنسیز پر خرچ ہونے والی بجلی بہت کم محسوس ہو گی۔

بلاک چین، کرپٹو کرنسیز فنانشل نظام کے ساتھ وہی کرے گی جو موبائل فون نے لینڈ لائن فون کے ساتھ اور ای میل نے ڈاکخانوں کے ساتھ کیا ہے۔

2020 تک دنیا میں 20 ارب ڈیوائسز ہونگے جو IoT (انٹرنیٹ آف تھنگز) سے جڑے ہونگے۔ یہ ڈیوائس آپس میں بھی رقوم کا تبادلہ کریں گے۔ ہمارا مائیکرو ویو، فرج، ائیر کنڈیشنر، حتّیٰ کہ ٹوتھ برش تک اپنے فارغ اوقات میں کرپٹو مائننگ کر رہا ہوگا جسے ہم اپلائنس مائننگ (Appliance-Mining) کہتے ہیں۔ دنیا بھر کا آبی نظام، معاشی نظام، جنگی نظام، امیگریشن، ذاتی شناخت سب بلاک چین کے ذریعے کنٹرول ہو رہی ہوگی۔

جب اقوام عالم اسمارٹ کانٹریکٹ کے ذریعے، مصنوعی ذہانت سے آراستہ روبوٹس کی مدد سے ملکوں کی تقدیر کا فیصلہ کر رہی ہونگی تب آپ کافر اور حرام کے نعرے لگا لگا کر شاید بوند بھر پانی کو ترسیں، مگر روبوٹس کو ترس کب آتا ہے۔

1903ء میں علامہ اقبال کے لکھے گئے علم الا قتصاد کے دیباچے کے ساتھ آپ سے رخصت چاہوں گا، اِسے پڑھنے کے بعد بھی اگر آپ کو اس کتاب میں شغف محسوس نہ ہو تو نہ پڑھئے گا ،ہو سکتا ہے آگے پچاس سال بعد کوئی ناعاقبت اندیش، اس دیباچے کو اپنی کتاب میں لکھ کر، پھر سے اپنی قوم کے ضمیر کو جھنجھوڑنے کی کوشش کرے۔

دیباچہ مصنف۔ علم الا قتصاد
(علامہ اقبالؒ-1903ء)

علم الا قتصاد انسانی زندگی کے معمولی کاروبار پر بحث کرتا ہے اور اس کا مقصد اس امر کا تحقیق کرنا ہے کہ لوگ اپنی آمدنی کس طرح حاصل کرتے ہیں اور اس کا استعمال کس طرح کرتے ہیں۔ پس ایک اعتبار سے تو اُس کا موضوع دولت ہے اور دوسرے اعتبار سے یہ اس وسیع علم کی ایک شاخ ہے جس کا موضوع خود انسان ہے۔ یہ امر مسلم ہے کہ انسان کا معمولی کام کاج،

اس کے اوضاع واطوار اور اس کے طرز پر زندگی پر بڑا اثر رکھتا ہے۔ بلکہ اس کے دماغی قویٰ بھی اس اثر سے کامل طور پر محفوظ نہیں رہ سکتے۔ اس میں کچھ شک نہیں کہ تاریخ انسانی کے سیل رواں میں اصول مذہب بھی انتہائی مؤثر ثابت ہوئے ہیں۔ مگر یہ بات بھی روزمرہ کے تجربے اور مشاہدے سے ثابت ہوتی ہے کہ روزی کمانے کا دھندا ہر وقت انسان کے ساتھ ساتھ ہے اور چپکے چپکے اس کے ظاہری اور باطنی قویٰ کو اپنے سانچے میں ڈھالتا رہتا ہے ذرا خیال کرو کہ غریبی یا یوں کہو کہ ضروریات زندگی کے کاملی طور پر پورا نہ ہونے سے انسانی طرزِ عمل کہاں تک متاثر ہوتا ہے۔ غریبی قویٰ انسانی پر بُرا اثر ڈالتی ہے، بلکہ بسا اوقات انسانی روح کے مجلّا آئینہ کو اس قدر زنگ آلود کر دیتی ہے کہ اخلاقی اور تمدنی لحاظ سے اس کا وجود و عدم برابر ہو جاتا ہے۔ معلم اوّل یعنی حکیم ارسطو سمجھتا تھا کہ غلامی تمدن انسانی کے قیام کے لئے ایک ضروری جزو ہے، مگر مذہب اور زمانہ حال کی تعلیم نے انسان کی جبلی آزادی پر زور دیا اور رفتہ رفتہ مہذب قومیں محسوس کرنے لگیں کہ یہ وحشیانہ تفاوتِ مدارج بجائے اس کے کہ قیام تمدن کے لئے ایک ضروری جزو ہو، اس کی تخریب کرتا ہے اور انسانی زندگی کے ہر پہلو پر نہایت مذموم اثر ڈالتا ہے۔ اس طرح اس زمانے میں یہ سوال پیدا ہوا کہ آیا مفلسی بھی نظم عالم میں ایک ضروری جزو ہے؟ کیا ممکن نہیں کہ ہر فرد مفلسی کے دُکھ سے آزاد ہو؟ کیا ایسا نہیں ہو سکتا ہے کہ گلی کوچوں میں چپکے چپکے کراہنے والوں کی دل خراش صدائیں ہمیشہ کے لئے صفحہ عالم سے حرف غلط کی طرح مٹ جائے؟ اس سوال کا شافی جواب دنیا علم الاقتصاد کا کام نہیں۔ کیونکہ کسی حد تک اس کے جواب کا انحصار انسانی فطرت کی اخلاقی قابلیتوں پر ہے جن کو معلوم کرنے کے لئے اس علم کے ماہرین کوئی خاص ذریعہ اپنے ہاتھ میں نہیں رکھتے۔ مگر چونکہ اس جواب کا انحصار زیادہ تر ان واقعات اور نتائج پر بھی ہے جو علم الاقتصاد کے دائرہ تحقیق میں داخل ہیں اس واسطے یہ علم انسان کے لئے انتہا درجہ کی دلچسپی رکھتا ہے اور اس کا مطالعہ

قریباً قریباً ضروریات زندگی میں سے ہے۔ بالخصوص اہل ہندوستان کے لئے تو اس علم کا پڑھنا اور اس کے نتائج پر غور کرنا نہایت ضروری ہے کیونکہ یہاں مفلسی کی عام شکایت ہو رہی ہے۔ ہمارا ملک کامل تعلیم نہ ہونے کی وجہ سے اپنی کمزوریوں اور نیز ان تمدنی اسباب سے بالکل ناواقف ہے جن کا جاننا قومی فلاح اور بہبود کے لئے اکسیر کا حکم رکھتا ہے۔ انسان کی تاریخ اس امر کی شاہد ہے کہ جو قومیں اپنی تمدنی اور اقتصادی حالات سے غافل رہی ہیں اُن کا حشر کیا ہوا ہے۔ ابھی حال میں مہاراجہ بڑودہ نے اپنی ایک گراں بہا تقریر میں فرمایا تھا کہ اپنی موجودہ اقتصادی حالت کو سنوارنا ہماری تمام بیماریوں کا آخری نسخہ ہے اور اگر یہ نسخہ استعمال نہ کیا گیا تو ہماری بربادی یقینی ہے۔ پس اگر اہل ہندوستان دفتر اقوام میں اپنا نام قائم رکھنا چاہتے ہوں تو ان کے لئے ضروری ہے کہ وہ اس اہم علم کے اصولوں سے آگاہی حاصل کر کے معلوم کریں کہ وہ کون سے اسباب ہیں جو ملکی عروج کے مانع ہو رہے ہیں۔ میری غرض اوراق کی تحریر سے یہ ہے کہ عام فہم طور پر اس علم کے نہایت ضروری اصول واضح کروں اور نیز بعض جگہ اس بات پر بھی بحث کروں کہ یہ عام اصول کہاں تک ہندوستان کی موجودہ حالت پر صادق آتے ہیں۔ اگر ان سطور سے کسی فردِ واحد کو بھی ان معاملات پر غور کرنے کی تحریک ہو گئی تو میں سمجھوں گا کی میری دماغ سوزی اکارت نہیں گئی۔

پیسے کی کہانی

کوئی تیس ہزار سال پہلے انسان روئے زمین پر خانہ بدوشی کی زندگی گزارتے تھے۔ایک جگہ سے دوسری جگہ کوئی موسم کی وجہ سے نقل مکانی کرتا تو کوئی اجناس و جانور کی تلاش میں۔ خانہ بدوش کا سامان ہی کیا ہو۔ایک آدھ جوڑا، کچھ اوزار اور کچھ برتن۔ جب کسی اور قبیلے یا کنبے سے ملنا ہو تو اپنی کوئی چیز دے کر ان کی لے لی۔ مثلاً گندم کے بدلے مچھلی یا اوڑھنی کے بدلے کوئی برتن ۔زر/ نقدی/ پیسہ کا کوئی وجود نہیں تھا، کسی کے پاس کوئی پیسہ نہیں تھا۔ چھوٹی سی ملکیت، محدود خواہشات سب کا ساجھا اور زندگی رواں دواں تھی۔ مسابقت انسان کی گھٹی میں ہے۔تو اس بات پر فخر و غرور کیا جانے لگا کہ کس کے پاس کتنا کچھ ہے۔ پیسہ ابھی بھی کسی کے پاس نہیں تھا مگر اجناس و مویشی کی تقسیم مساوی نہیں تھی۔ کوئی کسی فن کا کاریگر تھا تو کوئی کسی کا۔اور یہاں سے ایک دوسرے کے مابین باقاعدہ لین دین کی شروعات ہوئی جسے ہم آج تک بارٹر سسٹم کے طور پر جانتے ہیں اور یہ دنیا میں کسی نہ کسی صورت آج تک قائم ہے۔ تقریباً بیس ہزار سال اور آئس ایج (Ice Age) ایسے ہی گزر گئی۔

کوئی گیارہ ہزار سال پہلے انسانوں نے خانہ بدوشی کو چھوڑ کے اپنے مستقل ٹھکانوں پر رہنا شروع کیا۔ جانوروں کا صرف شکار کرنے کی بجائے ان کو پالنا اور ان کی نسل کی پرورش کرنا شروع کر دیا۔ سبزیاں اور اناج کاشت کرنے کی ریت اپنائی اب جب ایک جگہ سکون سے رہنا شروع کیا تو روزمرہ کے سامان میں بھی اضافہ شروع ہو گیا۔

تاریخ بتاتی ہے کہ آباد کاری کی ابتداء مشرق وسطی کے علاقے سے ہوئی جسے فرٹائل کریسنٹ(Fertile Crescent) کہا جاتا تھا۔ لوگ گاوں، قبیلوں، علاقوں، نسلوں اور زبانوں میں باقاعدہ بٹنا شروع ہوئے اور ایک جگہ سے دوسری جگہ تجارت ولین دین کی ابتداء ہوئی۔

دو ہزار سال اور گزر گئے اور بارٹر سسٹم مصر سے لے کر انڈیا تک اور مشرق وسطی سے لے کر اہل بابل تک مستحکم ہوتا چلا گیا۔ ہر وہ شے جس کی معاشرے میں کوئی نہ کوئی قدر ہو بارٹر کے طور پر لین دین میں استعمال ہونے لگی۔ گندم، جو، مکئی، گائے، بھینس، بکری، زعفران، مچھلی، چاول الغرض ہر شے جس کی ضرورت یا ڈیمانڈ ہو وہ بارٹر میں استعمال ہو سکتی تھی۔ کوئی لگ بھگ ہزار سال یوں گزر گئے اور قریباً دس ہزار سال پہلے لوگوں نے اشیاء کو گننا شروع کیا۔ ضرورت اس لیے پیش آئی کہ بارٹر میں دی اور لی جانے والی اشیاء کافی مختلف ہوتی تھیں۔ مثلاً آپ کے پاس گائے ہے اور آپ کو زعفران چاہیے تو ایک کلوز عفران کے بدلے کوئی اپنی گائے کیوں دے گا۔ تو اب وہ چاہتا ہے کہ اسے اتنا زعفران، اتنا کپڑا، اتنی گندم وغیرہ ملے۔

لوگ عموماً جانوروں واجناس کی شکلیں مٹی سے بنا کر ایک مٹی کے لفافے میں رکھ لیتے۔ پھر اسی لفافے پر تصویریں بنانے کا عمل شروع ہوا۔ پھر لوگوں نے مٹی کے اجسام کے درمیان سوراخ کر کے انہیں دھاگے میں پرونا شروع کر دیا۔ اب آپ کے قبیلے کے سردار کے گلے میں لٹکا ہوا ہار اس بات کی نشاندہی کرتا تھا کہ آپ کے پاس کتنے جانور، زمین اور اجناس ہے اور اس طرح سودے ہوتے تھے۔

بارٹر سسٹم جوں جوں پھیلتا گیا اس کی قبولیت اور پیچیدگیوں میں اضافہ ہوتا چلا گیا۔ آپ نے اپنے بکرے کو دے کر کچھ برتن لینے ہیں مگر جس کے پاس برتن ہیں اسے بکرا نہیں چاہیے، وہ

تو کپڑے چاہتا ہے۔اب آپ کو ایسا شخص ڈھونڈنا ہوگا جو بکرا لے کر کپڑے دے دے تاکہ آپ کپڑے دے کر برتن لے سکیں۔ پھر اس بات کی کیا ضمانت کہ آپ سب کو یہ چیزیں ایک ہی وقت میں چاہئیں۔ پھر گندم تو آرام سے مختلف اوزان میں بٹ سکتی ہے، بکرے کا کیا کریں گے۔اگر آدھا کاٹ دیا تو باقی ماندہ اپنی قدر کھو دے گا۔

دنیا چلتی رہی اور لوگوں کو مختلف میٹلز ملتے چلے گئے۔ کسی کے ہاتھ سونا لگا تو کسی کے ہاتھ چاندی یا تانبہ۔اگر آپ فرٹائل کریسینٹ کے میسوپوٹیما کے بادشاہ ایشونا کا چار ہزار سال پرانا قانون پڑھیں گے تو آپ کو پتہ چلے گا کہ کسی آدمی کی ناک پر کاٹنے کا جرمانہ چاندی کا ایک مینا تھا(جو ایک پاونڈ چاندی کے برابر ہوتا ہے)اور کسی کو تھپڑ مارنے کا جرمانہ 12 شیکل (مینا کا چھٹا حصہ) ہوتا تھا۔مزدور کے ایک دن کی اجرت مینا کا ہزارواں حصہ تھا۔یعنی کسی نے اگر ناک پر کاٹ لیا تو تین سال کی محنت کی اجرت دینا پڑے گی۔اس سے پتہ لگتا ہے کہ اس زمانے میں سونے اور چاندی کس طرح روزمرہ زندگی میں استعمال ہوتے تھے۔

لگ بھگ اسی زمانے کے آس پاس حضرت ابراہیمؑ نے اپنی زوجہ حضرت سارہؓ کی قبر کے لئے جگہ Machpelah میک پلا کی غار (آج کل کا الحرم ابراہیمی) چار سو شیکل میں خریدی تھی جو آج کے دور کے قریباً سوا کروڑ بنتے ہیں۔

میسوپوٹیما میں چاندی اور مصر میں تانبہ اور سونا بطور زر استعمال ہوتے تھے۔اب اگر ایک شخص کی روزانہ کی اجرت چاندی کے مینا کا ہزارواں حصہ ہے تو اسے ناپنے/تولنے کے لئے اسی معیار کے میزان درکار ہونگے۔ ایسے آلات و میزان عموماً عبادت گاہوں میں رکھے جاتے، لوگ جاتے اور اپنی اجرت کے بدلے سامان خورد نوش لے آتے۔

سونے چاندی کا حصول طاقتور کے لئے آسان اور غریب کے لئے مشکل تر ہوتا چلا گیا۔ کسی کے پاس اگر نہ تو سونا چاندی ہے اور نہ ہی کوئی جنس/اشیاء جسے بارٹر کر سکے تو وہ عموماً اگلی فصل آنے

تک اشیاء ادھار پہ لے لیتا تھا اور یہاں سے مٹی کی صلیبوں پر I Owe You (میں تمہارا مقروض ہوں) لکھنے کا رواج چلا۔ اب اگر آپ نے کسی سے دس گندم کے تھیلے لئے ہیں تو آپ یہ مٹی کی تختی پر لکھ کر اسے دے دیں گے، فصل آنے پر آپ اسے واپس کر دیں گے۔ اب اگر اس شخص کو پہلے ہی ضرورت پڑ گئی تو وہ کسی اور شخص سے کچھ لے کر یہ تختی اس کے حوالے کر دے گا اور آپ اس شخص کو جس کے پاس یہ تختی ہو گی اسے فصل دینے کے پابند ہوں گے۔

اور اس طرح معاشرے میں مٹی کی تختیوں کا یہ رواج چل نکلا۔ لینے والے کی حاجت زیادہ ہوتی ہے۔ دینے والے کو اتنا فرق نہیں پڑتا اور یہیں سے سود کا عفریت چل نکلا۔

آپ نے دس بوری اناج لیا مگر آپ کو لوٹانا بارہ بوری پڑا۔ جب سرکار نے عام آدمیوں کو ایسے کماتے دیکھا تو وہ خود کیسے پیچھے رہ سکتی تھی تو اب سارا اناج عبادت گاہوں اور مندروں میں رکھ دیا جاتا اور اس کے بدلے کوئی تختی جاری کر دی جاتی۔ جو شخص بھی یہ تختی لے کر چلا جائے اسے کسی مقدار میں اناج مل جاتا۔ حکومت اناج رکھوانے والے اور خریدنے والے دونوں سے منافع لیتی۔ جیسے ہمارے آج کل کے کاغذی نوٹوں پر لکھا ہوتا ہے۔ حامل ہذا کو مطالبے پر ادا کرے گا، وغیرہ۔

1100 قبل مسیح میں چین نے پہلی مرتبہ تانبے کے سکے جانوروں اور اجناس کی شبیہہ پر بنائے۔ 600 قبل مسیح میں لایئڈیا (آج کل کے ترکی) کے بادشاہ الیوتس نے دنیا کو سکوں سے متعارف کروایا۔ ایک ہی ساخت، وزن اور قدر کے سکے بادشاہ وقت جاری کر دے گا تاکہ عوام لین دین میں آسانی سے استعمال کر سکیں اور بوقت ضرورت کوئی بھی شخص انہیں دے کر سرکاری خزانے سے متبادل سونا اور چاندی لے سکے۔

اس وقت دنیا میں بلا مبالغہ سینکڑوں ریاستیں اور حکمران تھے اور ہر حکمران نے اپنا سکہ رائج الوقت نافذ کر دیا۔ لوگ ملکوں کے مابین تجارت کرنے کے قابل ہوئے سارے سکے یکساں وزن کے اور مالیت کے ساتھ تو نہ تو کوئی وزن کرنا پڑتا اور نہ ہی کوئی پریشانی۔

مشرق وسطی سے لے کر چین کے بلیک سی تک اور یورپ کے کلیسائوں سے لے کر لائیڈیا کے بازاروں تک دنیا سکوں پر آگئی۔ دنیا کا پہلا بازار جہاں آپ دکانوں سے اشیاء سکوں کے بدلے خرید سکیں، بھی لائیڈ میں ہی بنا۔

سرکار جب سکے بناتی تو ان کی مالیت اصل سے کچھ کم رکھتی تاکہ منافع کما سکے۔ بحری بندرگاہوں کے ساتھ جگہ جگہ لوگوں نے سکوں کی لین دین کا کاروبار شروع کر دیا اور خوب منافع کمایا۔ آپ انہیں قبل مسیح کے منی چینجرز کہہ لیں۔ دنیا کے پہلے بینکر کا نام پیشن تھا، یہ یونان میں غلام تھا مگر آہستہ آہستہ اس نے بینکنگ کی بنیاد رکھی، شہری حقوق حاصل کئے اور ایک کامیاب بینکر بنا۔ جب 370 قبل مسیح میں اس کی موت واقع ہوئی تو اس کے پاس 360،000 دینار یا ڈرماکس تھے۔ بینکنگ اس دور میں بھی منافع بخش تھا۔

پیسہ / زر کی ضمانت سکوں، چاقو اور طرح طرح کے ڈھلے ہوئے اجسام میں پائی جانے لگی۔ سونا، چاندی، تانبہ، الیکٹریم اور دوسری دھاتیں اس مقصد کے لئے استعمال ہونے لگیں۔ سات سو سال قبل مسیح سے چار سو سال قبل مسیح تک یہ فن چین، ترکی مصر، مشرق وسطی، یورپ سے لے کر انڈیا تک پھیل گیا۔

دنیا میں سب سے پہلے سکوں کا وزن اور قدر میڈی ٹرینین بادشاہ فیڈون نے طے کیا۔

پہلے سکے جن پر کسی حکمران کی مہر ثبت تھی۔ ایجینا جزیرہ میں سات سو قبل مسیح میں بنے۔

547 قبل مسیح میں اہل فارس نے سکوں کو اپنایا۔ 483 قبل مسیح میں اہل یونان نے اپنی افواج کو سکوں میں اجرت دینا شروع کی ۔یہ سکے چاندی کے بنے ہوئے تھے۔لوگوں نے جوق در جوق فوج میں شمولیت اختیار کی اور اہل یونان کی سلطنت پھیلتی چلی گئی۔

413 قبل مسیح میں روم،اٹلی میں ایک دیوی کی پوجا ہوتی تھی،اسی کے نام سے مندر تھا۔اس کانام مونیٹا تھا۔تاریخ دان اسی دیوی کی مناسبت سے منی(Money) اور منٹ (Mint)کے ناموں کی توجیہہ کرتے ہیں۔ زبان دان منی کو لاطینی زبان کے لفظ Monetaسے اخذ کرتے ہیں جس کا مطلب ہے"منفرد"۔

اہل فارس اور اہل یونان کی دیکھا دیکھی اہل روم نے بھی سکوں کا استعمال شروع کر دیا۔ یہ لوگ تانبے اور چاندی کے بنے سکے کا استعمال کرتے تھے اور رومن امپائر کے سینیٹرز(Senators) اپنے غلاموں کے ساتھ ہاتھ گاڑیوں میں اپنا خزانہ لادے پھرتے تھے۔انہوں نے ہی یہاں عوام پر ٹیکس لاگو کیا اور اگلے دو سو سال تک پیسے کے خبط میں یکے بعد دیگرے دنیا فتح کرتے چلے گئے۔ 167 قبل مسیح میں جب میساڈونیا کو شکست ہوئی تو روم میں مال غنیمت کے طور پر 75 ملین دینارے (300 ٹن چاندی) آیا۔

اتنی زیادہ دولت نے روم کو اور طاقتور اور مضبوط بنا دیا۔ شہر بڑھتا چلا گیا اور لوگ سامان عیش و عشرت خریدتے چلے گئے۔ منفرد پرندے ہوں یا نت نئی خوشبوئیں،انسانی غلام ہوں یا ایک سے بڑھ کر ایک گھوڑا اور فرنیچر، جنگی ساز و سامان ہوں یا چین و ہندوستان اور عرب سے درآمد کی گئی مصنوعات اور مصالحہ جات،روم خرچ کرتا چلا گیا۔ایک رومن تاریخ دان پلینی لکھتا ہے کہ روم سالانہ 25 ملین دینارے سامان عیش و عشرت پہ خرچ کرتا تھا۔ جہاں روم میں پیسوں کا راج تھا وہاں چین میں 118 قبل مسیح میں ہرن کی کھال کے چمڑے پر،رنگین سرخیوں کے ساتھ دنیا کے پہلے کرنسی نوٹ نے جنم لیا۔

اس کے بعد حکومت کا ''ضمانتی'' نوٹ مختلف شکلوں میں چلتا رہا، چمڑے پر درخت کی چھال پر جانوروں کی کھال اور ہڈیوں پر اور دھات کی پلیٹوں پر مگر دنیا ابھی تک سکوں، درہم و دینار پر ہی چل رہی تھی۔

روم سے درآمدات کی مد میں پیسہ باہر جاتا رہا۔ لوگ آتے رہے، لین دین اور کاروبار بڑھتا رہا فتوحات ہوتی رہیں اور مال غنیمت آتا رہا۔ مگر 117 سال قبل مسیح میں رومن امپائر پر فتوحات کا سلسلہ رک گیا۔ پیسوں کی قلت ہوئی تو سرکار نے اس کا حل یہ نکالا کہ سکوں میں صرف چاندی کی بجائے ٹن اور دوسری دھاتیں بھی ملانے لگی۔ دکاندار بھی چالاک تھے۔ انہوں نے اسی حساب سے نرخ بڑھا دیئے اور یوں اہل روم نے دنیا کو Inflation یا افراط زر سے متعارف کروایا۔ جو مرغی پانچ دینارے کی تھی وہ ایک سال میں بڑھ کے پندرہ اور اگلے سال 45 دنیارے کی ہوگئی۔ جولیس سیزر کی فوج کا سپاہی جو 46 قبل مسیح میں 225 دینارے تنخواہ لیتا تھا وہ 200 صدی عیسوی تک 600 اور 235 صدی عیسوی میں 1800 دنیارے لینے لگا۔

اسی اثناء میں ایک انوکھا کام ہوا۔ ویسٹرن پیسفک میں مائیکرونیشیا کے جزیرے یپ پر لوگوں نے 9 ہزار پاونڈ کے ایک بڑے سے گول پتھر کو زر کے ڈیپازٹ والٹ جیسا درجہ دے دیا۔ یہ قریبی پلائو جزیرے سے یہاں لایا گیا تھا اسے Stone of Rai رائی کا پتھر کہتے تھے۔

(تصویر 1: رائی کا پتھر جزیرہ ویپ میں)

اب جزیرے کے لوگ سینہ بہ سینہ یاد رکھتے تھے کہ اس کا مالک کون ہے اور وہ مالک چھوٹے چھوٹے پتھروں کے عوض جو چاہے خرید و فروخت کر سکتا تھا۔ اور وہ چھوٹے پتھر بالکل کرنسی یا سکوں کی طرح لوگوں میں مقبول ہو گئے۔ سینہ بہ سینہ چلنے والے پبلک کھاتے (Public Ledger) میں سب کو پتہ ہوتا کہ اصل مالک آج کل کون ہے۔ کچھ سو سال بعد اس پتھر کو ایک جگہ سے دوسری جگہ منتقل کرتے ہوئے کشتی ڈوب گئی اور پتھر سمندر کی تہہ میں چلا گیا مگر اس سے کوئی فرق نہیں پڑا۔ یہ سلسلہ دو ہزار سال تک چل کر بیسویں صدی کے اواخر میں بند ہوا ہے۔

رائی کے پتھر کی اس کہانی میں ہمارے لئے سیکھنے کو بہت کچھ ہے جو ہمیں آگے جا کر بٹ کوائن اور بلاک چین کو سمجھنے میں مدد دے گا۔ یہ بڑا پتھر منفرد تھا اور اس جیسا دوسرا دستیاب نہیں تھا (Scarcity)۔ یہ پائیدار بھی تھا اور اس پر موسم، بارش، دھوپ کا کوئی خاطر خواہ اثر نہیں پڑتا تھا (Durable)۔ اس کی نقل بنانا بھی ناممکن تھی۔

رائی جس کے لفظی معنی بھی پتھر ہے، لائم سٹون سے بنتا تھا جو قریبی جزیرے پلائو میں سے نکالا جاتا تھا۔ اس بڑے پتھر کے درمیان ڈونٹ (Donut) کی طرح سوراخ اس لئے

رکھا جاتا کہ پھر اسے ڈنڈوں کی مدد سے ایک جگہ سے دوسری جگہ منتقل کیا جا سکے۔ اب اتنا بڑا پتھر تو آرام سے منتقل ہو نہیں سکتا لہٰذا لوگوں نے "رائی" کے بدلے گندم، جو اور باقی اجناس کرنسی کے طور پر استعمال کرنا شروع کر دی مثلاً رائی کا مالک اتنے کلو گندم و جو کی ٹریڈ کر سکتا ہے۔ ایک کرنسی کے عوض دوسری کرنسی اور اس طرح کرنسی ٹریڈنگ دنیا میں متعارف ہوئی۔

"رائی کے پتھر" کو آپ کوئی مہنگا گھر سمجھ لیں۔ اب گھر تو منتقل ہونے سے رہا مگر اس کے مالک تبدیل ہوتے رہتے ہیں اور آپ گھر گروی رکھوا کر بینک سے اس کے بدلے پیسے لیتے رہتے ہیں۔ ہے نا حیرت کی بات کہ ہماری آج کل کی بینکنگ میں بنیادی خیالات ہزاروں سال سے چلے آ رہے ہیں۔ اسی طرح بارٹر سسٹم بھی آج تک کسی نہ کسی حالت میں جاری ہے لوگ آپس میں تحفے دیتے ہیں فصل اترنے پر اجناس شیئر کرتے ہیں اور ایران آج تک تیل کے بدلے باقی ملکوں سے باقی اشیاء لیتا ہے (انٹرنیشنل پابندیوں کی وجہ سے)۔

ڈیوڈ گرائیبر اپنی کتاب "قرض: پہلے 5000 سال" میں بحث کرتے ہیں کہ اس دور میں صرف بارٹر سسٹم نہیں تھا۔ بارٹر سسٹم تو وہاں استعمال ہوتا ہے جہاں دو قبیلے یا کنبے آپس میں لین دین کرتے یا اجنبی ایک دوسرے سے معاملات کرتے۔ اپنے ہی قبیلے اور کنبے میں تو ایک دوسرے کو ادھار دے دیا جاتا، مدد کر دی جاتی اور اپنی ہی کمیونٹی میں لوگوں کا خیال رکھنا بارٹر کا متبادل تھا۔ بارٹر، ادھار، کرنسی کا استعمال وہاں ہوتا جہاں اعتماد (trust) کا فقدان ہو۔ ایک ہی کمیونٹی یا قبیلے میں تو خیال رکھنا (favor) وہ اعتماد (trust) تھا جس نے سوسائٹی کو آپس میں جوڑا ہوا تھا۔

یعنی اگر لوگ آپس میں کسی سسٹم پر متفق ہو جائیں تو وہ لین دین کے لئے ہر طرح سے موزوں ہے اور اس سے فرق نہیں پڑتا کہ اس سسٹم کے پیچھے کیا چیز ہے جو اسے قابل اعتبار بناتی ہے۔ اس نظریے کو یاد رکھیں، یہ آپ کو آگے بلاک چین اور بٹ کوائن سمجھنے میں بڑی مدد کرے گا۔

ساتویں صدی عیسوی میں چین کے ژوان(Sichuan) صوبے میں ٹینگ ڈائی نیسٹی Tang Dynasty (618-907) نے دنیا کو پہلی کاغذی کرنسی سے متعارف کروایا۔ کچھ کاروباری گروپس نے مل کر ایک کاغذی کرنسی کا اجراء کیا جس کا نام تھا، ''جیائو ژی'' دنیا بھر کے تاجر چائنا آتے اور اپنے سکے، سونا اور چاندی یہاں جمع کروا دیتے اس کے بدلے انہیں جیائو ژی ملتے جس سے وہ باآسانی خریداری کر سکتے۔ اور واپس جاتے ہوئے جیائو ژی واپس کر کے باقی ماندہ سکے وصول کر سکتے ہیں۔ آپ اسے ایک لوگوں کا بینک کہہ لیں جو ایک قصبے یا صوبے کی سطح پر کام کرتا تھا۔ ڈاکہ زنی، لوٹ مار اور چوری کے خوف سے آج تک بولٹن مارکیٹ، جوڑیا بازار اور چھوٹے بڑے شہروں میں یہ رواج قائم ہے آپ ایک سیٹھ کے پاس جا کر اس سے کچھ سامان لیتے ہیں مگر ساری رقم جمع کروا دیتے ہیں۔ اس کے بدلے آپ کو پرچیاں ملتی ہیں اور پھر آپ ان پرچیوں سے دن بھر باقی دکانوں سے خریداری کرتے رہتے ہیں۔

جیائو ژی کا استعمال بڑھتا چلا گیا۔ کچھ لوگوں نے ضرورت سے زیادہ جیائو ژی کا اجراء کر دیا، لوگ انہیں کیش نہ کرا سکے، فراڈ کا مقدمہ بنا اور آخر کار گورنمنٹ کو نظام کار سنبھالنا پڑا۔ آٹھویں صدی عیسوی میں ڈینش آئرلینڈ میں ''ناک کے ذریعے ادائیگی'' کا محاورہ عام ہوا۔ To Pay Through The Nose) جو شخص ڈینش حکومت کو ٹول ٹیکس نہ دیتا اس کی ناک کاٹ دی جاتی۔

سونگ ڈائی نیسٹی(960-1279) Song Dynasty نے سن 1024 صدی عیسوی میں دنیا کو پہلی حکومت سے منظور شدہ کاغذی کرنسی دی۔ استعمال پھیلتا چلا گیا اور صرف بارہویں صدی عیسوی میں 26 ملین سکوں کے عوض کرنسی ایشو کی گئی۔

یوان ڈائی نیسٹی(1360-1368) Yuan Dynasty نے "چائو" کے نام سے 1273ء میں نئی کاغذی کرنسی متعارف کروائی۔ سن 1277 تک چائنا میں کاغذی کرنسی کا استعمال سکوں یا درہم و دینار سے زیادہ ہو گیا۔

بارہویں صدی عیسوی میں یورپ میں کرنسی کا باقاعدہ اجراء ہوا۔ 1250ء میں فلورینس، اٹلی نے فلورین کے نام سے سونے کے سکوں کا اجراء کیا جو جلد ہی ملکی و غیر ملکی، تجارت میں استعمال ہونے لگے۔

1290ء میں مارکو پولو نے چائنا کا سفر کیا اور دنیا کو کاغذی کرنسی سے متعارف کروایا۔ یورپ ابھی بھی کرنسی نوٹ لینے کو تیار نہ تھا۔ اسے مزید تین سو سال لگے نوٹ کو باقاعدہ تسلیم کرتے ہوئے۔ مارکو پولو اپنی کتاب "مارکو پولو کے اسفار"

(The Travels of Morco Polo) کے باب "عظیم خان کے درخت سے بنائے کاغذی نوٹ"

"How the Great Khan causeth the bark of trees, made into something like paper, to pass for money all over his country"

میں لکھتا ہے۔

"جیسا کہ میں نے بیان کیا، کبلائی خان، اپنی پوری سلطنت، جاگیر اور صوبوں میں الغرض جہاں جہاں اس کی طاقت اور حکومت چلتی ہے وہاں ان کاغذی ٹکڑوں کو کرنسی کے طور پر

استعمال کرتا ہے اور کسی میں اتنی مجال نہیں کہ وہ ان کاغذی نوٹوں سے لین دین سے منع کر دیں۔

مزید برآں، وہ تمام تاجر جو انڈیا اور باقی ملکوں سے آتے ہیں ان کو سکوں یا سونے چاندی میں تجارت کی اجازت نہیں وہ یہ سکے خان کے محل میں جمع کرواتے ہیں وہاں کبلای خان نے بارہ ماہرین رکھے ہوئے ہیں جو اپنی کرنسی میں ان سکوں، جواہرات سونے اور چاندی کے نرخ مقرر کرتے ہیں یہ اصل سے کم ہوتے ہیں مگر ایک تو سوائے لینے کے کوئی چارہ نہیں اور ملتے بھی فوراً ہیں تو تاجر انہیں لے کر تجارت کرتے ہیں اور جو چاہیں وہ خرید سکتے ہیں۔ یہ کاغذی ٹکڑے اٹھانے میں آسان اور انتہائی ہلکے ہوتے ہیں۔"

کئی سو سال گزر گئے، چینیوں نے کاغذی نوٹ کے ساتھ وہی کیا جو اہل روم نے سکوں کے ساتھ کیا تھا۔ پیسے کی ویلیو کم ہوتی چلی گئی۔ افراط زر (Inflation) بڑھتی چلی گئی حتی کہ چین میں 1455ء میں کاغذی کرنسی کو یکسر ختم کرنا پڑا اور پھر اسے واپس آنے میں کئی سو سال لگ گئے۔

انڈیا کے راستے جب پرتگالی چین پہنچے، تجارت کے لیے تو وہ اپنے ساتھ ہندوستان سے سکے لائے جن کو جنوبی ہندوستان کی زبان تامل میں "کاسو" کہتے تھے اور یہیں سے لفظ "CASH" دنیا کو ملا۔

پندرہویں صدی اور سولہویں صدی کے شروع میں جہاں چین واپس سکوں، ضمانتی تختیوں (Promissory-Notes) اور کاغذی کرنسی کی طرف واپسی کا سوچ رہا تھا۔ وہاں یورپ نے بڑھتی ہوئی ڈیمانڈ کے مد نظر سکوں کے حجم کو گھٹانا شروع کیا۔ چوکور سے گول سکے اسی Debasment کا نتیجہ تھے۔ 1606 کے ایک منی چینجر کے اشاعت شدہ

مینوئل کے مطابق اس وقت ایمسٹرڈیم میں 341 چاندی کے اور 505 قسم کے سونے کے سکے رائج الوقت تھے۔

شمالی امریکی انڈینز نے اپنے ایک تہوار کے نام پر Poltach پولٹیک کو لین دین کے لیے اپنایا تو باقی امریکیوں نے ویم پم جو کہ سفید شیلز سے بنی تسبیح کی طرح ہوتی تھی کو کرنسی کے طور پر استعمال کرنا شروع کیا۔

1609ء میں یورپ کے پہلے بینک کا قیام ایمسٹرڈیم میں عمل میں آیا۔ بینک نے لوگوں سے سکے، غیر ملکی سکے اور تحریف شدہ سکے (Debase Coins) لینے شروع کیے اور ان کے وزن اور قدر کے برابر بینک کا ضمانتی نوٹ (Bank Money) دینے شروع کر دیئے۔ جو اس بات کی ضمانت تھا کہ بینک حامل ہذا کو اتنے سکے طلب کرنے پر ادا کرے گا۔ یہ دنیا کی پہلی کاغذی کرنسی تھی جس کے پیچھے حکومتی گارنٹی تھی۔ اور جس نے قانوناً صرف اسی کرنسی کے استعمال کو لازمی قرار دیا۔

1642ء میں امریکی ریاست ورجینیا نے تمباکو کو قانونی زر (Legel Tender) کا درجہ دے دیا جو اگلے دو سو سالوں تک جاری رہا۔

1652ء میں سوئس حکومت نے جون پام اسٹریچ کو پہلا سوئس بینک کھولنے کی اجازت دی جس نے 16 جولائی 1661ء میں پہلا نوٹ جاری کیا۔

انگلستان کا نوٹ کہیں بعد میں 1694 میں شائع ہوا۔ اور امریکہ نے آزادی کے بعد 10 مئی 1775ء میں اپنے نوٹ کا اجراء کیا جو کونٹی نینٹل نوٹ کہلایا۔

(تصویر2: کونٹی نینٹل کرنسی)

یورپ میں بینکوں نے بل آف ایکسچینج کا اجراء شروع کیا جس میں اشیاء کے خریدار سے ایک ضمانتی نوٹ لیا جاتا کہ وہ مستقبل میں ادائیگی کرے گا۔ایسے نوٹ کے پیچھے خریدار کا اعتبار (Credibility) یا کسی مضبوط ضمانت کار (Guarantor) کی ضرورت ہوتی ہے ۔جیسے کہ آج کل بینک ایل سی کھولتے ہیں۔

(تصویر3)

1640ء میں انگلستان میں کنگ چارلس نے زبردستی رائل منٹ میں موجود لوگوں کا سونا قبضہ کر لیا۔تاجروں نے حکومت پر بھروسہ ختم کر کے لندن کے زرگروں کے پاس سونا

رکھوانا شروع کر دیا جن کے پاس بڑے محفوظ سیف اور جگہیں ہوتی تھیں۔اس سونے کے عوض وہ انہیں رسید دیتے اور ان رسیدوں کی مدد سے لین دین ممکن ہو جاتا کیونکہ رسیدوں کے پیچھے اصل سونا ہوتا لہذا بینک کے دیوالیہ ہونے یا فراڈ کا خدشہ تقریباً ختم ہو جاتا۔

بعد میں تاجروں نے سُناروں کو اس بات کی اجازت بھی دیدی کہ وہ چاہیں تو سونا یا اس مقدار کے ضمانتی نوٹ کسی اور کو ادھار دے دیں اور سود وصول کریں جس کا ایک حصہ سونا جمع کروانے والے کو بھی ملتا اور یوں ہلکے ہلکے ماڈرن بینکنگ کی داغ بیل پڑی۔

بینک آف ایمسٹرڈیم نے کاروبار اور لوگوں کو ادھار دینے شروع کر دیئے جس کا بڑا حصہ ڈچ ایسٹ انڈیا کمپنی کو گیا۔لوگوں نے پیسے لوٹانے میں دیر کی، کچھ نے غبن کیا اور بالآخر ایمسٹرڈیم شہر کو بینک کی بھاگ دوڑ سنبھالنی پڑی جس نے 1791 میں بینک لے کر 1819ء میں بند کر دیا۔

بینک آف ایمسٹرڈیم کے اچانک بند ہو جانے کا خلاء بینک آف انگلینڈ نے پورا کیا۔1694ء میں شروع ہونے والا یہ بینک دنیا کا سینٹرل بینک بن گیا اور پائونڈ آسٹرلنگ دنیا کی پہلی ریزرو (Reserve) کرنسی۔

بینک آف انگلینڈ اگلے کئی سو سالوں تک پرائیویٹ بینک رہا حتی کہ اسے 1946ء میں قومیالیا گیا۔

اٹھارویں صدی میں اسکاٹ لینڈ اور انیسویں صدی میں امریکہ نے نوٹوں کو دھڑا دھڑ چھاپنا شروع کیا۔ صرف انیس ویں صدی میں امریکہ میں دس ہزار سے زائد طرح کے کرنسی نوٹ گردش میں رہے۔ جیسے کہ آج آٹھ سو سے زائد کرپٹو کرنسیز موجود ہیں۔

جب کرسٹوفر کولمبس نے 1492ء میں اٹلانٹک کی طرف سفر شروع کیا تو وہ مشرقی ایشیاء کا راستہ ڈھونڈنے کے ساتھ ساتھ سونے کی بھی تلاش میں تھا۔اسے کیریبین کے پاس ہسپانولیہ

کے جزیرے پر کافی سونا ملا۔ مگر اتنا نہیں جتنا اس کے پیچھے جانے والوں کو وسطی اور جنوبی امریکہ میں ملا۔ کولمبس کے نصیب میں امریکہ آگیا۔

اسپینش لٹیرے جب ان علاقوں میں پہنچے تو انہوں نے دیکھا کہ مقامی آذٹیک باشندے میکسیکو میں اور انکاس پیرو میں سونے اور چاندی کو کرنسی کی بجائے زیور وآرائش کے لیے استعمال کرتے ہیں۔

اسپینش کو جلد ہی چاندی کا ماخذ پتہ چل گیا جو کہ پتوسی بولیویا میں تھا۔ یہاں دنیا کی تاریخ کی سب سے بڑی چاندی کی کان تھی۔

1556ء اور 1783ء کے درمیان یہاں سے 45 ہزار ٹن چاندی نکال کر اسپین بھیج دی گئی۔ مائننگ میں مرکری استعمال ہوتا تھا۔ احتیاطی تدابیر کی عدم موجودگی کی وجہ سے ہزاروں لوگ ہلاک ہوئے۔ لوگوں کی کمی کو پورا کرنے کیلئے افریقہ سے غلام لائے گئے جن کی ایک بڑی تعداد بھی ہلاک ہو گئی۔

سونے اور چاندی کی اس غیر معمولی سپلائی نے اگرچہ اسپین کو کچھ عرصہ کے لئے خوشحال تو کر دیا مگر یہ ملک کے مستقبل کیلئے اچھا ثابت نہ ہوا۔ اسپین نے اس پیسے سے کچھ جنگیں تو لڑیں مگر نہ کوئی نئی تجارت کی، نہ ہنر سیکھا اور نہ کچھ کاشت کیا۔ اتنے سارے پیسے کی وجہ سے اشیاء کے نرخ بڑھ گئے اور افراط زر کی وجہ سے غریب چیخ اٹھے۔ کتنی عجیب بات ہے کہ روم میں سونے چاندی کی قلت سے Inflation ہوئی تو یہاں زیادتی سے۔

سونے کی بات نکل چلی ہے تو آیئے تھوڑا تفصیل سے دیکھ لیتے ہیں۔

سونے کی تلاش، جانکاری دریافت و کھدائی میں ہزاروں سال لگانے اور ہزاروں جانوں کے ضائع کر دینے کے باوجود دنیا نے آج تک جتنا سونا بھی نکالا ہے وہ 65×65×65 فٹ یا 20×20×20 میٹر کے ایک رقبے میں سما سکتا ہے، ایک اولمپک کے سوئمنگ پول کے حجم

جتنا۔ایک اندازے کے مطابق دنیا نے کل 174,000 ٹن سونا نکالا ہے یعنی ہر شخص کے حصے میں 23 گرام آیا۔ہم سارا سونا پہاڑ کھود کے زمین کی تہہ سے نکالتے ہیں،اسے صاف کرتے ہیں اور پھر دنیا کے کسی فیڈرل بینک کے زیر زمین والٹ میں رکھ دیتے ہیں۔ سونے کو شاید زمین سے کچھ خاص انسیت ہے خود بھی وہاں رہتا ہے اور اپنے استعمال کرنے والوں کو بھی ایک دن وہیں لے جاتا ہے تو ہم سونے کو زیر زمین والٹ میں رکھ کر پھر سے ضمانتی رسید اور Promissory Notes پر کاروبار کرتے ہیں،چین کی مٹی کی تختیوں کی طرح وہی جو ہزاروں سال سے کرتے چلے آئے ہیں۔

کولمبس اور اس کے بعد اتنے سارے سونے اور چاندی کے بعد یورپ میں کرنسی کی قدر بہت کم ہو گئی اور افراط زر نے ملکوں کو کئی صدیوں تک جکڑے رکھا۔ سونے کو سب سے پہلے قدر کا معیار(Gold Stanadard)1816ء میں انگلستان میں بنایا گیا۔

کرنسی نوٹ کا اجراء تو اب تک صدیوں سے ہو رہا تھا مگر نوٹ کے پیچھے سونے کی گارنٹی کا سلسلہ اب شروع ہوا۔امریکہ نے انیس ویں صدی کے اوائل میں اس پر عمل کیا اور یہ وہ قانون ہے جسے دنیا آج ''سونے کا معیار''(Gold Stanadard) کے نام سے جانتی ہے۔

ان دنوں میں کوئی ملک صرف اتنی ہی کرنسی جاری کر سکتا تھا جتنا اسکے پاس سونا ہو۔ملک سونے کی کوئی رقم طے کرتا تھا اور پھر کرنسی جاری کی جاتی۔ مثلاً اگر امریکہ میں ایک اونس سونا بیس ڈالر کا ہے تو اس کا مطلب ہوا کہ ہر ایک ڈالر سونے کے اونس کا بیسواں حصہ ہے کوئی بھی شخص مرکزی بینک میں جا کر ڈالر دے کر اس کی قدر کے مطابق سونا لے سکتا تھا۔1930ء میں معاشی ابتری کے بعد دنیا نے آہستہ آہستہ ''سونے کے معیار'' کو خیر باد کہہ دیا اور آج دنیا میں کوئی ملک ایسا نہیں بچا جہاں گولڈ اسٹینڈرڈ باقی ہو یا جہاں سے آپ کو مرکزی بینک پیسے لے کر اس کے متبادل سونا دے سکے۔

سونا انسانوں کے لئے ہمیشہ سے کشش کا باعث اور قابل اعتبار رہا۔ وہ دھات کی صورت میں ہو یا جیولری کی۔ چڑھاوے کی صورت میں ہو یا سجاوٹ کی، دولت کی شکل ہو یا مال کی۔ آسٹریلیا کی ابرجینز سے لے کر پیرو کے انکاس تک، ہندوستان کے برہمن سے لے کر اسپین کے لٹیروں تک اس کی قدر سب نے کی۔

مڈل ایجز میں بازنطینی سلطنت کے زوال کے ساتھ ہی ان کے سکوں کی قدر ختم ہوتی چلی گئی اور دنیا ہلکے ہلکے چاندی یا سونے اور چاندی دونوں دھاتوں کی مشترکہ قدر پر آنے لگی اور یہ سلسلہ امریکہ کی آزادی تک چلتا رہا۔

سن 1717ء میں سر آئزک نیوٹن (جو اس وقت رائل منٹ کے ماسٹر تھے) نے چاندی اور سونے کے مابین ایک Ratio بنا کر چاندی کو مکمل طور پر عام سرکولیشن سے خارج کر دیا۔

گولڈ اسٹینڈرڈ یا سونے کے معیار تین طرح کے ہوتے ہیں۔ گولڈ اسپیشیز (Gold Species) جس میں سونے کے سکے عام سرکولیشن میں ہوں جس کی بنیاد پر رائج تمام کرنسی کی قدر متعین ہو۔

دوسرا گولڈ بلین (Gold-Bullion) جس میں رائج کرنسی کی بنیاد تو سونا ہو مگر خود سونے کے سکے سرکولیشن میں نہ ہوں۔ کوئی شخص کرنسی کے بدلے سونا خرید سکے مگر سونا بطور کرنسی استعمال نہ ہوتا ہو۔

(تصویر4: صحابہ کرام رضی اللہ عنہ کے دور میں استعمال ہونے والے سکے)

تیسرا گولڈ ایکسچینج (Gold-Exchange) جو صرف ملکوں کے مابین ہوتا ہو اور ایک ملک دوسرے ملک کی کرنسی کی قدر اس کے پاس موجود سونے کے ذخائر کے حساب سے کر سکے۔

1821ء میں رائل منٹ کی گارنٹی کے ساتھ انگلستان میں گولڈ اسٹینڈرڈ کا معیار اپنایا گیا۔ ریاست ہائے متحدہ، ریاست ہائے متحدہ کینیڈا، نیو فاونڈ لینڈ اور جرمنی نے بھی اپنالیا۔ امریکہ نے گولڈ ایگل اور کینیڈا نے حکومتی گولڈ متعارف کروایا۔ تمام ملکوں نے اس معیار کو عالمی جنگ عظیم اول کے شروع ہوتے ہی ختم کر دیا۔

1931ء کا عظیم معاشی انحطاط (گریٹ ڈپریشن) گولڈ اسٹینڈرڈ سے رخصت کی بنیادی وجہ بنا۔ لوگوں کو لگا کہ دنیا شاید ختم ہونے والی ہے تو انہوں نے دھڑا دھڑ پیسے دے کر سونا نکالنا شروع کر دیا۔ بینک آف انگلینڈ دیوالیہ ہونے کے قریب تھا۔ اس کا سربراہ مونٹاگو نارمن اس پریشانی میں بیمار ہو کر طویل رخصت پر چلا گیا اور اس کے جانے کے بعد اس کے ساتھیوں نے ایک دن اچانک گولڈ اسٹینڈرڈ ختم کر دیا۔ امریکہ میں فرینکلین ڈی روزویلٹ کی صدارت

تھی۔ایف ڈی آر کے تمام مشیران نے اسے گولڈ اسٹینڈرڈ پر رہنے کی تجویز دی، سوائے ایک کے: جارج واران زرعی معاشی ماہر تھا۔ صدر نے اس کی بات سنی اور امریکہ نے بھی سونے کے معیار کو تدریجاً خیر باد کہہ دیا، باقی دنیا نے انگلستان اور امریکہ کی پیروی ہی کرنی تھی اور اس طرح ہلکے ہلکے دنیا گولڈ اسٹینڈرڈ سے باہر آگئی۔اس معیار کو خدا حافظ کہنے والا آخری ملک سوئٹزرلینڈ تھا جس نے سن 2000 میں سونے کے معیار سے خلاصی چاہی۔

1970ء میں صدر نیکسن نے ڈالر سے سونے کے عالمی تبادلے پر یکسر پابندی لگادی اور یوں یہ باب ہمیشہ کے لئے بند ہوا۔امریکی نوٹ پر حامل ہذا کو مطالبے پر ادا کیا جائے گا کے بدلے" ہم خدا پہ بھروسہ کرتے ہیں "لکھ دیا گیا۔

اگرچہ عالمی جنگ عظیم دوئم کے فوراً بعد دنیا نے کسی طور گولڈ اسٹینڈرڈ پر جانے کی کوشش کی تھی مگر وہ کامیاب نہ ہو سکی۔جولائی 1944ء میں ماونٹ ڈیسپشن (Mount Deception) کے ساتھ بریٹن وڈز کانفرنس (Bretton Woods Conference) ہوئی اور اس میں بریٹن وڈز نام کا ایگریمنٹ طے پایا، کہ کوئی بھی ملک 35 ڈالر میں امریکہ سے ایک اونس سونا لے سکتا ہے۔اس طرح بلاواسطہ دنیا کے تمام ملک گولڈ سے جڑ گئے۔آئی ایم ایف کا قیام عمل میں آیا کہ ملکوں کے مابین ٹرانزیکشن کو موثر بنایا جائے مگر 1960ء تک پہنچتے پہنچتے پھر پیچیدگیاں ہو گئیں اور 1968ء میں یہ سسٹم بھی فیل ہو گیا۔ صدر نیکسن نے پندرہ اگست 1971ء میں گولڈ ونڈو کو بند کر دیا کہ کوئی بھی فکسڈ ریٹ پر اب امریکہ سے سونا نہیں لے سکتا اور یوں اس واقعہ جسے "نیکسن شاک" بھی کہا جاتا ہے نے سونے کے معیار کے تابوت پر آخری کیل ٹھونک دی۔

اس وقت دنیا کی کوئی بھی کرنسی کے پیچھے سونے کے ذخائر نہیں ہیں اور سب کی سب فیاٹ (Fiat) کرنسی (حکومتی ضمانت کے ساتھ) ہیں۔

امریکہ کا سونا ایک ہزار اونس کے بار کی شکل میں مختلف جگہوں پر محفوظ ہے۔
فورٹ ناکس بلین ڈیپازیٹوی میں 4600 ٹن سونا محفوظ ہے جس کی مالیت 58 بلین ڈالرز بنتی ہے۔ 1781 ٹن ویسٹ پوائنٹ، نیویارک میں 1368 ٹن ڈینور میں اور 1000 ٹن کے لگ بھگ فیڈرل ریزروز میں۔ امریکہ کے پاس اپنا کل آٹھ ہزار ٹن سونا ہے جس کی مالیت 100 بلین ڈالر ہے۔ Amazon کے سی ای او کی نیٹ ورتھ 113 بلین ڈالرز ہے۔ دنیا کے باقی ملکوں نے بھی نیویارک کے مین ہیٹن میں قائم فیڈرل ریزروز کے زیر زمین اسی فٹ نیچے والٹ میں اپنا سونا محفوظ کیا ہوا ہے۔ یہ کوئی دس ہزار ٹن سونا ہے جس کی مالیت 125 بلین ڈالرز ہے یہ چار سو ٹرائے اونس کے بار کی شکل میں ہے۔ ہر بار کی قیمت 160,000 ڈالر ہے یہ الگ الگ چیمبرز (کمروں) میں رکھا گیا ہے سب سے بڑے چیمبر میں 107,000 بار ہیں جو دس فٹ لمبے، دس فٹ چوڑے اور اٹھارہ فٹ گہرے رقبے میں محفوظ ہیں۔
دنیا میں کہیں سے سونا نکلے وہ افریقہ میں موجود نوبیا کی کانیں ہوں یا میکسکیو میں آزٹیک لوگوں کا سرمایہ وہ پیرو میں انکاس کی دولت ہو یا بازنطینی ایمپائر کے سکے، گھانا کے بادشاہ کے Mponeng میں لگے سونے کے ٹکڑے ہوں یا جنوبی افریقہ کی کانوں سے زولو اور ژوسا قبیلوں کی کار گزاری، دنیا کے سونے کی تاریخ مین ہیٹن کی اسی فٹ زیر زمین اس قبر تک پہنچ جاتی ہے۔
سونے کی قدر کا اندازہ اس بات سے لگائیں کہ 42 سینٹی میٹر کا ایک ٹکڑا جو کہ ایک ڈالر کے نوٹ کا دو تہائی حصہ بنتا ہے کی مالیت ایک ملین ڈالر ہے۔ ٹرمپ کی کل دولت 3.7 بلین ڈالر اگر سونے میں منتقل کی جائے تو سونے کی ڈلی کا حجم 1.7 میٹر بنے گا جو کہ خود ٹرمپ کے قد سے چھوٹی ہے۔ بٹ کوائن کی کل مارکیٹ 14.7 بلین ڈالرز یا 12.3 ملین اونس سونے کے برابر ہے۔

سونے کی سب سے بڑی کان:۔

انسان سونے کے لئے کچھ بھی کر سکتا ہے۔ کیاآپ کو یقین آئیگا کہ انسان زیر زمین ڈھائی میل جاکے ،جان جوکھوں میں ڈال کے صرف تیس انچ کی سونے کی تہہ میں جائے گا۔ جی ہاں یہ روز کا کام ہے سائوتھ افریقہ کے شہر یونانگ میں یہاں دنیا کی سب سے گہری سونے کی کان ہے جو کہ Witwatersend Basin وٹ واٹر سینڈ بیسن پر مبنی ہے۔ دنیا میں اگر کہیں بھی سونا ہو تو غالب امکان ہے کہ اس کا پچاس فیصد اسی پٹی سے نکلا ہے۔ یہ 1886ء میں دریافت ہوئی اور روایت یہ ہے کہ یہاں سے قریب موجود (Vredefort Crater) جس کا رقبہ دو سو میل ہے یہاں کسی شہاب ثاقب کے ٹکرانے سے 2.02 بلین سال پہلے وجود میں آیا تھا اور اس ٹکراو کے نتیجے میں یہ کان وجود میں آئی یا ظاہر ہوئی۔

یونانگ کی سونے کی کان جوہانس برگ سے مغرب میں واقع ہے اور اینگلو گولڈ اشانتی کی ملکیت ہے۔ یہاں دنیا کی لمبی ترین لفٹ ہے جو چار ہزار (4,000) کان کن مزدوروں کو روز زمین میں ڈھائی میل اندر لے جاتی ہے۔ چالیس میل فی گھنٹہ کی رفتار سے چلنے کے باوجود پہلے اسٹاپ پر پہنچنے میں نوے منٹ لگتے ہیں آپ سوچیں کہ ڈیڑھ گھنٹہ لفٹ میں زیر زمین سفر کیسا لگے گا۔ زیر زمین درجہ حرارت ساٹھ سینٹی گریڈ اور Humidity 95 فیصد ہے۔ روز چھ ہزار ٹن برف دھکیلی جاتی ہے تاکہ پنکھے سرد ہوا پھینک سکیں۔ پانچ ہزار پاونڈ دھماکہ خیز مواد، چھ ہزار چار سو ٹن پتھروں کو نکالنے کیلئے استعمال ہوتا ہے۔ ہر آئے دن انہیں مزید نیچے جا کر کھدائی کرنی ہوتی ہے اس کی گہرائی کا اندازہ اس بات سے لگائیں کہ یہاں دس ایمپائر اسٹیٹ بلڈنگ سما سکتی ہیں۔ یہاں بہت سے گھوسٹ مائنرز بھی چلے جاتے ہیں

جو غیر قانونی طور پر سونا نکالتے ہیں یہ لوگ زیر زمین رہتے ہیں اور سورج کی روشنی نہ ملنے سے انکی جلد کی رنگت تک بدل جاتی ہے۔

جائز کان کن، ان ناجائز کان کنوں کو کھانے پینے کی اشیاء اور باقی چیزیں اصل سے بارہ گنا تک بیچتے ہیں اور یہ سب کچھ سونے کی اس قبر میں زمین سے ڈھائی میل نیچے ہو رہا ہے۔

یہاں سائنسدانوں نے ایک بیکٹریا Desulforudis Audaxviator دریافت کیا جو سورج کی روشنی کے بغیر ماحول میں موجود ریڈیو ایکیٹو انرجی سے اپنی خوراک خود پیدا کرتا ہے اور یہاں سے سورج کی غیر موجودگی میں حیات کا فلسفہ چل نکلا کہ شاید کسی سیارے پر ایسی بھی کوئی حیاتیاتی مخلوق موجود ہو۔

آج کرپٹو کرنسی پر ماحولیاتی ظلم اور پیچیدگیوں کا الزام لگانے والوں کو یہ کانیں پتہ نہیں کیوں نظر نہیں آتیں۔ اور سونے کا ہی کیا رونا، ایسی کئی دھاتیں ہیں جو سونے سے زیادہ قیمتی ہیں ۔روڈیم ہے، پلاٹینم ہے۔ اینٹی میٹر کا ایک گرام ایک ٹریلین ڈالر کا اور اینٹی ہائیڈروجن کا ایک گرام 62 ٹریلین ڈالرز کا ہے۔ ریئرارتھ کی مائننگ میں پورا چائنا کھنگال ڈالا (یہ آئی فون میں استعمال ہوتی ہے) اور اس کی موجودگی آج تک افغانستان میں امریکی فوج کو روکے ہوئے ہے۔

یاد رکھنے کی بات ہے کہ پیسہ ایک سماجی تخیل (Social-Construct) ہے۔ اگر لوگوں کا اعتماد اس کے پیچھے ہے تو یہ پیسہ ہے ورنہ نہیں۔ ڈالر کے پیچھے لوگوں کے اعتماد کے سوا کچھ نہیں، جس دن یہ ختم ہو گیا اس کی قدر ردّی کے برابر بھی نہیں رہے گی۔

ہر پیسہ اپنے سماج، ماحول اور لوگوں کا پابند ہے مثلاً آپ بچوں کے کھیل مونوپلی میں مونوپلی منی سے خریداری کر سکتے ہیں اس کے باہر نہیں تو گیم کے اندر مونوپلی سو فیصد پیسہ میں شمار ہو گی۔ اس طرح آپ فرانس میں پاکستانی روپوں میں میں دودھ نہیں لے سکتے۔ پاکستان میں مل جائے گا۔ سونے کے معیار کے بہت سے فائدے اور نقصانات ہیں۔

فائدوں میں سب سے بڑا فائدہ تو یہ کہ سونے کی ایک یونیورسل ویلیو ہے جسے سب تسلیم کرتے ہیں اور اس کی سپلائی محدود ہے۔ یہ نا تو ناپید ہے اور نہ ہی تیل یا سبزیوں کی طرح عام۔ چھ سو قبل مسیح سے لے کر آج تک دنیا اور لوگوں کے دل میں سونے کا جو مقام اور عزت ہے وہ کسی اور دھات یا شے کے حصے میں نہیں آئی۔ حکومتی کاغذی نوٹوں کے پیچھے تو صرف لوگوں کا اعتماد ہے جس دن وہ اٹھ گیا یا حکومت نے پیسوں کو Null & Void ڈیکلیئر کر دیا اس کی کوئی قانونی حیثیت یا قدر باقی نہ رہے گی۔ سونے کے ساتھ یہ ہونا بہت مشکل ہے۔

دوسرا فائدہ یہ کہ حکومت کے پاس محدود طاقت ہوتی ہے۔ کوئی اپنی مرضی سے جتنے چاہے نوٹ نہیں پرنٹ کر سکتا۔ جس ملک کے پاس جتنا سونا ہو گا وہ صرف اتنے ہی نوٹ پرنٹ کر سکے گا۔ امریکہ نے جب گولڈ اسٹینڈرڈ کو خیر باد کہا تو اس وقت دنیا میں صرف 48 بلین ڈالر گردش میں تھے جو آج بڑھ کر 12 ٹریلین ڈالر تک پہنچ گئے ہیں۔

سونے کا معیار ایک جمہوری طریقہ کار ہے جو تاجر کو رعایت دیتا ہے جتنا سونا ہو گا مارکیٹ میں اتنی ہی پیسوں کی گردش ہو گی اس کے بغیر حکومت جب چاہے، جیسے چاہے مارکیٹ کو کنٹرول کر لے مرکزی بینک کی حیثیت مطلق العنان بادشاہ جیسی ہے اور عوام کو اس سے کیا فرق پڑتا ہے۔ وہ قوم کے "وسیع تر مفاد میں" جو چاہے کر گزریں، مثلاً پاکستانی حکومت نے ابھی حال ہی میں ڈالر کے مقابلے میں روپے کی قدر گرادی۔ کہتے ہیں کہ اس سے برآمدات میں اضافہ ہو گا مگر عام عوام کا اس فیصلے میں کوئی عمل دخل نہیں۔ ''سونے کے معیار'' میں یہ ممکن نہیں۔

''سونے کا معیار'' سے افراط زر کی شرح بھی بہت کم رہتی ہے۔ تاجر کا بھی فائدہ، اور عوام کا بھی۔ نقصان صرف حکومت کا ہوتا ہے۔ سن 1893 سے 1913ء تک امریکہ میں افراط زر کی شرح اوسطاً صرف 1.6 فیصد رہی۔ گولڈ اسٹینڈرڈ کے خاتمے کے بعد 1971ء میں 3.3

فیصد سے 1979ء میں بڑھ کر 133 فیصد تک پہنچ گئی۔امریکی فیڈرل ریزروز کی تحقیق کے مطابق اس وقت میں 15 ملکوں میں گولڈ اسٹینڈرڈ کے تحت افراط زر کی شرح اوسطاً 1.75 تھی جو بعد میں بڑھ کر 9.17% فیصد ہو گئی۔

1971ء اور 2003ء کے درمیان امریکی ڈالر اپنی قوت خرید اسی فیصد گنوا بیٹھا تھا۔1971ء کے 17 سینٹ (17 سینٹس) 2011ء کے ایک ڈالر کے برابر ٹھہرے۔

گولڈ اسٹینڈرڈ پر رہنے سے ملکوں کا مجموعی قرضہ بھی کم رہتا ہے جب ملک فیاٹ کرنسی میں ادائیگی کرتے ہیں تو باقی ملک اس کرنسی میں ملکی بانڈز لے لیتے ہیں۔امریکہ کے قرض کا پچاس فیصد سے اوپر حجم غیر ملکی سرمایہ کی صورت میں ہے۔

1971ء میں امریکہ کا کل قرضہ 406 بلین ڈالرز تھا جواب بڑھ کر 19 ٹریلین ڈالرز تک جا پہنچا ہے۔

گولڈ اسٹینڈرڈ سے جنگیں بھی کم ہوئیں۔صرف افغانستان اور عراق کی جنگوں میں امریکہ نے ایک اندازے کے مطابق تین ٹریلین ڈالرز لگائے ہیں اگر پیچھے سونا ضروری ہوتا تو اتنے پیسوں کا انتظام ممکن ہی نہ تھا۔آج تو صرف کچھ کلک کرنے پڑتے ہیں اور پیسہ "تخلیق" ہو جاتا ہے۔2008ء کے معاشی بحران میں امریکہ نے مارکیٹ میں تین ٹریلین ڈالرز شامل کیے۔کلک، کلک اور کلک، پہ رہے آپ کے تین ٹریلین ڈالرز۔

(تصویر 5: امریکی 500 ڈالر کا نوٹ)

رہی سہی کسر 1975ء کے اوپیک (OPEC) معاہدے نے پوری کر دی جس میں سعودی عرب کی سربراہی میں تمام ملکوں نے تیل بیچنے کے لئے صرف و صرف امریکی ڈالرز لینے پر اتفاق کیا۔ اب دنیا کے ہر ملک کو تیل چاہیے اور وہ صرف امریکی ڈالرز میں لے سکتے ہیں۔ عالمی ٹرانزیکشنز صرف امریکی ڈالرز میں ہونگی تو امریکہ جتنے چاہے پرنٹ کر لے اس کی کرنسی گرنے میں نہیں آتی۔ 1973ء میں جو آئل کا بیرل 20 ڈالر کا تھا وہ 2012ء تک 100 ڈالر کا ہو گیا۔ اگر کرنسی کے پیچھے سونا ہوتا تو تیل ایک ڈالر فی لیٹر سے مہنگا نہیں جا سکتا تھا۔

گولڈ اسٹینڈرڈ میں معاشی ترقی بھی تیزی سے ہوتی ہے۔ 1792 سے 1971ء تک امریکہ میں معاشی ترقی کی سطح اوسطاً 3.9 فیصد رہی جو کہ سونے کے معیار کی تلفی کے بعد سالانہ 2.8 فیصد کی اوسط پر آگئی اگر آج گولڈ اسٹینڈرڈ ہوتا تو امریکہ کم از کم آٹھ ٹریلین ڈالر کی معیشت پر ہوتا۔

2008ء میں اپنی مرضی سے پیسہ پرنٹ کر کے امریکہ پیسوں کی سالانہ سپلائی کی 2.6 فیصد اوسط کو 152.3 پر لے آیا دسمبر 2007ء سے دسمبر 2009ء تک جس کا اثر مستقبل میں

افراط زر کی نمو پر پڑا۔ مگر کیونکہ ڈالر کے پیچھے پوری دنیا کی سپورٹ ہے اور اگر ڈالر ڈوبا تو دنیا کو ساتھ لے ڈوبے گا اس لئے بہت سے "ہمدردوں" کا سہارا اسے ہمیشہ ہی مل جاتا ہے۔

گولڈ اسٹینڈرڈ میں بے روزگاری کا تناسب بھی کم ہوتا ہے۔ 5 فیصد بمقابلہ چھ فیصد اور ایک عام آدمی کی آمدنی میں بھی معقول اضافہ ہوتا ہے۔ 2.7 فیصد بمقابلہ صرف 0.2 فیصد۔

مگر ایک معیشت دانوں کا گروہ ایسا بھی ہو جو اس کے نقصانات بتاتے نہیں تھکتا مثلاً سونے کی قدر مستحکم نہیں ہے اور جس شدت کے ساتھ یہ گھٹتی بڑھتی ہے ملکی معیشت اس کی مستحکم نہیں ہو سکتی۔ مثلاً اگر سونے کی قدر کچھ عرصے میں پندرہ فیصد تبدیل ہو جائے تو ملک میں موجود ہر شے کی قیمت اسی تناسب سے پندرہ فیصد بدل جائے گی اور کوئی ملک یا عوام اس کی متحمل نہیں ہو سکتی۔ مثال کے طور پر 1890ء میں سونے کی قیمت 700 ڈالر تھی جو 1920 میں گھٹ کر 200 ڈالر رہ گئی کہ لوگوں نے مزید کھدائی کر کے زیادہ سونا نکالنا شروع کر دیا۔ 1933 میں (جب دنیا گولڈ بلین معیار پر تھی) سونا 563 ڈالر کا تھا جو 1971 تک 201 ڈالر کا ہو گیا۔ فیاٹ کرنسی کے بعد بھی سونا 2,337 ڈالر فی اونس سے لیکر 1672 ڈالر کے درمیان ڈولتا رہا ہے۔ سونے کی یہ صفت آج کرپٹو کرنسی پر اعتراض کرنے والوں کو ضرور سمجھنی چاہیے۔

فیاٹ کرنسی کا فائدہ یہ ہوتا ہے کہ آپ روپے کی قدر کا تعین کر کے باآسانی معاشی بحران سے نکل سکتے ہیں۔ امریکہ میں 1884، 1890، 1893، 1907، 1930، 1931، 1932، 1933 میں شدید معاشی بحران آئے۔ صرف 1933 میں چار ہزار بینکوں نے اپنے کام بند کر دیئے۔ مگر 2008ء میں باآسانی قابو پالیا گیا کیونکہ حکومت کے پاس پیسے تخلیق کرنے کی طاقت تھی۔

اگر کرنسی کو کسی بھی جنس (Commodity) کے ساتھ نتھی کریں تو آپ اپنی مرضی سے جتنی چاہیں تخلیق نہیں کر سکتے۔ اسی لئے آج کل کی کرنسی مختلف جنس کی ایک ٹوکری کے ساتھ نتھی ہیں اور حکومت اس بات کا تعین کرتی ہے کہ کتنے پیسوں میں ایک عام آدمی کیا کیا لے سکتا ہے۔ اب ملک سے موجود ہر جنس کی شے کے ساتھ بالواسطہ یا بلاواسطہ کرنسی نتھی ہو گئی جس سے یہ مزید محفوظ بھی ہو جاتی ہے۔

افراط زر کرنسی میں جان بوجھ کر رکھا جاتا ہے قریباً تین فیصد تاکہ لوگ نوٹ جمع کر کے نہ رکھ لیں۔ جب ان کو پتہ ہو گا کہ جمع کرنے سے ان کی قیمت کم ہو جائے گی تو وہ انہیں خرچ کریں گے جس کا بہتر اثر ملکی معیشت پر پڑے گا۔

سونے کی بات چل ہی رہی ہے تو گولڈ مائننگ پر بھی بات ہو جائے۔ لوگ کہتے ہیں کہ کرپٹو کرنسی کی مائننگ کا ماحول پر برا اثر پڑتا ہے اور یہ آدھی دنیا کی بجلی کھا جاتا ہے وغیرہ ان میں صداقت اتنی نہیں ہے۔ ایک اونس سونا زمین سے نکالنے کے لئے اوسطاً 70 ٹن کچرا (Mine-Watse) نکلتا ہے۔ دنیا کے سارے سونے کی قیمت صرف 9.1 ٹریلین ڈالرز ہے امریکہ کا قرضہ ہی 19 ٹریلین ڈالرز ہے۔ گولڈ اسٹینڈرڈ پر واپس جانے کی دنیا متحمل نہیں ہو سکتی۔

گولڈ مائننگ اور بٹ کوائن مائننگ میں بہت مماثلت پائی جاتی ہے۔ اگر آپ کو 1846 سے 1852ء کے درمیان کیلی فورنیا کا گولڈ رش (Gold Rush) یاد ہو تو وہاں بھی وہی ہوا تھا جو آج یہاں ہو رہا ہے۔

عام آدمی کے لئے گولڈ مائننگ بہت پر کشش ہو گئی تھی، آج بٹ کوائن مائننگ میں بھی ایسا ہی ہے۔

سونے کی قیمت دوگنی سے زیادہ بڑھ گئی تھی، بٹ کوائن بھی بڑھ رہا ہے۔

بہت سے لوگ سونا نکالنے چل پڑے تھے۔ 1846ء میں صرف 100 مائنرز بڑھ کر 1852ء تک 30 ہزار ہوگئے تھے۔ بٹ کوائن میں بھی فل نوڈز پندرہ ہزار سے تجاوز کر چکے ہیں۔

کچھ لوگ بہت امیر ہوگئے، تھوڑے لوگوں کو تھوڑا بہت ملا، باقی کو کچھ نہیں کرپٹو کرنسی میں بھی یہی کچھ ہو رہا ہے۔

بہت سے لوگ جو خود تو مائننگ نہیں کر رہے تھے امیر ہوگئے مثلاً جو سامان آلات بیچتے تھے۔ ایک پھاوڑے کی قیمت اس دور میں 36 ڈالر سے تجاوز کر گئی تھی۔ پھر سونا خریدنے اور بیچنے والے اور اس نئی رقم پر جوئے کے اڈے چلانے والے۔ کھانا دینے ولے رہائش گاہ کا انتظام کرنے والے۔

یہی کچھ آج ہو رہا ہے۔ 2000 ڈالر کا اینٹ مائنر (Ant Miner) آلہ پندرہ ہزار ڈالر کا ہو چکا ہے گرافکس کارڈ تین سے چار ماہ بعد مل رہے ہیں۔ اور کرایہ پر جگہ دینے والے بجلی والے اور تکنیکی ماہرین خوب کما رہے ہیں۔

اپنی تقدیر جگانے کے لئے لوگوں نے گروہ کی شکل میں سوناڈھونڈنا شروع کر دیا کہ ملے گا تو سب بانٹ لیں گے۔ کرپٹو کرنسی میں پولنگ اسی کو کہتے ہیں۔

جتنے زیادہ لوگ آتے گئے سوناڈھونڈنا اتنا ہی مشکل ہوتا چلا گیا۔ یہاں بھی یہی ہوتا ہے اسے ہم مائننگ ڈیفیکلٹی (Mining Difficulty) کہتے ہیں۔

اگر آپ سونے اور بٹ کوائن کے انرجی کے خرچے کو مد نظر رکھیں تو ایک بٹ کوائن سونے کے ایک اونس کے مقابلے میں سات گنا زیادہ انرجی خرچ کرتا ہے۔ مگر پھر بھی مکمل خرچ کم ہے کیونکہ دنیا بٹ کوائن کے مقابلے میں 135 گنا زیادہ سونا نکال رہی ہے۔

2017ء میں روز کے 1800 کوئنز کے حساب سے سال کے 650،000 بٹ کوائن بنے جب کہ اسی عرصے میں سونے کی دو سب سے بڑی کمپنیوں بیرک (Barrick) ارونیو مونٹ (New-Mont) نے 88 ملین اونس سونا نکالا اور ہر اونس پر 8.5 گیگا جولز بجلی لگی۔

جنوری 2018ء میں بجلی، آلات، مہارت سب کا خرچہ ملا کے ایک بٹ کوائن پر 1800 ڈالر کی لاگت آتی ہے اور یہ بکتا ہے 14 سے 15 ہزار ڈالر میں 2016 کی رپورٹ کے مطابق ایک اونس سونا نکالنے پر 1،115 ڈالر لاگت آتی ہے اور یہ بکتا ہے 1250 سے 1300 ڈالر کے درمیان۔

آج کل کی دنیا میں بٹ کوائن کی مائننگ، سونے کی مائننگ سے زیادہ نفع بخش ہے اور یہ حقیقتاً ڈیجٹل گولڈ ہے۔

(تصویر 6: سلور ڈالر)

چلیں ہم اپنے اصلی موضوع کی طرف واپس آتے ہیں۔ کیا آپ کو معلوم ہے کہ پیسہ غائب بھی ہو سکتا ہے؟ جی بالکل دنیا میں کیش / نقدی کل کرنسی کا تین فیصد بھی نہیں۔ باقی سب کمپیوٹرز

میں ڈیجٹل نمبرز کی شکل میں ہے آپ نے کسی کو آن لائن ٹرانسفر کروایا یا کریڈٹ /ڈیبٹ کارڈ سے پیمنٹ کی ایک جگہ سے نمبر کم ہو کر دوسری جگہ بڑھ گیا۔ کوئی پیسہ جسمانی طور پر ادھر سے ادھر منتقل نہیں ہوا۔ دنیا کی ستانوے فیصد کرنسی ایسے ہی زندہ ہے لوگ اگر بینکوں سے سارے پیسے لینے پہنچ جائے تو بینک دیوالیہ ہو جائے۔ بینک عموماً اپنے پاس محفوظ پیسوں کا بیس واں حصہ مرکزی بینک میں رکھوانے کے پابند ہوتے ہیں باقی وہ کلک کلک کر کے ادھار اور باقی مد میں ادھر سے ادھر کرتے رہتے ہیں۔

اگر لوگوں کا بینکوں سے حکومت سے یا کرنسی سے اعتماد اٹھ جائے تو وہ فوراً اسے متبادل کرنسی میں تبدیل کرنا چاہیں گے یا سارا پیسہ نکلوانا چاہیں گے جیسا کہ حالیہ سالوں میں ہنگری میں ہوا اور یوں ملک کے معاشی نظام کا بیڑہ غرق ہو جائے گا۔

آپ کو یاد ہو گا کہ نواز شریف نے مئی 1999 میں نیوکلیئر دھماکوں کے بعد سارے ڈالرز اکاونٹ فریز کر دیئے تھے۔ لوگوں کا پیسہ مگر اس پر اختیار ختم۔ وہ دن ہے اور آج کا دن، تاجر طبقہ اپنا پیسہ ملک سے باہر ہی رکھتا ہے۔ اور پھر آپ ان پر فارن اکاؤنٹس کے طعنے کستے ہیں۔

پیسوں کے غائب ہونے کا یہ سلسلہ گاہے بگاہے چلتا ہی رہتا ہے۔ کرپٹو کرنسی کے اس پورے دھندے میں اچنبھے کی بات صرف وہ ہے جو آپ نے پڑھی نہیں باقی سب دنیا دیکھ ہی چکی ہے۔

اور اگر پیسہ غائب نہ بھی ہو تو تب بھی Inflation کی وجہ سے اگر وہ اوسطاً صرف تین فیصد بھی ہو تو تقریباً تیس سال میں ہر شئے کی قیمت دوگنی ہو جاتی ہے۔ ریئل اسٹیٹ میں تو صرف دس سال لگتے ہیں۔

لوگ سمجھتے ہیں کہ پیسے کی قدر و قیمت قائم رہتی ہے یا یہ کہ یہ کوئی مجسم چیز ہے، یہ دونوں ہی نظریے باطل ہیں۔

آیئے کچھ مثالیں دیکھتے ہیں کہ پیسے نے اپنی قدر و منزلت سے کیسے آنکھیں پھریں۔

عالمی جنگ عظیم دوئم کے فوراً بعد 1946ء میں ہنگری کی کرنسی پینگو ہر چودہ گھنٹے میں دوگنی ہو رہی تھی مطلب کے جو روٹی آپ نے بدھ کو لی ہے وہ پیر کی صبح تک دس گنا مہنگی ہو جائے گی۔ لوگوں کو جیسے ہی پیسہ ملتا وہ اسے فوراً خرچ کرنے کو بھاگتے کہ اتنی دیر میں اس کی قدر مزید نہ گر جائے۔ لوگوں نے کچھ ہی عرصے میں پینگو چھوڑ کر بارٹر سسٹم اور سونے سے لین دین شروع کر دیا۔ اگست 1946 میں ہنگری حکومت نے نئی کرنسی فورنٹ (Forint) متعارف کروائی جس کا ایک روپیہ چار سو آکٹیلین (4,00,000,000,000,000,000,000,000,000,000) پینگو کے برابر تھا۔

تو حقیقتاً پینگو کی قیمت ختم ہو گئی اور لوگوں کے پاس جتنی جمع پونجی تھی وہ آگ لگانے کے کام آئی۔ اسے ہائپر انفلیشن (Hyper-Inflation) کہتے ہیں۔ صفر گرانے کا یہ کھیل آج تک جاری ہے۔

نومبر 2008ء میں زمبابوے میں ایک روٹی زمبابوے کی تین سو ملین ڈالر میں آتی تھی۔ دوسرے ملکوں کو باقاعدہ اشتہار دینے پڑے کہ ٹوائلٹ پیپرز کی جگہ زمبابوے ڈالر استعمال نہ کریں۔

لوگوں نے لین دین کے لئے اپنی ہی کرنسی بنالی اور اسے استعمال کرتے رہے پھر اس کرنسی کی نقل بھی بن گئی مگر لوگ اسے بھی قبول کرتے رہے کہ مزید کرنسی بنانے کے لیے کسی کے پاس سامان و آلات کہاں تھے۔ نہ پیچھے کوئی حکومت نہ سنٹرل بینک اور کرنسی پھر بھی زندہ کہ لوگوں کا اعتماد تھا کہ باقی لوگ بھی اسے قبول کریں گے۔ (اب کیا اس صورت میں آپ اس ملک کی ساری معاشیات کو حرام کہیں گے؟)

صومالیہ میں حالات سب کے سامنے ہیں۔ موگادیشو سے باہر حکومت کا وجود نہیں یہ لوگ بھی شیلنگز کو استعمال کرتے رہے جس کی قدر عالمی مارکیٹ میں مونوپلی یا بچوں کی کرنسی سے زیادہ نہیں مگر کام چلتا رہا اور چل رہا ہے۔

1994ء میں برازیل نے ریئل نام سے نئی کرنسی متعارف کروائی جو کہ پرانی کرنسی کروز بروریئل کے بدلے ملتی تھی ایک نیا ریئل 2750 کروز بروریئل میں بدلا گیا۔

2009 میں شمالی کوریا نے اپنی کرنسی سے دو صفر غائب کر دیئے اور اعلان کر دیا کہ نیا وان (Won)، پرانے سو وان کے برابر ہو گا۔ مزید لوگوں کے پاس صرف چوبیس گھنٹے ہیں پیسے تبدیل کرنے کے لئے اور ایک شخص 690 ڈالر سے زیادہ تبدیل نہیں کر سکتا۔ کتنے ہی لوگ لاکھوں سے محروم ہوئے اور کتنوں نے صرف اسی صدمے میں چوبیس گھنٹے گزار دیئے۔ شمالی کوریا کی کرنسی ملک سے باہر کہیں نہیں چلتی تو حکومت سرکاری طور پر 96 وان کو ایک ڈالر کے برابر بتاتی ہے مگر جب آپ منی چینجر سے حقیقتاً خریدنا چاہیں تو آپ کو آٹھ ہزار وان کا ایک ڈالر ملتا ہے۔ یعنی آپ کی عمر بھر کی جمع پونجی کے بدلے حکومت نے آپ کو صرف 35 ڈالر دیئے اور باقی سب مال چوبیس گھنٹوں میں ایک حکم کے ساتھ ردی ہو گیا ہے یہ ہے وہ حکومتی گارنٹی جو ہم بار بار کرپٹو کرنسی میں مانگتے ہیں۔ 1923ء میں جرمنی نے جنگ کے لیے نوٹ چھاپے جو ڈالر 6.7 جرمن مارک میں 1919 میں ملتا تھا اس کی قیمت 1923 میں 4،210،500،000،000 مارکس ہو گئی اور لوگوں نے جرمن مارک کو وال پیپرز کے طور پر استعمال کرنا شروع کر دیا۔

امریکی صدر لنکن نے سول جنگ سے نمٹنے کے لئے 450 ملین ڈالرز پرنٹ کرنے کا حکم دے دیا جسے گرین بیگز کہا جاتا ہے۔

(تصویر 7:امریکی گولڈ ڈالر)

ابھی حال ہی میں انڈیا نے تین نومبر 2016ء کو کرنسی ڈی مونوٹائزیشن پہ کام کیا اور لوگوں کو تیس دنوں کا وقت دیا تمام ہزار اور پانچ سو والے نوٹ تبدیل کروانے کے لیے تاکہ نقلی نوٹوں، دہشت گردی کی فنڈنگ اور بلیک منی کو روکا جاسکے۔ تیس دنوں میں لوگوں نے 32 ہزار کروڑ تبدیل کروائے اور بہت سوں کو کروڑوں کا نقصان اٹھانا پڑا۔ وینزویلا میں جنوری 2017 کو تین ہزار بولیوار دے کر ایک ڈالر لیا جاسکتا تھا، دسمبر 2017ء میں ایک ڈالر 191,000 بولیوار میں ملتا تھا جب کہ دنیا میں سب سے زیادہ تیل اسی ملک کے پاس ہے۔

300 ملین بیرل ملک میں کوئی شخصی بینک سے چوبیس گھنٹوں میں چھ سینٹس سے زیادہ نہیں نکال سکتا اور اس کے لیے بھی چار گھنٹوں کی لائن ہے۔ معاشی ماہرین کے مطابق 2018ء میں وینزویلا میں افراط زر کی شرح 13،000 فیصد رہے گی۔ اب اگر یہ مظلوم لوگ کرپٹو کرنسی کو استعمال کریں تو کیا آپ اسے حرام کہیں گے؟

اگر آپ کو لگتا ہے کہ کرنسی نوٹ اور ڈیجٹل کرنسی ہی اصل نقد ہے اور باقی کچھ نہیں تو آیئے ہمارے زمانے میں موجود کرنسی کی اور کچھ مثالیں دیکھتے ہیں۔

2010ء میں ہیٹی کے زلزلے کے بعد لوگوں میں راشن تقسیم کرنا کھٹن ثابت ہوا کہ ایک جم غفیر ہوتا، چاول کی بوریاں ہیلی کاپٹر سے بھی نہیں گرائی جاسکتی تھیں کہ لوگ زخمی نہ ہو جائیں تو اقوام متحدہ نے ہزاروں سال پرانی عبادت گاہوں کی طرح اسٹور میں راشن ذخیرہ کر لیا اور لوگوں کو کوپن کی شکل میں پرچیاں بانٹ دیں۔ صرف چوبیس گھنٹوں کے اندر ہی وہ پرچیاں بطور کرنسی استعمال ہونے لگیں کہ سب کو پتہ ہے کہ اس کے پیچھے کتنا راشن ملے گا۔

جیل میں عموماً نقد رقم کی جازت نہیں ہوتی تو وہاں مچھلی، سگریٹ اور موبائل کریڈٹ عام طور پر لین دین خرید و فروخت کے لئے استعمال ہوتا ہے۔

بچے عموماً پیسے گرا دیتے ہیں امریکہ بھر کے سکولوں میں کنٹین میں ماں باپ پیسے جمع کروا دیتے ہیں اور بچوں کو اس کے بدلے کھانے کے کوپن مل جاتے ہیں جسے وہ کنٹین میں بطور کرنسی استعمال کر سکتے ہیں۔

کینیا اور تنزانیہ میں ایم۔ پیسہ کے نام سے موبائل پیمنٹ سسٹم موجود ہے۔آپ موبائل کریڈٹ کو پیسے ٹرانسفر سے لے کر کچھ بھی خرید و فروخت کے لیے استعمال کر سکتے ہیں۔

کینیا میں ساٹھ فیصد لوگ ایم پیسہ، تیس فیصد بینک اور سات فیصد اے ٹی ایم استعمال کرتے ہیں۔اب اس ایم پیسہ (M Pesa) کے پیچھے بھی کوئی حکومت نہیں۔

آپ ڈزنی ٹوکنز پر پورا ہفتہ گزار لیں اور پارک گھومتے رہیں، میرٹ ریوارڈ کے تحت ہوٹل میں قیام کر لیں، کریڈٹ کارڈز کے انعامی پوائنٹس سے پٹرول بھروالیں۔اسکائی مائلز کے ذریعے جہاز کا ٹکٹ خرید لیں۔پوائنٹس کو نقدی میں کیش کروالیں۔کھاڈی پوائنٹس سے جوڑے خرید لیں۔ایزی پیسہ سے لوڈ کروالیں یا پیسے بھجوادیں۔آپ کو ہر ملک و معاشرے میں درجنوں ایسی مثالیں مل جائیں گی جہاں ہم آسانی اور سہولت کے لیے کسی بھی چیز کو متفقہ طور پر کرنسی

کے طور پر استعمال کر لیتے ہیں ایک ضروری چیز جو چاہیے وہ ہے لوگوں کا اعتماد اور اسے استعمال کرنے پر رضامندی۔

نہ حکومت نہ کوئی جنس/پیداوار۔ شخصی کمپنی، سوسائٹی، کسی بھی گارنٹی، یا گارنٹی کے احساس پر کہانی چل پڑتی ہے۔

آپ کو یہ جان کر یقیناً حیرت ہو گی کہ دنیا کا پہلا الیکٹرانک ٹرانسفر 1871 میں ہوا تھا۔ جی ہاں ویسٹرن یونین 1851ء میں نیویارک اور مسی پپی پرنٹنگ ٹیلی گراف کمپنی کے نام سے وجود میں آئی اور اس نے براعظم امریکہ میں 1861ء میں ٹیلی فون لائنیں بچھائیں۔ سی آکسی واریرز (حملہ آوروں) نے یہ تاریں جگہ جگہ سے کاٹ کر ان کے بریسلیٹ بنا لئے جس سے یہ کام رک سا گیا مگر پھر ہار پہننے والے کچھ لوگ بیمار پڑ گئے۔ تو حملہ آوروں کے طبیب نے انکشاف کیا کہ انہیں بولنے والی تاروں کے بھوت نے نقصان پہنچایا ہے اور ایک دم تاروں کے ساتھ چھیڑ خانی کے واقعات بند ہو گئے۔ دنیا کا پہلا منی ٹرانسفر ٹیلی گرام کے ذریعے 1871 میں پیش آیا۔

1950ء میں فرینک میک نمارا نام کا شخص ہوٹل میں کھانے کو گیا مگر بل دیتے وقت کچھ پیسے کم پڑ گئے اس نے فون پر اپنی بیگم کو بلایا باقی پیسوں کے ساتھ اس شرمندگی کے بعد اس نے تہیہ کر لیا کہ آج کے بعد یہ نہیں ہو گا اور یوں ڈائنرز کلب کارڈ کے نام پر دنیا کا پہلا کریڈٹ کارڈ وجود میں آیا۔

امریکہ اور برطانیہ کی آج پچاس فیصد ٹرانزیکشن پلاسٹک کارڈز کے ذریعے ہی ہوتی ہیں۔

شیفرڈ بیر بن نام کے شخص نے 1967ء میں دنیا کی پہلی اے ٹی ایم مشین بنائی اور یہ آئیڈیا بارکلے بینک کو پیش کیا۔ این فیلڈ، شمالی لندن میں یہ انسٹال ہوئی۔

(تصویر 8:1000ڈالر کا گولڈ نوٹ)

شروع کی اے ٹی ایم میں پلاسٹک کارڈز کی بجائے کاربن 14 سے پرنٹ کیے گئے چیکس ڈلتے تھے اور یہ ایک وقت میں صرف 10 پائونڈز تک دے سکتی تھی۔

1983ء میں بینک آف اسکاٹ لینڈ نے ناٹنگھم بلڈنگ سوسائٹی کے صارفین کو دنیا کی پہلی انٹرنیٹ بینکنگ سروس دی جس میں اپنے بلز جمع کروا سکتے تھے اور اس کے لئے انہیں اپنے ٹی وی اور ٹیلی فون کی مدد درکار ہوتی تھی۔

1990ء میں ویب اور صحیح معنوں میں انٹرنیٹ بینکنگ کا آغاز ہوا مگر بینک آف امریکہ کو پہلے دو ملین کسٹمرز کے لئے پورے دس سال کا انتظار کرنا پڑا جو اسے استعمال کریں۔

1997ء میں موبل آئل کارپوریشن نے (Speed Pass) کے نام سے پٹرول بھروانے کے لئے دنیا کا پہلا کونٹیکٹ لیس کارڈ متعارف کروایا۔

2005ء سے کریڈٹ کارڈز میں چپ اور پن نمبرز کا آغاز ہوا۔

2008ء میں ساتوشی ناکاموتو نے بٹ کوائن کا پیپر لکھا اور بٹ کوائن کی پہلی ٹرانزیکشن 2009ء میں ظہور پذیر ہوئی۔

2010ء میں 10,000 بٹ کوئنز دے کر پاپا جونز سے دو پیزا خریدے گئے۔اور اس طرح دنیا Programmable Money سے متعارف ہوئی۔ حیرت کی بات یہ ہے کہ 1994 میں پہلی آن لائن ٹرانزیکشن میں بھی پزاہٹ (Pizza Hut) سے پزا خریدا گیا تھا۔

2014ء میں ایپل پے کا آغاز ہوا کہ آپ بغیر کسی کارڈ یا والٹ کے اپنے فون سے چھوئے بغیر (Contact Less) پیمنٹ کر سکیں۔آج امریکہ کے 40 فیصد سے زائد بزنس ایپل پے (Apple Pay) کو لین دین کے لئے استعمال کرتے ہیں اور جلد ہی دنیا سے کریڈٹ کارڈز ختم ہو جائیں گے۔

2015ء بٹ کوئن کی دیکھا دیکھی بلاک چین ٹیکنالوجی کو استعمال کرتے ہوئے سینکڑوں کرپٹو کرنسی مارکیٹ میں آچکی ہیں۔ کینیڈا، جاپان، آسٹریلیا، ایسٹونیا اور سنگاپور کے علاوہ دس سے زائد ممالک اسے تسلیم کر چکے ہیں۔ امریکہ میں کرپٹو کرنسی مال (Asset) میں شمار ہوتی ہے جس پر ٹیکس ہے۔ کینیڈا میں اس کی حیثیت بارٹر کی ہے۔ جاپان میں کرنسی اور لیگل ٹینڈر اور آسٹریلیا میں کرنسی کی حیثیت ہے۔ کاغذی نوٹ کی طرح جلد ہی دنیا کے باقی ممالک اسے کسی نہ کسی حیثیت میں تسلیم کرتے چلے جائیں گے۔

(تصویر 9: گولڈ ڈالر)

کچھ تاریخی حقائق:

تاریخ اس بات کی گواہ ہے کہ عموماً پیسہ جنگیں لڑنے کے لئے وجود میں آیا۔ دس ڈالر کا نوٹ 1861ء میں اس بنیادی وجہ سے بنا تھا کہ سول وار کے خرچے برداشت کئے جا سکیں۔ اس دور میں سارا کاپر جنگوں میں لگ رہا تھا تو دنیا نے پہلی بار روپے سے کم حیثیت کے نوٹ دیکھے جنہیں ہم Frictional notes کہتے ہیں۔ 0.25، 0.15، 0.10، 0.05، 0.03 اور 0.5 کے نوٹ وجود میں آئے۔ ایک دور میں امریکی پینی (Penny) اسٹیل کی بنائی گئی کہ کاپر تو جنگوں کے لئے چاہیے تھا۔ 1955ء میں امریکہ نے کرنسی نوٹوں پر حامل ہذا کو مطالبے پر ادا کیا جائے گا کہ بدلے ہمیں خدا پر بھروسہ ہے۔ In God We Trust لکھوایا۔ ہم امریکی ڈالر کے لئے Buck کا لفظ استعمال کرتے ہیں۔ Buck اصل میں مذکّر ہرن کی کھال کو کہتے ہیں جو کہ ایک دور میں امریکی زراعتی علاقوں میں بالکل پیسے کی طرح ہی استعمال ہوتی تھی۔

19 ویں صدی میں ایک تہائی نوٹ جعلی تھے، آج ٹیکنالوجی کی بدولت صرف 0.01 فیصد جعلی ہیں۔ آپ کو حیرت ہو گی کہ سیکرٹ سروس کا قیام 1865ء میں اسی نوٹوں کی جعل سازی کو روکنے کے لئے عمل میں آیا کہ کارخانے بینکوں کے لئے نوٹ چھاپنے کی اصل مشینیں اور ڈائیز بلیک مارکیٹ میں کرایے پر دے دیتے تھے۔

دنیا روز کا ڈھائی ملین اور سال کا نو سو ملین پاونڈ سلور نکالتی ہے۔

نوٹ کی عمر:

ایک عام کاغذ کو آپ چار سو بار تہہ کر سکتے ہیں اس کے بعد وہ پھٹنا شروع ہو جائے گا۔ کرنسی نوٹ آپ آٹھ ہزار بار تہہ کر سکتے ہیں یہ 75 فیصد کاٹن اور 25 فیصد لینن کا بنا ہوتا ہے۔

ایک سکے کی اوسط عمر25 سال ہے جب کہ نوٹ کی اس کی قدر کے حساب سے مختلف ہے ایک ڈالر کا نوٹ عموماً5.8 سال چلتا ہے۔ پانچ ڈالر کا 5.5، دس ڈالر کا 4.5، 20 ڈالر کا 7.9، پچاس ڈالر کا8.5 اور100 ڈالر کی زندگی پندرہ سال ہوتی ہے۔ ایک سروے کے مطابق امریکہ کے نوے فیصد نوٹوں پر جو گردش میں ہیں کوکین کے ذرے پائے جاتے ہیں کیونکہ نقد زیادہ تر جرائم پیشہ افراد کے زیر استعمال رہتا ہے۔

(US State Beurue of Engraving and Printing)روز کے38 ملین نوٹ چھاپتی ہے جس کی مالیت 541 ملین ڈالر ہے۔

امریکی عوام سال کے 62 ملین ڈالرز کے سکے پھینک دیتے ہیں۔ اور امریکی حکومت سالانہ چالیس ملین کے صرف Collectible سکے جاری کرتی ہے جو عام استعمال میں عموماً نہیں آتے۔

شمالی کوریا دنیا میں سب سے زیادہ جعلی ڈالر بناتا ہے اس لیے ڈالر کا ڈیزائن بار بار بدلتا رہتا ہے اور اسی لئے آپ کو منی چینجر پرانے ڈالر کا ریٹ نئے ڈالر سے کم دیتا ہے۔ ایک ڈالر کا نوٹ کوئی نقلی نہیں چھاپتا کیونکہ اس کی قدر کم ہے لہذا یہ 1929ء سے ایسا ہی چلا آرہا ہے۔

امریکی قانون کے مطابق نوٹ پر صرف اس شخص کی تصویر ہو سکتی ہے جو مر چکا ہو تو اگر آپ کو ڈالر پر اوبامہ یا ٹرمپ نظر آئیں تو وہ سو فیصد جعلی ہے۔

1775ء میں بننے والا کونٹی نینٹل ڈالر صرف پانچ سال میں اپنی قدر کھو چکا تھا اور یہی محاورہ نکلا Not worth a Continental جسے ہم اپنی زبان میں کہتے ہیں "دو کوڑی کا بھی نہیں ہے"

نقدی کے خلاف جنگ(War on Cash):

آپ نے شاید دھیان نہ دیا ہو مگر پچھلے دس ایک سالوں سے دنیا نے نقدی کیش کے خلاف اعلان جنگ کیا ہوا ہے۔ کیونکہ کیش میں کی گئی ٹرانزیکشن کو ریکارڈ کرنا یا ٹریس کرنا تقریباً ناممکن ہے ملکی سطح پر جرائم پیشہ افراد کا یہ محبوب مشغلہ ہے اس لیے ملک بڑے کرنسی نوٹ نہیں چھاپتے۔ایک ملین ڈالز کا وزن صرف دس کلو گرام یا بائیس پائونڈز ہوتا ہے۔ جرائم پیشہ افراد سالانہ دو ٹریلین ڈالرز ادھر سے ادھر کرتے ہیں۔آپ کیش لیس ٹرانزیکشن کریں گے تو ہر چیز ریکارڈ ہو گی اور تھرڈ پارٹیز مثلاً بینک وغیرہ ٹرانزیکشن پر فیس بھی لے گی۔

امریکہ میں کچھ پالیسی بنانے والے ماہرین کافی عرصے سے 50 اور 100 ڈالر کے نوٹ کو ختم کرنے کی تجویز دے رہے ہیں۔

2014ء میں سنگاپور نے 10,000 کا نوٹ یکسر ختم کر دیا۔

سویڈن نے دیہی علاقوں سے اے ٹی ایم مشین تدریجاً ہٹانا شروع کر دی ہیں تاکہ لوگ زیادہ کیش استعمال نہ کریں۔

جنوبی کوریا نے 2020 تک ملک کو کیش لیس بنانے کا عہد کیا ہوا ہے۔

فرانس نے ہزار پائونڈ سے زیادہ کی جانے والی ٹرائزیکشن کیش میں کرنے پر پابندی لگا دی ہے۔

وینزویلا نے 100 بولیوار کا نوٹ منسوخ کر دیا ہے۔

یورپ نے اس سال 2018ء سے پانچ سو پائونڈز کے نوٹ کی سرکولیشن بند کر دینی ہے۔

گریس (Greece) نے کسی بھی شہری کو پندرہ ہزار پاونڈ سے زیادہ کیش رکھنے پر پابندی لگا دی ہے اور آسٹریلیا اور ناروے بھی اس مد میں کام کر رہے ہیں۔ابھی حال ہی میں جب انڈیا نے پانچ سو روپے کے نوٹ پر پابندی لگائی تو کل سرکولیشن سے 86 فیصد نوٹ خارج ہو گئے ایک شخص صرف چار ہزار روپے تک تبدیل کروا سکتا تھا کیش میں ۔انڈیا میں پچاس فیصد

لوگوں کا کوئی بینک اکاونٹ نہیں ہے اس اعلان کے بعد خود کشی اور قطاروں میں دم گھٹنے سے 112 لوگوں کا انتقال ہو گیا۔

ان اقدامات کی وجہ سے صرف 2015 میں دنیا نے 426.3 ملین ٹرانزیکشن کیش لیس کیں مگر آج بھی دنیا کی 85 فیصد ٹرانزیکشن کیش نقدی پر ہی ہوتی ہے۔

پیسے کی تعریف:

اس ساری بحث کا مقصد یہ تھا کہ آپ کو انسانی تاریخ میں پیسے کا وجود اس کی اقسام شکلیں اور اہمیت کا اندازہ ہو جائے اور ایک تصور مل جائے کہ اس کی ہماری معاشرے میں کیا نوعیت اور ضرورت ہے اور پیسے کی اس تصور کو بدلنے یا اس میں اختراعات کرنے سے کیا کیا اور کس طرح تبدیلیاں واقع ہو نگی۔

آیئے اب یہ سمجھ لیتے ہیں کہ ہم پیسہ کی کس طرح تعریف کریں گے۔

ماہرین معاشیات کے مطابق کسی بھی چیز کو پیسہ منی زر سمجھنے کے لیے اسے مندرجہ ذیل تین شرائط پورا کرنی ہوں گی۔

1۔آلہ مبادلہ (Medium of Exchange)

2۔قدر زر کا پیمانہ (Unit of Account) اور

3۔اس کے ذریعے مالیت کو محفوظ (Store of Value) کیا جا سکے۔

1۔آلہ مبادلہ (Medium of Exchange)

ان میں سب سے اہم کام جو پیسہ نے کرنا ہوتا ہے وہ ہے میڈیم آف ایکسچینج یعنی آلہ مبادلہ۔اس کے ذریعے چیزوں اور خدمات کی خرید و فروخت کی جا سکے۔ جیسے کہ ہم نے باب کے شروع

میں دیکھا کہ بارٹر سسٹم میں Double Coincidence of Wants کا مسئلہ تھا یعنی آپ نے زعفران کے بدلے مرغی لینی ہے مگر جس شخص کے پاس مرغی ہے اسے زعفران نہیں چاہیے، اسے کوئلے چاہئیں تو آپ کو ایسا شخص ڈھونڈنا ہوگا جس کے پاس کوئلے ہوں اور وہ زعفران چاہتا ہو۔ کاغذی نوٹ سے یہ مسئلہ حل ہو جاتا ہے۔

آلہ مبادلہ کی شرط پوری کرنے پر پیسہ ایک درمیانی راستہ بن جاتا ہے جس کے ذریعے ہر شخص اپنی مرضی سے لین دین کر سکتا ہے یہ ایک متفقہ راستہ دیتا ہے تمام صارفین کے لئے۔

میڈیم آف ایکسچینج کی یہی وہ شرط یا مقصد ہے جو پیسے کو مال Asset یعنی گھر، بونڈز، کار وغیرہ سے ممتاز بناتا ہے۔

بارٹر کی بجائے پیسے کے استعمال سے معاشی ترقی ہوتی ہے، لین دین کی قیمت کم ہو جاتی ہے۔ لوگوں کے کام کی صلاحیت اور نتائج میں اضافہ ہوتا ہے اور پیشوں کی تقسیم (Division of Labor) ممکن ہو پاتی ہے۔

مثال کے طور پر میں ایک پروفیسر ہوں اور مجھے بٹ کوائن پر لیکچر دینا ہے، اب بارٹر سسٹم میں مجھے کوئی ایسا کسان ڈھونڈنا ہوگا جو مجھ سے لیکچر سن کر گندم کھانے کو دے سکے۔ اب آپ خود سوچیں کہ اس میں کتنا وقت خرچ ہوگا اور ملک میں کوئی کتنے کسان ایسے ملیں گے جو بٹ کوائن پر لیکچر سننا پسند کریں گے یا تو میں بھوکا مروں گا یا بٹ کوائن چھوڑ کر خود بھی زراعت شروع کر دوں گا۔ کاغذی نوٹ یا پیسہ نے یہ مسئلہ حل کر دیا، ہر شخص اسی پیشے میں دھیان لگا سکتا ہے جو وہ بہتر کرتا ہے اور ہم سب پیسہ کو میڈیم آف ایکسچینج کے طور پر استعمال کر کے جو چاہے خرید و فروخت کر سکتے ہیں۔

کسی بھی پیسہ کے میڈیم آف ایکسچینج ہونے کے لیے یہ ضروری ہے کہ اس میں مندرجہ ذیل سات خصوصیات پائی جائیں۔

1۔ محدود سپلائی، قلت(Scartcity):

پیسے کی قدر کے استحکام کے لئے یہ ضروری ہے کہ اس کی سپلائی محدود ہو ورنہ وہ اپنی قدر کھودے گا۔ جیسا کہ ہم نے رومن ایمپائرز سکوں میں، چائنا کے نویں صدی عیسوی کے نوٹوں میں اور حالیہ وینزویلا کے بولیوار میں دیکھا۔

آپ کی حکومت آنکھ بند کر کے صبح وشام نوٹ چھاپتی رہے تو اس کی قدر گرتی چلی جائے گی۔ بٹ کوائن کی سپلائی بھی محدود ہے اور یہ کل صرف اکیس ملین کی تعداد میں جاری ہونگے۔

2۔ پائیدار(Durability):

پیسہ کے لئے ضروری ہے کہ اس پر ماحول وموسم کا باآسانی اثر نہ ہوتا ہو۔ جتنا زیادہ Durable ہوگا اتنا ہی اچھا ہے۔ جیسا کہ ہم نے دیکھا کہ سکے کی عمر 25 سال اور 100 ڈالر کی عمر پندرہ سال تک ہوتی ہے اور آپ کرنسی نوٹ کو آٹھ ہزار بار تک فولڈ کر سکتے ہیں۔ سونا اس خوبی پر پورا اترتا ہے نہ اس کی چمک ماند پڑتی ہے اور نہ اس پر گرمی، سردی، یا بارش کا ہی کچھ اثر پڑتا ہے۔ جانوروں کی کھالیں بھی دباغت کے بعد خوب چلتی ہیں اور اس لیے ایک لمبے عرصے تک میڈیم آف ایکسچینج بنی رہیں۔ شروع شروع میں جب نمک نیا نیا دریافت ہوا تھا اس وقت نمک کی ویلیو سونے کے برابر تھی اور لوگ دس گرام سونا دے کر دس گرام نمک لے جاتے تھے۔ بعد ازاں رومن ایمپائر نے اپنی فوج کو بھی نمک میں تنخواہ دینی شروع کی۔ آرمی سولجرز کے لئے Not worth your Salt کا محاورہ آج تک رائج ہے۔ بٹ کوائن بھی Durable ہے اور ماحول کا اثر اس پر نہیں پڑتا۔

3۔ قابل تقسیم(Divisibility):

پیسہ قابل تقسیم ہونا چاہیے تاکہ چھوٹی قیمتوں کا لین دین ممکن ہو۔ سو روپے کی چیز ہو۔ پچاس کی یا 25 کی آپ آرام سے خرید سکیں اور پچاس کے دو نوٹ سو کے ایک نوٹ کے برابر ہوں

اور کسی کو اس تقسیم پر اعتراض نہ ہو۔ایک بٹ کوائن سو ملین دس کروڑ ٹکڑوں میں بٹ سکتا ہے جسے ستوشی(Satoshi)کہتے ہیں جو اس کے موجد کا نام ہے۔

4۔ نقل پذیری(Transportability /Portability):

میڈیم آف ایکسچینج کے لیے یہ ضروری ہے کہ اسے باآسانی ایک جگہ سے دوسری جگہ منتقل کیا جاسکے۔ تھوڑی قیمت کے لئے تو سونا بھی آسان ہے مگر جیسے جیسے قیمت بڑھتی جاتی ہے۔ سونے کا انتقال مشکل ہوتا چلا جاتا ہے۔ کاغذی نوٹ منتقل کرنا آسان ہے نسبتا مگر دنیا بھر نے دس ہزار ڈالر سے زائد رقم کو ایک ملک سے دوسرے ملک میں منتقل کرنے پر کے وائی سی یا (Know Your Customer)کے قوانین اور ٹیکس لگا رکھے ہیں، بینکوں کو بھاری فیس الگ ،بٹ کوائن دنیا کے ایک کونے سے دوسرے کونے تک چند منٹوں میں صرف کلک کے ذریعے ٹرانسفر ہو جاتا ہے اور فیس بھی انتہائی کم۔

5۔ ممکن الثبوت(Verifiability):

آپ باآسانی نقلی اور اصلی میں تمیز کر سکیں۔ نقلی ہیرا اصل سے نقلی سونا اصلی ہے۔ سونے میں یہ کام مخصوص آلہ جات کی مدد سے ہوتا ہے اور ایک عام آدمی باآسانی دھوکا کھا سکتا ہے کاغذی کرنسی میں یہ کام ہوتا ہے مگر جیسے جیسے پرنٹنگ کی صنعت ترقی کر رہی ہے ویسے ویسے یہ کام مشکل ہوتا چلا جارہا ہے بٹ کوائن کی نقل بنانا ریاضی کی رو سے ناممکن ہے اور اس کو Verify کرنا بھی بہت آسان ہے۔

6۔ قابل تبادلہ(Fungibility):

ہر ایک یونٹ دوسرے جیسا ہو اور کسی کو تبادلے پر اعتراض نہ ہو۔ ہزار کے دو نوٹ ہر جگہ یکساں حیثیت رکھتے ہیں اور ان کو کھلا کروانے کی صورت میں نوٹ کی مالیت پر اثر نہ

پڑے۔ مثلاً آپ ایک نوٹ دے کر دوسرا نوٹ باآسانی لے لیں گے۔ایک سونے کی ڈلی دے کر اسی وزن کے ایک اور ڈلی لے لیں گے بٹ کوائن بھی بالکل اسی طرح قابل تبادلہ ہے۔

7۔ قابل قبول(Acceptability):

میڈیم آف ایکسچینج ضروری ہے کہ تمام لوگوں اداروں اور کاروبار کی اکثریت میں قابل قبول ہو۔تاکہ کوئی بھی شخص باآسانی اس سے خرید وفروخت کر سکے۔بٹ کوائن رفتہ رفتہ یہاں اپنی جگہ بنا رہا ہے۔

2۔قدر زر کا پیمانہ(Unit of Account):

یونٹ آف اکاونٹ سے مراد وہ معیار ہے جس پر معاشیات اشیاء اور خدمات کو جانچا جا سکے اور انکی قیمتوں کا تعین ممکن ہو۔ مثلا ہم وزن کو کلو گرام یا پائونڈز میں ناپتے ہیں۔ فاصلوں کو کلو میٹر یا میلوں میں بجلی کو وولٹ اور پٹرول یا دودھ کو لیٹر یا گیلن میں بالکل اسی طرح اشیائے خورد نوش اور معاشی کارگزاری کو ناپنے کا طریقہ یونٹ آفا کائونٹ ہے ہم اپنی پچھلی مثال واپس دیکھتے ہیں۔ فرض کریں کہ دنیا میں صرف تین چیزیں ہیں میرے بٹ کوائن کے لیکچرز، گندم اور ٹماٹر۔ تو ہمیں تمام ٹرانزیکشنز کے لیے صرف تین قیمتیں درکار ہوں گی۔ایک بٹ کوائن کے لیکچر کے بدلے میں کتنے ٹماٹر یا گندم آئے گی اور گندم اور ٹماٹروں کا تبادلہ کس بنیاد پر ہو گا مثلا ایک کلو گرام گندم کے بدلے ایک کلو ٹماٹر۔ مگر اگر 10 اشیاء ہو گئی تو یہ لسٹ 45 قیمتوں پر جائے گی۔

$$\frac{N(N-1)}{2}$$

$$\frac{10(10-1)}{2} = \frac{90}{2} = 45$$

اگر100 اشیاہوئیں تو4،950اور ہزار اشیاء کیلئے499،500 اگر آپ بارٹر سسٹم میں غلطی سے سوپر مارکیٹ چلے گئے تو آپ کی باقی زندگی صرف قیمتیں پڑھنے میں گزر جائے گی۔ پیسہ اس مسئلے کو حل کرتا ہے اور ہر شئے کی قیمت رائج الوقت کرنسی میں لکھ دی جاتی ہے۔ جن ملکوں میں افراط زر کی وجہ سے کرنسی کی قدر و قیمت انحطاط کا شکار ہوتی ہے وہاں قیمتیں ڈالر میں لکھی جاتی ہے۔(Unit of Account)جبکہ لین دین(Medium of Exchange) مقامی کرنسی میں ہوتا ہے۔ جیسا کہ دنیا بھر کے ایئرپورٹس پر قیمتیں عموماً ڈالر میں لکھی جاتی ہیں اور جب دنیا کے امیر ترین لوگوں کی فہرست شائع ہوتی ہے تو ان کی دولت کا تخمینہ بھی ڈالرز میں ہی لگایا جاتا ہے۔

میڈیم آف ایکسچینج کے لیے ضروری نہیں کہ وہ یونٹ آف اکائونٹ بھی ہو مگر عموماً ایسا ہی ہوتا ہے۔

بٹ کوائن اپنی Volatility کی وجہ سے ایک اچھا یونٹ آف اکائونٹ نہیں ہے۔

9۔مالیت محفوظ کرنے کا ذریعہ (Store of Value):

پیسہ کا تیسرا ضروری مقصد یا کام اسے اسٹور آف ویلیو کا فنکشن ادا کرنا ہوتا ہے۔آپ کو آج پیسے / تنخواہ ملے تو آپ نے آج ہی نہیں خرچ کر دینی، آپ کو اس بات کا اطمینان ہوتا ہے کہ آپ اگلے ہفتے یا مہینے جا کر اس سے اندازً کتنا اناج یا اشیائے صرف خرید سکتے ہیں۔ یہ فنکشن پیسہ اور مال Asset جیسے کہ گھر، بانڈز وغیرہ میں یکساں ہے۔

زر کی کوئی بھی قسم اسٹور آف ویلیو کے لئے آئیڈیل نہیں۔آپ پیسے پلنگ کے نیچے چھپا کر رکھ دیں،وہ افراط زرInflation کی وجہ سے کم از کم ہر سال تین فیصد اپنی قوت خرید کھوتے چلے جائیں گے اور کم وبیش تیس سالوں میں اپنی آدھی سے زائد قدر کھو چکے ہونگے۔

اس کے بدلے سونا یا گھر کی ویلیو شاید بڑھ ہی جائے۔زمین، جائیداد گولڈ ہر دن کے ساتھ اپنی قدر میں بڑھتے ہیں مگر جو Liquidity فوراً خرچ کرنے کی صلاحیت آپ کو نقد دیتا ہے وہ باقی مال Asset میں ممکن نہیں۔

دنیا کا کوئی بھی زر، پیسہ، منی ان تینوں فنکشنز میڈیم آف ایکسچینج، اسٹور آف ویلیو اور یونٹ آف اکائونٹ میں سو فیصدی پوری نہیں اترتا اور ہر ایک قسم کے اپنے فوائد و کمزوریاں ہیں۔

یہاں ایک بات اور سمجھ لیں کہ کرنسی ،مال Asset اور آمدن (Income) میں فرق ہے۔کرنسی سے مراد وہ نوٹ یا سکے ہیں جو آپ کے پاس سر دست دستیاب ہیں کوئی اگر آپ کے سر پر بندوق رکھ کے کہے کہ سارا مال دو ورنہ جان جائے گی تو آپ اس کے سامنے اپنی جیبیں خالی کردیں گے نہ کہ اس سے زر کی اقسام وحالات پر بحث کریں گے۔ مال دولت (Asset/Wealth) سے مراد آپ کا بینک میں رکھا پیسہ گھر، گاڑی، بانڈز اسٹاک، شیئرز وغیرہ ہیں۔امریکہ کرپٹو کرنسی کو Asset کا ہی درجہ دیتا ہے۔

آمدن سے مراد پیسے کا بہاو ہے کسی متعین وقت کے ساتھ مثلاً اگر آپ یہ کہیں کہ میری آمدنی دس لاکھ ہے تو میں پوچھوں گا ماہانہ، سالانہ یا دن کی ۔اور ایسا کہنے سے یہ مطلب نہیں نکالا جاسکتا کہ آپ کے پاس اس وقت دس لاکھ موجود بھی ہونگے۔

پیسے کی پھر مزید بہت سے قسمیں اور اصلاحات ہیں جیسے کہ بینکوں کی اصطلاح میں ایم ون، ایم ٹو یا کموڈٹی بیسڈ منی، فیاٹ اور ڈیجٹل کیش وغیرہ مگر ہم ان تفصیلات میں گئے تو پوری کتاب پیسے کی نذر ہو جائے گی۔

پیسے کی جو تعریف ہم نے اب تک کی ہے اس سے علمائے کرام بھی اتفاق کرتے ہیں مثلا: مولانا مفتی تقی عثمانی صاحب اپنی تصنیف (اسلام اور جدید معیشت و تجارت، شائع کردہ ادارہ المعارف کراچی، طبع اول (1419ھ) میں لکھتے ہیں کہ :۔

"جو چیز عرفاً آلہ مبادلہ کے طور پر استعمال ہوتی ہے، اور وہ قدر زر کا پیمانہ ہو اور اس کے ذریعے مالیت کو محفوظ کیا جاتا ہے۔ اسے ''زر'' کہتے ہیں۔"

مولانا سود سے متعلق سپریم کورٹ کے تاریخی فیصلے میں اس پر تفصیلی روشنی ڈالتے ہوئے فرماتے ہیں کہ زر براہ راست انسانی ضروریات کو پورا نہیں کر سکتا بلکہ اسے اشیاء خورد و نوش اور خدمات کے لئے استعمال کیا جاتا ہے۔ زر کی کیفیت پیمانہ قدر، آلہ مبادلہ اور مساوی یونٹ کے کچھ نہیں، شے انسانی ضرورت کو پورا کرتی ہے۔

مجموعہ الفتادی میں شیخ ابن تیمیہ لکھتے ہیں کہ :۔

"دراہم اور دینار مقصود بالذات نہیں، بلکہ باہمی معاملات کا ایک ذریعہ ہیں، اسی وجہ سے اثمان شمار ہو جائے، بر خلاف دیگر اشیا کے کہ یہ خود مقصود بالذات ہیں"

علامہ ابن القیم لکھتے ہیں کہ :۔

زر مقصود بالذات نہیں۔ بلکہ سامان کے حصول کا ذریعہ ہے اگر زر سامان میں شمار ہو جاتے، تو لوگوں کے معاملات فاسد ہو جائیں گے۔

ڈارون کے نظریہ ارتقاء کی طرح پیسہ۔ زر کا بھی معاشرے کے ساتھ ارتقاء ہوتا ہے۔ پچھلے سو سالوں میں بلا مبالغہ ہزاروں کرنسیز بنیں مگر اس وقت صرف 193 باقی رہ پائیں۔ نئے دور، نئے چیلنجز اور ان سے نمٹنے کے لئے زر کے نئے نئے بھیس، یہ سلسلہ یوں ہی چلتا رہے گا۔Survival of Fittest کی طرح جو پیسہ معاشرے کے ساتھ چل پایا وہ رہ جائے گا باقی ختم۔

ایک بات معلوم ہے کہ اگر آج ڈارون زندہ ہوتا تو وہ اپنی کتاب Origin of Species کا معاوضہ برٹش اسٹرلنگ کی بجائے بٹ کوائن میں ہی لینا پسند کرتا۔

آیئے بلاک چین اور بٹ کوائن کی طرف سفر جاری رکھتے ہیں۔

بلاک چین کا تعارف

اِنسان پیدائش سے لے کر موت تک اور شاید موت کے بعد بھی ایک ریکارڈ کے طور پر ایک رجسٹر (کھاتے) سے دوسرے رجسٹر میں سفر کرتا رہتا ہے۔اُس کی ذات اور اُس سے جڑی تمام ضروریات اور مسائل کسی نہ کسی کھاتے کے مرہونِ منّت ہوتے ہیں۔اگر آپ اِنسان کو لاتعداد و کھاتوں کی زنجیر کی ایک اکائی مان لیں تو کچھ غلط نہ ہو گا۔

لاتعداد ولا محدود کھاتے جو ایک زنجیر میں پرو کر ایک ساتھ جوڑ دیئے گئے ہوں۔ان میں درج ایک حقیقت، ایک اکائی اِنسان کہلاتی ہے اور اسے اپنے وجود کا ثبوت دینے کے لئے بھی اِن کھاتوں کے اندراج کی ضرورت ہوتی ہے۔

آپ یقین جانیئے میں کوئی مذہبی یا فلسفہ کی بحث نہیں کر رہا، یہ وہ طریقہ کار ہے جس کے مطابق ہم جیتے ہیں اور جو ہو بہو بلاک چین کا عملی نمونہ ہے۔

ہم پیدا ہوتے ہیں تو پیدائش کا برتھ سرٹیفیکیٹ بنتا ہے، ہسپتال سے، یا ضلع ناظم کونسلر کے آفس سے "ب" فارم اور پھر نادرا سے حتمی ثبوت کے طور پر پکا برتھ سرٹیفیکیٹ یا فیملی سرٹیفیکیٹ۔یہ سرٹیفیکیٹ اِس بات کی سند ہے کہ آپ ہیں۔اِس کے بغیر قانونی طور پر آپ کا وجود ثابت نہیں۔

آپ نے حفاظتی ٹیکے لگوائے تو ایک اور رجسٹر میں اِندراج ہو گیا۔گھر لیا، شناختی کارڈ یا پاسپورٹ بنوایا، ڈرائیونگ لائسنس، بینک اکاؤنٹ، اسلحہ لائسنس، شادی و نکاح، بچوں کی

پیدائش، اسکول میں داخلہ، یونیورسٹی ڈگری حتٰی کہ موت تک آپ کو کوئی نہ کوئی سرٹیفیکیٹ ملتا ہی رہتا ہے جو کسی نہ کسی کھاتے میں اندراج کی گواہی ہوتا ہے۔ میں اس نظام کو غیر مرئی بلاک چین(Invisible block chain) سے تشبیہ دیتا ہوں۔ اور نامہ اعمال وہ بھی تو ایک رجسٹر ہے۔ جس میں سب لکھا جارہا ہے۔

قیمتی اشیاء، قدرتی ذخائر، ملکی وسائل اور آبادی کا شمار ہمیشہ سے ہی اس بات کا متقاضی رہا ھے کہ اسکا درست اندراج ممکن بنایا جائے۔ عالمی جنگ عظیم دوئم کے بعد میں سن 1944ء میں بریٹن وڈز کانفرنس ہوئی جس کے نتیجے میں انٹرنیشنل مونیٹری فنڈ (IMF)، ورلڈ بینک اور بعدازاں اقوام متحدہ(United-Namtions) اور ورلڈ ٹریڈ آرگنائزیشن (WTO) جیسے اِداروں کا قیام عمل میں آیا کہ دنیا کے تمام تر وسائل کو ایک مرکزی نظام کے تحت کنٹرول کیا جاسکے اور چلایا جاسکے اور چھوٹے بڑے سب ممالک اور اُن میں بسے سب لوگ، کیا مسکین اور کیا طاقتور سب ہی اس مرکزی نظام کے تحت آجائیں اور اپنے تئیں جتنی آزادی اور شخصی حیثیت کا ڈھنڈورا پیٹ لیں۔ بالآخر ان کی ساری توانائیاں اور وسائل اِسی مرکزی نظام سے ہوتے ہوئے ان معدودے چند لوگوں یا اداروں تک پہنچ جائیں جو پالیسی سازی کے نام پر آزاد لوگوں کو غلام اِبن غلام بنانے کا عزم لئے پھرتے ھیں۔

آپ آس پاس میں نظر دوڑایئں اور اگر غور کریں تو آپ کو اپنی زندگی کچھ مرکزی کھاتوں میں جڑی نظر آئے گی۔ بینک، گھر کے کاغذات (پٹواری)، ہسپتال، شناختی کارڈ، شادی دفتر وغیرہ وغیرہ۔

چلیں مان لیا کہ ہم ہمہ وقت کسی نہ کسی مرکزی کھاتے یا نظام میں بندھے ہوئے ہیں تو اس میں آخر ہوا کیا ہے۔ کیوں ہمیں ایک متبادل نظام کی ضرورت ہے؟ ہم کیوں کھوج کریں ایک نئے نظام کی جب سب کچھ ٹھیک ٹھاک چل رہا ہے؟

مرکزی نظام پر اعتماد (یا اندھے اعتماد) میں تین بڑی خرابیاں ہیں۔

1۔ من مانی علیحدگی (Exclusion) :-

یہ نظام یا اِس کے چلانے والے جب چاہیں، جیسے چاہیں، مسابقت کے نام پر یا سینسر شپ (Censorship) کے نام پر یا ملک کے وسیع تر مفاد میں جِسے چاہیں سسٹم سے الگ کر دیں۔ پاکستان کو ٹیرازم واچ لِسٹ میں ڈال کر پیسوں اور اشیاء کی آمدورفت پر پابندیاں لگا دیں۔ کسی اور حیلے بہانے سے ایران، وینزویلا، فلسطین، شمالی کوریا اور ہر وہ ملک، ادارہ یا شخص جو آپ کے سامنے سرنگوں نہیں ہو رہا اُسے خارِج کر دیں یا اُس کی شمولیت ناممکن بنا دیں۔ Pay-Pal پاکستان میں نہیں۔ دنیا میں ایک ارب سے زائد لوگوں کے پاس اپنی شخصی شناخت کے دستاویزات نہیں یعنی امیگریشن ہونے کی حکومتی اِمداد تک، نوکری سے لے کر طبّی اِمداد تک وہ اپنا وجود تک ثابت نہیں کر سکتے۔

2۔ بے اِیمانی :-

لوگ آپ پر اعتماد (Trust) کریں مگر آپ ناانصافی، لوٹ مار اور کرپشن کا بازار گرم رکھیں۔ لوگ اپنی زندگی بھر کی جمع پونجی کسی اِدارے میں رکھوائیں اور وہ اِدارہ اُسے امانت سمجھتے ہوئے جیسے چاہیں برباد کر دے۔ لوگ ملک کو ٹیکس دیں اور حکمران اِسے اعوام کی فلاح و بہبود پر خرچ کرنے کی بجائے اپنی عیاشیوں میں صرف کر دیں۔

3-اِندراج میں گڑبڑ (Loss of Records) :-

مرکزی اِدارے یا بینک کو کوئی شخص ہیک کر کے سارے کھاتے صفر کر دے تو؟ غلطی سے کوئی بینک کا ملازم آپ کے اکاؤنٹ میں غلط اِندراج کر دے یا کوئی اور قدرتی یا اِنسانی حادثے

میں ریکارڈ ضائع ہو جائے؟ جیسا کے عموماً ملک عزیز میں فائلوں کو آگ لگ جاتی ہے تو اِس صورت میں حقدار کے حق کی کیا ضمانت ہو؟

وسائل کی غیر منصفانہ تقسیم، اختیارت کا نا جائز اِستعمال اور جِس کی لاٹھی اُس کی بھینس کے مصداق اپنی من مانی سے نظام چلانا وہ وجوہات ہیں جن کی وجہ سے بتدریج عدم اعتماد کی فضاء قائم ہوئی۔

اگر پچھلی صدی کا بغور جائزہ لیں تو اِنسانوں میں سب سے زیادہ تنزلی اعتماد میں آئی ہے۔ لوگوں کا اعتماد یکسر اُٹھ گیا ہے۔ خواہ وہ اِدارے ہوں، حکومت ہو، عدالت ہو، رشتے ناطے ہوں، مذہب ہو، لیڈر ہو یا کوئی اور ضامن۔ بحثیت مجموعی اِنسانوں کو کسی پر اعتماد نہ رہا۔ یہ وہ مسئلہ ہے جو پچھلے پچاس سالوں سے زیرِ بحث ہے کہ ہم آخر دو یا دو سے زائد فریقین میں اعتماد (Trust) کیسے قائم کریں بغیر کسی مرکزی کردار کے؟

کیا ہم ایسا رجسٹر (کھاتا) بنا سکتے ھیں جِس کو لکھ/پڑھ سکیں تاکہ تمام اِندراجات شفافیت سے وجود میں آسکیں؟ کیا ہم پیسے کھاتے کو کسی حکومت، ادارے یا شخص کی دسترس سے باہر نکالنے کے قابل ہو سکیں گے؟ کوئی بھی ادارہ یا فرد کیونکر ایسے رجسٹر یا کھاتے کو آپ ڈیٹ کرنے کی ذُمہ داری لے گا؟ کیسے ممکن ہے کہ ایسے اوپن کھاتے میں بُرے لوگوں کے فراڈ اور بے ایمانی کو روکا جا سکے اور پکڑا جا سکے؟

کیا اِس بات کی اِجازت ہو گی کہ اِس کھاتے میں تبدیلی کر سکیں؟ اور اِس جیسے درجنوں سوالات کے جوابات ڈھونڈنے میں ریاضی، کمپیوٹر سائنس، معاشیات اور سائیکلوجی کے ریسرچرز نے کئی دہائیاں لگا دیں۔ بارش کے قطروں کی طرح، ہلکے ہلکے ٹکڑوں میں اِس نئے نظام کے مختلف حِصّے بنتے رہے یہاں تک کہ 2008ء میں فرضی نام کے شخص شوشی ناکاماٹو

نے اِس مسئلے کا قابل عمل حل دنیا کو پیش کر دیا جسے ہم بلاک چین Block Chain کہتے ہیں۔

بلاک چین کیا ہے اور یہ کیسے کام کرتا ہے اِسے سمجھنا تھوڑا مشکل ہے کیونکہ اِس کے لئے آپکو اِس میں شامل تمام جزئیات کو سمجھنا ہو گا۔

پہلے ہم اِس نظام کی تعریف کر لیتے ہیں، پھر مثالوں سے بتدریج سمجھنے کی کوشش کرتے ہیں۔

"بلاک چین ایک کھلا (Open)، منقسم (Distributed)، رجسٹر (کھاتا) ہے۔ جِسے ہر کوئی دیکھ سکتا ہے اور جس میں ہر کوئی اِندراج کر سکتا ہے (مخصوص شرائط کے ساتھ) اور جِسے ریاضی کے پیچیدہ عمل کے ذریعے محفوظ بنایا جاتا ہے۔

یہ ایک بنیادی تصّور ہے، میں آپکو اس کی ایک جامع تعریف اگلے باب میں مثالوں کے بعد دیتا ہوں۔

جیسا کے ہم نے دیکھا کے ریکارڈ رکھنے کے لئے انسان صدّیوں سے کھاتے استعمال کرتا آیا ہے کبھی یہ مٹی کی تختیوں کی شکل میں تھے (باب نمبر 1) تو کبھی کاغذی دفتر کی شکل میں، آج کل یہ بائٹس کے مجموعے کی شکل میں کمپیوٹرز میں محفوظ ہوتے ہیں۔

بلاک چین (منقسم کھاتا) ایک ایسا ڈسٹری بیوٹر لیجر ہے جو ہونے والی ٹرانزیکشنز کا وقت کے حساب سے (Chronologically) مکمل حساب رکھتا ہے۔ نیٹ ورک میں شامل ہر فرد کے پاس اِس کی مکمل کاپی ہوتی ہے۔ جب کوئی تبدیلی آتی ہے یا کوئی ٹرانزیکشن ہوتی ہے تو تمام لوگ اپنے اپنے کھاتوں کو اَپ ڈیٹ کر لیتے ہیں۔ اگر کوئی شخص کسی جعلی ٹرانزیکشن کو ریکارڈ کروانے کی بات کرے گا تو باقی لوگ اُسے مسترد کر دیں گے کہ اُن کے پاس کاپی میں اس ٹرانزیکشن کا وجود نہیں ہو گا۔

آپ نے نکاح کے وقت بہت سے مہمان دیکھے ہوں گے، دراصل یہ سب ایک شعوری بلاک چین ہے جو اِس شادی کے گواہ ہیں۔ اگر کل کوئی شخص شادی کا دعویٰ کرے گا تو سب اُس کی مخالفت کریں گے کہ اِس خاتون کی تو پہلے ہی شادی ہو چکی ہے۔

آپ قرآنِ پاک کے حفظ کو دیکھ لیں ہر حافظ قرآن ایک نوڈ (Node) ہے۔ سب کے پاس ایک ہی پبلک لیجر (Public Ledger) قرآنِ پاک کی کاپی موجود ہے۔ جو سب نے اپنے اپنے دماغوں میں محفوظ کی ہوئی ہے اب اگر کل کوئی ناعاقبت اندیش شخص نعوذ باللہ کوئی نئی آیت گھڑ لاتا ہے تو حفاظ کا بلاک چین سسٹم اُسے مسترد کر کے اسے نظام سے باہر پھینک دے گا۔ بالکل ایسے ہی بلاک چین کام کرتا ہے۔

آیئے ایک اور مثال سمجھتے ہیں۔

عبداللہ نے اپنے دوست جمشید کو فون کیا کہ مجھے پیسوں کی ضرورت ہے کچھ بھیج دو۔ جمشید نے فوراً اپنا آن لائن اکاؤنٹ کھولا اور دس ہزار روپے عبداللہ کے اکاؤنٹ میں بھیج دیئے۔ عبداللہ کو چند منٹوں میں اپنے اکاؤنٹ میں مل گئی۔

اب اس معمولی سی سادہ ٹرانزیکشن کے پیچھے کیا ہوا؟

کوئی نقدی یا پیسے اِدھر سے اُدھر نہیں ہوئے۔

جمشید نے اپنے آن لائن اکاؤنٹ میں جا کر دس ہزار روپے بھیجنے کی (Request) درخواست کی تو کمپیوٹر سسٹم نے اس کے کھاتے میں رقم کی موجودگی کو چیک کیا اگر اس کے اکاؤنٹ میں دس ہزار سے کم رقم ہوتی تو یہ ٹرانزیکشن نہ ہو پاتی اس کے اکاؤنٹ میں رقم زیادہ تھی لہٰذا اس کے کھاتے میں سے دس ہزار کم ہوئی عبداللہ کے کھاتے میں بڑھ گئے۔ اس پورے عمل میں رقم کا وجود "کھاتے کے اندراج" سے زیادہ نہیں۔ مسئلہ صرف یہ ہے کہ دو

لوگوں کی رقم کی منتقلی کے لئے کسی تیسرے ادارے پر اعتماد کرنا پڑا اور عموماً یہ تیسرا ادارہ ان سروسز کے بدلے رقم لیتا ہے۔

شہروں اور ملکوں کے درمیان یہ عام سی ٹرانزیکشن 10 فی صد تک وصول کر لیتی ہے اور 3 سے 7 دنوں تک کا وقفہ آجاتا ہے۔ یعنی جمشید کے اکاؤنٹ سے رقم تو فوراً منتقل ہو جائے گی مگر عبداللہ تک پہنچنے میں کئی دن لگ جائیں گے۔

کسی تیسرے ادارے (Third Party) کے استعمال میں وہ ساری قباحتیں موجود ہیں جو ہم مرکزی نظام کے مسائل میں اوپر ڈسکس کر چکے ہیں اور مزید یہ کہ اس میں زیادہ فیس اور وقت بھی لگتا ہے۔ حکومت اور اداروں کی اجازت بھی درکار ہوتی ہے اور فارن ایکسچینج کے تبادلے کی صورت میں بھی کٹوتی ہوتی ہے۔ چوری کا احتمال ہے، اِنسانی غلطی کا بھی اور سہولت بھی کوئی زیادہ نہیں۔

یہ تو ہم نے تمام انڈے ایک ہی ٹوکری میں رکھ دیئے ہیں اور وہ بھی کسی اور کی جسے عُرفِ عام میں ہم بینک کہتے ہیں۔

تو کیا ہم ایسا نہیں کر سکتے کہ آپس میں خود ہی ایک رجسٹر بنالیں اور اس میں اندراج کرتے رہیں؟ بالکل ایسا کیا جا سکتا ہے مگر یہاں ڈبل سپنیڈنگ (Double-Spending) دوہرے خرچے کا مسئلہ آتا ہے جسے ساتوشی ٹاکاموٹو نے بخوبی حل کیا اس حل کو بلاک چین کہتے ہیں۔

ہم ایک پبلک لیجر بنا لیتے ہیں اور اس میں شروع سے لے کر رہتی دنیا تک ہونے والی تمام ٹرانزیکشن کا ریکارڈ رکھتے رہیں گے۔ اگر عبداللہ آگے کسی کو 5 ہزار دیتا ہے تو سب کو پتہ ہے کہ اُس کے پاس 10 ہزار ہیں اور وہ 5 ہزار دے سکتا ہے اور یہ 10 ہزار اُس کے پاس جمشید کی

طرف سے آئے تھے۔ اب اگر اس نظام پر ہزاروں، لاکھوں لوگ ہیں تو یہ سب ٹرانزیکشن کرتے رہیں گے اور بلاک چین کے پبلک رجسٹر میں سب کا اندراج ہوتا رہے گا۔

جب بہت سی ٹرانزیکشن کو لکھنے کی وجہ سے صفحہ بھر جائے گا تو تمام لوگ (Nodes) اُسے ہیش فنکشن کی مدد سے سِیل کر کے بلاک بنا دیں گے اور اگلے بلاک پر کام شروع ہو جائے گا۔

اِس سیل (Sale) کا مطلب یہ ہے کہ جو بھی صفحے / بلاک پر لکھا ہوا ہے وہ ٹھیک اور اب رہتی دنیا تک اِس میں کوئی تبدیلی ممکن نہیں جسے ہم بلاک چین کی (Immutability) کہتے ہیں۔

ہیش فنکشن آسان زبان میں ریاضی کا وہ پیچیدہ فنکشن ہے جس میں آپ جو چاہیں تحریر ڈال دیں وہ جواب میں آپکو ایک ہی سائز کے مختلف جواب دے گا۔ آپ اسے ایک مشین کہہ لیں اب اگر ہم اس میں 4 ڈالتے ہیں تو جواب آئے گا dcbea

4 ⟶ Hash Function ⟶ dcbea

اب 26 ڈال کے دیکھتے ہیں

26 ⟶ Hash Function ⟶ 94c8e

یعنی جواب میں حروفِ تہجی کے علاوہ ہندسے بھی شامل ہو سکتے ہیں۔ ھیش فنکشن ون وے (یک طرفہ) فنکشن کہلاتا ہے۔ پھر جب بھی کوئی اِن پُٹ ڈالیں گے اس کا جواب یکساں آئے

گا مثلا 4 کا جواب ہمیشہ dcbea ہی آئے گا مگر کوئی طریقہ ایسا نہیں کہ آپ جواب سے اصل اِن پٹ تک پہنچ سکیں۔

ہاں اس کی جانچ آسان ہے۔ اگر آپکو 4 اور dcbea دونوں معلوم ہوں تو آپ اس فنکشن کی مدد سے ایک سیکنڈ میں چیک کر سکتے ہیں کہ اس اِن پُٹ کا آؤٹ پُٹ یہی آئے گا کہ نہیں۔

اب اگر میں آپ سے کہوں کہ مجھے ایسا اِن پُٹ بنایئے جس کی مدد سے جو آؤٹ پٹ آئے اس کے شروع میں 3 صفر ہوں۔

Hash Function ⟶ 000... ? ⟶

آپ اسے کیسے معلوم کریں گے؟

اِسے معلوم کرنے کا واحد طریقہ (Brute force) ہے کہ آپ ایک کے بعد ایک نمبر اِن پُٹ کے طور پر دیتے چلے جائیں اور دیکھیں کہ آؤٹ پُٹ کیا ہے، کبھی نہ کبھی تو آپ کی مرضی کا آؤٹ پُٹ آ ہی جائے گا۔

237 ⟶ HASH ⟶ 2bc7

C75ae ⟶ HASH ⟶ 9082

11802 ⟶ HASH ⟶ 09aef

.

.

.

72533 ⟶ HASH ⟶ 000ca

آہا، مل گیا۔اب یہی 72533 آپ کا مطلوبہ نمبر ہے۔ کوئی بھی شخص اسے ویری فائی کر سکتا ہے کہ 72533 اگر ان پُٹ میں دیا جائے تو آؤٹ پُٹ کے شروع میں 3 صفر ہوتے ہیں۔

اب ہمیں اپنے ٹرانزیکشنز کے صفحے (بلاک) کو سیل کرنا ہے۔ ہم صفحے میں موجود تمام ٹرانزیکشنز کو جمع کرتے ہیں (یا کسی اور طریقے سے نمبر نکالتے ہیں)۔اب ہم یہ سوال پوچھتے ہیں کہ صفحے کے مجموعے میں وہ کون سا نمبر شامل کروں کہ آؤٹ پُٹ کے شروع میں 3 صفر ہوں۔

مثال کے طور پر صفحے کا مجموعہ 20893 ہے تو سوال بنا

20893 ⟶ HASH ⟶ 000

+

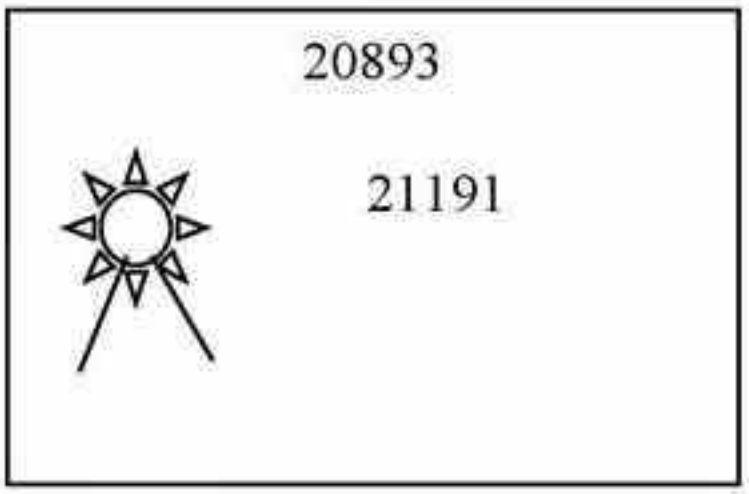
?

ہم پھر ایک کے بعد ایک نمبر سے ٹرائی (قسمت آزمائی) کرتے ہیں، کچھ عرصے میں نمبر ملا 21191تو

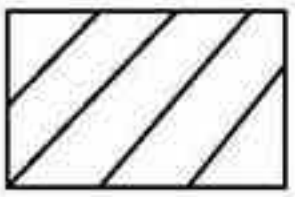
21191 + 20893 = 42084

42084 ⟶ HASH ⟶ 00078

یہی ہمارا مطلوبہ نمبر تھا۔اب ہم اس کی مدد سے صفحہ (بلاک) کو سیل کر دیں گے۔ یہ پورا عمل مائننگ کہلاتا ہے جسے بِٹ کوائن کی تکنیکی اِصلاح میں ہم پروف آف ورک (کام کی گواہی) کہتے ہیں۔



اس بلاک کو سیل کرنے کے ساتھ ہی ہم بلاک چین میں جوڑ دیتے ہیں۔ ہر نئے بلاک کو بلاک چین میں جوڑنے سے پہلے ریاضی معمّہ (Puzzle) حل کرنا ہوتا ہے۔ جس میں سابقہ صفحہ کا ملنے والا نمبر، نیا نمبر جس کی اب ہمیں تلاش ہے اور نیا ویری ایبل نمبر (Nonce) جوڑ کر آؤٹ پُٹ تک پہنچنا ہوتا ہے۔



+

? ⟶ HASH ⟶ 0 0 0 . . .

+

0 0 0

اب اگر کسی شخص کو جعلی بلاک شامل کرنا ہو گا تو اسے نہ صرف اس موجودہ بلاک بلکہ آج تک بلاک چین میں جتنے بلاک بن گئے ہیں ان سب کو پھر سے جوڑنا ہو گا اور ان کے ریاضی معمّے کو حل کرنا ہو گا۔ اس کے لیئے جب تک دنیا میں موجود اس نیٹ ورک کی 51% قوت اس کے پاس نہیں آجاتی، یہ ممکن نہیں ہے۔ اسے (51% اٹیک) کہتے ہیں۔

ہر نئے بلاک پر مائنرز کو کرپٹو کرنسی اِنعام میں ملتی ہے شروع میں 50 بِٹ کوائن ملتے تھے، پھر 25، آج کل 12.5، 51% پاور رکھنے والے کے لئے مزید بلاکس مائن کر کے رقم کمانا زیادہ سود مند ہو گا بجائے اس کے کہ وہ پورے نظام کو تباہ کرے جس میں کسی کو کچھ نہیں ملنا۔ اور اسطرح پورا نیٹ ورک سچا اور ایماندار رہتا ہے۔

بلاک چین کی تین قسمیں ہیں۔

پبلک بلاک چین:-

جیسا کہ آپ نے دیکھا بِٹ کوائن اور ایتھیریم اس کی مثالیں ہیں۔ اس میں کوئی بھی کسی جگہ سے نیٹ ورک کو جب چاہے جوائن کر سکتا ہے اور جب چاہے چھوڑ سکتا ہے نوڈز کو ایماندار رکھنے کے لئے انھیں کام پر معاوضہ دیا جاتا ہے۔ نئے کوائنز اور ٹرانزیکشن فیس کی صورت میں، اور ریاضی کے پیچیدہ فنکشنز اسے ہیکنگ پروف بناتے ہیں۔

پرائیویٹ بلاک چین:-

کسی کمپنی کا اندرونی پبلک لیجر جسے صرف وہی جوائن کر سکتے ہیں جنہیں کمپنی اجازت دے۔ یہاں کیونکہ لوگوں کا آپس میں اعتماد قائم ہوتا ہے اور بے ایمانی کی صورت میں قانونی کاروائی ہو سکتی ہے اور یوں نوڈ کی اصل شناخت معلوم ہوتی ہے کہ کون اسے چلا رہا ہے تو یہاں مائننگ کا عمل اتنا مشکل نہیں ہوتا۔ نتیجتاً اس کی رفتار اور کام کرنے کی صلاحیت پبلک بلاک چین سے ہزاروں گناہ زیادہ ہوتی ہے۔

مثال کے طور پر بِٹ کوائن بلاک چین ہر سات سیکنڈ میں ایک ٹرانزیکشن کر پاتا ہے اور ایک بلاک 10 منٹ میں بنتا ہے۔ ایتھیریم میں ایک بلاک ہر 15 سیکنڈ میں بنتا ہے۔ مگر پے پال اور کریڈٹ کارڈز کمپنیاں لاکھوں ٹرانزیکشنز فی سیکنڈز میں کرتی ہیں۔ اِن صلاحیتوں کے لئے کرپٹو کرنسی میں لائٹننگ (Lightning) نیٹ ورکس متعارف کروائے جا رہے ہیں۔

کن سور شیم(Consortium)بلاک چین:-

کمپنی یا پارٹنرز کے مجموعے کے درمیان بلاک چین جس میں صرف ممبرز جوائن کر سکیں۔ یہاںConsensusکی بجائے ممبر شپ کے اصول طے کئے جاتے ہیں۔

بلاک چین ایک خاص قسم کا پبلک لیجر (عوامی کھاتا) ہوتا ہے جو کہ بنیادی ٹیکنالوجی ہے کرپٹو کرنسی مثلاً بٹ کوائن کی۔ یہ ایک ایسا ڈیٹا اسٹرکچر ہے جس میں ٹرانزیکشنز بلاکس کی صورت میں ایک زنجیر کی کڑی کی طرح ایک دوسری سے جڑی ہوتی ہیں۔ ریاضی کے ہیش فنکشن کی مدد سے۔

بلاک چین کی قسموں میں پبلک بلاک چین کھلی یا اوپن ہوتی ہیں جس میں شمولیت اور اخراج کے لئے کسی پرمیشن (اِجازت) کی ضرورت نہیں ہوتی، جو چاہے، جب چاہے اِسے جوائن کر سکتا ہے اور اس سے باہر نکل سکتا ہے۔ انجانے لوگوں اور نوڈز کے درمیان اعتماد بحال رکھنے کے لئے اس میں انعامی طور پر کرپٹو کرنسی دی جاتی ہے اور ریاضی کے پیچیدہ مرحلوں سے اس کے نظم و نسق کو ممکن بنایا جاتا ہے۔

دوسری طرف پرائیویٹ یا کلوز بلاک چین میں اعتماد عموماً ایک ہی کمپنی کی پالیسیوں اور معاہدوں کے ذریعے ممکن بنایا گیا ہوتا ہے لہٰذا یہاں کرپٹو کرنسی انعام کے طور پر نہیں دی جاتی۔ باقی تمام مراحل مثلاً Consensus (اتفاقِ رائے) اور ووٹنگ وغیرہ کم و بیش یکساں ہی ہوتے ہیں۔

جیسا کے ہم پہلے باب میں پڑھ چکے ہیں کہ زر کی ابتدا اور صورتیں مختلف رہیں، نمک سے لے کر جانوروں کی کھال تک، اور رائی اسٹون سے لے کر تمباکو تک، جس شئے کی رسد و طلب رہی وہ کرنسی کے طور پر زیرِ استعمال رہی۔

انٹرنیٹ کے ساتھ ہی ڈیجیٹل کرنسی کا وجود بھی عمل میں آیا۔

ڈیوڈ چوم(David Chaum)نے1982ء میں بلائینڈ سگنیچر(Blind signature)اور e_ Cash کا نظریہ پیش کیا۔آدم بیک(Adam Back) نے1997ء میں Hash Cash،وائی ڈائی(Wai Dai)نے1990ء میں B-Money نِک زابو(Nick Szabo)نے1998ء میں Bit- Goldاور ہال فینی(Hal Finney)نے2004میں(Reusable Proof of work) (R Pow)کا نظریہ پیش کیا۔اوران تمام نظریات وایجادات کی بناپر2008ء میں ستوشی ناکاموٹو نے بِٹ کوائن کو دنیا سے متعارف کروایا۔

اس وقت شاید ہی دنیا کا کوئی بڑا بینک ہو جو کسی نہ کسی طور پر بلاک چین کو اسٹڈی نہ کر رہا ہو۔ آئی بی ایم(IBM)نے2015ء میں لنکس فاؤنڈیشن کے ساتھ Hyper Ledger Fabricپر اجیکٹ شروع کیا جسے اب تک سینکڑوں کمپنیاں استعمال میں لا چکی ہیں۔اربوں کی انوسٹمنٹ (سرمائے)، ڈھائی ہزار سے اوپر Patentsاور 800 سے اوپر کرپٹو ایسٹس (Crypto Assets)کے ساتھ بلاک چین معاشی نظام میں وہ تبدیلیاں لانے والا ہے جو ای- میل ڈاکخانہ کے نظام میں اور سیل فون، عام لینڈ لائن ٹیلی فون کے نظام میں لایا۔

ضرورت اس امر کی ہے کہ ہم اس ٹیکنالوجی کو زیادہ سے زیادہ سیکھیں اور آنے والے سالوں میں اس کے بہتر استعمال کو ممکن بنا سکیں۔ایک سروے کے مطابق 2020ء میں دنیا میں کم از کم 5 لاکھ بلاک چین ڈویلپرز درکار ہونگے۔اِس وقت کوئی 5 ہزار بھی نہیں ہیں۔اگر آپ آج سے اسی پر کام کرنا شروع کر دیں گے تو مستقبل میں آپ کی نوکری اور بزنس کے امکانات اظہر من الشمس ہیں۔

اگلے باب میں ہم بلاک چین کی تکنیکی تعریف اور ماہیّت پر بات کریں گے۔

بلاک چین— تکنیکی ماہیت اَور تعریف

پچھلے باب کو ذہن میں رکھتے ہوئے، بلاک چین کی جامع اَور تکنیکی تعریف کچھ یوں ہو گی:-

"بلاک چین کمپیوٹر کے مابین(Peer-To-Peer)، غیر مرکزی (Decentralized)اور منقسم(Distributed)عوامی کھاتا (Public Ledger)ہے جو کہ ہونیوالی ٹرانزیکشن(Transaction)کا مکمل، پائیدار اَور تبدیل نہ ہونیوالا ریکارڈ رکھتا ہے۔ یہ ریکارڈ وقت کی مناسبت سے رکھا جاتا ہے کہ ہر ٹرانزیکشن کے ساتھ اس کے وقوع پذیر ہونے کا وقت بھی لکھا جاتا ہے۔ ایک ایسے ماحول میں جہاں لوگوں، اِداروں یا آلات کا آپس میں کوئی اعتماد نہ ہو یا اِس کا فقدان ہو، وہاں بلاک چین ٹرانزیکشن کو ممکن بناتا ہے۔

بلاک چین سیکیورٹی کے لئے ریاضی کے پیچیدہ الگورتھم Cryptography اِستعمال کرتا ہے اَور اِس نظام میں شامل نوڈز کو ایماندار رکھنے کے لئے انھیں انعام بھی دیتا ہے اور سزا بھی۔

بلاک چین میں درج ہونے والی ٹرانزیکشن پھر کبھی تبدیل نہیں ہو سکتی۔ یہ رجسٹر میں لکھی جانے والی وہ اِنٹری ہے جو کہ ٹرانزیکشن کی تاریخ بتاتی ہے اور اس طرح ہم دوہرے اخراجات (Double Spends)کے مسئلے کو حل کرتے ہیں کہ ہر رقم کا مکمل حساب موجود ہے

کہ وہ کب معرضِ وجود میں آئی، کب اور کہاں خرچ ہوئی اور اس کی موجودہ ملکیت کس کے پاس ہے۔

چلیں مثال سے بلاک چین میں بٹ کوائن کا ایک بلاک شامل کر کے دیکھتے ہیں کہ اِس پورے عمل میں تکنیکی طور پر کیا ہوتا ہے؟

فرض کریں کہ ہم نے بِٹ کوائن کی مکمل بلاک چین پبلک سسٹم سے ڈاؤن لوڈ کر لی اور اب ہمارے کمپیوٹر نوڈ نے اِس میں نیا بلاک شامل کرنا ہے۔

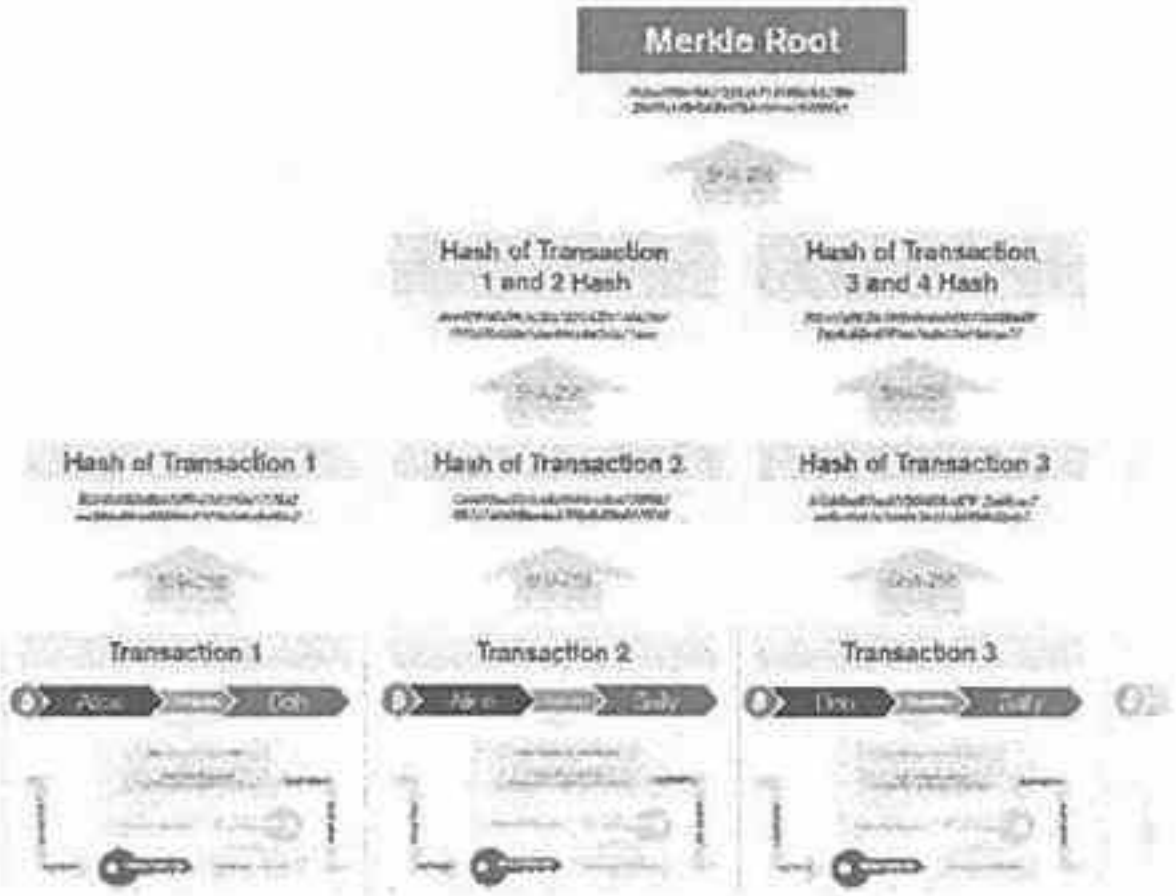
آخری اور سب سے نیا بلاک 349 نمبر کا ہے، ہمارے بلاک کا نمبر 350 ہو گا۔

ایک بلاک میں پچھلے 10 منٹوں میں ہونے والی تمام ٹرانزیکشن کا ریکارڈ ہوتا ہے۔ جیسے ہی کوئی ٹرانزیکشن عمل میں آتی ہے تو بلاک چین کا نظام اس نیٹ ورک میں شامل تمام نوڈز کو براڈ کاسٹ کر دیتا ہے، سب چیک کرتے ہیں کہ آیا یہ درست ٹرانزیکشن ہے یا نہیں (یعنی دوہرے خرچے کی چیکنگ کرتے ہیں) اور پھر اسے کرپٹو گرافک ہیش فنکشن سے گزار کر بلاک میں شامل کر دیتے ہیں۔ بِٹ کوائن SHA-256 نام کا ہیش فنکشن استعمال کرتا ہے۔ اِن کا بنیادی تصّور تو وہی ہے جو ہم پچھلے باب میں پیش کر چکے ہیں۔ مزید معلومات کے لئے آپ بلاک گیکس Block. Geeks ویب سائٹ پر ہیش فنکشن کا صفحہ دیکھ لیں۔ اب نوڈز سے ملنے والی فائنل ٹرانزیکشن کرپٹو گرافی ہیش سے گزرنے کے بعد بلاک میں شامل ہوتی ہیں جسے مارکل ٹری کی مدد سے اِسٹور کیا جاتا ہے۔ اگر کسی بھی ٹرانزیکشن میں کوئی بھی ردّوبدل کیا گیا تو پھر سے پورے مارکل ٹری (Markle Tree) کو پراسیس کرنا پڑے گا۔

اب مارکل روٹ (Markle Root) کو بلاک چین میں شامل کرنے سے پہلے ہم بلاک کے ہیڈر (Header) کا ہیش معلوم کرینگے جس میں Nonce ویلیو والے معّمے کو حل کرنا ہو گا۔ ایسا کرنے کے لئے ہم پچھلے بلاک 349 کا ہیڈر ہیش، مارکل روٹ اور نانس ویلیو کی مدد

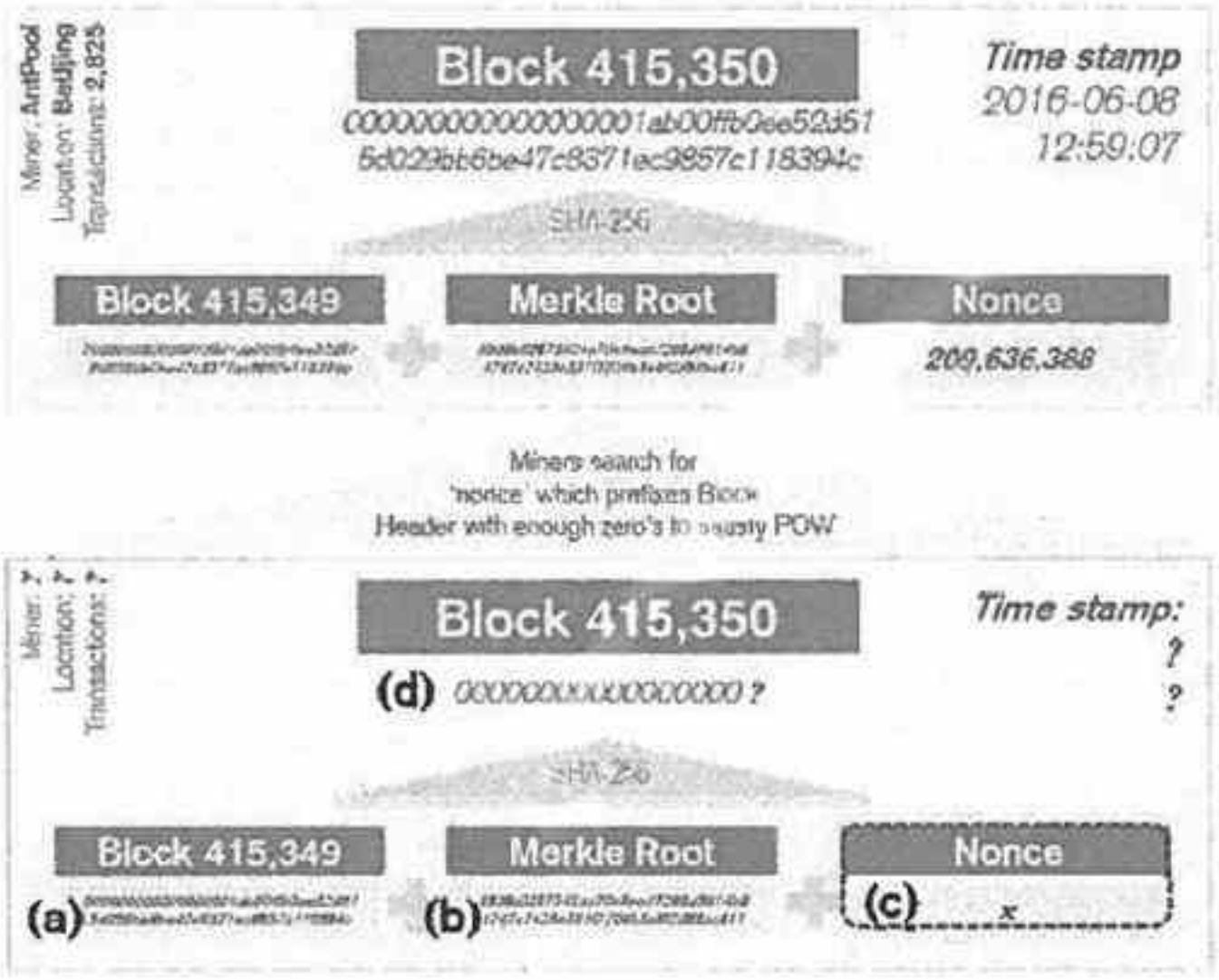
سے وہ سیل (Seal) تلاش کرینگے جو بلاک 350 میں لگے گی۔ جیسے ہی ریاضی کا یہ معمّہ حل ہو جائے گا تو ہم پچھلے بلاک کا ہیڈر ہیش، مارکل روٹ، نانس ویلیو اور ملنے والا نمبر نیٹ ورک پر براڈکاسٹ کر دینگے۔ تمام نوڈز ان ویلیوز کو چیک کریں گے اور اگر یہ درست ثابت ہوئیں تو نئے بلاک 350 کو بلاک چین میں شامل کر لیں گے اور مائنر کو انعامی بٹ کوائنز مل جائیں گے۔ تصویر نمبر 2، 1 اور 3 میں اس سارے عمل کی وضاحت کر دی گئی ہے۔

Figure 1: Calculating the Merkle Root



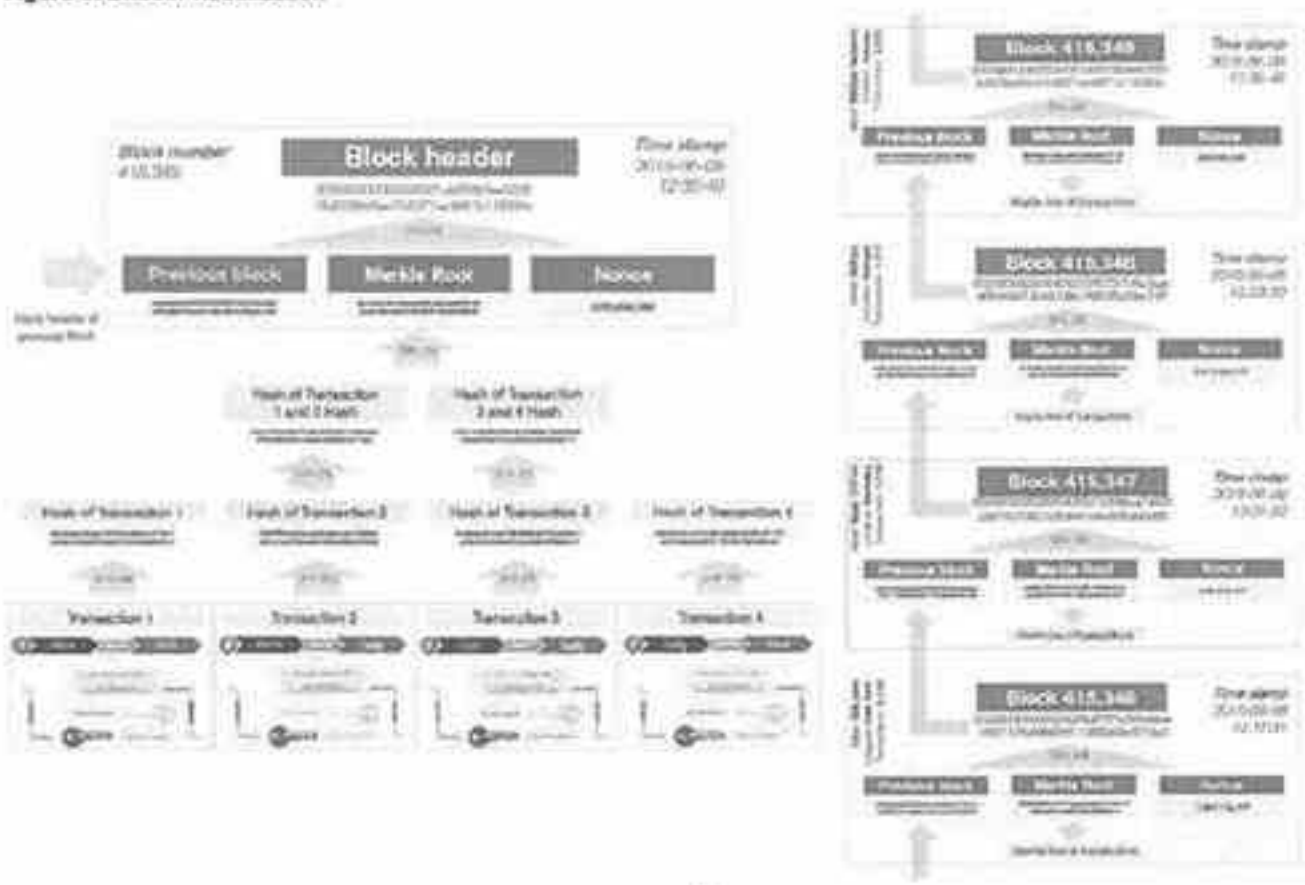
تصویر 1

Figure 2: Mining a block



تصویر2

Figure 3: Bitcoin visualization



تصویر3

اگر سافٹ ویئر کی نظر سے دیکھیں تو بلاک چین کو ہم 3 حصّوں میں بانٹ سکتے ہیں۔

1. پروٹوکول لیئر Protocol Layer
2. نیٹ ورک لیئر Network Layer
3. ایپلی کیشن لیئر Application Layer

پروٹوکول لیئر بتاتی ہے کہ ہم کون سی پروگرامنگ لینگویج اور کمپیوٹنگ ریسورسز اِستعمال کر رہے ہیں۔ نوڈز کیسے نظام میں شمولیت اختیار کرینگے، اِتفاق رائے (Consensus) کیسے ہوگا، ویلیو یا رقم کا تبادلہ کیسے ہوگا اور اِنعام کیسے دیا جائے گا۔ نیٹ ورک لیئر بتاتی ہے کہ نظام کا باہمی تعلق کیسے طے پائے گا۔ مائنرز، نوڈز، ڈیٹا اور ایپلی کیشن کس طرح آپس میں بات کریں گے۔

ایپلی کیشن لیئر بتاتی ہے کہ کون سی ایپلی کیشن یا کلائنڈ، اس نیٹ ورک پر چل سکیں گے اور اِن کے نظام کے قوانین وضوابط کیا ہونگے۔

بلاک چین کے نظام میں چھ بنیادی خصوصیات ہیں۔

یہ ڈسٹری بیوٹڈ ہوتا ہے، کرپٹو گرافی کی مدد سے اِن کو انکرپٹڈ (Encrypted) ہوتا ہے، مکمل تاریخ (History) رکھتا ہے، تبدیل نہیں کیا جا سکتا (Immutable)، پبلک ہوتا ہے اور ویلیو ٹرانسفر کے لئے کوئی نہ کوئی کرنسی یا ویلیو ٹوکن استعمال کرتا ہے۔

اگر آپ کو معلوم کرنا ہو کہ آپ کا سسٹم بلاک چین پر لے جانے کے قابل ہے یا نہیں یا آپ اپنے موجودہ نظام کو چھوڑ کر بلاک چین کی طرف ہجرت کریں یا نہیں تو مندرجہ ذیل چھ سوال پوچھ لیں۔ اگر سب کا جواب ہاں میں ہے تو یقیناً بلاک چین کے استعمال سے آپ کو بہت فائدہ ہوگا۔

1. کیا کوئی ایسا پراسیس ہے جسے بار بار کرنا پڑتا ہے اور جو بآسانی آٹومیشن سے سرانجام پا سکتا ہے؟

2. کیا کوئی پراسیس ایسا ہے جو بہت دیر تک چلتا رہتا ہے یا بار بار ایک طویل مدّت تک چلتا ہے؟
3. کیا آپ کے نظام میں بہت سے شراکت دار ہیں؟
4. کیا مختلف لوگوں /اداروں سے بہت سا ڈیٹا مختلف فارمیٹ اور اوقات میں آتا ہے؟
5. پیسوں کے علاوہ بھی کوئی اور ویلیو ٹرانسفر ہوتا ہے جیسے کہ میوزک، آرٹ، قانونی کاغذات، ووٹ وغیرہ؟
6. کیا یہ ضروری ہے کہ ٹرانزیکشن کی مکمل ہسٹری رکھی جائے اور ان میں بدل ممکن نہ ہو؟

اگر آپ کے نظام کو یہ خوبیاں درکار ہیں تو بلاک چین آپ کے لئے ایک آئیڈیل حل پیش کرتا ہے۔

ستوشی اور اس کا پیپر

ستوشی ناکاموتو کون ہے؟

بٹ کوائن کا خالق، ستوشی ناکاموتو (جس نے چھ صفحات کے ایک پیپر سے دنیا کو ہلا کے رکھ دیا) کون ہے؟ اس سوال کا جواب تاوقت کوئی نہیں جانتا۔

31 اکتوبر 2008ء کو شائع ہونے والا یہ پیپر دنیا کی معاشی انڈسٹری میں ایک زلزلے کی حیثیت رکھتا ہے۔

ساتوشی کوئی فرد ہے یا گروہ، ادارہ یا ملک، مذکر یا مونث کوئی کچھ نہیں کہہ سکتا۔ بٹ کوائن پیپر کی اشاعت سے بھی پہلے جب ستوشی نے P2P فائونڈیشن پر اپنی پروفائل بنائی تو اپنے آپ کو 37 سالہ مرد اور جاپان کا رہائشی بنایا۔

قیاس گروں نے اسے امریکن، برطانوی، کیریبین، مرکزی اور جنوبی امریکہ کا شہری اور حتی کہ ملک تک بتایا۔ کسی نے اس کی شاندار انگریزی کو امریکی ہونے کے ثبوت کے طور پر پیش کیا تو کسی نے اس کے برطانوی محاوروں کے استعمال کو برطانوی شہریت کا ثبوت مانا۔ کسی نے نیوز گروپ پر پوسٹنگ کے اوقات کار کی بنا پر اس کا تعلق سائوتھ امریکہ اور کریبین سے جوڑا تو کسی نے اس کی بیک وقت کمپیوٹر سائنس، کرپٹو گرافی، انگریزی اور اکنامکس میں مہارت کو اصل میں کسی منظم گروہ کی کارستانی بتایا۔ بہت سے جھوٹے ستوشی بھی سامنے آئے جنہیں بعد میں رد کر دیا گیا۔

ستوشی کوئی بھی ہو۔اس کا چھپنا بالکل بجا ہے جب ایک آدمی دنیا بھر کے مرکزی بینکوں، اداروں اور حکومتوں سے ٹکرائے گا تو اس کا خفیہ رہنا ہی اسکی زندگی کی ضمانت ہے ورنہ اسے بھی جولین اسانجے (وکی لیکس) اور ایڈورڈ سنوڈن کی طرح پناہ لینی پڑے گی۔

آیئے پہلے من و عن ستوشی ناکاموتو کے بٹ کوائن پر لکھے گئے پرچے کا متن لفظ بہ لفظ دیکھ لیں پھر ہم اگلے ابواب میں آسان لفظوں میں بٹ کوائن کو سمجھنے کی کوشش کریں گے۔

بِٹ کوائن: کمپیوٹروں کے مابین (P2P) برقی نقدی کی براہِ راست منتقلی کا نظام

Bitcoin: A Peer-to-Peer Electronic Cash System

مصنف: ستوشی ناکاموتو

ای میل: satoshin@gmx.com

ویب سائٹ: www.bitcoin.org

خلاصہ:

برقی نقدی (الیکٹرونک کیش) کی خالصتاً اور براہِ راست کمپیوٹروں کے مابین (P2P) منتقلی کا نظام جو فریقین کو اس قابل بنائے گا کہ وہ (فریقین) کسی مالیاتی ادارے کی دخل اندازی کے بغیر آن لائن رقوم کی ادائیگی (ایک دوسرے کو، براہِ راست) کر سکیں۔ ڈیجیٹل دستخط اس حوالے سے ایک جزوی حل تو فراہم کرتے ہیں لیکن اگر دوہرے اخراجات سے بچنے کے لیے کسی قابلِ بھروسہ فریقِ ثالث کی ضرورت ہو تو کلیدی فوائد ضائع ہو جاتے ہیں۔ ہم دوہرے اخراجات کے مسئلے کا ایک حل تجویز کر رہے ہیں جس میں کمپیوٹروں کے مابین براہِ راست رابطے کا نظام (P2P-Network) استعمال کیا گیا ہے۔ یہ نیٹ ورک تبادلوں (ٹرانزیکشنز) پر "ہیشنگ" کا عمل کرتے ہوئے وقت کی مہر (ٹائم اسٹیمپ) لگاتا ہے جبکہ یہ عمل ہیش پر منحصر (hash-based) ثبوتِ کار (پروف آف ورک) کی جاری زنجیر کا حصہ ہوتا ہے۔ اس طرح ایک ریکارڈ وجود میں آتا ہے جو از سرِ نو ثبوتِ کار انجام دیئے بغیر تبدیل

نہیں کیا جا سکتا۔ طویل ترین زنجیر نہ صرف مشاہدے میں آنے والے واقعات کے ثبوت کا کام کرتی ہے بلکہ یہ بھی ثابت کرتی ہے کہ وہ سی پی یو کی طاقت کے سب سے بڑے مجموعے (pool) سے آئی ہے۔ جب تک سی پی یو کی اکثریتی طاقت ایسے اتصالی مقامات (nodes) سے کنٹرول کی جارہی ہو جو کسی نیٹ ورک پر حملے کے لیے (آپس میں) تعاون نہ کر رہے ہوں، وہ طویل ترین زنجیر تخلیق کریں گے اور حملہ آوروں سے تیز رفتار رہیں گے۔ خود نیٹ ورک کو کم سے کم ساخت درکار ہوتی ہے۔ بہترین کوشش کی بنیاد پر پیغامات نشر (براڈکاسٹ) کیے جاتے ہیں، اور اتصالی مقامات نیٹ ورک کو اپنی مرضی سے چھوڑ سکتے ہیں اور دوبارہ اس میں شامل بھی ہو سکتے ہیں۔ اس مقصد کے لیے وہ ثبوتِ کار کی طویل ترین زنجیر کو اس سب کے ثبوت کے طور پر قبول کرتے ہیں جو پہلے ہو چکا ہو جبکہ وہ وہاں (نیٹ ورک پر) موجود نہیں تھے۔

1۔ تعارف

انٹرنیٹ پر تجارت (کامرس) کم و بیش مکمل طور پر ایسے مالیاتی اداروں پر منحصر ہو کر رہ گئی ہے جو برقی ادائیگیوں کی عمل کاری (پروسیسنگ) کے لیے قابلِ بھروسہ فریقِ ثالث کا کردار ادا کرتے ہیں۔ اگرچہ رقوم کی بالعموم منتقلی کے لیے یہ نظام بخوبی کام کرتا ہے، تاہم یہ بھروسے پر مبنی (trust based) ماڈل کی موروثی خامیوں کا شکار بھی ہے۔ مکمل طور پر ناقابلِ تنسیخ (non-reversible) منتقلیاں درحقیقت (اس نظام کے تحت) ممکن ہی نہیں، کیونکہ ایسے کسی بھی تنازعے میں مالیاتی اداروں سے بطور ثالث بچا ہی نہیں جا سکتا۔ ثالثی (mediation) سے رقم کی منتقلی (ٹرانزیکشن) کی لاگت بھی بڑھ جاتی ہے، جس کے باعث عملی منتقلی کی کم سے کم مالیت محدود ہو جاتی ہے جبکہ بہت کم مالیت والی عمومی منتقلیوں کا

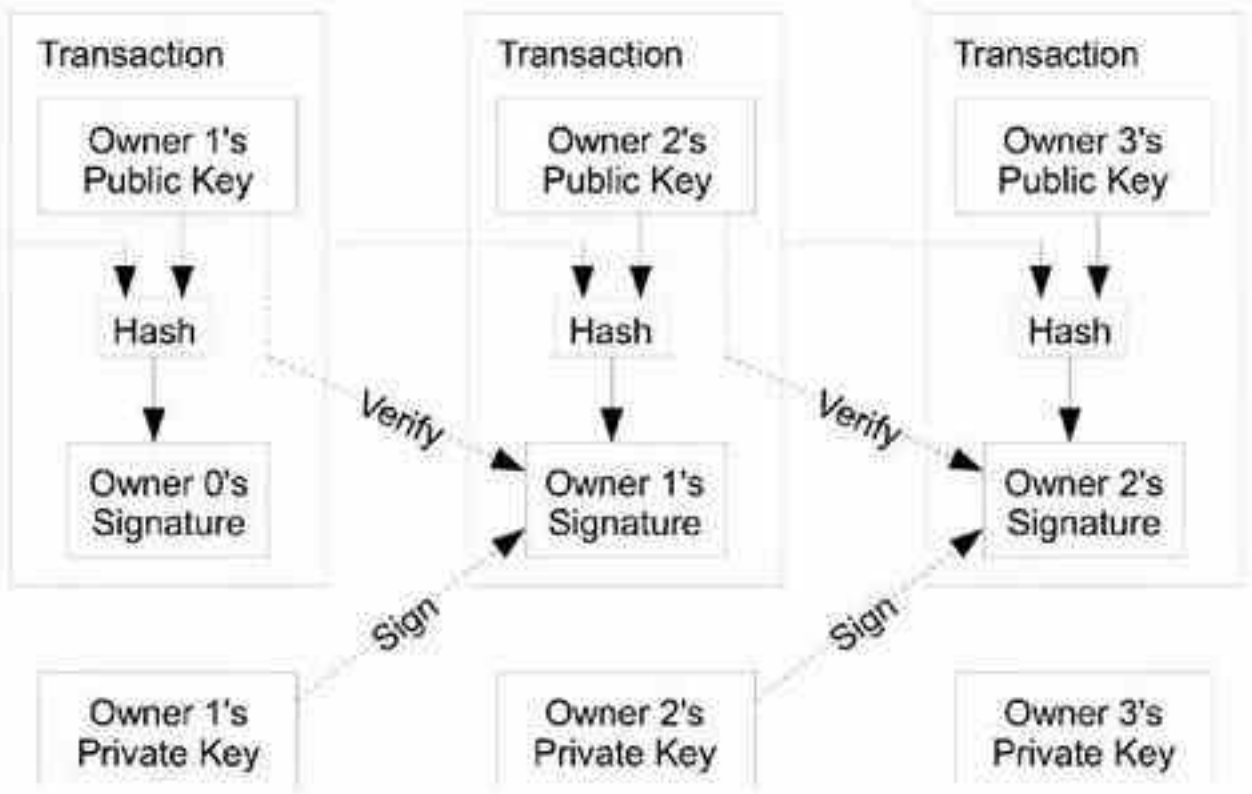
امکان بھی نہ ہونے کے برابر رہ جاتا ہے؛ اور ناقابلِ تنسیخ خدمات کے لیے ناقابلِ تنسیخ ادائیگیوں کے ذیل میں مطلوبہ صلاحیت نہ ہونے کے باعث نقصان کی لاگت بھی وسیع تر ہوتی ہے۔ تنسیخ (reversal) کے امکان کے ساتھ ہی بھروسے کی ضرورت بھی بڑھ جاتی ہے۔ تاجروں کو بھی اپنے گاہکوں کے بارے میں ہوشیار رہنا پڑتا ہے جو ان سے دیگر حالات کی نسبت زیادہ معلومات حاصل کرنے کے لیے الجھتے ہیں۔ یہاں دھوکہ دہی (فراڈ) کے ایک مخصوص فیصد کو ''ناگزیر'' کے طور پر قبول کیا جاتا ہے۔ لاگت اور ادائیگیوں کے بارے میں اس بے یقینی سے انفرادی طور پر روایتی یعنی ایک ''وجود رکھنے والی'' (فزیکل) کرنسی کے ذریعے بچا جاسکتا ہے لیکن مواصلاتی چینل کے ذریعے، کسی قابلِ بھروسہ فریقِ ثالث کے بغیر، ادائیگیوں کو ممکن بنانے والا کوئی نظام موجود ہی نہیں۔

(اس صورتِ حال کے پیشِ نظر) برقی ادائیگی (الیکٹرونک پیمنٹ) کے ایک ایسے نظام کی ضرورت ہے جو محض ''بھروسے'' کے بجائے ''رمز نگاری پر مبنی ثبوت'' (cryptographic proof) پر انحصار کرتا ہو؛ لین دین کے خواہش مند، کوئی سے بھی دو فریقین کے مابین (رقم کی) منتقلی کو کسی قابلِ بھروسہ فریقِ ثالث کی ضرورت کے بغیر ہی ممکن بنائے۔ ایسی منتقلیاں (ٹرانزیکشنز) جنہیں حسابی نقطۂ نگاہ سے واپس پلٹانا یعنی منسوخ کرنا ممکن نہ ہو، فروخت کنندہ کو فراڈ سے بچائیں گی، جبکہ قابلِ بھروسہ فریقِ ثالث والے نظام (escrow mechanism) بھی استعمال کیے جاسکیں گے تاکہ خریداروں کو بھی تحفظ فراہم کیا جاسکے۔ اس مقالے میں ہم دوہرے اخراجات کے مسئلے کا ایک حل پیش کررہے ہیں جس میں کمپیوٹروں کے مابین براہِ راست رابطے (P2P) کا منقسم مہرِ وقت سرور (distributed timestamp server) استعمال کیا گیا ہے تاکہ لین دین یعنی منتقلیوں (ٹرانزیکشنز) کی زمانی ترتیب کا حسابی ثبوت تخلیق کیا جاتا رہے۔ یہ نظام تب تک محفوظ

ہے کہ جب تک دیانتدار مقاماتِ اتصال (nodes)، باہم مربوط حملہ آور مقاماتِ اتصال کے مقابلے میں مجموعی طور پر زیادہ سی پی یو پاور (کمپیوٹروں کی حسابی طاقت) پر کنٹرول رکھتے ہوں۔

2۔ منتقلیاں (ٹرانزیکشنز)

ہم ایک ''برقی سکے'' (الیکٹرونک کوائن) کی توجیح، ڈیجیٹل دستخطوں کی ایک زنجیر کے طور پر کررہے ہیں۔ ہر مالک ''سکے'' کی اگلے مالک تک منتقلی کے لیے پچھلی منتقلی کے ایک ''ہیش'' (hash) اور اگلے مالک کے لیے عوامی کلید (پبلک کی) کو ڈیجیٹل طور پر دستخط کرتا ہے اور (ان سب کو) سکے کے اختتام پر جمع کردیتا ہے۔ وصول کنندہ (payee)، زنجیر کی ملکیت کی تصدیق کرنے کے لیے (ڈیجیٹل) دستخطوں کی تصدیق کرسکتا ہے۔



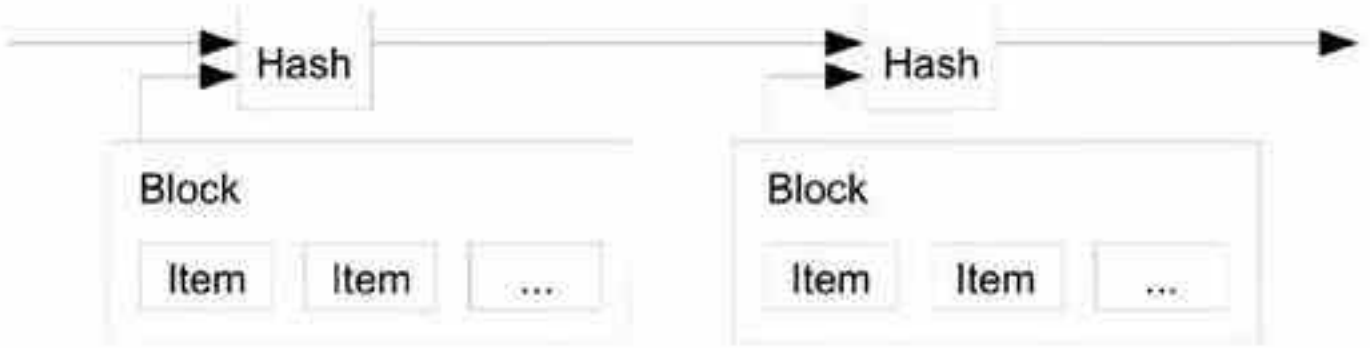
خاکہ

یقیناً، یہاں مسئلہ یہ ہے کہ وصول کنندہ اس بات کی تصدیق نہیں کر سکتا کہ کہیں (سابقہ) مالکان میں سے کسی نے سکے کو دوہرا خرچ تو نہیں کیا۔ اس کا ایک عام حل کوئی قابل بھروسہ مرکزی مختار (سینٹرل اتھارٹی) یا "منٹ" (mint) متعارف کروایا جائے، جو ہر منتقلی کو دوہرے خرچ کے لیے چیک کرے۔ ہر منتقلی کے بعد، سکّہ لازماً "منٹ" کو لوٹا کر (اس کے بدلے) نیا سکّہ جاری کروایا جائے، اور صرف "منٹ" کے جاری کردہ سکّوں ہی پر بھروسہ کیا جائے کہ انہیں دوہرے انداز میں خرچ نہیں کیا گیا ہے۔ اس حل کے ساتھ یہ مسئلہ ہے کہ اس سارے نظامِ دولت کا مکمل انحصار اُس کمپنی پر ہے جو "منٹ" کو چلا رہی ہے، کیونکہ ہر منتقلی (ٹرانزیکشن) کا وہاں سے ہو کر جانا لازمی ہے، بالکل کسی بینک کی طرح۔

ہمیں ایک ایسے طریقے کی ضرورت ہے جس کے ذریعے (سکے کا) وصول کنندہ یہ جان سکے کہ سابقہ مالکان نے قبل ازیں کسی اور منتقلی پر (ڈیجیٹل) دستخط کیے ہیں یا نہیں۔ ہمارے کام کے لیے سب سے پہلی منتقلی ہی اہمیت رکھتی ہے، لہٰذا ماضی میں دوہرا خرچ کرنے کی کوششوں کی ہمیں کوئی پروا نہیں۔ منتقلی کی عدم موجودگی کی تصدیق کرنے کا واحد راستہ یہی ہے کہ (درمیان میں ہونے والی) تمام منتقلیوں سے آگاہ رہا جائے۔ "منٹ" پر مشتمل ماڈل میں صرف "منٹ" ہی تمام منتقلیوں سے آگاہ رہتا تھا اور وہی یہ فیصلہ بھی کرتا تھا کہ کونسی منتقلی (ٹرانزیکشن) پہلے پہنچی یا پہلے کی گئی۔ قابل بھروسہ فریق کی ضرورت کے بغیر یہ کام سرانجام دینے کے لیے منتقلیوں (ٹرانزیکشنز) کا عوامی اعلان کرنا لازمی ہے (1)، اور ہمیں شرکاء کے لیے ایک نظام کی ضرورت ہے جو ترتیب کی اُس ایک تاریخ پر متفق ہو سکیں کہ جس سے انہوں نے موصول کیا ہے۔ وصول کنندہ کو ہر منتقلی (ٹرانزیکشن) کے وقت ایسا ثبوت دینا ہوگا جس پر اتصالی مقامات (نوڈز) کی اکثریت متفق ہو کہ وہ سب سے پہلے موصول کی گئی۔

3۔ مہرِ وقت کا سرور (ٹائم اسٹیمپ سرور)

ہم جو حل پیش کررہے ہیں وہ ایک عدد ''مہرِ وقت کے سرور'' (ٹائم اسٹیمپ سرور) سے شروع ہوتا ہے۔ ٹائم اسٹیمپ سرور کچھ ایسے کام کرتا ہے: یہ بلاگ آئٹمز سے، جنہیں ٹائم اسٹیمپ کیا جانا ہوتا ہے، ایک ''ہیش'' (hash) لیتا ہے اور اس ہیش کو بڑے پیمانے پر شائع (پبلش) کرتا ہے، جیسا کہ اخبار یا ''یوزنیٹ'' پوسٹ میں ہوتا ہے (5 – 2)۔ ٹائم اسٹیم ثابت کرتی ہے کہ اس خاص وقت پر ڈیٹا لازماً موجود رہا ہے تاکہ، ظاہری سی بات ہے، ہیش میں شامل ہو سکے۔ ہر ٹائم اسٹیمپ کے ہیش میں پچھلی ٹائم اسٹیمپ بھی شامل ہوتی ہے؛ یوں ایک زنجیر بن جاتی ہے، جس میں ہر اضافی ٹائم اسٹیمپ، پہلے والی (ٹائم اسٹیمپ) کو تقویت پہنچا رہی ہوتی ہے۔



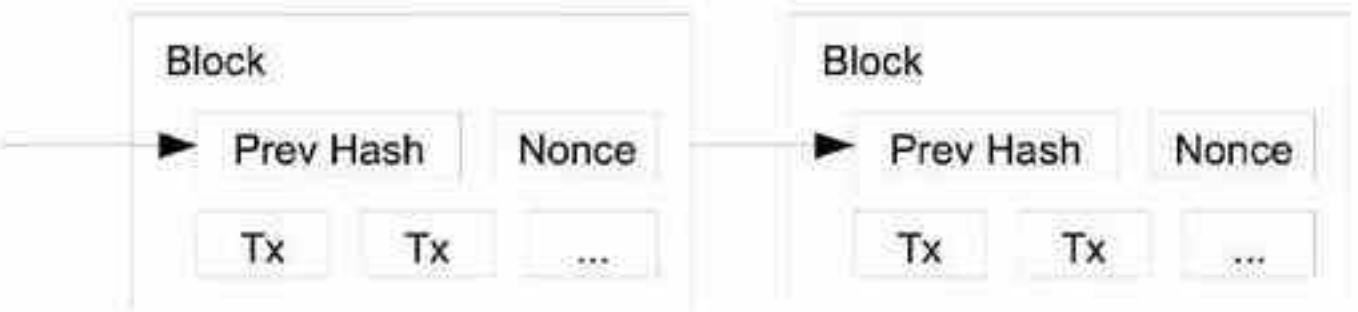
خاکہ

4۔ ثبوتِ کار (Proof-of-Work)

ایک منقسم ٹائم اسٹیمپ سرور کے P2P بنیادوں پر اطلاق کرنے کے لیے ہمیں ''ثبوتِ کار'' کے ایک نظام کی ضرورت ہوگی جو ایڈم بیک کے ''ہیش کیش'' (Hashcash) سے زیادہ مشابہت رکھتا ہے بہ نسبت اخبار یا یوزنیٹ کی پوسٹوں کے (6)۔ ثبوتِ کار کے تحت قدر کی

اسکیننگ شامل ہے کہ جب اسے ہیش کیا جائے، مثلاً SHA-256 کے ساتھ، تو ہیش کا آغاز صفر بٹس والے ایک عدد سے ہوتا ہے۔ اوسط درکار کام صفر بٹس والے عدد کے لیے درکار (کام کی نسبت) قوت نمائی (exponential) ہوتا ہے اور اس کی تصدیق اکہرے (سنگل) ہیش کے عملدرآمد (ایگزیکیوشن) سے کی جاسکتی ہے۔

ہمارے ٹائم اسٹیمپ نیٹ ورک کے لیے ہمیں ثبوتِ کار (پروف آف ورک) کا اطلاق ایسے کرنا ہوگا کہ بلاک (block) میں اضافہ کیا جاتا رہے، حتیٰ کہ وہ قدر مل جائے جو بلاک کے ہیش کو مطلوبہ صفر بٹس کے لیے درکار ہے۔ اسے قابل اطمینان ثبوتِ کار بنانے کے لیے ایک بار (کامیاب) کوشش کرنے کے بعد بلاک کو یہ سارا کام دوبارہ سے کیے بغیر تبدیل نہیں کیا جاسکتا۔ چونکہ بعد والے بلاکس اس کے بعد ہی گویا زنجیر میں پروئے ہوئے ہوتے ہیں، لہٰذا (کسی ایک) بلاک کو تبدیل کرنے کے لیے ان تمام بلاکس پر دوبارہ سے کام کرنا ہوگا جو جس کے بعد ہیں۔



خاکہ

ثبوتِ کار (پروف آف ورک) کا یہ طریقہ اکثریت پر مبنی فیصلہ سازی میں نمائندگی کے تعین کا مسئلہ بھی حل کرتا ہے۔ اگر اکثریت کا انحصار "ایک آئی پی ایڈریس، ایک ووٹ" پر منحصر ہو، تو اسے ایسا کوئی بھی الٹ پلٹ کر رکھ سکتا ہے جو ایک ہی وقت میں کئی آئی پی ایڈریسز رکھنے کے

قابل ہو۔ (اسی لیے) ثبوتِ کار والی تکنیک کا دار و مدار "ایک سی پی یو، ایک ووٹ" پر ہے۔ اکثریتی فیصلے کی نمائندگی طویل ترین زنجیر (chain) سے کی جاتی ہے، یعنی وہ کہ جس پر ثبوتِ کار کے ضمن میں سب سے زیادہ کوشش صرف کی گئی ہو۔ اگر سی پی یو کی طاقت کی اکثریت "دیانتدار مقاماتِ اتصال" (honest nodes) سے کنٹرول کی جارہی ہو، تو دیانتدارانہ زنجیر سب سے زیادہ تیز رفتاری کے ساتھ نمو پائے گی اور (رفتار میں) دوسری مسابقتی زنجیروں کو پیچھے چھوڑ دے گی۔ پچھلے بلاک میں ترمیم کرنے کے لیے ایک حملہ آور کو نہ صرف اس بلاک سے متعلق ثبوتِ کار کا سارا کام دوبارہ سے کرنا پڑے گا بلکہ اس کے بعد والے تمام بلاکس پر بھی یہی ساری کارروائی دوہرانی ہوگی؛ اس کے بعد ہی وہ دیانتدار مقاماتِ اتصال کے برابر پہنچ پائے گا اور پھر ان کے کیے ہوئے کام سے آگے نکل سکے گا۔ یہ ہم بعد میں ثابت کریں گے کہ جیسے جیسے بعد والے بلاکس شامل کیے جاتے ہیں تو (کیسے) ایک سست رفتار حملہ آور کے لیے ان کے برابر پہنچنے کا امکان قوت نمائی شرح سے کم تر ہوتا چلا جاتا ہے۔

ہارڈ ویئر کی بڑھتی ہوئی (درکار) رفتار کا ازالہ کرنے اور وقت گزرنے کے ساتھ ساتھ مقاماتِ اتصال کو چلانے میں تبدیل ہوتی ہوئی دلچسپی کا ازالہ کرنے کے لیے، ثبوتِ کار سے وابستہ مشکل کا تعین ایک متحرک اوسط (moving average) کے ذریعے، بلاکس کی فی گھنٹہ تعداد کو مدنظر رکھتے ہوئے کیا جاتا ہے۔ اگر وہ بڑی تیزی سے (بلاکس) بنا رہے ہوں گے تو مشکل میں بھی اضافہ ہوتا جائے گا۔

5۔ نیٹ ورک

نیٹ ورک کو چلانے کے مراحل حسبِ ذیل ہیں:

1۔ نئی منتقلیاں (ٹرانزیکشنز) تمام مقاماتِ اتصال تک نشر کی جاتی ہیں۔

2۔ہر مقامِ اتصال نئی منتقلیوں کو ایک بلاک میں جمع کرتا ہے۔

3۔ہر مقامِ اتصال اپنے بلاک کے لیے ایک مشکل ثبوتِ کار تلاش کرتا ہے۔

4۔جب مقامِ اتصال کو ایک ثبوتِ کار مل جاتا ہے تو وہ بلاک کو دیگر تمام مقاماتِ اتصال تک نشر کر دیتا ہے۔

5۔مقاماتِ اتصال کسی بلاک کو صرف تب قبول کرتے ہیں جب تمام منتقلیاں درست ہوں اور پہلے ہی خرچ نہ کی جا چکی ہوں۔

6۔مقاماتِ اتصال کسی بلاک کے لیے اپنی قبولیت کا اظہار کچھ اس طرح کرتے ہیں کہ وہ زنجیر میں اگلے بلاک کی تخلیق پر کام شروع کر دیتے ہیں، جس کے لیے وہ قبول شدہ بلاک کے ''ہیش'' کو سابقہ ''ہیش'' کے طور پر استعمال کرتے ہیں۔

مقاماتِ اتصال ہمیشہ طویل ترین زنجیر ہی کو درست قرار دیتے ہیں اور اسی کو بڑھانے پر کام جاری رکھتے ہیں۔اگر دو مقاماتِ اتصال اگلے بلاک کے مختلف نمونے (ورژنز) ایک ساتھ نشر کریں تو کچھ مقاماتِ اتصال ان میں سے کسی ایک کو پہلے اور دوسرے کو بعد میں موصول کریں گے۔اس صورت میں وہ پہلے موصول ہونے والے (بلاک) پر کام شروع کر دیں گے، لیکن دوسری شاخ کو محفوظ کر لیں گے بشرطیکہ وہ زیادہ طویل ہو جائے۔یہ برابری تب ختم ہو گی جب اگلا ثبوتِ کار مل جائے گا اور ایک شاخ زیادہ لمبی ہو جائے گی؛ پھر دوسری شاخ پر کام کرنے والے مقاماتِ اتصال جو دوسری شاخ پر کام کر رہے تھے، وہ طویل تر شاخ پر کام شروع کر دیں گے۔

نئی منتقلی کی نشریات کے لیے ضروری نہیں کہ وہ تمام مقاماتِ اتصال (نوڈز) تک پہنچیں۔کئی مقاماتِ اتصال تک پہنچنے پر وہ بہت پہلے ہی بلاک میں شامل ہو چکے ہوں گی۔بلاک کی نشریات بھی عدم ترسیل شدہ پیغامات کو برداشت کرنے کے قابل ہوتی ہیں۔اگر کسی مقامِ اتصال کو

بلاک موصول نہ ہو، تو وہ نئے بلاک کی موصولی کے ساتھ یہ معلوم ہونے پر پچھلا بلاک بھیجنے کی درخواست کرے گا جس کی ترسیل اسے نہیں ہوئی تھی۔

6۔ محرک (Incentive)

مروجہ طور پر کسی بلاک میں پہلی منتقلی ہی خصوصی منتقلی ہوتی ہے جو ایک ایسے نئے سکے (کوائن) کا آغاز کرتی ہے جو بلاک کے خالق کی ملکیت ہوتا ہے۔ یہ مقاماتِ اتصال کے لیے ایک اضافی محرک کا کام کرتا ہے کہ وہ نیٹ ورک کی معاونت کریں، اور گردش کی غرض سے سکّوں کی ابتدائی تقسیم کا ایک طریقہ فراہم کرتا ہے، کیونکہ انہیں جاری کرنے والا کوئی مرکزی مختار (ادارہ) موجود نہیں۔ نئے سکّوں کی شمولیت کے باعث مستقل کی مالیت میں بتدریج اور مسلسل اضافہ، سونے کی کان کنی کرنے والوں سے مشابہت رکھتا ہے جو (مالیاتی) گردش میں سونے کا اضافہ کرتے ہوئے وسائل کو وسیع تر کرتے ہیں۔ ہمارے معاملے میں سی پی یو کا وقت اور بجلی وہ چیزیں ہیں جن میں وسعت آئی ہے۔

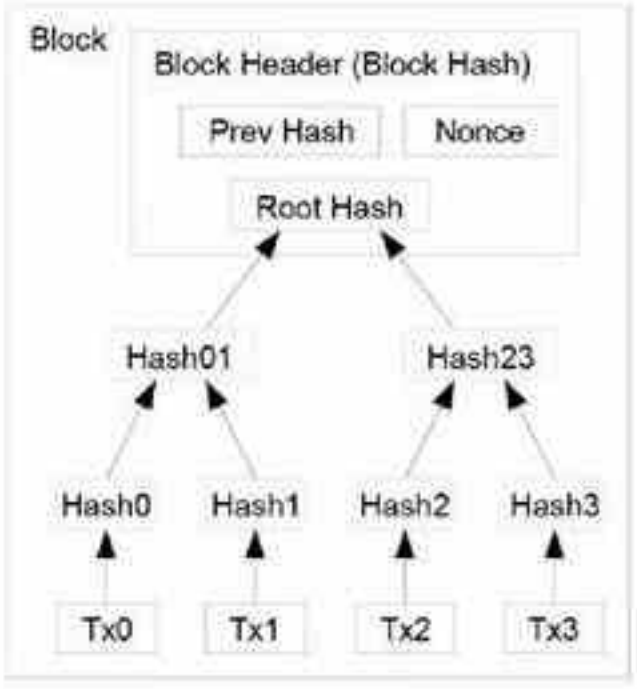
محرک یا ترغیب پر منتقلی کی فیس (ٹرانزیکشن فیس) کے ذریعے بھی سرمایہ کاری کی جاسکتی ہے۔ اگر ایک منتقلی کی آؤٹ پٹ قدر اس کی اِن پُٹ قدر سے کم ہوگی، تو ان کا فرق وہ ٹرانزیکشن فیس ہوگی جو اس منتقلی کے حامل بلاک کی ترغیبی قدر (incentive-value) میں جمع ہوچکی ہے۔ ایک مرتبہ سکّوں کی ایک متعین تعداد گردش میں شامل ہوجائے، تو محرک/ترغیب مکمل طور پر ٹرانزیکشن فیس میں تبدیل ہوسکتا ہے اور افراطِ زر (inflation) سے بالکل پاک بھی ہوسکتا ہے۔

محرک/ترغیب، مقاماتِ اتصال کے دیانتدار رہنے کے لیے حوصلہ افزائی میں مددگار ہوسکتا ہے۔ اگر کوئی لالچی حملہ آور تمام دیانتدار مقاماتِ اتصال کے مقابلے میں سی پی یو کی زیادہ

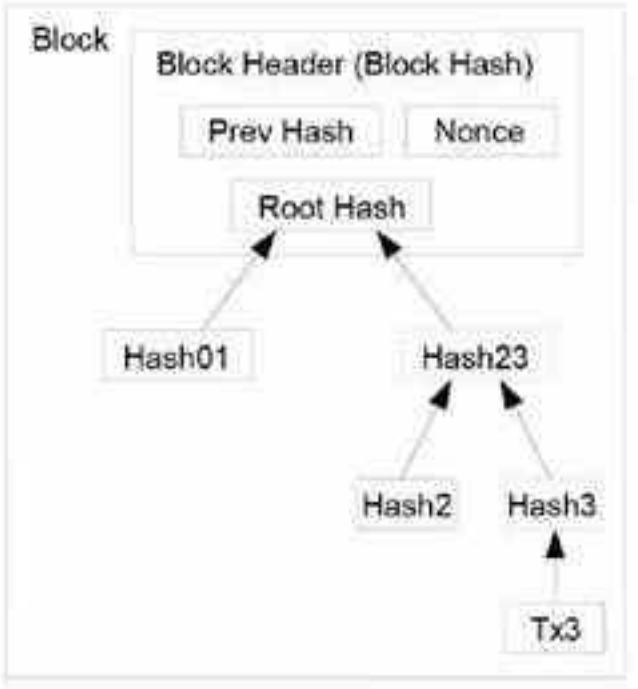
طاقت جمع کرنے کے قابل ہو جائے، تو اسے دو باتوں میں سے کسی ایک کا انتخاب کرنا ہو گا: یا تو وہ اس (طاقت) کو استعمال کرتے ہوئے لوگوں کو دھوکا دے، یا پھر اس سے نئے سکے تخلیق کرے۔ اصولوں کی پاسداری کرتے ہوئے کام کرنا اس کے لیے زیادہ منافع بخش رہے گا، یعنی وہ ان اصولوں پر عمل کرتے ہوئے کسی دوسرے کے مقابلے میں وہ کہیں زیادہ سکے تخلیق کر سکے گا؛ بجائے اس کے کہ وہ نظام کو کمزور کرتے ہوئے خود اپنی ہی دولت کو جواز سے محروم کر دے۔

7۔ ڈسک اسپیس کی واگزاری

ایک بار کسی سکے میں تازہ ترین منتقلی کافی بلاکس کے نیچے دب جائے تو اس سے پہلے کی خرچ شدہ منتقلیوں (ٹرانزیکشنز) کو ڈسک اسپیس بچانے کے لیے تلف کیا جا سکتا ہے۔ بلاک کا ہیش توڑے بغیر اس عمل میں سہولت کاری کے لیے منتقلیوں کو مرکل ٹری (7)(2)(5) میں ہیش کیا جاتا ہے، جس کے تحت صرف جزر (root) کو بلاک کے ہیش میں شامل کیا جاتا ہے۔ اس کے بعد درخت (ٹری) کی شاخیں تراش کر پرانے بلاکس کو مختصر کیا جا سکتا ہے۔ اندرونی ہیشز کو محفوظ رکھنے کی ضرورت نہیں۔



Transactions Hashed in a Merkle Tree



After Pruning Tx0-2 from the Block

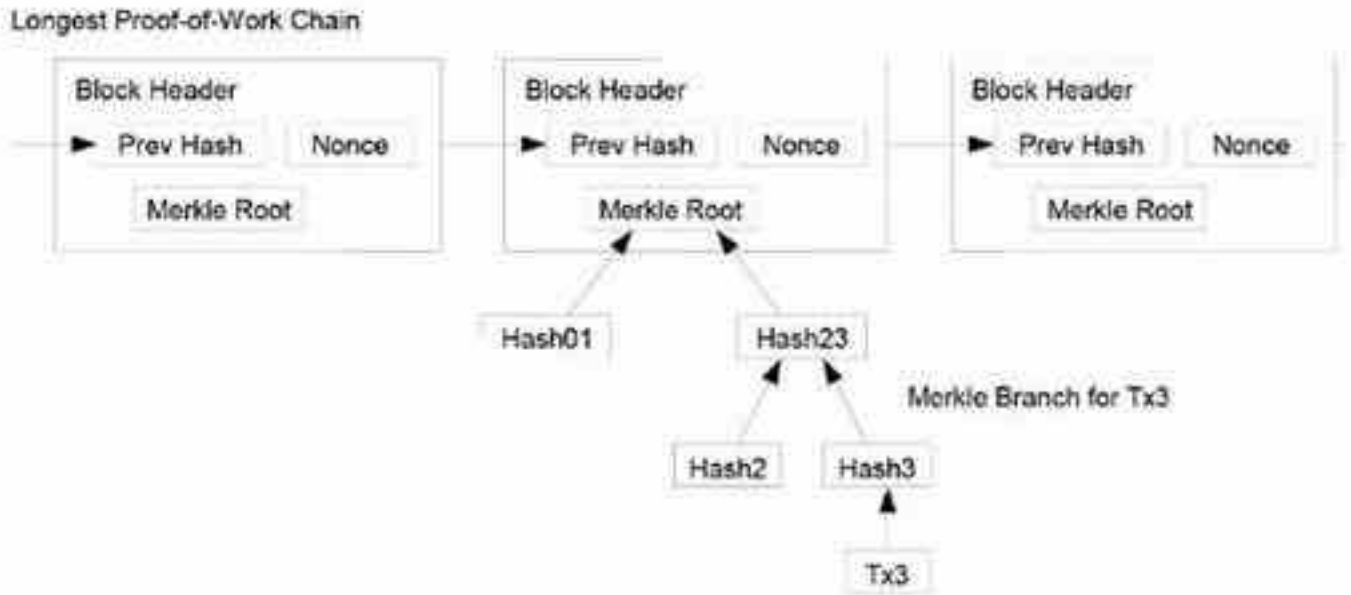
خاکہ

ایک بلاک ہیڈر جس میں کوئی منتقلیاں نہ ہوں، وہ تقریباً 80 بائٹس کا ہوگا۔ اگر ہم فرض کریں کہ ہر دس منٹ میں بلاکس تخلیق کیے جارہے ہیں تو 80 bytes * 6 * 24 * 365 = 4.2 MB، یعنی سال میں 4.2 میگا بائٹس سالانہ استعمال ہوں گے۔ 2008 میں ایک عام کمپیوٹر 2 گیگا بائٹس ریم کے ساتھ فروخت کیا جارہا ہے، اور مور کے قانون کے مطابق اس میں 1.2 گیگا بائٹس کے سالانہ اضافے کی پیش گوئی ہے، تو اگر بلاک ہیڈرز کو میموری میں محفوظ رکھنا پڑے تب بھی کوئی کوئی مسئلہ نہیں ہونا چاہیے۔

8۔ ادائیگی کی سادہ تصدیق

نیٹ ورک میں شامل تمام مقاماتِ اتصال کو چلائے بغیر ادائیگیوں کی تصدیق ممکن ہے۔ صارف کو صرف سب سے لمبے ثبوتِ کار کی زنجیر کے ہیڈر (header) کی ایک نقل رکھنی پڑتی ہے، جسے وہ نیٹ ورک نوڈز (مقاماتِ اتصال) سے استفسار (query) کر کے حاصل کر سکتا ہے، یہاں تک کہ وہ اس بات پر قائل ہو جائے کہ طویل ترین زنجیر اسی کے پاس ہے؛

اور وہ مرکل شاخ حاصل کرلے جو اس بلاک سے منسلک ہے جس میں اس نے ٹائم اسٹیمپ (مہرِ وقت) لگائی ہے۔ وہ (پوری) ٹرانزیکشن کی خود پڑتال تو نہیں کر سکتا، لیکن اسے زنجیر میں کسی مقام سے منسلک کر کے، وہ دیکھ سکتا ہے کہ نیٹ ورک کے مقامِ اتصال نے اسے قبول کر لیا ہے؛ اور اس کے بعد شامل کیے جانے والے بلاکس مزید تصدیق کرتے ہیں کہ نیٹ ورک نے اسے قبول کر لیا ہے۔



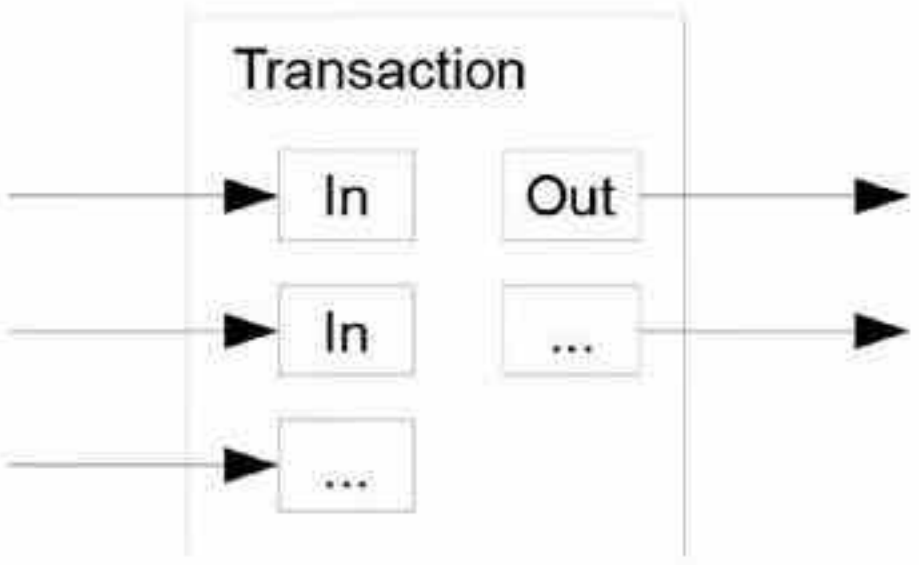
خاکہ: ثبوتِ کار کی طویل ترین زنجیر

ویسے تو تصدیق کا یہ طریقہ تب تک قابلِ اعتماد ہے کہ جب تک دیانتدار نوڈز نیٹ ورک کو کنٹرول کر رہی ہوں، لیکن اگر کسی حملہ آور کی طاقت اس (پورے) نیٹ ورک کی طاقت سے بڑھ جائے تو یہ بہت زیادہ غیر محفوظ ہو جاتا ہے۔ اگرچہ نیٹ ورک نوڈز (مقاماتِ اتصال) خود ہی منتقلیوں کی تصدیق کر سکتے ہیں، البتہ حملہ آور کی جعلی منتقلیوں کے ذریعے اس سادہ طریقے کو بے وقوف بنایا جا سکتا ہے، بشرطیکہ حملہ آور اس نیٹ ورک کی مجموعی طاقت پر حاوی رہنے کا سلسلہ جاری رکھے۔ اس سے بچنے کی ایک حکمتِ عملی تو یہ ہو گی کہ نیٹ ورک نوڈز سے جاری ہونے والی وہ تنبیہات (alerts) قبول کی جو وہ کسی ناجائز (invalid) بلاک کا انکشاف

ہوتے ہی جاری کریں، تاکہ صارف کا سافٹ ویئر فوری طور پر پورا بلاک اور تنبیہ سے متعلق منتقلیوں کو اس بے ضابطگی کی تصدیق کے لیے ڈاؤن لوڈ کر سکے۔ وہ کاروباری یا تجارتی ادارے جو جلدی جلدی ادائیگیاں وصول کرتے ہیں، وہ تب بھی چاہیں گے کہ زیادہ آزادانہ تحفظ اور تیز رفتار تصدیق کے لیے اپنی (خود کی زیرِ ملکیت) نوڈز چلائیں۔

9۔ قدر کی تقسیم اور یکجائی

اگرچہ سکّوں کو جداگانہ طور پر سنبھالنا ممکن ہوگا، ہر سینٹ کی منتقلی کے لیے ایک علیحدہ ٹرانزیکشن تشکیل دینا (عملاً) بہت مشکل رہے گا۔ قدر (ویلیو) کی تقسیم اور یکجائی کی گنجائش کے پیشِ نظر، منتقلیوں (ٹرانزیکشنز) میں متعدد اِن پٹ اور آؤٹ پُٹ موجود ہوتے ہیں۔ عموماً کسی ایک پچھلی بڑی ٹرانزیکشن سے صرف ایک اِن پُٹ ہوگا یا پھر کئی اِن پُٹ ہوں گے جو چھوٹی رقوم سے منسلک ہوں گے؛ اور زیادہ سے زیادہ دو آؤٹ پُٹ ہوں گے: ایک ادائیگی کے لیے اور دوسرا ممکنہ طور پر بچ جانے والی رقم (چینج) کو ارسال کنندہ کو واپس لوٹانے کے لیے۔

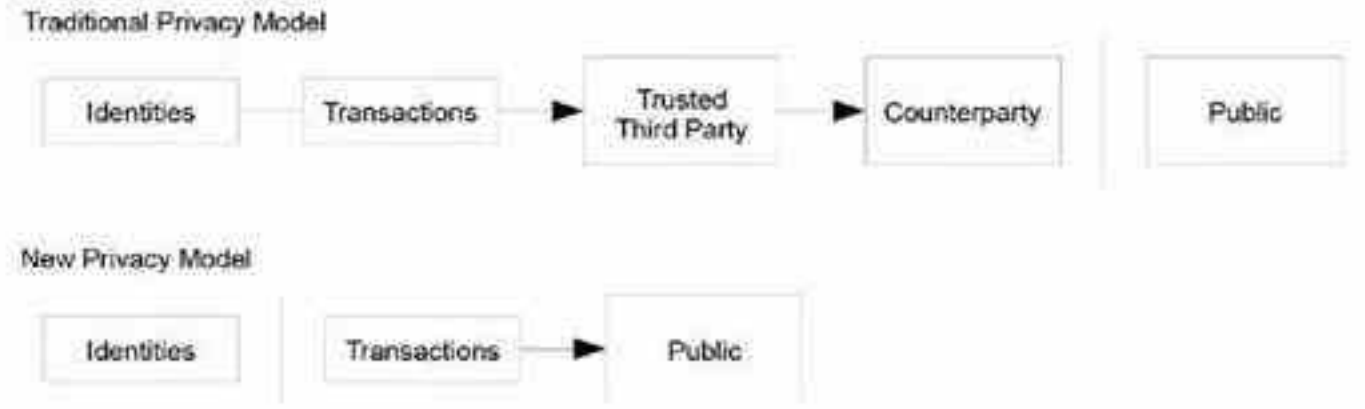


خاکہ

یہاں توجہ طلب بات یہ ہے کہ ''فین آؤٹ''(fan-out) قسم کے اِن پُٹ، کہ جب ایک ٹرانزیکشن کا انحصار کئی ٹرانزیکشنز پر ہو جبکہ وہ ٹرانزیکشنز خود بھی دیگر کئی (ٹرانزیکشنز) پر انحصار کر رہی ہوں، اس طریقے کے تحت کوئی مسئلہ نہیں۔ اس میں کسی ٹرانزیکشن کی تاریخ (ٹرانزیکشن ہسٹری) کی مکمل اور آزادانہ نقل حاصل کرنے کی کبھی ضرورت نہیں پڑتی۔

10۔ تخلیہ (پرائیویسی)

بینکاری کا روایتی ماڈل تخلیہ (پرائیویسی) حاصل کرنے کی غرض سے متعلقہ فریقین اور قابلِ بھروسہ فریقِ ثالث تک اطلاعات کی فراہمی (یا اطلاعات تک ان کی رسائی) کو محدود کر دیتا ہے۔ تمام منتقلیوں (ٹرانزیکشنز) کا عوامی طور پر اعلان کرنے کی ضرورت، اس انداز کی نفی کرتی ہے، لیکن پھر بھی اطلاعات کے بہاؤ کو ایک اور جگہ توڑتے ہوئے تخلیہ برقرار رکھا جاتا ہے: یعنی عوامی کلیدوں (public keys) کو گمنام رکھتے ہوئے۔ عام لوگ یہ تو دیکھ سکتے ہیں کہ ایک شخص کسی دوسرے شخص کو کچھ رقم بھیج رہا ہے، مگر اُن کے پاس ایسی کوئی اطلاع نہیں ہوتی جس کے ذریعے وہ اس (منتقلی) کو کسی سے بھی جوڑ سکیں۔ یہ بازارِ حصص (اسٹاک ایکسچینج) سے جاری ہونے والی اطلاعات سے مشابہت رکھتا ہے، جہاں انفرادی کاروبار کے وقت اور حجم کو، یعنی ''ٹیپ''(tape) کو، عوام کے سامنے پیش کیا جاتا ہے، لیکن یہ نہیں بتایا جاتا کہ فریقین کون تھے۔



خاکہ

ایک اضافی فائروال کی حیثیت سے، نئی کلیدوں کا ایک جوڑا(key pair)ہر ٹرانزیکشن کے لیے استعمال کیا جانا چاہیے تاکہ انہیں کسی عام مالک سے منسلک رہنے سے باز رکھ سکے۔تاہم زیادہ(multiple)اِن پُٹ والی ٹرانزیکشنز میں بعض رابطوں(linking)سے پھر بھی بچا نہیں جاسکتا، جو لازماً یہ ظاہر کردیتے ہیں کہ ان سے متعلق اِن پُٹس کسی یکساں شخص کی ملکیت تھے۔ خطرہ یہ ہے کہ اگر کسی ایک کلید کا مالک بھی ظاہر ہو گیا، تو(دیگر متعلقہ)رابطوں سے یہ بھی ظاہر ہو سکتا ہے کہ دوسری ٹرانزیکشنز بھی اسی مالک سے تعلق رکھتی ہیں۔

11۔حسابی عمل(Calculations)

ہم ایک منظر نامے پر غور کرتے ہیں جس میں ایک حملہ آور، دیانتدار زنجیر کے مقابلے میں زیادہ تیزی سے ایک متبادل زنجیر بنانے کی کوشش کر رہا ہے۔اگر یہ کام ہو بھی گیا، تب بھی اس سے نظام اٹکل پچو سے کی جانے والی تبدیلیوں کے لیے کھلا میدان نہیں بن جائے گا؛ جیسے کہ ایک غیر موجود قدر تخلیق کر لینا یا وہ رقم ہتھیا لینا جو حملہ آور کی تھی ہی نہیں وغیرہ۔ مقاماتِ اتصال(نوڈز)کسی ناجائز/باطل ٹرانزیکشن کو ادائیگی کے طور پر قبول نہیں کریں گے، اور دیانتدار نوڈز ایسا کوئی بلاک کبھی قبول نہیں کریں گی جس میں یہ(ناجائز یا باطل ٹرانزیکشنز)

شامل ہوں۔ حملہ آور اپنی ہی ٹرانزیکشنز میں سے کسی کو تبدیل کرنے کی کوشش کر سکتا ہے تاکہ اپنی حالیہ خرچ کردہ رقم واپس لے سکے۔

دیانتدار زنجیر اور حملہ آور زنجیر کے مابین دوڑ کی خصوصیات ایک "ثنائی جزافی چہل قدمی" (Binomial Random Walk) کے طور پر بیان کی جاسکتی ہیں۔ ہر کامیاب واقعہ (event) وہ ہے کہ جس میں دیانتدار زنجیر میں ایک بلاک کا اضافہ ہو رہا ہو، جو اس کی برتری کو 1+ کے بقدر بڑھا رہا ہو؛ جبکہ ناکام واقعہ وہ ہے کہ جس میں حملہ آور کی زنجیر میں ایک بلاک کا اضافہ ہو رہا ہو، اور فرق (gap) میں 1- کے بقدر کمی واقع ہو رہی ہو۔

یہ احتمال/امکان (probability) کہ حملہ آور کسی دیئے گئے خسارے کا ازالہ کرے، "جواری کی تباہی" والے مسئلے سے مشابہت رکھتا ہے۔ فرض کیجیے کہ جواری لامحدود ادھار (کریڈٹ) کے ساتھ ایک مخصوص خسارے سے ابتداء کرتا ہے اور اپنا نقصان برابر کرنے (breakeven) کی کوشش میں ممکنہ طور پر ان گنت مرتبہ بازیاں کھیلتا ہے۔ ذیل میں دیئے گئے طریقے پر عمل کرتے ہوئے ہم اس امکان کا حساب لگا سکتے ہیں کہ کیا وہ (جواری) کبھی "نہ نفع نہ نقصان" (بریک ایون) تک پہنچ پائے گا، یا یہ کہ حملہ آور کبھی دیانتدار زنجیر کے برابر پہنچ پائے گا (8):

p=امکان کہ دیانتدار نوڈ کو اگلا بلاک مل جائے گا

q=امکان کہ حملہ آور کو اگلا بلاک مل جائے گا

q_z=امکان کہ حملہ آور z بلاکس پیچھے سے بڑھتے ہوئے برابر پہنچ پائے گا

$$q_z = \begin{cases} 1 & if\ p \le q \\ (q/p)^z & if\ p > q \end{cases}$$

اس مفروضے کے پیش نظر کہ p بڑا ہے q سے (p > q)، اس بات کا امکان کہ حملہ آور کبھی دیانتدار نوڈ کے برابر پہنچ جائے گا، اسے (دیانتدار نوڈ تک پہنچنے کے لیے) درکار بلاکس کی تعداد بڑھنے کے ساتھ قوت نمائی انداز (exponentially) میں کم ہوتا چلا جائے گا۔ چونکہ اسے مشکلات کا سامنا ہوگا، اس لیے اگر اس نے شروع ہی میں بہت زیادہ تیز رفتار پیش رفت نہ دکھائی تو وہ مزید پیچھے ہوتا چلا جائے گا اور (دیانتدارانہ نوڈ کے برابر پہنچنے کے لیے) اس کے امکانات نہ ہونے کے برابر رہ جائیں گے۔

اب ہم دیکھتے ہیں کہ نئی ٹرانزیکشن کے وصول کنندہ کو اطمینان بخش حد تک یہ یقین کرنے کے لیے ارسال کنندہ اس ٹرانزیکشن کو تبدیل نہیں کر سکتا، کتنی دیر تک انتظار کرنا ہوگا۔ ہم فرض کرتے ہیں کہ ارسال کنندہ (sender) ایک حملہ آور ہے جو وصول کنندہ کو کچھ وقت کے لیے یقین دلانا چاہتا ہے کہ اس نے ادائیگی کر دی ہے، پھر (اس جعلی ادائیگی کو) کچھ وقت گزرنے کے بعد وہ اپنی جانب واپس منتقل (پے بیک) کر لیتا ہے۔ جونہی ایسا ہوگا، وصول کنندہ فوراً خبردار کر دیا جائے گا، لیکن ارسال کنندہ امید رکھتا ہے کہ تب تک بہت دیر ہو چکی ہوگی۔

وصول کنندہ، دستخط کرنے سے ذرا پہلے کلیدوں کا ایک نیا جوڑا (key pair) بناتا ہے اور ارسال کنندہ کو عوامی کلید (پبلک کی) فراہم کرتا ہے۔ اس طرح ارسال کنندہ کو موقع ہی نہیں مل پاتا کہ وہ وقت سے پہلے بلاکس کی زنجیر تیار کر سکے، اس پر مسلسل کام کرتے ہوئے، یہاں تک کہ وہ اتنا خوش نصیب ہو جائے کہ خاصا آگے نکل جائے؛ اور پھر اسی وقت ٹرانزیکشن کو عمل پذیر (ایگزیکیوٹ) کر دے۔ جب ایک بار ٹرانزیکشن بھیج دی گئی، تو بے ایمان ارسال

کنندہ خفیہ طور سے ایک اور متوازی زنجیر پر کام شروع کر دیتا ہے جس میں اس کی ٹرانزیکشن کا متبادل روپ (ورژن) ہوتا ہے۔

وصول کنندہ تب تک انتظار کرتا ہے کہ جب تک یہ ٹرانزیکشن کسی ایک بلاک میں شامل ہو جائے اور اس کے بعد z کی تعداد میں بلاکس جوڑے جا چکے ہوں۔ وہ ٹھیک نہیں جانتا کہ حملہ آور کس قدر پیش رفت کر چکا ہے، لیکن یہ فرض کرتے ہوئے کہ دیانتدار بلاکس نے ہر بلاک کے لیے اوسط متوقع وقت لیا ہوگا، حملہ آور کی ممکنہ پیش رفت ایک "پوائسن ڈسٹری بیوشن" (Poisson distribution) ہوگی جس کی متوقع قدر اس مساوات میں دی گئی ہے:

$$\lambda = z\frac{q}{p}$$

مساوات

یہ امکان معلوم کرنے کے لیے کہ حملہ آور اب بھی برابر پہنچ سکتا ہے، ہم اس کی ہر ممکنہ پیش رفت سے متعلق پوائسن کثافت (Poisson density) کو اس امکان/احتمال سے ضرب دیتے ہیں کہ جو وہ اس مقام سے (آگے بڑھ کر) برابر پہنچنے کے لیے رکھتا ہے:

$$\sum_{k=0}^{\infty} \frac{\lambda^k e^{-\lambda}}{k!} \cdot \begin{cases} (q/p)^{(z-k)} & \text{if } k \le z \\ 1 & \text{if } k > z \end{cases}$$

ریاضیاتی اظہاریہ

ڈسٹری بیوشن کی لامتناہی دُم سے بچنے کے لیے دوبارہ ترتیب دینے پر یہ حاصل ہوگا:

$$1-\sum_{k=0}^{z}\frac{\lambda^{k}e^{-\lambda}}{k!}\left(1-(q/p)^{(z-k)}\right)$$

ریاضیاتی اظہاریہ

اب اسے ہم ''سی''(C) لینگویج کے کوڈ میں تبدیل کریں گے:

```
#include <math.h>
double AttackerSuccessProbability(double q, int z)
{
double p = 1.0 - q;
double lambda = z * (q / p);
double sum = 1.0;
int i, k;
for (k = 0; k <= z; k++)
{
double poisson = exp(-lambda);
```

```
for (i = 1; i <= k; i++)
poisson *= lambda / i;
sum -= poisson * (1 - pow(q / p, z - k));
}
return sum;
}
```

کچھ نتائج چلانے کے بعد ہم دیکھ سکتے ہیں کہ z بڑھنے کے ساتھ امکان میں قوت نمائی انداز سے کمی آتی ہے:

```
q=0.1
z=0    P=1.0000000
z=1    P=0.2045873
z=2    P=0.0509779
z=3    P=0.0131722
z=4    P=0.0034552
z=5    P=0.0009137
z=6    P=0.0002428
z=7    P=0.0000647
z=8    P=0.0000173
```

z=9 P=0.0000046

z=10 P=0.0000012

q=0.3

z=0 P=1.0000000

z=5 P=0.1773523

z=10 P=0.0416605

z=15 P=0.0101008

z=20 P=0.0024804

z=25 P=0.0006132

z=30 P=0.0001522

z=35 P=0.0000379

z=40 P=0.0000095

z=45 P=0.0000024

z=50 P=0.0000006

اگر ہم اسے P کی قدر 0.1% سے کم کے لیے حل کریں تو:

$P < 0.001$

q=0.10 z=5

q=0.15	z=8
q=0.20	z=11
q=0.25	z=15
q=0.30	z=24
q=0.35	z=41
q=0.40	z=89
q=0.45	z=340

12۔ حرفِ آخر

ہم نے برقی متقلیوں (الیکٹرونک ٹرانزیکشنز) کے لیے ایک ایسا نظام تجویز کیا ہے جو بھروسے پر انحصار نہیں کرتا۔ ہم نے ڈیجیٹل دستخطوں سے بننے والے سکّوں کے عمومی فریم ورک سے شروع کیا جو ملکیت کو مضبوط کنٹرول فراہم کرتا ہے، لیکن دوہری ادائیگیوں سے بچنے کے کسی طریقے کے بغیر نامکمل ہے۔ اسے حل کرنے کے لیے ہم نے ثبوتِ کار (پروف آف ورک) استعمال کرتے ہوئے ہم نے P2P نیٹ ورک تجویز کیا جو متقلیوں کی عوامی تاریخ ریکارڈ کرتا ہے؛ اور جسے تبدیل کرنا کسی بھی حملہ آور کے لیے بڑی تیزی سے ناممکن العمل ہو جاتا ہے بشرطیکہ دیانتدار مقاماتِ اتصال، سی پی یو کی اکثریتی طاقت کنٹرول کر رہے ہوں۔ یہ نیٹ ورک اپنی غیر ساختیاتی سادگی (unstructured simplicity) کے نقطۂ نگاہ سے بہت مضبوط ہے۔ تمام مقاماتِ اتصال (نوڈز) معمولی تعاونِ باہمی کے ذریعے ایک ساتھ کام کرتے ہیں۔ انہیں شناخت کیے جانے کی بھی ضرورت نہیں، کیونکہ پیغامات کسی خاص مقام کے لیے نہیں بھیجے جاتے بلکہ انہیں صرف بہترین کوشش کی بنیاد پر پہنچایا جاتا ہے۔ مقاماتِ

اتصال اپنی مرضی سے نیٹ ورک چھوڑ سکتے ہیں اور اس میں دوبارہ شامل بھی ہو سکتے ہیں، جس کے لیے وہ ثبوتِ کار (پروف آف ورک) کی زنجیر کو اس کے ثبوت کے طور پر قبول کرتے ہیں جو ان کی عدم موجودگی میں ہو چکا ہے۔ وہ اپنے سی پی یو کی طاقت کے ساتھ ووٹ دیتے ہیں، یعنی جائز/درست بلاکس کی قبولیت کا اظہار کرنے کے لیے انہیں بڑھانے پر کام کرتے ہیں جبکہ ناجائز/باطل بلاکس پر کام کرنے سے انکار کرتے ہوئے انہیں مسترد کرتے ہیں۔ وسیع تر اتفاقِ رائے (consensus) پر مبنی اس نظام کے ساتھ کوئی سے بھی ضروری اصول اور ترغیبات/محرکات لاگو کیے جا سکتے ہیں۔

حوالہ جات (باب نمبر 2)

[1] W. Dai, "b-money," http://www.weidai.com/bmoney.txt, 1998.

[2] H. Massias, X.S. Avila, and J.-J. Quisquater, "Design of a secure timestamping service with minimaltrust requirements," In 20th Symposium on Information Theory in the Benelux, May 1999.

[3] S. Haber, W.S. Stornetta, "How to time-stamp a digital document," In Journal of Cryptology, vol 3, no2, pages 99-111, 1991.

[4] D. Bayer, S. Haber, W.S. Stornetta, "Improving the efficiency and reliability of digital time-stamping,"In Sequences II: Methods in Communication, Security and Computer Science, pages 329-334, 1993.

[5] S. Haber, W.S. Stornetta, "Secure names for bit-strings," In Proceedings of the 4th ACM Conferenceon Computer and Communications Security, pages 28-35, April 1997.

[6] A. Back, "Hashcash - a denial of service counter-measure," http://www.hashcash.org/papers/hashcash.pdf, 2002.

[7] R.C. Merkle, "Protocols for public key cryptosystems," In Proc. 1980 Symposium on Security andPrivacy, IEEE Computer Society, pages 122-133, April 1980.

[8] W. Feller, "An introduction to probability theory and its applications," 1957.

بِٹ کوائن

بٹ کوائن ایک کرپٹو کرنسی ہے اور دنیا بھر میں ادائیگی کے نظام کے طور پر جانا جاتا ہے۔ یہ پہلی غیر مرکزی ڈیجیٹل کرنسی ہے جس کا نظام کسی مرکزی بینک یا واحد ایڈمنسٹریٹر کے بغیر کام کرتا ہے۔ اس نیٹ ورک کا نظام پیئر-ٹو-پیئر کی بنیاد پر کام کرتا ہے جس میں صارفین براہ راست بغیر کسی مداخلت کے اپنی ٹرانزیکشنز ایک دوسرے کو بھیج یا وصول کر سکتے ہیں۔ نیٹ ورک پر موجود نوڈز ان تمام ٹرانزیکشنز کی پہلے تصدیق کرتے ہیں اور پھر ایک عوامی تقسیم شدہ لیجر میں ریکارڈ کرتے ہیں، جو بلاک چین کہلاتا ہے۔ بٹ کوائن کو ایک نامعلوم فرد یا گروہ نے تخلیق کیا۔ بٹ کوائن کے ساتھ ساتوشی ناکاموٹو کا نام عام طور پر سُننے کو ملتا ہے مگر یہ نہیں بتایا جا سکتا کہ یہ فرد کا نام ہے یا گروپ، جس کے ماتحت مختلف لوگ کام کرتے رہے تھے۔ اسے 2009 میں اوپن سورس سافٹ ویئر کے طور پر جاری کیا گیا۔

بٹ کوائن کا اجراء ایک عمل سے گزرنے پر انعام کے طور پر کیا گیا۔ یہ دیگر کرپٹو کرنسیز، اشیاء و مصنوعات سے اور خدمات (سروسز) میں تبادلے کے طور پر استعمال ہوتی ہے۔ فروری 2015 کے مطابق، دنیا بھر سے 1 لاکھ کے لگ بھگ تاجروں اور سوداگروں نے بٹ کوائن کے ذریعے پیسوں کی ادائیگی کو قبول کیا تھا۔ اور اب تو یہ تعداد دنیا کے تمام ممالک میں تیزی سے بڑھ رہی ہے۔

بٹ کوائن مائینگ

بٹ کوائن مائینگ ایک غیر مرکزی کمپی ٹیشنل Computational عمل ہے جو دو مقاصد کو پورا کرتا ہے۔

1۔ جب بہت زیادہ کمپیوٹنگ طاقت کو بلاک کے لئے استعمال کیا جاتا ہے اس وقت یہ قابل اعتماد طریقے سے ٹرانزیکشنز کی تصدیق کرتا ہے۔

2۔ ہر بلاک میں سے نئے بٹ کوائن جاری کرتا ہے۔

بٹ کوائن مائینگ بنیادی طور پر 5 مراحل میں کام سرانجام دیتا ہے۔

1۔ اس بات کی تصدیق کرتا ہے کہ معاملات درست ہیں۔

2۔ یہ ٹرانزیکشنز کو ایک بلاک میں بند کرتا ہے۔

3۔ سب سے حالیہ بلاک کا ہیڈر منتخب کرتا ہے اور اسے ہیش کے طور پر نئے بلاک میں استعمال کرتا ہے۔

4۔ پروف آف ورک کے مسئلے کو حل کرتا ہے۔ (ہم تھوڑی دیر میں اس کے عمل کو سیکھیں گے)

5۔ جب حل مل جاتا ہے تو نیا بلاک مقامی بلاک چین میں شامل کر دیا جاتا ہے اور نیٹ ورک پر موجود تمام صارفین کو مطلع کیا جاتا ہے۔

بٹ کوائن ٹرانزیکشنز اور بلاک کا سائز

کوئی بھی صارف اس نظام میں غیر مخصوص وقفوں سے ٹرانزیکشنز کو نشر کرتا ہے۔ تمام نشر شدہ ٹرانزیکشنز جن کو اس سسٹم میں شامل کرنا ہوتا ہے، مائینرز پر منحصر ہے، کیونکہ یہ مائینرز ہی ہوتے ہیں جو ان کو اکھٹا کر کے انہیں بلاک میں شامل کرتا ہے۔ بی ٹی سی (BTC) کے اس

نظام میں بلاک سائز کی حد 1 ایم بی (1000000 بائٹس) ہے جو کہ ایک بلاک میں محفوظ ہونے والی ٹرانزیکشنز پر حد مقرر کرتا ہے۔ اوسطاً بی ٹی سی ٹرانزیکشن کا سائز تقریباً 495 بائٹس ہوتا ہے۔

بلاک سائز کی یہ حد بڑے بلاک بنانے سے روکتا ہے جو کہ نیٹ ورک میں رکاوٹ کا باعث بن سکتے ہے۔

بی ٹی سی کی کتنی ٹرانزیکشنز بٹ کوائن کے ایک بلاک کو بھرتی ہیں؟

اس بات کا پتہ اس فارمولے سے باآسانی جانا جا سکتا ہے۔

$$\text{اوسط ٹرانزیکشن فی بلاک} = \frac{\text{زیادہ سے زیادہ بلاک سائز}}{\text{اوسط ٹرانزیکشن سائز}}$$

$$= \frac{\text{1000000 بائٹس}}{\text{495 بائٹس}} = \text{2020 ٹرانزیکشنز}$$

ٹرانزیکشنز میں استحکام اور کم وقت میں جواب موصول کرنے کے لئے، نیٹ ورک ہر 10 منٹ میں ایک بلاک پیدا کرنے کی کوشش کرتا ہے۔ ہر 10 منٹ کے بعد مائینز کو ایک نیا بلاک ملتا ہے۔ 10 منٹوں میں 600 سیکنڈ ہیں۔ ہر سیکنڈ میں عمل درآمد ہونے والی ٹرانزیکشنز کا حساب اس فارمولے سے لگایا جا سکتا ہے۔

$$\frac{\text{بلاک میں ٹرانزیکشنز کی تعداد}}{\text{بلاک کا وقت سیکنڈ میں}}$$

$$\frac{\text{2020 ٹرانزیکشنز}}{\text{600 سیکنڈز}} = \text{3.37 ٹرانزیکشنز فی سیکنڈ}$$

بی ٹی سی نے بلاک سائز کے لئے ایک اچھی سطح کی حد متعین کی ہے جو باآسانی پوری ہو جاتی ہے۔ وہ ٹرانزیکشنز جو اپنے حالیہ وقت میں عملدرآمد نہیں ہو پاتیں وہ اگلے بلاک میں داخل ہو

جاتی ہیں۔ ٹرانزیکشن کے انتخاب میں ترجیح ان ٹرانزیکشنز کو دی جاتی ہے جس میں بڑی ٹرانزیکشن فیس شامل ہو۔

پروف آف ورک کیا ہے؟

پروف آف روک وہ طریقہ کار ہے جو اس بات کا تصدیق کرتا ہے کہ وقت، قیمتی ہارڈ ویئر اور بجلی کے لحاظ سے بنائے جانے والا نیا بلاک مشکل سے بنتا ہے۔ اس عمل میں مائینز کو ایک منفرد ہیش نمبر تلاش کرنا ہوتا ہے جسے ٹارگیٹ ویلیو (ھدف قیمت) سے ضرور کم ہونا چاہیئے۔ اس نظام میں یہی پروسیس سب سے زیادہ وقت لیتا ہے۔

پروف آف ورک کے کام کرنے کے طریقے کو تفصیل سے سمجھنے کے لئے تصویر نمبر 1 ملاحظہ کریں۔

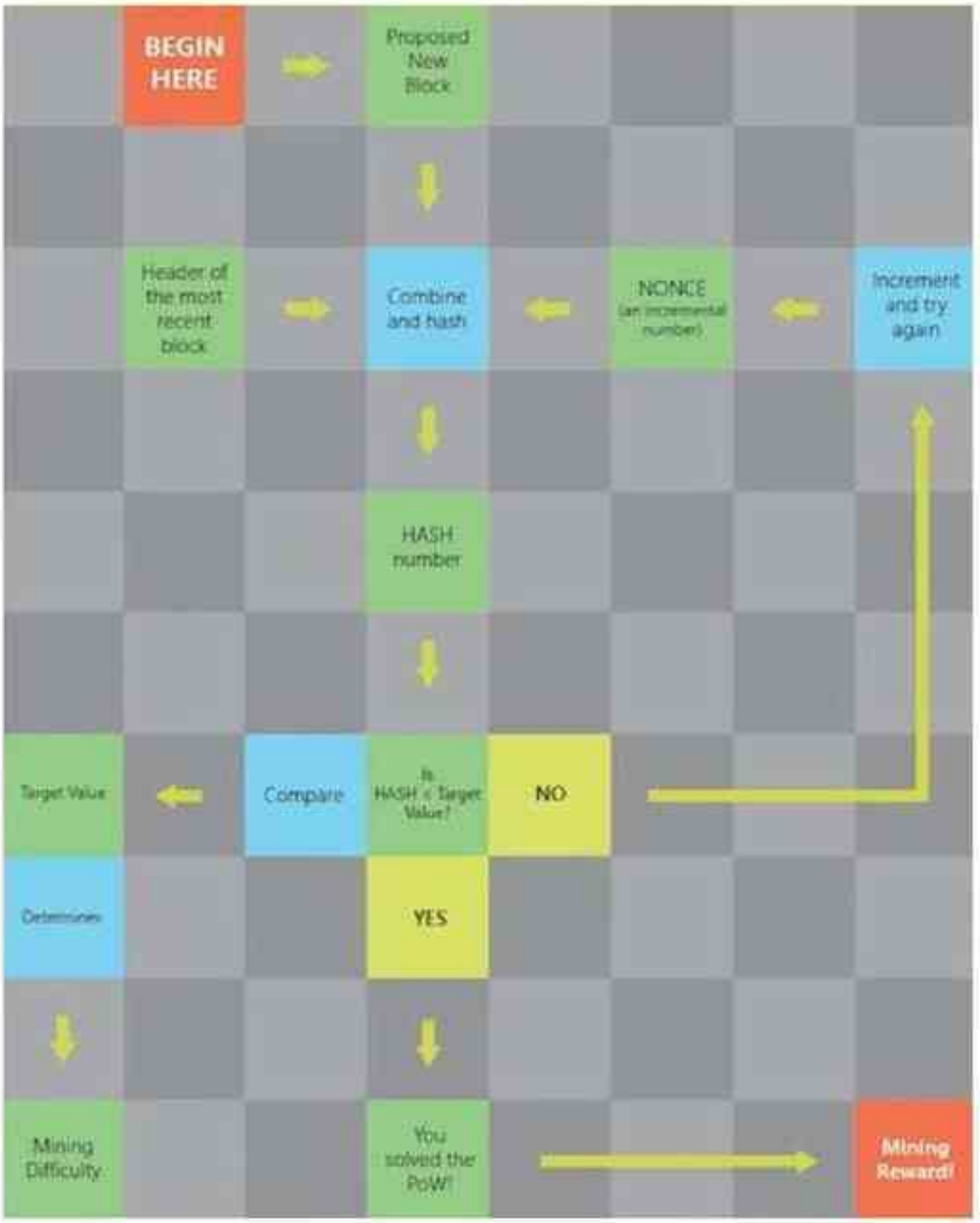
جب ایک نیا بلاک بنانے کی تجویز پیش کی جاتی ہے تو اس کے ساتھ دو کام ہونے ہیں۔

1)۔ حالیہ بلاک کا ہیڈر اٹھایا جاتا ہے۔

2)۔ نانس (Nance) (ایک ہندسہ) لیا جاتا ہے۔

ان دونوں کو ملا کر ایک ہیش نمبر نکالا جاتا ہے جس کا موازنہ ٹارگیٹ ویلیو سے کیا جاتا ہے۔

اگر جاری شُدہ ہیش نمبر ٹارگیٹ ویلیو سے چھوٹا ہو تو پروف آف ورک کا مسئلہ حل ہو گیا، بلاک کو نیٹ ورک میں شامل کر لیا جاتا اور آپ کو مائینگ کا انعام مل جاتا ہے۔ اور اگر ہیش نمبر ٹارگیٹ ویلیو سے چھوٹا نہ ہو تو نینس کی ویلیو میں ایک نمبر کا اضافہ کر کے اور حالیہ بلاک کا ہیڈر سے ملا کر پھر سے ایک نیا ہیش نمبر نکالا جاتا ہے اور پھر سے اس کا موازنہ ٹارگیٹ ویلیو سے کیا جاتا ہے۔ یہ سلسلہ اس وقت تک چلتا رہتا ہے جب تک کہ جاری شُدہ ہیش نمبر ٹارگیٹ ویلیو سے چھوٹی نہ نکل آئے۔



تصویر نمبر 1

ٹارگیٹ ویلیو اور مائینگ ڈیفیکلٹی کیا ہے؟

ٹارگیٹ ویلیو ایک 256 بٹ پر مبنی ایک بہت بڑا نمبر ہے جسے بٹ کوائن کے تمام صارفین سے شئیر کیا جاتا ہے۔ ٹارگیٹ ویلیو کا تعین مائینگ ڈیفیکلٹی سے ہوتا ہے۔ مائینگ ڈیفیکلٹی جسے آپ

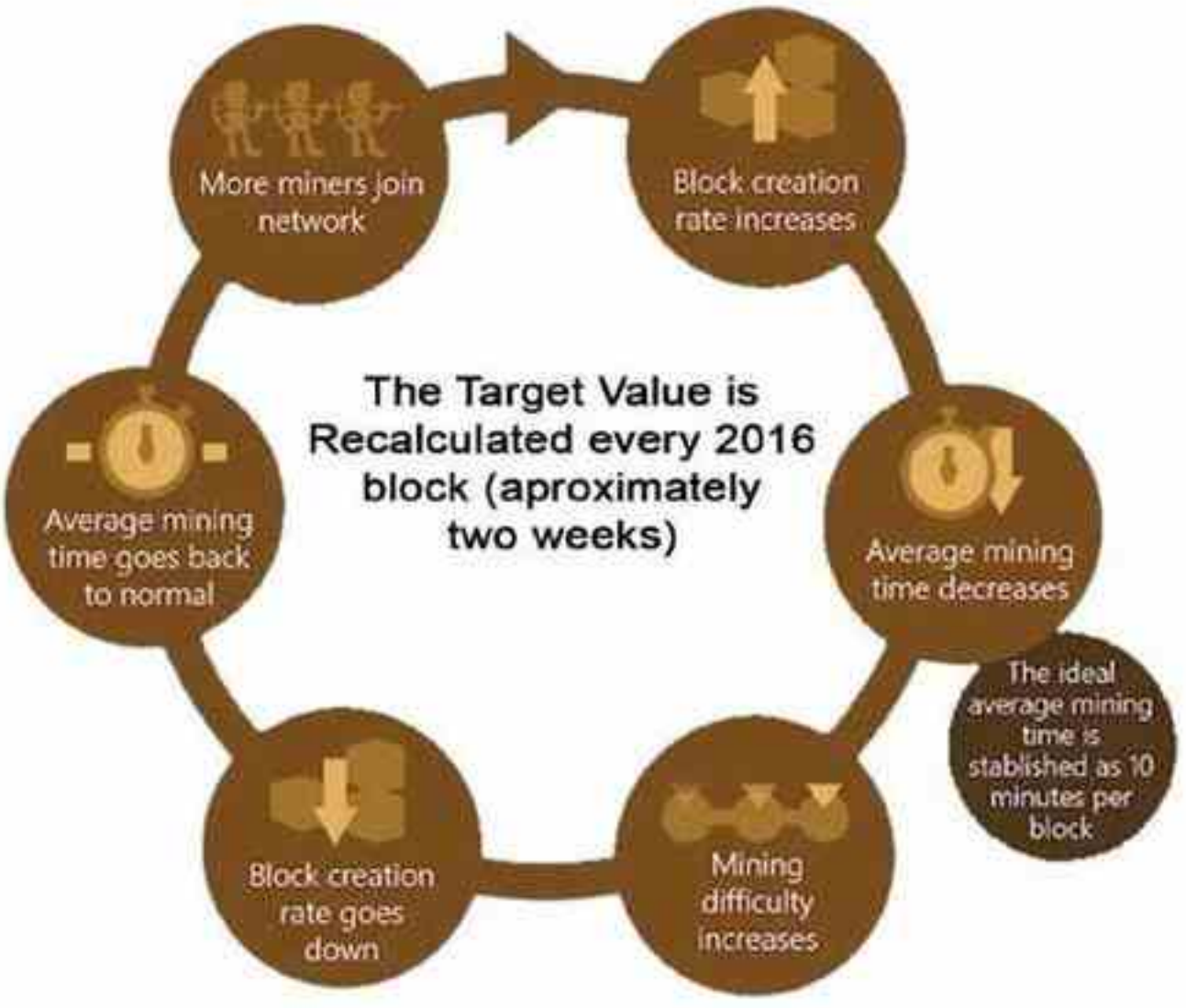
مائینگ کی مشکل بھی کہہ سکتے ہیں۔ یہ ایک جانچنے کا پیمانہ ہے جو یہ بتاتا ہے کہ پروف آف ورک کے دوران ایک ایسے ہیش ویلیو کو ڈھونڈنا کتنا مشکل ہے جو ٹارگیٹ ویلیو سے چھوٹی ہو۔

☆اگر مائینگ ڈیفیکلٹی زیادہ ہے تو ٹارگیٹ ویلیو کم ہو گی۔

☆اگر مائینگ ڈیفیکلٹی کم ہے تو ٹارگیٹ ویلیو زیادہ ہو گی۔

مائینگ ڈیفیکلٹی دو عوامل پر منحصر ہے: 1)۔ بلاک کے بنانے کی شرح 2)۔ اوسطاً مائینگ کا وقت۔ نیچے دی گئی تصویر سے بھی مائینگ ڈیفیکلٹی کو سمجھا جا سکتا ہے۔

نیٹ ورک پر ہر 10 منٹ میں ایک نیا بلاک نکلتا ہے۔ ہر 2016 بلاکس کے بعد، جو کہ تقریباً 2 ہفتے لیتے ہیں، بٹ کوائن کا ہر صارف ان دو ہفتوں میں نکلنے والے نئے بلاکس اور ان پر لگنے والے وقت کا موازنہ کرتا ہے اور ٹارگیٹ ویلیو کو چند فیصد فرق کے ساتھ تبدیل کرتا ہے۔ پروف آف ورک میں یہ ٹارگیٹ ویلیو ہی اصل میں مسئلے کو کم یا زیادہ مشکل بناتی ہے۔



تصویر نمبر2

حوالہ جات

https://blockchain.info/charts/n-transactions-per-block

https://www.bitcoinplus.org/blog/block-size-and-transactions-second

https://www.bitcoinmining.com/

بین الاقوامی ممالک میں بِٹ کوائن کی قانونی حیثیت

لوگوں میں کرپٹو کرنسی، خاص کر بٹ کوائن کا رجحان تیزی سے بڑھ رہا ہے۔اس باب میں ہم دنیا بھر کے ممالک کی سرکاری حکومتوں کا کرپٹو کرنسی کی طرف رویہ دیکھتے ہیں۔ کچھ ممالک کرپٹو کرنسی کے گلوبل وکلاء بن گئے ہیں، جبکہ دیگر نے اسے مختلف رنگ دے کر مکمل طور پر ممنوع قرار دے دیا ہے۔ جاپان کا نام قابل ذکر ہے جس نے بٹ کوائن کو قانونی ٹینڈر کے طور پر قبول کیا ہے۔ جب کہ دوسری طرف بنگلہ دیش نے 2014 میں یہ قانون پاس کیا تھا کہ اگر کوئی فرد ورچیول (کرپٹو) کرنسی استعمال کرتا ہوا پکڑا گیا تو اسے 12 سال تک کی جیل کی سزا سنائی جائے گی۔

کسی بھی ملک کی انفرادی صورتحال سے بالائے نظر، گزشتہ دہائی سے کرپٹو کرنسیز کے بڑھتے ہوئے رجحان سے پتہ چلتا ہے کہ نئی ٹیکنالوجی کو جلد یا بدیر سب اپنا کے ہی رہیں گے۔ ایسٹونیا، ریاست ہائے متحدہ امریکہ، ڈنمارک، سویڈن، جنوبی کوریا، نیدرلینڈ، فن لینڈ، کینیڈا، برطانیہ اور آسٹریلیا دنیا کے ٹاپ 10 بٹ کوائن دوست ممالک ہیں جن کی عوام نے یا حکومت نے یا پھر دونوں نے اس جدید ٹیکنالوجی کو فوراً ہی اپنا لیا تھا۔

اب تک کل 7 ممالک نے بٹ کوائن کو اثاثے کے طور پر قبول کیا ہے، 2 نے بارٹر، 6 نے پیسہ، 1 نے تجارت اور ٹینڈر کے طور پر قبول کیا ہے۔ تقریباً 17 ممالک نے اس کی قانونی حیثیت واضح نہیں کی۔ اس کے برعکس، کل 10 ممالک نے واضح الفاظ میں بٹ کوائن اور کرپٹو کرنسی

کے استعمال کو غیر قانونی قرار دے دیا ہے اور دیگر ممالک ابھی تک کوئی حتمی فیصلہ نہیں لے سکے۔

درج ذیل فہرست میں بین القوامی ممالک اور ان میں بٹ کوائن کی قانونی حیثیت بتائی جارہی ہے۔ جن ممالک نے بٹ کوائن کو قانونی طور پر قبول کر لیا ہے وہاں اس کی قانونی حیثیت بھی واضح کر دی گئی ہے۔

نمبر	ملک	تاریخ	حیثیت	تفصیل
1	آسٹریلیا	دسمبر 2014	پیسہ	آسٹریلیا کی حکومت نے بٹ کوائنز کو پیسے کے طور پر استعمال کرنے کا درجہ دیا ہے۔ اور اس پر سے ڈبل ٹیکس پالیسی بھی ہٹا دی گئی ہے۔
2	برازیل	اپریل 2014	اثاثہ	برازیل کی حکومت نے اعلان کیا ہے کہ بٹ کوائن ایک کرنسی نہیں بلکہ اثاثہ ہے اور اس پر ٹیکس 15 فیصد لاگو ہو گا۔
3	بلغاریہ	اپریل 2014	اثاثہ	بلغاریہ نے ڈیجیٹل کرنسی کو اثاثے کے طور پر قبول کیا ہے اور اس پر ٹیکس 10 فیصد لاگو ہو گا۔

4	کینیڈا	نومبر 2013	بارٹر	کینیڈا ریونیو ایجنسی نے نومبر 2013 میں اعلان کیا کہ بٹ کوائن کی ادائیگیوں کو بارٹر (لین دین) کے طور پر استعمال کیا جائے۔
5	چلی	2015	قانونی	2015 میں سب سے پہلے بٹ کوائن ایکسچینج کو حکومت کے فنڈ کی مدد سے شروع کیا گیا تھا جہاں شہری پیسوں کے بدلے بٹ کوائن خرید سکتے تھے۔
6	کروشیا	دسمبر 2016	قانونی	6 دسمبر، 2013 کو کروشیا نیشنل بینک نے مبینہ طور پر ڈیجیٹل کرنسیوں کی گردش پر ایک بحث کا آغاز کیا اور نتیجہ یہ اخذ کیا کہ بٹ کوائن غیر قانونی نہیں ہے۔
7	ڈنمارک	مارچ 2014	قانونی	ڈنمارک کی حکومت اور مالی نگرانی اتھارٹی نے اعلان کیا ہے کہ بٹ کوائن کے کاروبار پر عام ٹیکس ہی لاگو کیا جائے گا۔

8	ایسٹونیا	فروری2014	پیسہ	بٹ کوائن اور ڈیجیٹل کرنسیوں کو ایک متبادل ادائیگی کے طور پر ااستعمال کیا جاسکتا ہے۔
9	فن لینڈ	نومبر2014	اثاثہ	فینیش ریگولیٹری باڈی نے اعلان کیا تھا کہ بٹ کوائن کو ایک اثاثہ کے طور پر استعمال کیا جاسکتا ہے۔
10	جرمنی	اگست2013	تجارت	جرمن حکومت نے اگست 2013 میں ایک رپورٹ جاری کی جس میں کہا گیا تھا کہ بٹ کوائنز کو ایک تجارتی سرگرمی کے طور پر استعمال کیا جاسکتا ہے اور اس بدولت سرمایہ کاروں پر ایک سال بعد ٹیکس بھی لاگو ہو گا۔
11	آئس لینڈ	2017	قانونی	مرکزی بینک آف آئس لینڈ نے 2014 میں بٹ کوائن اور دیگر ڈیجیٹل کرنسیوں میں کی جانے والی ٹرانزیکشنز پر پابندی عائد کر دی گئی تھی لیکن

				2017 میں، مرکزی بینک نے کچھ قواعد متعارف کیئے جن کی بدولت پچھلی عائد شدہ پابندیاں ختم کردی گئیں۔[1]
12	اسرائیل	فروری 2014	اثاثہ	اسرائیلی حکومت بٹ کوائن پر ٹیکس لاگو کررہی ہے۔
13	اٹلی	فروری 2014	پیسہ	اٹلی حکومت نے بٹ کوائن کو کرنسی کے طور پر قبول کیا ہے۔
14	جاپان	مارچ 2014	ٹینڈر	جاپان نے 1 اپریل، 2017 میں بٹ کوائن ٹریڈنگ پر ٹیکس ختم کرکے اب اسے باضابطہ طور پر قانونی ٹینڈر کی حیثیت دی دے ہے۔
15	قازقستان	فروری 2014	قانونی	قازقستان نے جون 2017 میں بلاک چین کو فروغ دینے کا اعلان کیا اور صدر مملکت نے اعلان کیا کہ اب انٹرنیشنل پیمنٹس کے لیے ایک یونٹ تشکیل دے لینی چاہیئے۔

[1] https://cointelegraph.com/bitcoin-for-beginners/is-bitcoin-legal#germany

16	لیگزمبرگ	مارچ2014	قانونی	اپریل2016میں حکومت نے بٹ کوائن ایکسچینج کے ادارے کو لائسنس دیا، جس سے کمپنی دنیا کی سب سے پہلی قومی لائسنس یافتہ ایکسچینج بن گئی۔
17	مراکش	نومبر2017	اثاثہ	15نومبر2017میں مراکش کی ڈیجیٹل سروسز مہیا کرنے والی کمپنی ایم ٹی ڈی ایس نے پیسوں کی وصولی کے لئے بٹ کوائن کو متعارف کرایا۔19 دسمبر2017کو بینک المغرب کے گورنر عبدالطیف جوہری نے پریس کانفرس میں کہا کہ بٹ کوائن ایک کرنسی نہیں ہے بلکہ ایک مالی اثاثہ ہے۔
18	نیدرلینڈز	جون2013	بارٹر	جون2013میں، ڈچ فنانس وزیر نے ایک رپورٹ جاری کی جس نے بکٹوئن کو بارٹر کی حیثیت دی۔

19	نائیجیریا	جنوری 2017	متنازعہ	17 جنوری 2017 کے مطابق، مرکزی بینک آف نائجیریا (سی بی عن) نے نائجیریا کے تمام بینکوں کو مطلع کرنے کے لئے ایک سرکلر منظور کیا تھا جس میں نائیجیریا میں بٹ کوائن اور دیگر کرپٹو کرنسیز پر پابندی لگادی گئی تھی۔ بعد میں اس بات کی تردید کرتے ہوئے سی بی عن کے ڈپٹی ڈائریکٹر نے کہا کہ بٹ کوائن اور بلاک چین کو مرکزی بینک کنٹرول نہیں کر سکتا، جیسے انٹرنیٹ کو کوئی کنٹرول نہیں کر سکتا۔ لیکن ابھی تک واضح فیصلہ نہیں سامنے آیا۔
20	فلپائن	فروری 2017	قانونی	بی ایس ایس فلپائن سینٹرل بینک نے باقاعدہ جائزادائیگی کے طریقہ کار کے طور پر بٹ کوائن کو تسلیم کیا ہے۔

21	پولینڈ	مئی2014	قانونی	پولینڈ نے سرکاری طور پر کرپٹو کرنسیز کی ٹریڈنگ اور مائننگ کو تسلیم کیا ہے لیکن ساتھ ہی کہا ہے کہ ریگولیشن یورپی یونین سے آنی چاہئے۔
22	سلووینیا	دسمبر2013	قانونی	سلووینیا نے دسمبر2013 میں ایک درمیانی راہ اختیار کی اور اعلان کیا کہ بٹ کوائن نہ تو مالی اثاثے ہے اور نہ ہی کرنسی۔اس کے استعمال کے مطابق ٹیکس لگایا جائے گا۔
23	جنوبی افریقہ	فروری2014	قانونی	جنوبی افریقی ریوینیو سروس نے کہا ہے کہ بٹ کوئن کی کسی بھی قسم کی ٹرانزیکشن پر عام ٹیکس لاگو ہوگا۔
24	جنوبی کوریا	فروری2014	متنازعہ	فی الحال بٹ کوائن کے استعمال کو منظم کرنے کے لئے جنوبی کوریا نے کوئی قانون نہیں بنایا لیکن لوگ باآسانی 11-7-(سیون-ایلیوں)سٹورز سے

				بٹ کوائن خرید سکتے ہیں۔
25	اسپین	فروری2014	قانونی	اسپین کرپٹو کرنسی ریگولیٹری فریم ورک قائم کر رہا ہے اور حکومت نے کرپٹو کرنسی کو ٹیکس سے مستثنیٰ قرار دے دیا ہے۔ اسپین کے تقریباً ہر اسٹور پر بٹ کوائن استعمال ہو رہا ہے۔
26	سویڈن	جولائی2014	پیسہ	ریگولیٹر نے بٹ کوائن کو عوامی کرنسی کے طور پر قبول کیا ہے۔
27	سوئٹزرلینڈ		اثاثہ	سوئٹزرلینڈ کے مالیاتی ریگولیٹر نے پہلے نجی سوئس بینک کی منظوری دی ہے جو بٹ کوائن اثاثوں کے انتظام کو سنبھالے گا۔
28	سعودی عرب		قانونی	سعودی عرب میں کسی بھی سرکاری پارٹی کی طرف سے بٹ کوائن کے استعمال پر اعتراض نہیں کیا گیا ہے۔ صرف سعودی عرب کے

				مُنیٹری کمیٹی (ساما) نے اسے استعمال کرنے سے خبر دار کیا ہے اور کہا ہے کہ اس کے ڈیلروں کو کسی بھی تحفظ یا حقوق کی ضمانت نہیں دی جائے گی۔
29	برطانیہ	مارچ 2015	پیسہ	بینک آف انگلینڈ میں بٹ کوائن ٹیکنالوجی کی ابھی بھی جانچ پڑتال جاری ہے پھر بھی اسے نجی پیسے کی حیثیت دے رکھتی ہے۔
30	ریاست ہائے متحدہ امریکہ	مارچ 2014	قانونی	کرپٹو کرنسی کے صارفین اور بٹ کوائن کے اے ٹی ایمز پوری دنیا کے مقابلے میں سب سے زیادہ امریکہ میں پائے جاتے ہیں اور بٹ کوائن کی تجارت بھی زیادہ ہے۔ امریکہ میں ابھی بھی بہت سی ریاستیں ایسی ہیں جنہوں نے ابھی تک کرپٹو کرنسی کو قانونی طور پر قبول نہیں کیا جیسا کہ :

				نیویارک، نیو ہیمپشائر، کنیکٹک، ہواوئے، جورجیا، شمالی کیرولینا، واشنگٹن اور نیو میکسیکو وغیرہ۔ ٹیکساس، کینساس، ٹینیسی، جنوبی کیرولینا اور مونٹانا، یہ وہ ریاستیں ہیں جہاں کرپٹو کرنسیز کو حکومتی سطح پر اپنایا گیا ہے اور باقی کی 37 ریاستوں کا فیصلہ ابھی تک واضح نہیں ہے۔
31	البانیہ	مئی 2015	متنازعہ	البانیہ کے مرکزی بینک نے سرمایہ کاروں کے لئے ڈیجیٹل کرنسیز خریدنے یا ٹرانزیکشنز کے طور پر اپنانے کے خطرات کے بارے میں انتباہ جاری کی ہے۔[2]
32	ارجنٹائن	اپریل 2015	متنازعہ	بٹ کوائن قانونی کرنسی نہیں ہے کیونکہ یہ حکومتی مالیاتی اتھارٹی کی طرف سے جاری

[2] https://www.ccn.com/albanian-central-bank-issues-warning-bitcoin-investors/

				شدہ نہیں ہیں اور نہ ہی قانونی ٹینڈر کی حیثیت رکھتی ہے۔
33	بیلاروس	دسمبر 2017	قانونی	بیلاروس نے نجی سیکٹر کی ترقی اور غیر ملکی سرمایہ کاری کو فروغ دینے کیلئے کرپٹو کرنسیوں میں ٹرانزیکشن کو قانونی طور پر اپنایا ہے۔[3]
34	ڈومینیکن ریپبلک	اپریل 2016	متنازعہ	مرکزی بینک کا کہنا ہے کہ کرپٹو کرنسیز کو قانونی طور پر حمایت حاصل نہیں ہے اور ساتھ ہی مرکزی بینک نے بٹ کوائن اور دیگر کرپٹو کرنسیز کے استعمال پر انتباہ جاری کر دی تھی۔[4] اس کے باوجود ملک کے 3 شہروں میں بٹ کوائن اے ٹی ایم نصب ہیں۔[5]

[3] https://www.reuters.com/article/us-belarus-cryptocurrency/belarus-adopts-crypto-currency-law-to-woo-foreign-investors-idUSKBN1EG0XO

[4] https://dominicantoday.com/dr/economy/2017/06/29/central-bank-says-virtual-currencies-dont-have-legal-backing/

[5] https://coinatmradar.com/country/61/bitcoin-atm-dominican-republic/

53	آسٹریا	مارچ2014	متنازعہ	حکومتی سطح پر ابھی تک کوئی قانون یا پالیسی نافذ نہیں کی گئی۔
63	بیلجیم	جنوری2014	متنازعہ	حکومت نے بٹ کوائن کے بارے میں کوئی موقف جاری نہیں کیااور دوسرے یورپی ملکوں کی طرح یورپی یونین کی ہدایات کا منتظر ہے۔
73	کولمبیا	مارچ2014	متنازعہ	کولمبیانے کہاہے کہ کرپٹو کرنسی غیر قانونی نہیں ہے لیکن ساتھ ہی یہ کہاہے کہ یہ اسے جلدی قبول نہیں کریں گے۔
83	چین	مارچ2014	قانونی	پیپلز بینک آف چائینا(پی بی او سی)نے تمام مالیاتی اداروں پر بٹ کوائن سے متعلقہ ٹرانزیکشن، خرید وفروخت، قیمتوں کا تعین کرناوغیرہ پر پابندی لگائی ہے۔ جبکہ عام عوام میں بٹ کوائن کااستعمال باطور

				تجارت قانونی ہے۔
93	چیک ریپبلک	جنوری 2014	قانونی	چیک ریپبلک حکومت نے حال ہی میں ایک قانون متعارف کرایا ہے جس میں کرپٹو کرنسی ایکسچینجز کو اپنے گاہکوں کی شناخت محفوظ رکھنے کے لئے کہا گیا ہے۔اس کے علاوہ، عوام پر مستقبل قریب میں کرپٹو کرنسیوں پر ویلیو ایڈڈ ٹیکس لاگو کیا جائے گا۔
40	سائپرس	دسمبر 2013	متنازعہ	بٹ کوائن کا استعمال سائپرس میں منظم نہیں ہے۔11 دسمبر 2013 کو سائپرس کے مرکزی بینک نے بٹ کوائن پر ایک بیان جاری کیا کہ کسی بھی قسم کی کرپٹو کرنسی کا استعمال خطرناک ہے کیونکہ یہ کسی بھی ریگولیٹری نظام کے تحت نہیں ہے اس لئے اس کے استعمال کو غیر مقفل کیا جاتا ہے۔

41	فرانس	جنوری2014	متنازعہ	فرانسیسی حکومت نے ٹیکنالوجی میں کچھ دلچسپی ظاہر کی ہے، لیکن اعلیٰ احکام کے مطابق اس میدان میں ابھی تک اہم پہلوؤں کا آغاز نہیں ہوا ہے۔
42	یونان	فروری2014	متنازعہ	بٹ کوائن پر کوئی مخصوص قانون ابھی تک نہیں بنایا گیا ہے اور نہ ہی نیشنل بینک اُف یونان نے بٹ کوائن پر کوئی بیان جاری کیا ہے۔
34	ہانگ کانگ	جنوری2014	متنازعہ	ہانگ کانگ مَنی اتھارٹی نے بٹ کوائن ٹریڈ نگ سے کسی بینک کو باقاعدہ طور پر نہیں روکا اور نہ ہی کسی بینک نے حکومت سے واضح احکامات طلب کئے۔
44	ہنگری	فروری2014	متنازعہ	نیشنل بینک آف ہنگری نے کرپٹو کرنسی کے استعمال پر شہریوں کو انتباہ جاری کی ہے۔
54	بھارت	جنوری2014	متنازعہ	جیسا کہ بٹ کوائن پہلے ہی سے وسیع پیمانے پر بھارت میں

				استعمال ہو رہا ہے لیکن پھر بھی ابھی تک واضح قانون نافذ نہیں کیا گیا جو یہ بتا سکے کہ آیا بھارت میں بٹ کوائن اور دیگر کرپٹو کرنسیز کا استعمال قانونی ہے یا نہیں۔
64	انڈونیشیا	فروری 2014	متنازعہ	بٹ کوائن انڈونیشیا کی مارکیٹ میں استعمال ہو رہا ہے لیکن حکومت نے ابھی تک اسے کوئی قانونی حیثیت نہیں دی۔
47	آئرلینڈ	جنوری 2014	متنازعہ	کرپٹو کرنسی کو آئرلینڈ میں قانونی حیثیت حاصل نہیں لیکن بینک آف آئرلینڈ کی انوویشن ٹیم، ڈیلیوٹ کمپنی کے ساتھ مل کر تجربات کر رہی ہے جن سے ظاہر ہوتا ہے کہ بلاک چین ٹیکنالوجی خودکار طریقے سے ٹرانزیکشنز کو ٹریس کرنے کے لئے استعمال کیا جا سکتا ہے اور یہ یورپی یونین کے مالیاتی

				قوانین کے ہم آہنگ بھی ہے۔
48	ایران	مارچ2014	متنازعہ	ایرانی مرکزی بینک نے کرپٹو کرنسی پر انتظار کی پالیسی اختیار کر رکھی ہے. گو کہ ملک میں اس کی حیثیت غیر قانونی ہے لیکن ابھی تک پولیس نے اسے روکنے کے لئے کوئی قانونی مینڈیٹ تیار نہیں کی۔ 2013میں 15 سرکاری اداروں کے ایک گروپ نے ملک میں ڈیجیٹل کرنسیز کو ریگولیٹ کرنے کے لئے ایک فریم ورک کی تیاری پر کام کرنا شروع کر دیا تھا لیکن ابھی تک حتمی فیصلہ سامنے نہیں آتا۔[6]
49	اردن	فروری2014	متنازعہ	اردن کی حکومت نے بٹ کوائن اور دیگر کرپٹو کرنسیز کے استعمال پر انتباہ جاری کی ہے۔ اردن کے مرکزی بینک نے

[6] https://financialtribune.com/articles/economy-business-and-markets/66396/iran-digital-currency-regulation-on-the-way

				بینکوں، کرنسی ایکسچینجز، مالیاتی کمپنیوں اور ادائیگی سروس کمپنیوں کو بٹ کوائن اور دیگر ڈیجیٹل کرنسیوں کے استعمال سے منع کیا ہے اور اس کے خطرات سے عوام کو خبردار کیا ہے۔ جبکہ بٹ کوائن اب بھی چھوٹے سطح کے کاروبار اور تاجروں کی طرف سے قبول کئے جارہے ہیں۔
50	جمیکا	اپریل 2016	متنازعہ	نیشنل سینٹرل بینک اور بینک آف جمیکا نے اعلان کیا ہے کہ ٹیکنالوجیز کے استحصال کے لئے مواقع پیدا کرنا لازمی ہے جس میں کرپٹو کرنسیز بھی شامل ہیں۔
51	کینیا		متنازعہ	مرکزی بینک آف کینیا (سی بی کے) نے خبردار کیا ہے کہ کرپٹو کرنسیز غیر محفوظ ہے اور دہشت گردوں تک فنڈز

				پہنچانے کا کام دے سکتے ہیں۔
52	لاتویا	فروری2014	متنازعہ	جس دن لاتویا کی قومی ایئرلائن نے اعلان کیا کہ وہ متبادل ادائیگی کے طور پر بٹ کوائن کو قبول کرے گی۔اس کے آگے ہی دن حکومت نے بٹ کوائن اور دوسری کرپٹو کرنسیز پر انتباہ جاری کر دی۔
53	لبنان	2013	متنازعہ	لبنان کے مرکزی بینک نے 2013میں بٹ کوائن پر انتباہ جاری کی کہ ملک کے تمام مالیاتی اداروں میں بٹ کوائن کا استعمال ممنوعہ ہے۔ لیکن عام عوام کے لئے کوئی حکم جاری نہیں کیا گیا۔
54	لیتھونیا	فروری2014	متنازعہ	لیتھونیا نے ویٹ-اینڈ-واچ (انتظار) کی پالیسی اپنا رکھی ہے یہ دیکھنے کے لئے کہ یورپ بٹ کوائن کے لئے کیا پالیسی اپناتا ہے۔

55	مالٹا	2017	متنازعہ	حکومت نے خاص طور پر بٹ کوائنز سے متعلق کوئی قواعد نافذ نہیں کئے لیکن ملک کے وزیراعظم جوزف مسکٹ نے بٹ کوائن اور بلاک چین ٹیکنالوجی کو فروغ دینے کے لئے ایک قومی حکمت عملی کی منظوری دی ہے۔ وزیراعظم نے خاص طور پر بٹ کوائن اور بلاک چین کے غیر مستحکم اور غیر مرکزی نظام کی صلاحیتوں کو سراہا ہے۔
56	ملائیشیا	2014فروری	متنازعہ	ملائیشیا نے بٹ کوائن کو ابھی تک کوئی قانونی حیثیت نہیں دی اور ساتھ ہی مرکزی بینک نے عوام کو ڈیجیٹل کرنسیوں کے استعمال سے متعلق خطرات سے محتاط رہنے کا مشورہ دیا ہے۔
57	میکسیکو	دسمب2015	متنازعہ	میکسیکن حکومت نے متبادل ڈیجیٹل کرنسیوں کا استعمال

				ممنوعہ قرار نہیں دیا مگر حکومت اپنابٹ کوائن اور بلاک چین متعارف کروانے کے لئے جدوجہد کر رہی ہے۔
58	نامیبیا	ستمبر 2017	غیر قانونی	ستمبر 2017 میں بینک آف نامیبیا نے ورچیول/ڈیجیٹل کرنسیوں پر ایک پوزیشن پیپر جاری کیا جس میں اس نے اعلان کیا کہ ملک میں کرپٹو کرنسی ایکسچینجز کی اجازت نہیں ہے اور کرپٹو کرنسی کو اشیاء کی رقم کی ادائیگی کے طور پر قبول نہیں کیا جاسکتا۔[7]
59	نیوزی لینڈ	فروری 2014	متنازعہ	ریزرو بینک کرپٹو کرنسی کو خطرہ سمجھتا ہے اور کرپٹو کرنسی کو کرنسی کے بجائے ایک ادائیگی کا نظام سمجھتا ہے۔
60	ناروے	جنوری 2014	اثاثہ	ناروے ٹیکس اتھارٹی کے

[7] https://www.coindesk.com/namibian-central-bank-bitcoin-purchases-illegal-law/

				مطابق بٹ کوائن کی حیثیت اثاثے کی ہے۔[8]
61	پاکستان		متنازعہ	پاکستانی حکومت نے ابھی تک بٹ کوائن پر کوئی موقف اختیار نہیں کیا ہے مگر اس کا ماننا ہے کہ بٹ کوائن مال زر ہے، کرنسی نہیں۔
62	پرتگال	فروری 2014	متنازعہ	پرتگالی حکومت نے بٹ کوائن کے لئے کوئی قانونی فریم ورک تجویز نہیں کیا۔
63	روس	ستمبر 2017	غیر قانونی	روسی فیڈریشن کے نائب وزیر خزانہ الیکسی مویسف نے کہا کہ کرپٹو کرنسیز میں رقم کی ادائیگیوں کو قبول کرنا غیر قانونی ہے۔ تاہم بٹ کوائن مارکیٹ والے علاقوں پر پابندی عائد کر دی گئی ہے اور عدالت کے فیصلے میں کہا گیا ہے کہ بٹ

[8] http://www.loc.gov/law/foreign-news/article/norway-bitcoins-are-capital-property-not-currency-says-norwegian-tax-authority/

				کوائن کرنسی کا متبادل ہے اور روسی فیڈریشن کی حدود میں اس کا استعمال غیر قانونی ہے۔
64	سنگاپور	2014مارچ	پیسہ	2014 کے آغاز میں سنگاپور حکومت نے بٹ کوائن کو اشیاء خریدنے کے لئے ایک بہتر کرنسی کے طور پر قبول کیا ہے جس پر مخصوص ٹیکس لاگو ہوگا۔
65	سلووا کیا	فروری2014	متنازعہ	نیشنل بینک آف سلوا کیا (این بی ایس) کے مطابق بٹ کوائن میں ملکی کرنسی جیسی صفات نہیں پائی جاتیں اس لئے یہ حکومتی کنٹرول میں نہیں آتی۔ ساتھ ہی این بی ایس نے عوام کو اس کے استعمال کے خطرات سے انتباہ کیا ہے۔
66	تائیوان	فروری2014	متنازعہ	تائیوان کی مال نگران کمیشن نے بٹ کوائن کی طرف غیر جانبدارانہ طرز عمل کو اپنایا ہے

				لیکن ساتھ ہی اس پر اور زیادہ محدود پالیسیاں بنانے کی کوشش کر رہا ہے۔
67	تھائی لینڈ	جولائی 2014	قانونی	2013 میں تھائی مرکزی بینک نے تھائی لینڈ میں بٹ کوائن کے استعمال کو غیر قانونی قرار دیا، لیکن 2014 کے آغاز میں اپنی رائے تبدیل کی کہ اس کا استعمال غیر قانونی نہیں ہے. تاہم تھائی لینڈ میں بٹ کوائن خریدنے اور پھر ملک سے باہر فروخت کرنا سختی سے منع کیا گیا ہے۔
68	ترکی	فروری 2014	متنازعہ	بٹ کوائن کو باقاعدہ طور پر منظم نہیں کیا گیا کیونکہ قانون کے مطابق یہ الیکٹرانک پیسہ نہیں ہے۔
69	یوگنڈا		متنازعہ	ملک میں بٹ کوائن کا استعمال غیر قانونی نہیں ہے مگر حکومت نے اس کے فریم ورک کو ملک

				میں منظم بھی نہیں کیا۔ بینک آف یوگینڈا نے عوام کو انتباہ کی ہے کہ وہ بٹ کوائن اور دیگر ڈیجیٹل کرنسیوں سے دور رہیں۔
70	یوکرائن	2014نومبر	متنازعہ	بعض علاقوں میں غیر سرکاری حکمرانوں اور غیر یقینی سیاسی صورتحال کے باوجود، ملک کے ایک بڑے بینک نے اپنے ملک بھر میں لگے اے ٹی ایم ٹرمینلز سے بٹ کوائنز خریدنے کی صلاحیت کا اعلان کیا ہے۔
71	متحدہ عرب امارات		متنازعہ	حکومت کرپٹو کرنسیز کی صحیح حیثیت، فوائد و نقصانات کا اس وقت جائزہ لے رہی ہے۔
72	وینیزویلا		متنازعہ	بٹ کوائن کی بڑھتی ہوئے مقبولیت اور استعمال کے رجحان کے باوجود، حکومت ان لوگوں کو قانونی خلاف ورزی کے الزام میں گرفتار کر رہی ہے۔ جبکہ

				ملک میں اس کے استعمال پر کوئی قانون نہیں پیش کیا گیا۔[9]
73	زمبابوے		متنازعہ	حکومت وقت کا کہنا ہے کہ ملک ابھی کرپٹو کرنسیز کے نظام کو منظم کرنے کے لئے تیار نہیں ہے۔
74	ٹرینیڈاڈ اور ٹوباگو		متنازعہ	حکومت میں بٹ کوائن اور کرپٹو کرنسیز کی نفاذ کے بارے میں زیادہ واضح دلائل نہیں ملے مگر ملک کی عوام بٹ کوائن کا استعمال کر رہی ہے۔[10]
75	نکاراگوا		متنازعہ	اطلاعات سے پتہ چلتا ہے کہ بٹکوز ملک میں استعمال کیا جارہا ہے۔
76	بوسنیااور ہرزیگوینا		متنازعہ	بوسنیااور ہرزیگوینامیں بٹ کوائن پر کوئی خاص قانون نافذ نہیں کیا گیا۔

9 https://www.washingtonpost.com/news/worldviews/wp/2017/03/10/bitcoin-mining-is-big-business-in-venezuela-but-the-government-wants-to-shut-it-down/?utm_term=.42dc6139a56f

10 http://www.guardian.co.tt/technology/2015-03-22/bitcoin-coming-tt

77	بنگلہ دیش	2014	غیر قانونی	بنگلہ دیش بینک نے کرپٹو کرنسی استعمال پر انتباہ جاری کی اور مبینہ طور پر کہا گیا ہے کہ کوئی فرد کرپٹو کرنسیز استعمال کرتا ہوا پکڑا گیا تو اسے 12 سال تک کی جیل کی سزا سنائی جائے گی۔
78	بولیویا		غیر قانونی	بولیویا حکومت نے بٹ کوائن کے استعمال پر پابندی عائد کر دی ہے کہ اس میں ٹیکس کی چوری اور مالیاتی عدم استحکام کے امکان ہیں۔
79	ایکواڈور		غیر قانونی	ایک ریاستی الیکٹرانک پیسے کے نظام کے قیام کی وجہ سے ایکواڈور حکومت نے بٹ کوائن اور دیگر تمام ڈیجیٹل کرنسیوں پر پابندی لگادی ہے۔[11]
80	الجزائر	دسمبر 2017	غیر قانونی	2017 کے آغاز میں بٹ کوائن کی حیثیت قانونی سمجھی جاتی تھی لیکن اب اس کے

[11] https://cointelegraph.com/bitcoin-for-beginners/is-bitcoin-legal#countries-in-which-bitcoin-is-banned

				استعمال پر پابندی لگادی گئی ہے۔ جرنل آفیسیل (28 دسمبر 2017) کے مطابق: آرٹیکل 117 – نام نہاد ورچیول (کرپٹو) کرنسی کے خرید و فروخت اور کسی قسم کے استعمال پر پابندی ہے۔ ورچیول کرنسی وہ ہے جو انٹرنیٹ صارفین استعمال کرتے ہیں۔ اس کی خاصیت یہ ہے کہ اس کی جسمانی شکل و صورت نہیں جیسے کہ سکّوں اور نوٹوں کی ہوتی ہے یا پیسے دینے کے لئے چیکز یا کریڈٹ کارڈز۔ اس اصول کی کسی بھی طرح کی خلاف ورزی کرنے والے کو قوانین اور قواعد و ضوابط کے مطابق مجرم قرار دیا جائے گا۔
81	کرغیزستان		غیر	کرغزستان کی حکومت نے اپنی

			قانونی	سرحدوں کے اندر بٹ کوائن کے استعمال پر پابندی لگائی ہے۔
82	نائیجریا	جنوری 2017	غیر قانونی	19 جنوری 2017 کو مرکزی بینک آف نائیجیریا نے سرکاری طور پر ڈیجیٹل کرنسیوں کو غیر قانونی قرار دیا اور وجہ یہ بتائی کہ اس سے منی لانڈرنگ اور معاشی خطرات کا سامنا ہو سکتا ہے۔
83	ویت نام	2014	غیر قانونی	ویت نام نے سب سے پہلے 2014 میں بٹ کوائن پر پابندی لگائی۔ اگست 2017 میں وزیر اعظم بٹ کوائن اور دوسری کرپٹو کرنسیوں کو پیسوں کی ادائیگی کے طور پر قبول کرنے کے منصوبے بنا ہی رہے تھے کہ اکتوبر میں یکدم پھر سے بٹ کوائن کو مکمل طور پر بین کر دیا گیا اور ساتھ یہ اعلان کر دیا کہ 2018 کے

				آغاز سے اگر کوئی فرد کرپٹو کرنسی استعمال کرتا ہوا پکڑا گیا تو اس پر جرمانہ عائد کیا جائے گا۔
84	نیپال	اگست 2017	غیر قانونی	13 اگست 2017 کو نیپال ریسٹرا بینک نے بٹ کوائن کو غیر قانونی قرار دیا۔

بٹ کوائن اے ٹی ایم والے ممالک

دنیا میں کل 66 ممالک میں بٹ کوائن اے ٹی ایم نصب ہیں جن کی کل تعداد 2309 ہیں۔[12] بٹ کوائن کی خرید پر اے ٹی ایم فیس کی لاگت اوسط 5.55 فیصد آتی ہے اور فروخت پر اوسط 7 فیصد۔

بٹ کوائن اے ٹی ایم والے ممالک کی فہرست درج ذیل ہے۔

شمار نمبر	ملک	کل اے ٹی ایمز
1	ریاستہائے متحدہ امریکہ	1403

شمار نمبر	ملک	کل اے ٹی ایمز
34	کولمبیا	3

[12] https://coinatmradar.com/countries/

2	کینیڈا	354
3	برطانیہ	105
4	آسٹریا	100
5	سپین	40
6	آسٹریلیا	24
7	فن لینڈ	21
8	چیک جمہوریہ	21
9	سوئٹزرلینڈ	20
10	اٹلی	18
11	نیدرلینڈز	16
12	میکسیکو	12
13	سلووا کیا	12
14	جاپان	11
15	روسی فیڈریشن	11
16	پاناما	10
17	سلووینیا	9
18	فلپائن	7
19	ہانگ کانگ	7
20	ڈومینیکن جمہوریہ	6

35	نیوزی لینڈ	2
36	ناروے	2
37	بلغاریہ	2
38	لیتھوانیا	2
39	ڈنمارک	2
40	ہنگری	2
41	گوام	2
42	چلی	2
43	فرانس	2
44	ایسٹونیا	2
45	کوسٹاریکا	2
46	سعودی عرب	1
47	یوکرائن	1
48	سویڈن	1
49	جنوبی کوریا	1
50	سائپرس	1
51	انڈونیشیا	1
52	چین	1
53	برازیل	1

21	تائیوان	6
22	یونان	6
23	سنگاپور	5
24	رومانیہ	5
25	کروشیا	4
26	بیلجیم	4
27	ویت نام	4
28	سربیا	4
29	پولینڈ	4
30	کوسوو	4
31	اسرائیل	4
32	قازقستان	3
33	مالٹا	3

54	اروبا	1
55	باربادوس	1
56	جمیکا	1
57	انگویلا	1
58	نائجیریا	1
59	پیرو	1
60	منگولیا	1
61	ملائیشیا	1
62	لیچسٹنسٹین	1
63	پرتگال	1
64	ملائیشیا	1
65	لیچسٹنسٹین	1
66	پرتگال	1

متبادل کرنسیز (آلٹ کوائنز)

بٹ کوائن ایک اوپن سورس منصوبہ ہے اور اس کا کوڈ بہت سے دوسرے سافٹ ویئر کے منصوبوں میں بنیاد کے طور پر استعمال کیا جا سکتا ہے۔ چونکہ بٹ کوائن کرپٹو کرنسی کی پہلی ایجاد تھی اس لئے اس میں کچھ کمی بیشی اور مسائل کا رہ جانا لازمی بات ہے۔ ان مسائل میں سے ایک ٹرانزیکشنز کی معلومات کو خفیہ رکھنا ہے جسے بٹ کوائن حل نہیں کرتا۔ بٹ کوائن کی اس خامی نے ایک نئی نسل کی کرپٹو کرنسی کو جنم دیا جس کا نام انونیمس (بے نام) کرپٹو کرنسیز رکھا گا۔ انونیمس کرپٹو کرنسیز دو طرح کی ہو سکتی ہیں۔ 1۔ میٹا کوائنز 2۔ آلٹ (متبادل) کوائنز (Alt Coins)

1 میٹا کوائنز: (Meta Coins)

بٹ کوائن کے بلاک چین پر بے شمار پروٹوکول (اصولوں کا وہ نظام جو درست طرز عمل اور طریقہ کار کو جاری کرتا ہے) کی تہوں کو تشکیل دے کر لاگو کیا گیا ہے۔ میٹا کوائنز وہ سافٹ ویئر لئیر (پرت) ہیں جو بٹ کوائن کے اوپر بنائے جاتے ہیں۔ ان سافٹ ویئر کے ذریعے یا تو کرنسی کے اندر ایک اور کرنسی بنائی جاتی ہے یا پھر اس کے پروٹوکول بٹ کوائن کے اصل سسٹم میں کچھ ردوبدل کرتے ہیں۔ یہ اضافی لئیرز بٹ کوائن پروٹوکول کی خوبیوں کو بڑھاتے ہیں اور

اسے یہ صلاحیت دیتے ہیں کہ بٹ کوائن اپنی ٹرانزیکشنز میں اضافی ڈیٹا محفوظ کر سکیں۔ میٹا کوائنز کی مزید تین اقسام ہیں۔

1.1۔رنگین سکے :(Colored Coins)

رنگین کوائنز میٹاپروٹوکول پر مبنی ہیں جو کہ بٹ کوائن کی اصل حیثیت میں تھوڑی سی تبدیلی کر کے شائع کیا جاتا ہے۔ آسان لفظوں میں کلرڈ کوائن بٹ کوائن کی ہی ایک قسم ہے جس کی حیثیت بدل کر اثاثہ کر دی جاتی ہے۔ مثال کے طور پر آپ کے پاس ایک ڈالر کا کاغذی نوٹ ہے اور اس پر یہ مہر لگا دی جائے کہ "یہ کسی کمپنی میں ایک حصہ کی شراکت کا سرٹیفکیٹ ہے "۔اب یہ کاغذی نوٹ دو مقاصد پورے کرے گا،ایک، یہ کرنسی نوٹ ہے اور دوسرا، حصے کی شراکت کی سند۔ اب چونکہ یہ ایک حصہ کے طور پر زیادہ قیمتی ہے آپ اس کی ٹافی خرید کر نہیں کھائیں گے۔ لہذا اب اسے کرنسی کے طور پر استعمال کرنا مفید نہیں ہے۔ بلکل اسی طرح کلرڈ کوائن، بٹ کوائن کے کچھ مخصوص کوائنز کو تجارتی سرٹیفکیٹ میں تبدیل کر دیتا ہے جو کہ اثاثے کی نمائندگی کرتی ہے۔

1.2۔ماسٹر کوائنز: (Master Coins)

ماسٹر کوائن ایک پروٹوکول لئیر ہے جو بٹ کوائن کے اوپر بنائی گئی ہے۔اس کا مقصد بٹ کوائن کے نظام کو بڑھانے کے لئے ایک ایسے پلیٹ فارم کی تشکیل ہے جو مختلف اپیلی کیشنز کی حمایت کرتا ہو۔ یہ ایم ایس ٹی نام کی کرنسی کو بطور ٹوکن استعمال کرتا ہے تاکہ ماسٹر کوائن کی ٹرانزیکشنز کی جا سکیں۔ یہ ٹوکن کرنسی کی حیثیت نہیں رکھتا بلکہ یہ دیگر چیزوں مثلاً صارف کی کرنسیوں، معاہدوں، جائیداد کے ٹوکنز، غیر مرکزی اثاثوں کے تبادلے وغیرہ کی اپیلی کیشنز کی تشکیل کے لئے استعمال ہوتے ہیں۔ اگر آپ نیٹ ورکنگ کے تصور سے واقف ہیں تو آپ

اسے اپلی کیشن لیئر سمجھیں جو کہ بٹ کوائن کے فنانشل ٹرانزیکشن ٹرانسپورٹ لیئر کے اوپر بنائی گئی ہے۔ جیسا کہ ایچ ٹی ٹی پی (HTTP) پروٹوکول، ٹی سی پی (TCP) کے اوپر چلتا ہے۔

1.3۔کاونٹر پارٹی:(Counter Party)

کاونٹر پارٹی ایک اور پروٹوکول لیئر ہے جو کہ بٹ کوائن کے اوپر تشکیل دی گئی ہے۔ یہ لیئر بھی صارفین کو اثاثوں، کرنسیوں، تجارتی ٹوکنز اور مالی وسائل وغیرہ کے تبادلے کی سہولت فراہم کرتا ہے۔ کاونٹر پارٹی کی ٹرانزیکشنز کے لئے ایکس سی پی (XCP) نامی کرنسی کو بطور ٹوکن استعمال کیا جاتا ہے۔

2۔آلٹ کوائنز:(Alt Coins)

الٹ کوائنز کو بٹ کوائن کے متبادل کے طور پر شمار کیا جاتا ہے جن کا مقصد بٹ کوائن کی خامیوں کو مد نظر رکھتے ہوئے اس کے تخلیقی ڈھانچے (اور یجنل کوڈ) میں کچھ ترمیم کر کے ان کو اور بہتر بنانا ہے۔ اس کا دوسرا مقصد آج کی بڑھتی ہوئی مسابقتی مارکیٹ کی وجہ سے، صارفین کو مستقبل میں بہتر متبادل کرپٹو کرنسیز مہیا کرنا ہے۔

دنیا میں سب سے پہلے بٹ کوائن کا اِجراء جنوری 2009 میں ہوا۔ ابھی دو سال بھی مکمل نہیں گزرے تھے کہ بٹ کوائن سے مشابہت رکھتے ہوئے پہلے الٹ کوائن کا اِجراء ہوا جس کا نام نیم کوائن (NAME Coin) رکھا گیا۔ نیم کوائن اپریل 2011 میں معرض موجود میں آیا اور اگلے دو سالوں میں چند اور الٹ کوائنز مثلاً لائٹ کوائن (Lite coin) اور پیئر کوائن (Peer coin) بھی ظہور میں آچکے تھے۔ لیکن 2013 کے آغاز سے متعدد

نت نئے الٹ کوائنز دیکھنے کو ملے جو تقریباہر ہفتے ہی نکالے جارہے تھے اور یہ سلسلہ اب بھی متواتر جاری ہے۔

ویکیپیڈیا کے مطابق اس وقت دنیا میں 1,520 سے زائد کرپٹو کرنسیز پائی جاتی ہیں۔[1] جو وقت کے ساتھ ساتھ بڑھتی جارہی ہیں۔ کچھ الٹ کوائنز صرف اعلانیہ طور پر سامنے آئے تھے اور چند ایک کے پروگرام کوڈز بھی جاری ہوئے تھے مگر ان کے جینیسز بلاک نہ بن سکنے کی وجہ سے وہ فوراسے بیشتر ختم ہو گئے اور کچھ الٹ کوائنز وجود میں آنے کے ساتھ ہی ختم ہو گئے۔

جب بھی کسی نئے آلٹ کوائن کے نظام کو شروع کیا جاتا ہے تو اس کی بنیاد نئے سرے سے نہیں رکھی جاتی۔ اصل میں کوئی بھی نیا کوائن بذات خود بٹ کوائن کی سانچے میں ڈھل کر کھڑا ہوتا ہے۔ مثلاآپ لائٹ کوائن کو ہی لے لیں۔ یہ بٹ کوائن کی ساخت پر ہی بنا ہے۔ ہر الٹ کوائن کی کچھ نہ کچھ خصوصیت ہوتی ہے جو اسے دوسرے سے منفرد بناتی ہے۔ یہ خصوصیات سکریپٹنگ لینگویج کی بنیاد پر ٹرانزیکشنز کو محفوظ کرنے کے طریقے یا سیکورٹی کے نئے الگورتھم کی بنیاد پر ہوتے ہیں یا مائننگ کے نئی تکنیک یا صارفین کی ٹرانزیکشن کو اور رازدار بننے کے طریقے بھی ہو سکتے ہیں۔

یہاں پر ہم چند اہم اور منفرد الٹ کوائنز کا تفصیلی جائزہ لیں گے جو اپنی خوبیوں اور صلاحیتوں کی بنیاد پر آج بھی مشہور ہیں۔

2.1۔ نیم کوائن:(Name Coin)

یہ پہلا آلٹ کوائن ہے جو دنیا کے پہلے بٹ کوائن کے 2 سال بعد 2011 کے وسط میں وجود میں آیا۔ نیم کوائن [28] بہت دلچسپی کا حامل ہے کیونکہ یہ ایک نئے تکنیکی خصوصیت ڈومین

نام رجسٹریشن پر مبنی ہے۔ جیسا کہ آپ جانتے ہیں یہ ہمارے انٹرنیٹ اور دنیا بھر کے ویب ڈھانچہ کا مرکزی حصہ ہے۔ نیم کوائن اس مقصد سے بنایا گیا تھا کہ ڈومین نام کے نظام کو غیر مرکزی بنایا جاسکے۔ مثال کے طور پر اگر آپ براؤزر میں (example.bit) لکھیں تو یہ خودکار طریقے سے آپ کو محفوظ کردہ رجسٹری کی اصل جگہ پر لے جائے گا۔ نیم کوائن میں ایک نام رجسٹر کرنے کے لئے اور اسے برقرار رکھنے کے لئے صرف ایک ٹرانزیکشنز بھیجتے ہیں جیسے کہ بٹ کوائن کرنسی کے منتقل کرنے کے لئے بٹ کوائن کے نیٹ ورک پر ایک ٹرانزیکشن بھیجی جاتی ہے۔ نیم کوائن موجودہ ڈومین نام کے نظام کے بہت سے پہلوؤں کی عکاسی کرتا ہے۔ مثال کے طور پر آپ ایک ڈومین نیم، جو ابھی تک کسی نے نہ لیا ہو، حقیر سی رقم ادا کر رجسٹر کروا سکتے ہیں اور تجدید کروانے کے لئے بھی کوئی اضافی رقم نہیں۔ اب رجسٹرڈ شدہ ڈومین کے سب-ڈومین نکال کر استعمال کر سکتے ہیں اور کسی اور کو منتقل بھی سکتے ہیں۔ کہا جاتا ہے کہ اس وقت نیم کوائن کے ذریعے رجسٹریشن کروانے کی لاگت صرف 0.01$ آتی تھی جو کے اصل سسٹم کا ہزارواں حصہ ہے۔

2.2۔لائٹ کوائن: (Lite Coin)

نیم کوائن کے بعد 2011 میں ہی لائٹ کوائن [2] کا اجراء ہوا۔ بٹ کوائن کے مدمقابل متبادل (آلٹ) کوائنز میں لائٹ کوائن اب بھی ٹاپ 10 لسٹ میں آتا ہے۔ لائٹ کوائن اور بٹ کوائن میں ایک امتیازی فرق ہے۔ بٹ کوائن مائنگ کے لئے گرافکس پروسیسنگ یونٹ استعمال کرتا ہے اور یہ مائنگ کے لئے سنٹرل پروسیسنگ یونٹ استعمال کرتا ہے۔ لائٹ کوائن بنانے کا مقصد اسے جی۔پی۔یو کے بجائے سی۔پی۔یو بیس مائنگ الگورتھم بنانا تھا۔ جس وقت لائٹ کوائن کا افتتاح ہوا اس وقت جو لوگ بٹ کوائن مائن کر رہے تھے وہ ساتھ ہی باآسانی

لائٹ کوائن بھی استعمال کر سکیں گے۔لائٹ کوائن کی دوسری خصوصیات میں چند پیرامیٹرز کی تبدیلیاں اور ہر 5۔2 منٹ کے بعد بلاکس کا چار گنا تیزی سے پہنچ جانا شامل ہے۔بٹ کوائن میں بہتری کے لئے جو نئی تبدیلی لائی جاتی ہے لائٹ کوائن بھی اسے اپنالیتا ہے۔وقت کے ساتھ ساتھ جس طرح بٹ کوائن ٹیکنالوجی میں آگے بڑھتا جارہا ہے اسی طرح لائٹ کوائن بھی ترقی کی راہ میں گامزن ہے۔اسی لئے یہ کوائن اب تک الٹ کوائنز کی ٹاپ لسٹ میں بٹ کوائن کے آس پاس ہی نظر آتا ہے۔اگر بٹ کوائن سونا ہے تو لائٹ کوائن کو چاندی کہتے ہیں۔

کرپٹو کرنسی کی دنیا میں کل 84 ملین لائٹ کوائنز جاری کئے جائیں گے جن میں سے اب تک تقریب 55.58 ملین کوائنز جاری ہو چکے ہیں۔84 ملین کی تعداد کا تعین بٹ کوائن کی 21 ملین کی حد پر مبنی ہے اور حقیقت یہ ہے کہ لائٹ کوائن کو ایسے بنایا گیا تھا کہ وہ بٹ کوائن کے مقابلے میں چار گنا تیزی سے کام کرتا ہو۔

2.3۔پیئر کوائن:(Peer Coin)

بٹ کوائن اور لائٹ کوائن میں ایک چیز مشترک ہے کہ ان میں نئے سکے صرف مائننگ کے ذریعہ بنتے ہیں۔پیئر کوائن [3](PPC) اپنی ذات کا پہلا کوائن تھا جس نے نئے کوائن پیدا کرنے کے لئے ایک نیا نظام پیش کیا جو پروف اف سٹیک کے نام سے جانا جاتا ہے۔پروف اف سٹیک کے کام کرنے کا طریقہ یہ ہے کہ آپ کی کچھ مخصوص رقم، بغیر خرچ یا کہیں اور منتقل کئے آپ کے بٹوے (والٹ) میں ایک متعین مدت تک پڑی رہے۔جیسے ہی یہ مدت پوری ہو گی تو آپ کو کچھ فیصد اضافی کوائن مل جائیں گے۔یہ نظام ہو بہو ہمارے بینک کے بچت اکاؤنٹ کے طرح کام کرتا ہے، لیکن مکمل طور پر غیر مرکزی طریقے سے۔اس میں صارف کو ہر وقت اپنے فنڈز کی پوری نگرانی حاصل ہوتی ہے۔

پروف اف سٹیک کی مدد سے پیر کوائن کی پیداوار اس نیٹ ورک کو اور مستحکم بناتی ہے۔ کیونکہ ممکن ہے کہ وقت سے ساتھ کان کن ماہرین کم ہو جائیں لیکن صارفین اپنے کوائنز کو سٹیک (جمع) کرتے رہیں گے ۔ اس کے علاوہ پیر کوائن ڈویلپرز نے اس کی افراط زر کی شرح ہر گزرتے سال کی 1 فیصد رکھی ہے، بغیر کسی اضافی نرخ کے۔[4]

2.4۔ایتھیریم اور ایتھیریم کلاسیک

:(Ethereum & Ethereum Classic)

ایتھیریم اس تحریک میں شامل ہونے والی نئی کرنسی میں سے ایک ہے جس کا اِجراء جولائی 2015 میں ہوا اور اس کی قیمت میں خاطر خواہ اضافہ دیکھا گیا۔ گزشتہ سال 2.226 فیصد اضافہ ہوا جس کی وجہ سے ایتھیریم اس وقت مارکیٹ کیپ کے لحاظ سے دوسری بڑی کرپٹو کرنسی ہے اور ایتیریم کلاسک کی درجہ بندی بھی ٹاپ کرپٹو کرنسیز میں ہوتی ہے۔

ایتھریم کو باآسانی سمجھنے کے لئے ہم پہلے انٹرنیٹ کے انفراسٹرکچر کو سمجھ لیتے ہے۔ انٹرنیٹ پر ہمارا ذاتی ڈیٹا، پاس ورڈ اور تمام مالی معلومات بڑے پیمانے پر دوسرے لوگوں کے کمپیوٹرز پر محفوظ ہیں۔ایمیزون، فیس بک اور گوگل کے کلاوڈ سرورز (cloud servers) بہت مشہور ہیں۔ جب ہم اپنا ڈیٹا دوسروں کے کمپیوٹرز میں محفوظ کرتے ہیں تو ہماری تمام معلومات دوسرے کی ملکیت میں چلی جاتی ہیں۔ اب وہ اس کے ساتھ کچھ بھی کریں آپ کا اختیار نہیں رہا۔ مثال کے طور پر آپ ایک موبائل ایپلی کیشنز بنا کر اسے پبلش کرنا چاہتے ہیں۔ یہ کام آپ صرف گوگل پلے یا ایپل سٹور کے ذریعے ہی کر پائیں گے ۔ یہاں اتھارٹی گوگل پلے یا ایپل سٹور کے پاس ہے کہ وہ کب اور کیسے آپ کی ایپلی کیشنز (APP) کو صارفین تک پہنچاتے ہیں۔

اس میں کوئی شک نہیں کہ انٹرنیٹ کے اس نظام نے ہمیں کئی سہولیات فراہم کی ہیں، کیونکہ ان کمپنیوں نے ہمارے ڈیٹا کو محفوظ کرنے کے لئے بہت سے ماہرین کو تعینات کیا ہے۔ لیکن اس سہولت کے ساتھ اس کے کچھ نقصانات بھی جوڑیں ہیں۔ جیسا کہ ہم جانتے ہیں کہ کوئی ہیکر یا حکومتی ادارہ کسی تیسری پارٹی سروس کے ذریعے آپ کی تمام معلومات تک، بغیر آپ کو اطلاع ہوئے قانونی و غیر قانونی طور سے باآسانی رسائی حاصل کر سکتا ہے۔ اپاچی ویب سرور کے خالق برائن بہلینڈوف (Brian Behlendorf) انٹرنیٹ کے اس مرکزی نظام کو "غلطی" کا نام دیتے ہوئے کہتے ہیں کہ انٹرنیٹ کو شروع دن سے غیر مرکزی ہونا چاہئیے تھا۔ اب چونکہ ٹیکنالوجی بہت ترقی کر گئی ہے اور بلاک چین ٹیکنالوجی کا بھی اجراء ہو چکا ہے تو اس کی مدد سے انٹرنیٹ کو غیر مرکزی بنا سکتے ہیں۔

ایتھیریم آج کل زیادہ مقبولیت حاصل کر رہی ہے۔ ایتھیریم ایک اوپن سورس (آزاد مصدر) سوفٹ ویئر پلیٹ فارم ہے جسے بلاک چین ٹیکنالوجی کی بنیاد پر بنایا گیا ہے۔ اسے غیر مرکزی خود مختار تنظیم (Decentralized Autonomous Organization - DAO) -(ڈی اے او) کے نام سے بھی جانا جاتا ہے۔ اس کا پبلک بلاک چین سافٹ ویئر ڈیجیٹل کرنسی کے علاوہ اور بہت سے مفید کام سرانجام دے سکتا ہے۔ یہ مکمل طور پر ڈویلپرز کو غیر مرکزی ایپلی کیشنز تیار کرنے اور پبلش کرنے کی مکمل سہولت فراہم کرتا ہے۔ ایتھیریم بلاک چین میں مائنرز، بٹ کوائن کو کھوجنے کے بجائے، ایتھر کمانے کی کوشش کرتے ہیں۔ یہ ایک طرح کا کرپٹو ٹوکن ہے جو نیٹ ورک کو مضبوط بنانے کا کام دیتا ہے۔ ایتھر قابل تجارت کرپٹو کرنسی ہونے کے علاوہ، ایتھیریم کے نیٹ ورک پر ٹرانزیکشن فیس کی ادائیگی، سسٹم کی پروسیسنگ پاور کی خرید و فروخت کے طور پر بھی استعمال کیا جاتا ہے۔

بٹ کوائن کا مقصد پے پال (Paypal) اور آن لائن بینکنگ سسٹم کو ختم کرنا ہے، جبکہ ایتھیریم کا مقصد بلاک چین کو استعمال کرتے ہوئے، انٹرنیٹ کی دنیا میں تیسرے فرد کی شمولیت اور اسے اختیار دینے کے نظام کو ختم کرنا ہے۔

ایتھیریم جولائی 2016 میں کچھ سیکورٹی خامیوں کی وجہ سے جب ہیک ہوا تو تقریباً 50 ملین ڈالرز کے کوائن چوری ہوئے۔ اس وقت ایتھیریم کمیونٹی میں بہت مباحث ہوئیں کہ اب کیا کیا جائے۔ نتیجتاً، کمیونٹی دو حصوں میں بٹ گئی۔ ایک طرف کا کہنا تھا کہ ہیک کوائنز کو واپس لاکر ان کے مالکان کو واپس دیئے جائیں۔ دوسری طرف والوں کا کہنا تھا کہ ٹرانزیکشنز کو تبدیل نہیں کیا جا سکتا اور نہ ہی خارج کیا جا سکتا ہے کیوں کہ یہ بلاک چین کے اصولوں کے خلاف ہے

۔

نتیجے کے طور پر ایتھیریم نے ہیکڈ شدہ ڈی اے او کو واپس لانے کے لئے مرکزی کوڈ کی کاپی کر کے اس میں کچھ ضروری ترمیم کرلی۔ جسے ٹیکنالوجی کی دنیا میں ہارڈ فورک (Hard fork) کہتے ہیں۔ ہاڈ فورک کبھی بھی کوڈ کے پچھلے ورژن کے ساتھ مطابقت نہیں رکھتا۔ جب ایک بار اسے استعمال کر لیا جائے تو اسے واپس نہیں کیا جا سکتا۔[5] جس کمیونٹی نے اس ہاڈ فورک کو قبول کیا وہ ایتھیریم (ETH) [29] کے نام سے جانی جاتی ہے۔ اس کے برعکس جو لوگ ہاڈ فورک کے خلاف تھے اور بلاک چین کے اصل اصولوں پر یقین رکھتے تھے انہیں ایتھیریم کلاسیک (ETC) [30] کا نام دے دیا گیا۔ آج ایتھیریم اور ایتھیریم کلاسیک دونوں علیحدہ سکوں کے طور پر کام کر رہا ہے جبکہ ان دونوں کا مقصد اور نقطۂ نظر ایک ہی ہے۔[6]

2.5۔بٹ کوائن پلس:(Bitcoin Plus)

بٹ کوائن پلس[8] متبادل کرپٹو کرنسیز میں سے ایک ہے جو کہ جدید اور موثر طریقے سے کام کرنے والے والیٹ پر مبنی ہے۔ یہ ایکس بی سی(XBC) کے نام سے بھی جانا جاتا ہے۔ ایکس بی سی کوائنز کا اجراء صرف 10 لاکھ تک ہوگا۔ یہ کوائنز پروف آف سٹیک ٹیکنیک کے ذریعے پیدا کیے جاتے ہیں۔ کوائنز کو سٹیکنگ کے اہل بنانے کے لئے انہیں 12 گھنٹوں کے لئے والیٹ میں رکھنا ضروری ہے۔ اس وقت تقریبا2۔1 لاکھ کے قریب سکے گردش کر رہے ہیں۔ اس کا ایک فائدہ یہ بھی ہے کہ اگر آپ کے پاس اپنے والیٹ (بٹوے) میں ایکس بی سی سکے ہیں تو یہ ایک سال کے اندر 20% بڑھ جائیں گے۔ مثلاً اگر 100,000 سکے موجود ہیں، تو 1 سال کے وقت میں 120,000 سکے ہو جائیں گے۔

اس کے بلاک سائز کی حد 1.5 MB ہے جس میں تقریبا3,030 ٹرانزیکشنز سما سکتی ہیں، مطلب 50.5 ٹرانزیکشنز ایک سیکنڈ میں پروسیس ہوتی ہیں۔ بٹ کوائن کے مقابلے میں ایکس بی سی بلاک کو پروسیس کرنے کے لئے بہت کم وقت لیتا ہے۔ بٹ کوائن 600 سیکنڈز لیتا ہے جبکہ بٹ کوائن پلس 60 سیکنڈ۔[7] اس لحاظ سے ایکس بی سی نیٹ ورک 10 منٹ میں 10% زیادہ ٹرانزیکشنز سنبھالتا ہے۔

ایکس بی سی والیٹ صارفین کی ائی پی (IP) کو پوشیدہ رکھنے کے لئے ٹی اوآر (TOR) نیٹ ورک استعمال کرتا ہے۔ یہ نیٹ ورک صارفین کی تمام ٹرانزیکشنز کو متعدد تہوں میں انکرپٹ (Encrypt) کر کے محفوظ رکھتا ہے۔ [8]

بٹ کوائن پلس دنیا کی مشہور کرپٹو کرنسی ایکسچینج "پولونیکس(Poloniex) "اور دیگر ایکسچینجز مثلاً کرپٹوپیہ (Cryptopia)، کوائن ایکسچینج (Coin Exchange)، نوا ایکسچینج Novaexchange) وغیرہ پر تجارت کے لئے دستیاب ہے۔

2.5۔رِپّل (Ripple):

رِپّل[9] کرپٹو کرنسی کا اجراء 2012 میں ہوا اور یہ اس وقت تیسری بڑی کرپٹو کرنسی ہے۔ رِپّل ڈیجیٹل کرنسی کی ادائیگی کے نیٹ ورک کا نام ہے جس میں اس کرنسی کی منتقلی کی جاتی ہے ۔یہ ایک تقسیم شدہ، واضح ذریعہِ ادائیگی کا نظام ہے جو ابھی بیٹا (Beta) ورژن میں ہے۔ رِپّل سسٹم کا مقصد لوگوں کو ایسا غیر مرکزی مالیاتی نیٹ ورک مہیا کرنا ہے جس میں کسی قسم کی حدود نہ لگائی جا سکیں۔ مثال کے طور پر کریڈٹ کارڈز، بینکوں، پے پال (Paypal) اور دیگر اداروں جو پیسوں کے تبادلے پر یا کرنسی ایکسچینج پر فیس کی حد لگا دیتے ہیں یا پھر ٹرانزیکشن کی پروسیسنگ تاخیر کا شکار ہو جاتی ہے۔ جس طرح انٹرنیٹ تمام معلومات محفوظ رکھنے اور ضرورت پڑھنے پر آسان رسائی دیتا ہے بالکل اسی طرح رِپّل یہ کام معلومات کی بجائے پیسوں کے لئے کرنا چاہتا ہے۔

بٹ کوائن کی طرح، رِپّل کی ایکس آر پی (XRP) یونٹ بھی ریاضی فارمولوں پر مبنی کرپٹو کرنسی کی ایک شکل ہے۔ دوسرے کرپٹو کرنسیز کی طرح اس کے کوائنز کو مائننگ کی مدد سے کھوجنے کی تعداد بھی محدود ہے۔ اس میں بھی کسی بھی تیسری پارٹی کی مداخلت کے بغیر پیسے ایک اکاؤنٹ سے دوسرے اکاؤنٹ میں منتقل کئے جا سکتے ہیں اور یہ جعلی سکوں کے امکان کے خلاف ڈیجیٹل سیکورٹی فراہم کرتی ہے۔ رِپّل نیٹ ورک کو اس طرح بنایا گیا ہے کہ کسی بھی کرنسی کو باآسانی منتقل کیا جا سکے، چاہے وہ کرنسی ڈالر ہو یا یورو، پاؤنڈ ہو یا ین، یا پھر بٹ کوائنز۔

2.7۔ڈیش :(Dash)

ڈیش[10]18 جنوری2014میں اصل میں ایکس کوائنایکس سی او(XCO) کے نام سے جاری کیا گیا تھا۔28 جنوری کو یہ نام "ڈارک کوائن" میں بدلا گیا تھا۔25مارچ2015 کو دوبارا اس کا نام تبدیل کر کے "ڈیش" رکھ دیا گیا۔ڈیش یاڈیجیٹل کیش ایک مستحکم متبادل کوائنز میں سے ایک ہے۔یہ بٹ کوائن کے بنیادی اوپن سورس کوڈ پر بنایا گیا ہے جو بٹ کوائن کی تمام خصوصیات رکھنے کے ساتھ کچھ اعلی درجے کی صلاحیتیں بھی رکھتا ہے جن میں فوری ٹرانزیکشن، نجی ٹرانزیکشن اور تقسیم شدہ نظام شامل ہیں۔ڈیش کا غیر مرکزی طریقہ کار اور بجٹ سازی کا نظام اس کو ایک غیر مرکزی خود مختار تنظیم(ڈی اے او) بناتا ہے۔

بٹ کوائن کی طرح اس کا بھی اپنا بلاک چین، والیٹ انفرا اسٹکچر اور کمیونٹی ہے لیکن بٹ کوائن کے برعکس،اس کی ٹرانزیکشن فیس چند سینٹس ہے جو ویسٹرن یونین، پے پال، یا منی گرام (Moneygram) کے مقابلے میں بہت سستا ہے۔ڈیش کی تین خصوصیات ایسی ہیں جو اسے دوسروں سے منفرد بناتی ہیں۔[11]

پرائیوٹ سینڈ - (Private Send) نجی ٹرانزیکشن:ڈیش آپ کو ذاتی طور پر کئی دوسرے ٹرانزیکشنز کے درمیان اختلاط کر کے اپنے فنڈز کو بھیجنے کی اجازت دیتا ہے۔یہ اختلاط کسی مخصوص ٹرانزیکشن کو شناخت کرنا مشکل بنا دیتی ہے۔یہ خصوصیت اختیاری ہے اگر کوئی صارف اسے استعمال کرنا چاہے تو باآسانی کر سکتا ہے۔صارف یہ خصوصیت صرف 1000 کوائنز پر استعمال کر سکتا ہے۔

انسٹنٹ سینڈ- (Instant Send) فوری ٹرانزیکشن:یہ سروس ڈیش ٹرانزیکشنز کو فوری طور پر 1.5 سیکنڈ کے اندر بھیجنے کی اجازت دیتا ہے۔یہ سروس فوری طور پر ڈبل

اخراجات کے مسئلے کو بھی حل کرتی ہے۔ لیکن ماسٹر نوڈاس طرح کی ٹرانزیکشن کی پروسیسنگ پر زیادہ فیس لاگو کرتی ہے۔

ماسٹر نوڈز :(Master Node)بٹ کوائن کے برعکس جہاں نیٹ ورک پر سب نوڈز برابر ہوتے ہیں، ڈیش میں کچھ خصوصی نوڈز ہوتے ہیں جنہیں ماسٹر نوڈز کہتے ہیں۔ یہ نوڈنیٹ ورک پر موجود وہ شخص بنا سکتا ہے جس کے پاس 100 ڈیش کوائنز ہوں۔ یہ خاص نوڈ پرائیوٹ سینڈ اور انسٹنٹ سینڈ کے کام سرانجام دیتے ہیں اور اور 45 فیصد بلاک انعام حاصل کرتے ہیں۔

ڈیش کے کل 18 ملین کوائنز وجود میں آئیں گے۔ اب تک تقریبا 7 ملین کوائنز گردش کر رہے ہیں اور سال 2300 میں (جب ہم میں سے کوئی زندہ نہیں ہو گا) 18 میلین کوائنز کا ہندسہ پورا ہو جائے گا۔ ڈیش کے بلاک کا انعام ہر سال تدریجن 1%۔7 گھٹتا جائے گا۔ ڈیش بلاک چین ایک بلاک کو مائن کرنے کے لئے اوسط 5۔2 منٹ وقت لیتا ہے جو کہ بٹ کوائن کے موازنہ میں 4 گنا جلدی کام کرتا ہے۔

2.8۔ برسٹ کوائن:[Brust Coin)

برسٹ کوائن [12]، جو برسٹ کے نام سے بھی پہچانا جاتا ہے، کرپٹو کرنسی کا نظام بھی دوسری کرپٹو کرنسیوں کی طرح بلاک چین کی ٹیکنالوجی پر کھڑا ہے۔ 10 اگست 2014 میں ایک گمنام صارف نے پہلی بار بٹ کوائن ٹاک [13] کے پلیٹ فارم پر اسے یہ کہہ کر متعارف کروایا گیا کہ اسے نکسٹ (Nxt) پلیٹ فارم کی مدد سے تیار کیا گیا ہے اسی لئے یہ اس سے ملتی جلتی خصوصیات پیش کرتا ہے۔

ساتوشی ناکاموتو کی طرح اس کے بنانے والے نے بھی اپنی شناخت ظاہر نہیں کی۔ بنانے والے کے غائب ہونے کے بعد کرپٹو کرنسی کمیونٹی نے اس پر کام کرنا جاری رکھا۔ ایک ٹیم جو پروف آف کاپسٹی کنسوٹئیم (Prood of Capacity Consortium) کے نام سے جانی جاتی ہے وہ آج کل برسٹ کوائن پر کام کر رہی ہے۔

بٹ کوائن نے مائینگ الگورتھم پروف آف ورک کے برعکس، برسٹ کوائن مائن کے لئے پروف آف کاپسٹی استعمال کرتی ہے جس میں مائینرز کمپیوٹر کی اسٹوریج کو استعمال کرتے ہیں۔ جتنی زیادہ جگہ (اسٹوریج) کمپیوٹر میں موجود ہو گئی اتنی تیزی سے کمپیوٹنگ آپریشن عمل سے گزریں گے۔ اب اگر ہم اس کا موازنہ بٹ کوائن سے کریں جس میں بجلی وافر مقدار میں خرچ ہوتی ہے، تو برسٹ کوائن میں بجلی کا خرچ صرف عام استعمال کے مطابق ہے۔ اس کی توانائی کا موثر استعمال کرنے کی صلاحیت اسے دوسری کرپٹو کرنسی سے منفرد کرتی ہے[14] اس میں مائینگ اتنی موثر ہے کہ آپ اپنے آنڈرویڈ (Android) فون سے یا رسبری پائی(Resberry Pi)آلے کے استعمال سے بھی حاصل کر سکتے ہیں۔

اگرچہ کہ اس میں اسٹوریج کی جگہ ایک ضروری امر ہے مگر دسمبر 2017 کے مطابق اندازہ لگایا گیا ہے کہ نیٹ ورک کا سائز 157,000 ٹیرابائیٹس تک پہنچایا گیا ہے۔ اور وہ صارفین جنہوں نے کچھ گیگابائیٹس (Gigabytes) کی ڈسک سپیس کے ساتھ نیٹ روک میں شمولیت حاصل کی تھی ان کے لئے اب اچھا زر مبادلہ کمانے کے امکانات بہت کم ہیں۔

برسٹ کوائن نیٹ ورک پر بلاک انعام 10,000 کوائنز فی بلاک سے شروع ہوئی تھی اور ہر مہینہ اس میں تدریجاً 5 فیصد کمی ہوتی جائے گئی جب تک کہ تمام 2,158,812,800 برسٹ کوائنز جاری نہیں ہو جاتے۔ یہ متحرک طور پر مائننگ معمہ [puzzle] کو ایڈجسٹ کرتا ہے تاکہ ایک بلاک اوسط 4 منٹوں میں عملدرآمد ہو جائے۔[15]

اسی وجہ سے یہ کوائن آنے والی نئی کرپٹو کرنسیز کے لئے بنیاد رکھنے کا کام سرانجام دے گی۔ برسٹ کوائن نہ صرف پروف آف کاپیسیٹی کی وجہ سے مشہور ہے بلکہ یہ پہلا بلاک چین تھا جس نے "ٹیورنگ کمپلیٹ (Turing Complete) "سمارٹ کونٹریکٹز (smart contracts) کولاگو کیا تھا۔اس سمارٹ کونٹریک کی سب سے مشہور ایپلی کیشن غیر مرکزی لاٹری ایپلی کیشن تھی۔

2.10۔آیوٹا : (IOTA)

آیوٹا (ائی اوٹی اے) [16] دوسری متبادل کرپٹو کرنسی سے بہت منفرد حیثیت رکھتا ہے۔ اسے ایم آیوٹا (MIOTA) کے نام سے بھی جانا جاتا ہے۔یہ دوسری کرنسیوں کی طرح روایتی بلاک چین کے ڈیزائن کو استعمال نہیں کرتا بلکہ اس کے برعکس آلات کی بنیاد پر پیسوں کی ادائیگیوں پر یقین رکھتا ہے۔اس نظام کے لئے اس نے ٹینگل (Tangle) نامی ایک نیا پلیٹ فارم تیار کیا ہے، جو ایک ریاضیاتی ٹیکنیک ڈیریکٹیڈ اے سائیکلیک گرافز-ڈی اے جی (Directed Acyclic Graphs - DAG) استعمال کرتا ہے۔اس کے اپنے ٹرانزیکشن کو صحیح کہلانے کے لئے، ڈی اے جی ٹینگل (Tangle) میں ہر نوڈ کو دوسرے نوڈ پر دو پچھلے ٹرانزیکشنز کو منظور کرنا ضروری ہے ۔ اس کے دو نتائج نکلتے ہیں۔ [17]

ا۔یہ مائینرز کی کردار کو ختم کرتا ہے کیونکہ یہ ٹرانزیکشنز کی رفتار اور تعداد زیادہ ہونے پر رکاوٹ کا باعث بنتا تھا۔

۲۔نیٹ ورک کی ترقی اور رفتار کا تناسب براہ راست اس کے صارفین کی تعداد سے بنتا ہے۔

جیسا کہ آپ جانتے ہیں کہ آج کل انٹرنیٹ اف تھنگز (Internet of Things) کا دور دورہ ہے جہاں ہر آلہ دوسرے آلے سے نیٹ ورک پر جوڑا ہوتا ہے اور یہ آپس میں بات چیت (ڈیٹا کی لین دین) کر سکتے ہیں۔ اسی نظام کو مد نظر رکھتے ہوئے آیوٹا کرپٹو کرنسی تخلیق کی گئی ہے۔ اس پلیٹ فارم پر کسی قسم کی ٹرانزیکشن فیس نہیں ہے اور یہ دعوی کرتا ہے کہ یہ کرپٹو کرنسیز کے اسکیلنگ (scaling) کے مسائل کو مکمل طور پر حل کرتا ہے۔

آیوٹا سنسر والے آلات پر ٹرانزیکشنز اور پروسیسنگ کو بہت آسان بناتا ہے۔ سمجھنے کے لئے اس کی ایک آسان سی مثال یہ ہو سکتی ہے کہ آیوٹا کی اہلیت رکھنے والی وینڈنگ مشین (وہ سلاٹ مشین جس سے کھانے پینے کی اشیاء خریدی جاتی ہیں) سے، بغیر کسی ٹرانزیکشن فیس اور بٹ کوائن کی وابستگی کے، سوڈے کی بوتل حاصل کر سکتے ہیں۔ اس کی اعلیٰ درجے کی مثال یہ ہو سکتی ہے کہ آپ اپنے گھر میں پڑھے دودھ کے خالی کارٹن سے بار کوڈ کو اسکین کریں۔ یہ کوڈ خود بخود ایمازون (Amazon) کو منتقل ہو جائے اور وہاں سے دودھ کے نیا ڈبہ آپ کے گھر پر آ جائے۔ اس میں کوئی شک نہیں کہ جلد ہی یہ کرپٹو کرنسی سینسر سے لیس مشینوں پر ڈیٹا کے تبادلے کی اہلیت اختیار کر لے گی۔[18]

2.11۔ نِم: (NEM)

نِم[19] دوسری کرپٹو کرنسیز کے مقابلے میں ایک مختلف ساخت پر بنائی گئی نئی معاشیاتی تحریک ہے۔ اس کوائن کی یونٹ ایکس ای ایم (XEM) ہے اور دوسرے لفظوں میں اسی نام سے جانا جاتا ہے۔ اس کی ٹرانزیکشن پروسیسنگ پاور بہت تیز ہے جو ایک سیکنڈ میں تقریبا 3،000 ٹرانزیکشنز ہینڈل کرتا ہے۔ اس نیٹ ورک پر بھیجی گئی ٹرانزیکشن کی مجموعی رقم پر 0.1% فیس چارج کرتا ہے۔[20]

دوسرے کرپٹو کرنسیز کے برعکس، اس کا ارکیٹیکچر نِم کوائنز کو اصل میں ٹریس کرنے کی صلاحیت مہیا کرتا ہے اور ایک صارف کے طور پر یہ کافی اعتماد فراہم کرتا ہے۔ یہ خصوصیت اس لحاظ سے بہت فائدہ مند ہے جب اسے مالیاتی اداروں اور انشورنس سروس فراہم کرنے والے اداروں کے ساتھ منسلک کرنے کی ضرورت درپیش ہو۔ اگر آپ یوٹیلیٹی بلز کی ادائیگیوں پر کچھ بچت کرنا چاہتے ہیں تو بٹ کوائن کے مقابلے میں نم کی ایپلی کیشن آپ کو 100 فیصد تک کی بچت کرنے میں مدد دیتا ہے۔ یہ نظام ماحول دوست ہے اور اس کو بحال اور برقرار رکھنا آسان ہے۔[21]

2.12۔اسٹاٹ کوائن:(START)

اسٹاٹ کوائن[22] ایک کراوڈ فنڈنگ پلیٹ فارم ہے جو صرف امداد جمع کرنے اور انعامات دینے کے لئے بنائی گئی ہے۔ کراوڈ فنڈنگ پلیٹ فارم اسے کہتے ہیں جہاں کوئی بھی شخص جا کر اپنا منفرد خیال یا منصوبہ، جسے وہ عمل میں لانا چاہتا ہے وہ سب سے شیئر کرتا ہے۔ صارفین کو اگر وہ منصوبہ پسند آتا ہے تو وہ اس کی مالی مدد کرتے ہیں۔

اسٹاٹ کوائن صرف ان صارفین کو انعام دیتا ہے جو اسٹاٹ جوائن[23] کی ویب سائٹ پر اپنے اسٹاٹ کوائنز یا تو خود رکھتے ہیں یا پھر دوسروں سے بانٹتے ہیں۔ کراوڈ فنڈنگ کے اسٹاٹ جوائن پلیٹ فارم نے کافی مقبولیت حاصل کر لی ہے جو لوگوں کو خیالات، تصورات اور منصوبوں کو فنڈ دینے کی اجازت دیتا ہے۔ وہ لوگ جو اس ویب سائٹ کے ذریعہ فنڈز جمع کرتے ہیں ان کی حوصلہ افزائی کرتے ہوئے اضافی انعام کے طور پر اسٹاٹ کوائنز دیئے جاتے ہیں۔[24]

2.13۔ نکسٹ :(NXT)

نکسٹ[25] ٹرانزیکشن پر اتفاق رائے کروانے کے لئے پروف آف سٹیک کی ٹیکنیک کو استعمال کرتا ہے۔ بٹ کوائن میں ٹرانزیکشن پر اتفاق رائے (کنسنشز) لینے کے لئے مائیننگ معمّہ (puzzle) کو حل کرنا پڑھتا ہے۔اس کے برعکس نکسٹ میں اتفاق رائے کے لئے پروف آف سٹیک کو استعمال کیا جاتا ہے۔ نکسٹ کا شمار ان چند کرپٹو کرنسیز میں ہوتا ہے جو مائیننگ ٹیکنیک کو استعمال نہیں کرتیں۔اس آلٹ کوائن کے افتتاح ہوتے ہی ان کے کوائنز تقسیم کر دیئے جاتے ہیں۔ سکوں کی مسلسل فراہمی اور کسی بھی وقت ان کی دستیابی، کرپٹو کرنسی کی دنیا میں ایک نیا ماحولیاتی نظام بناتی ہے۔اس کی ایک دلچسپ حقیقت یہ بھی ہے کہ نیکسٹ کے نظام میں صارفین اپنی کرپٹو کرنسی متعارف کر سکتے ہیں۔

2.14۔ کیسینو کوائن:(Casino)

کیسینو کوائن[26] جیسا کہ نام سے ہی ظاہر ہے کہ یہ جوئے بازی کے بازار اور اس کے گاہکوں کے لئے متعارف کروائی گئی ہے۔ کیسینو کوائن کی ٹیکنالوجی (سکریپٹ الگورتھم) کی بنیاد بھی وہی ہے جس پر لائٹ کوائن کو تعمیر کیا گیا تھا۔ لیکن صرف برانڈ کا نام ہونے سے عوام باآسانی سمجھ سکتے ہیں کہ اس کے ہدف صارفین کون اور کہاں ہوں گے۔[127]

حوالہ جات:

1۔ https://coinmarketcap.com/all/views/all

2۔ https:// litecoin.org

3۔ https://peercoin.net

4- Prypto, "Bitcoin for Dummies", ch. 13, p 183

5- https://blockgeeks.com/guides/what-is-ethereum-classic

6- https://www.finder.com/ethereum-classic

7-https://www.bitcoinplus.org/xbc_specifications.php

8- https://www.bitcoinplus.org

9- https:// ripple.com

10- https://dash.org

11- https://coinsutra.com/dash-cryptocurrency

12- https://www.burst-coin.org

13- https://bitcointalk.org

14- https://en.wikipedia.org/wiki/Burstcoin

15- https://coincentral.com/what-is-burstcoin-beginners-guide

16- https://iota.org

17- https://www.investopedia.com/news/closer-look-iota

18- Ibid.

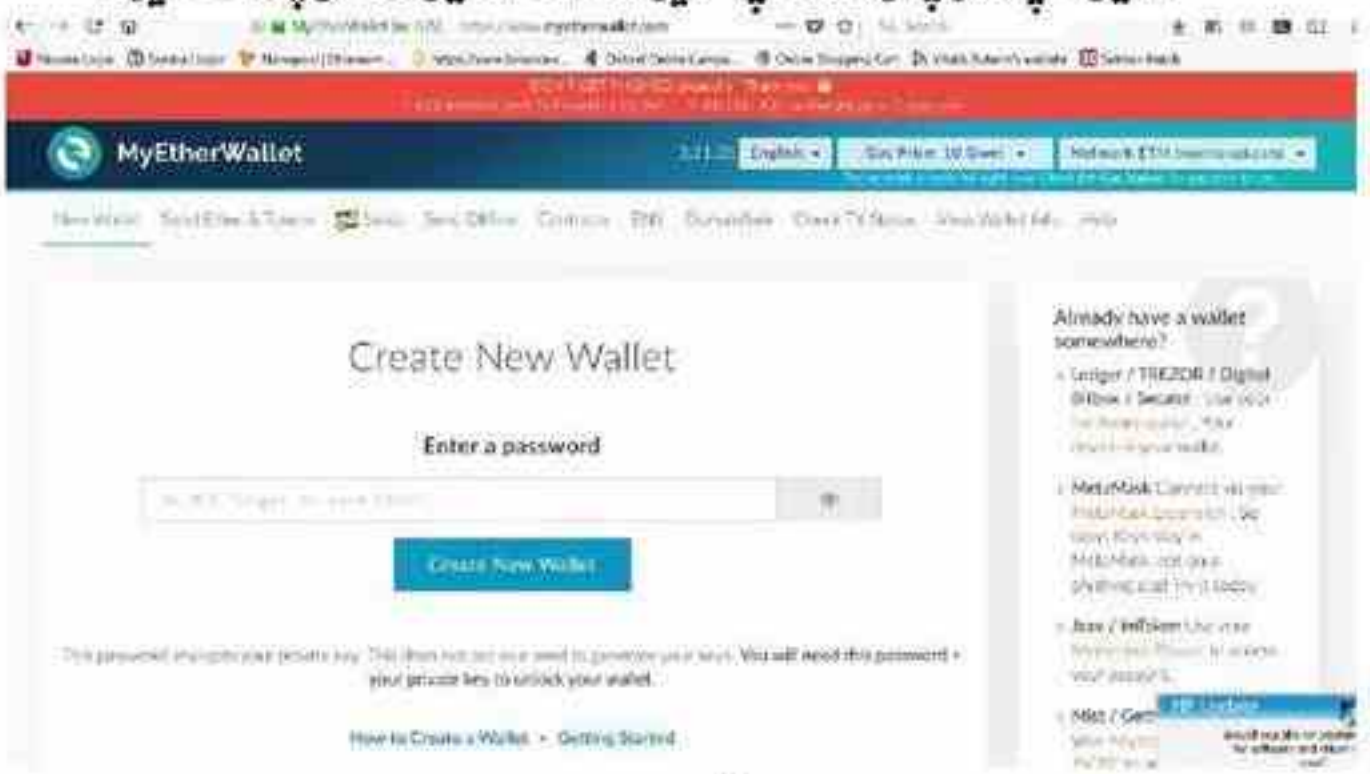
19- https://nem.io

20- https://www.cryptorecorder.com/2018/01/18/ripple-xrp-three-altcoins-buy-3
21- Ibid.
22- https://startcoin.org
23- https://startjoin.com
24- Prypto, "Bitcoin for Dummies", ch. 13, p 184
25- https://nxtplatform.org
26- ttp://casinocoin.org
27- Prypto, "Bitcoin for Dummies", ch. 13, p 185
28- https://namecoin.org
29- https://www.ethereum.org
30- https://ethereumclassic.github.io

اِیتھریم مائننگ

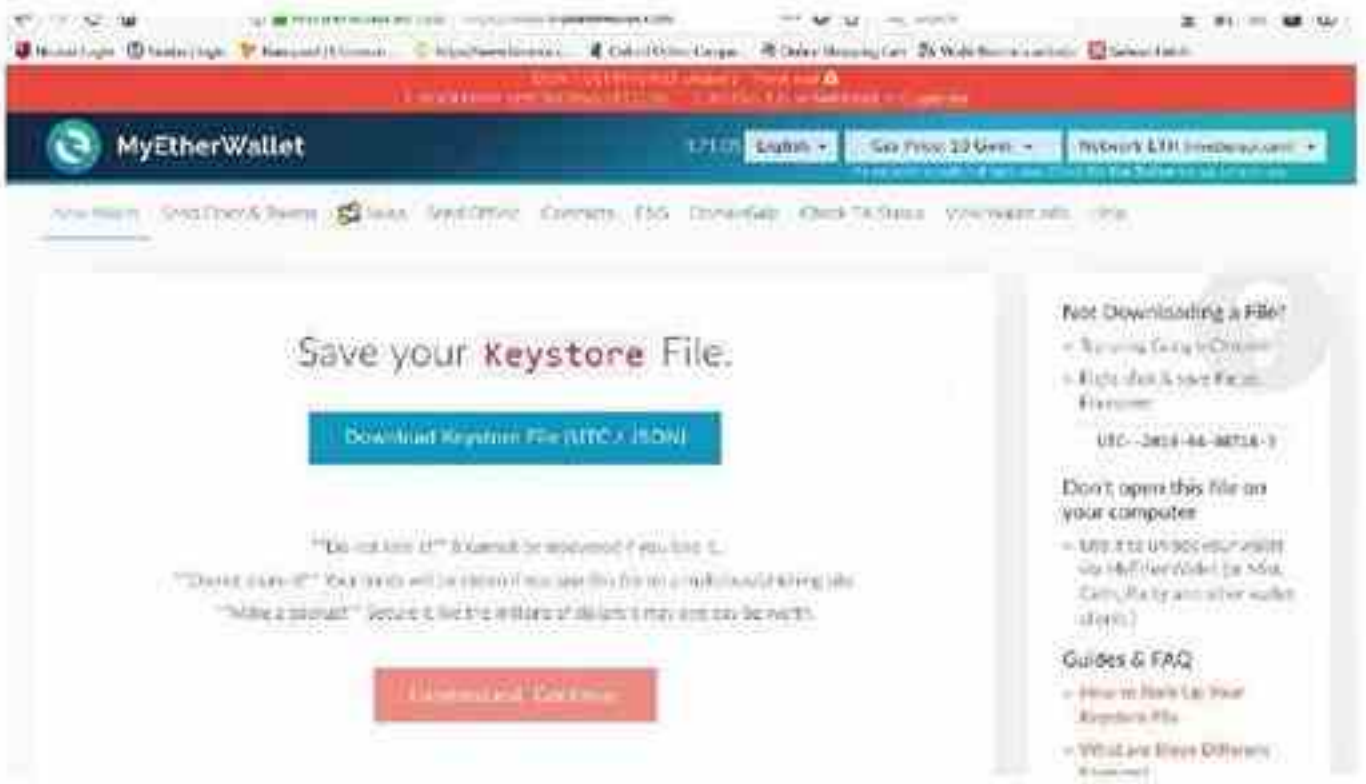
بہت سے لوگ سوال کرتے ہیں کہ اِیتھریم مائننگ کیسے کرتے ہیں۔اِس باب میں ہم آپ کو اِیتھریم، ایتھریم کلاسک اور وہ تمام کرپٹو کرنسیز جن کی مائننگ گرافکل پروسیسنگ یونٹ Graphical Processing Unit (GPU)سے ہو سکتی ہے، کا آسان ترین طریقہ بتائیں گے۔

1. سب سے پہلے تو آپ MYETHERWALLETپر جا کر اپنا والٹ بنائیں آپ کوئی پاس ورڈ ٹائپ کریں اور والٹ بنائیں اور بٹن پر کلک کریں۔



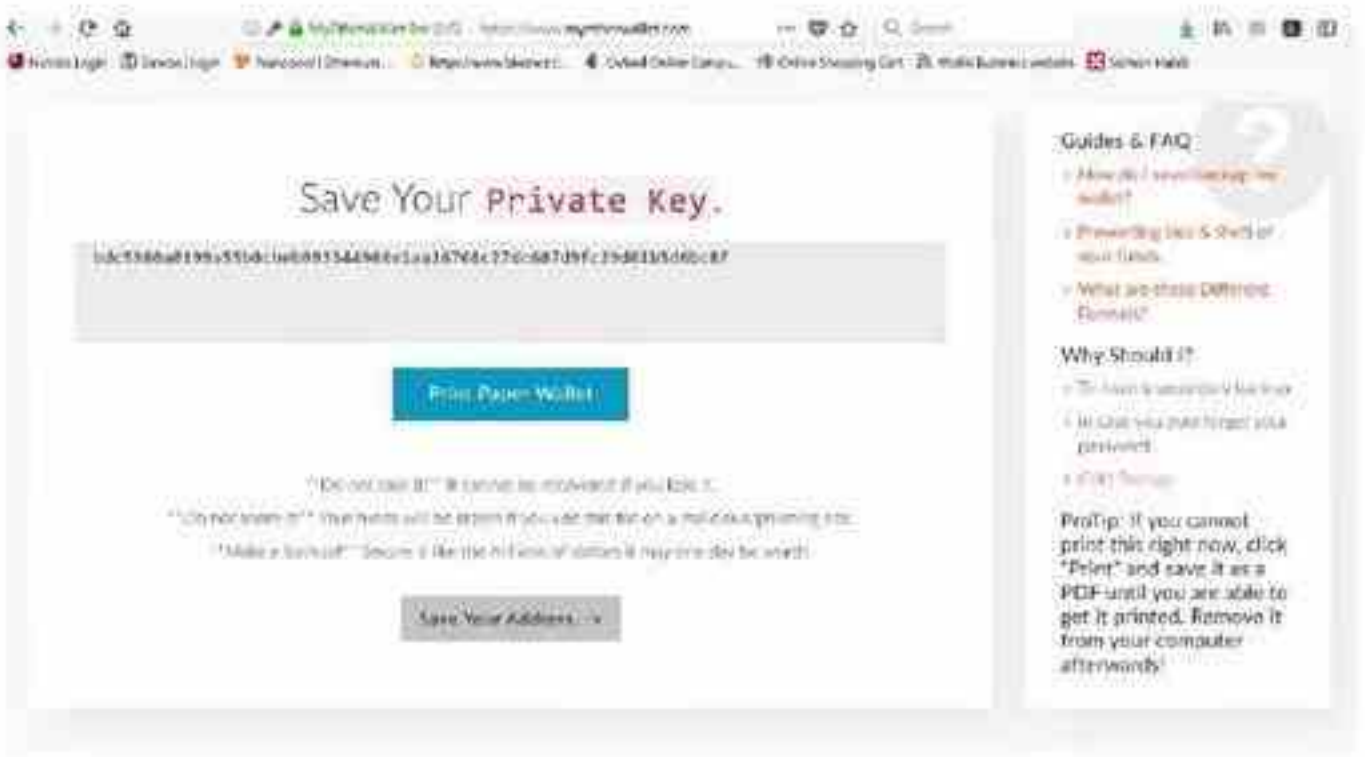
تصویر 1

2. اب کی اسٹروک(Keystroke)فائل کو اپنی ہارڈ ڈسک میں محفوظ کر لیں۔



تصویر2

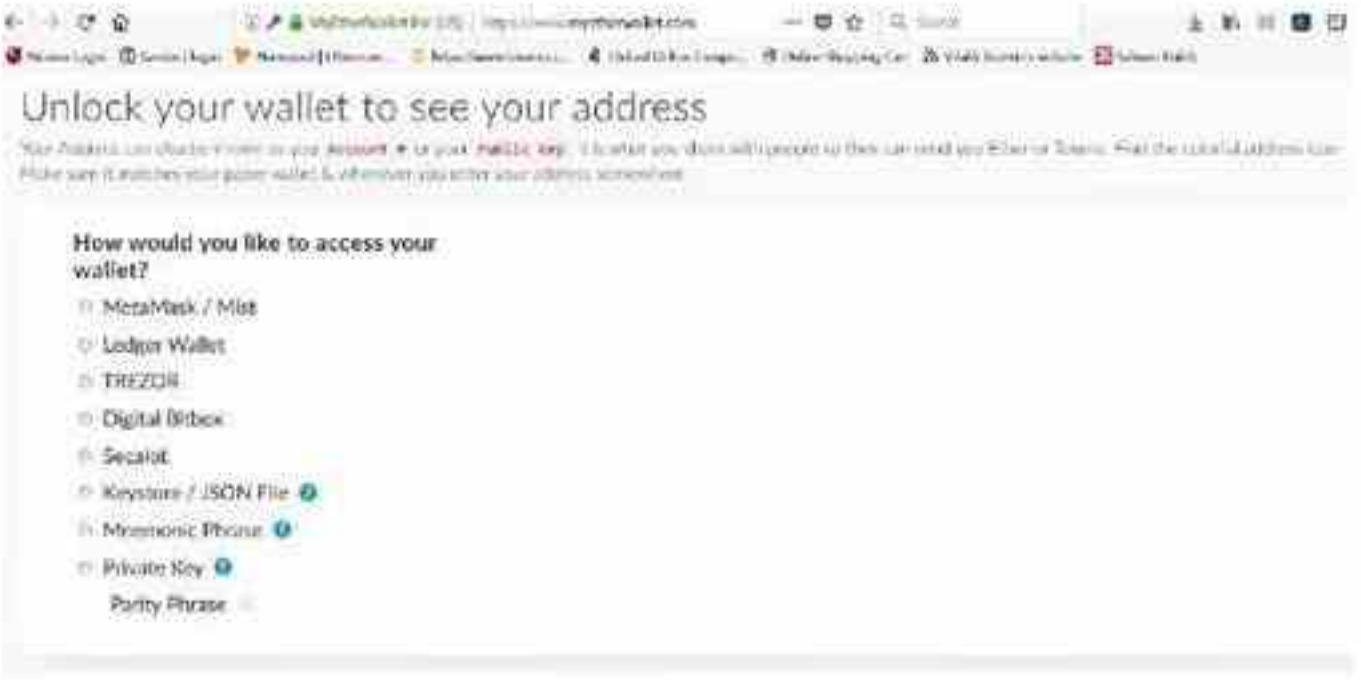
3. اب اپنی پرائیویٹ کی (Private Key) کو کاپی پیسٹ کر کے محفوظ کرلیں



تصویر3

یہ کی اگر آپ سے گم ہو گئی تو آپ اپنا والٹ استعمال نہیں کر سکیں گے اور اس میں موجود ساری رقم ضائع ہو جائے گی۔

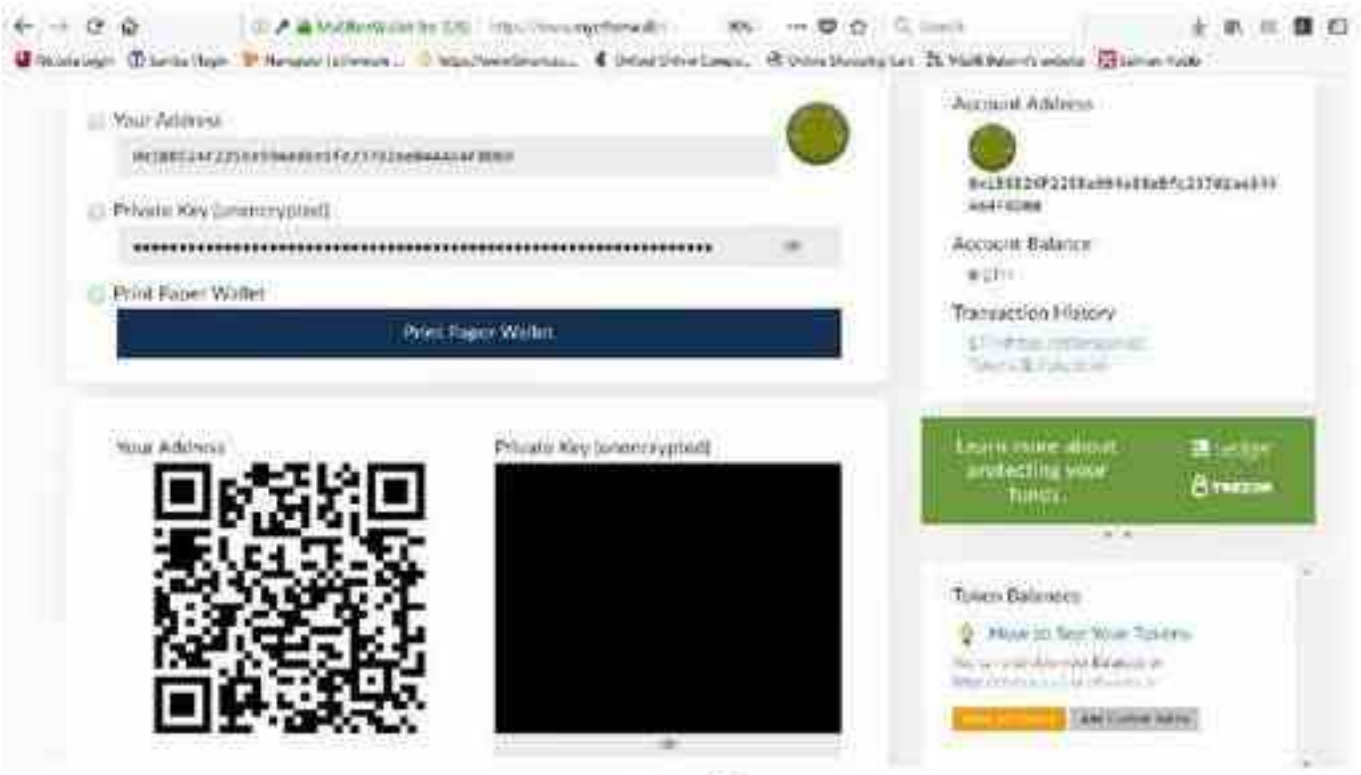
4. اب کی اسٹروک فائل یا پرائیویٹ کی کی مدد سے اپنا والٹ کھولیں۔



تصویر 4

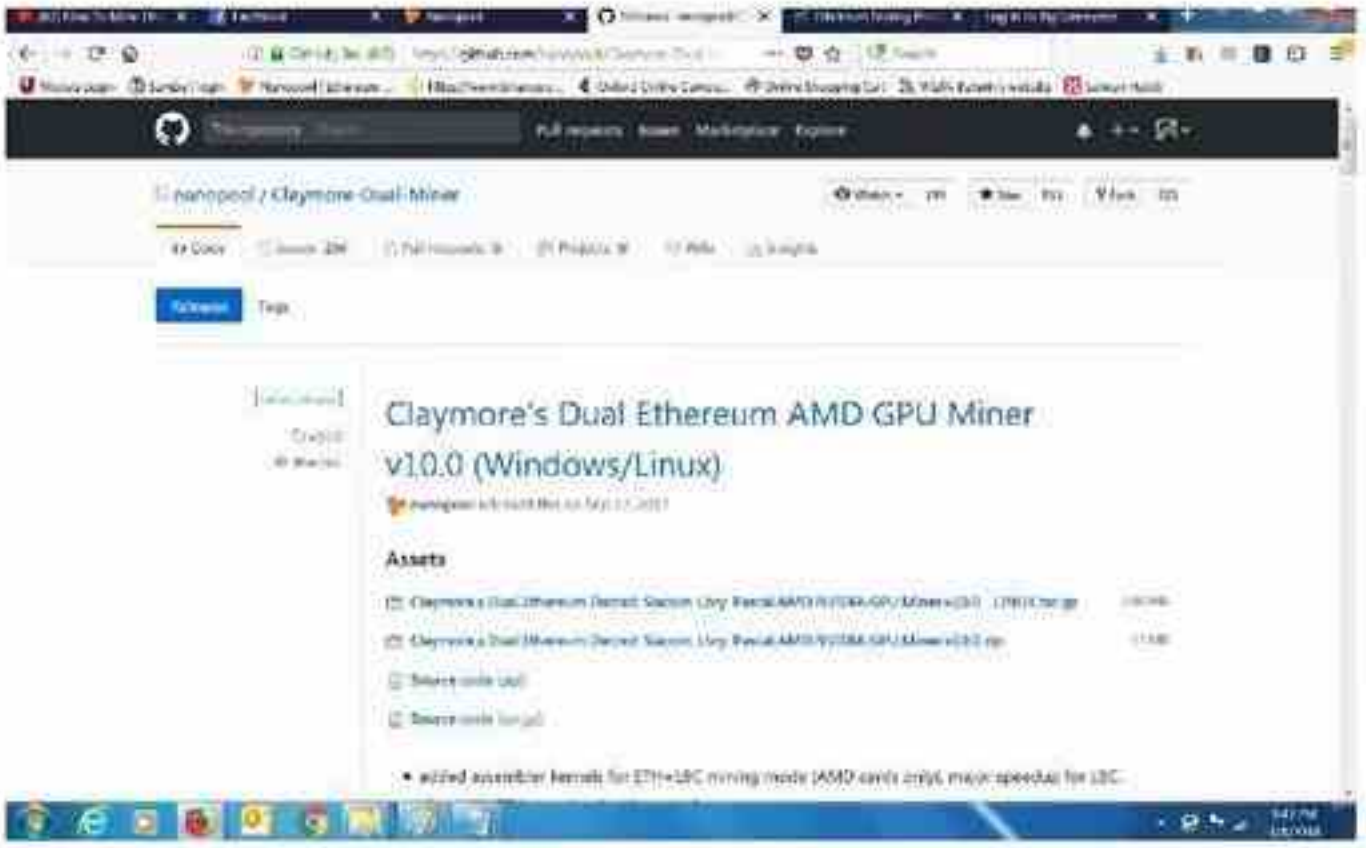
5. آپ کو نظر آئے گا کہ آپ کے والٹ میں کوئی رقم موجود نہیں

6.



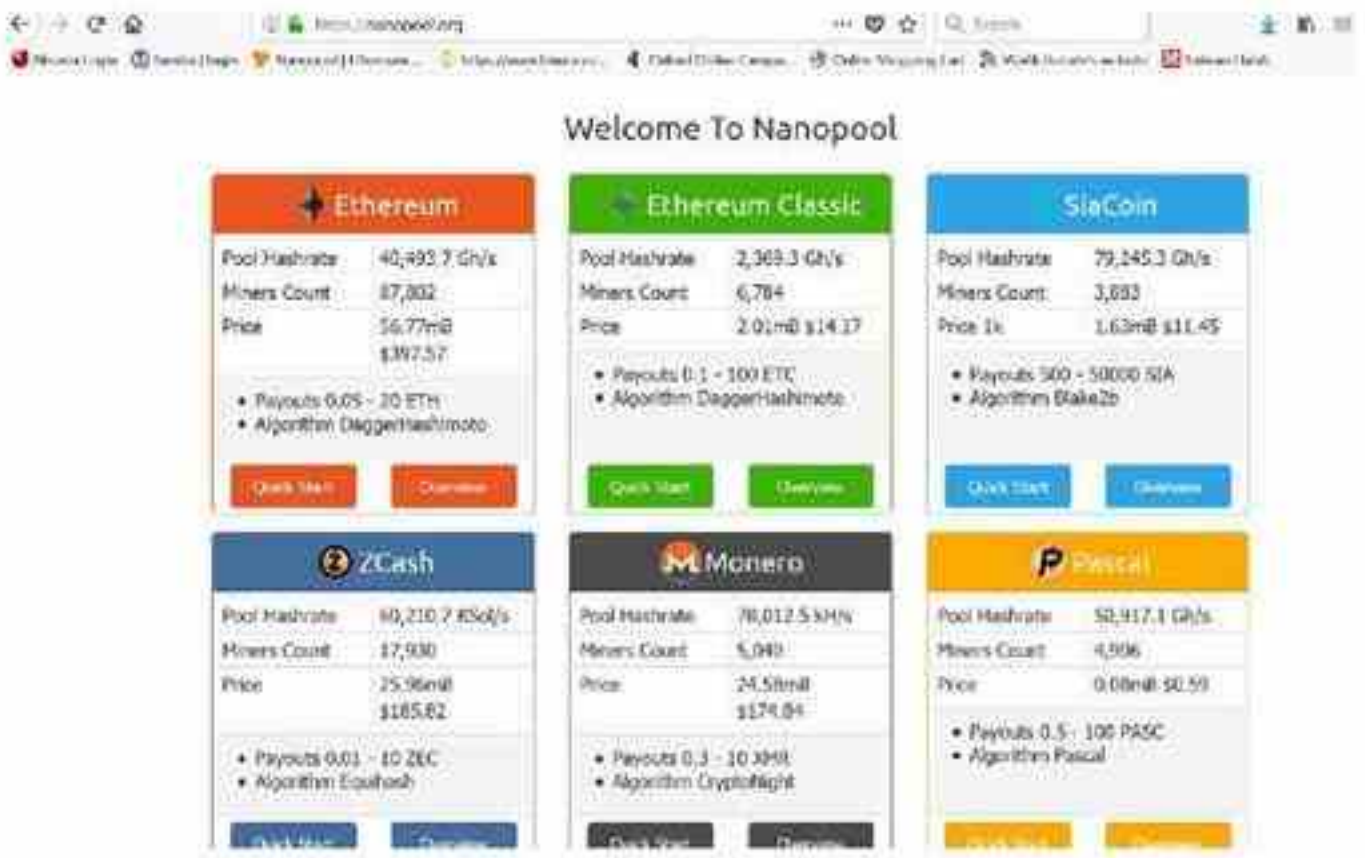
تصویر 5

7. اب آپ گوگل پر Clay More مائنر سرچ کر کے ڈاؤن لوڈ کر لیں



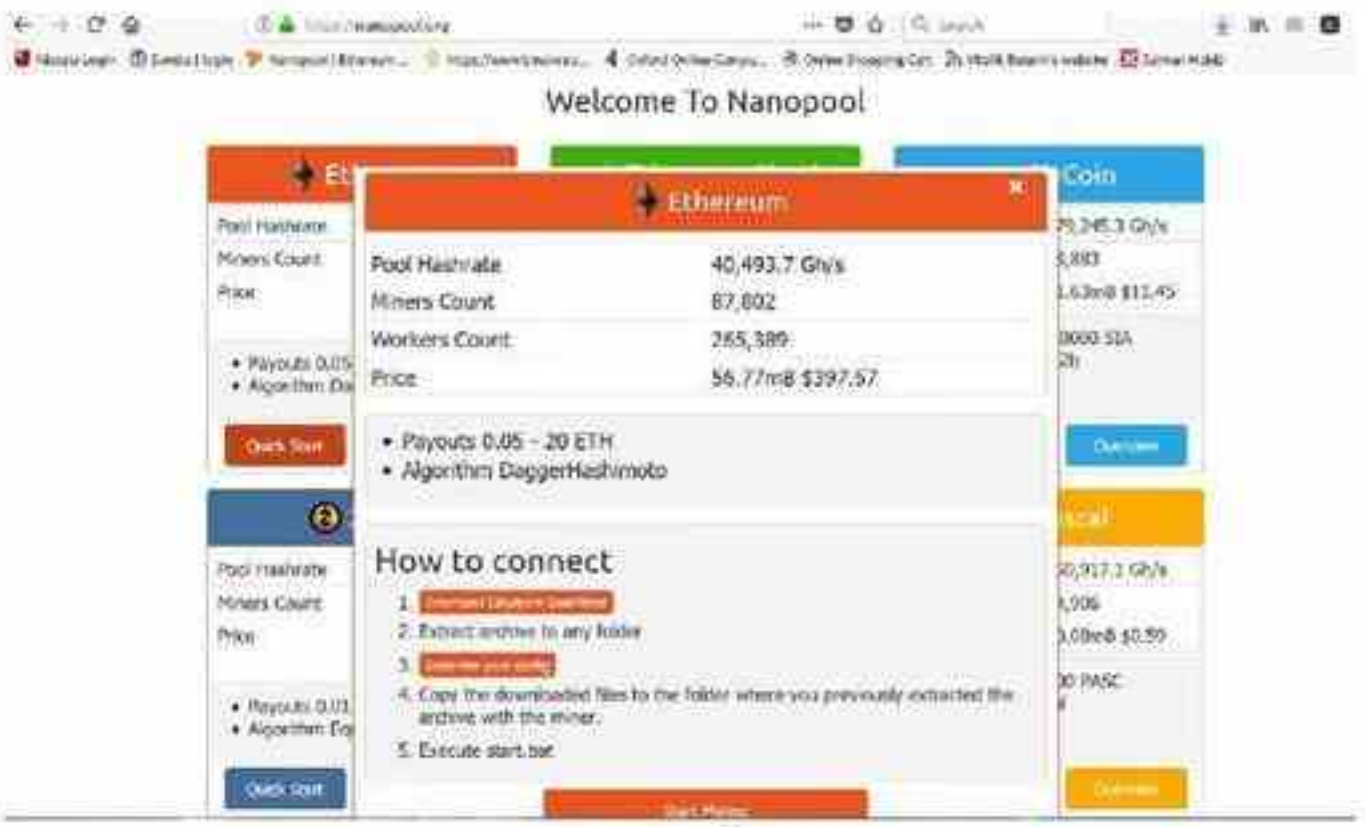
تصویر6

8. اب نینو پول Nano Pool کی ویب سائٹ پر جا کر، ایتھریم پر کوئک سٹارٹ پر کلک کریں



تصویر 7

9. کونفگ فائل پر کلک کریں

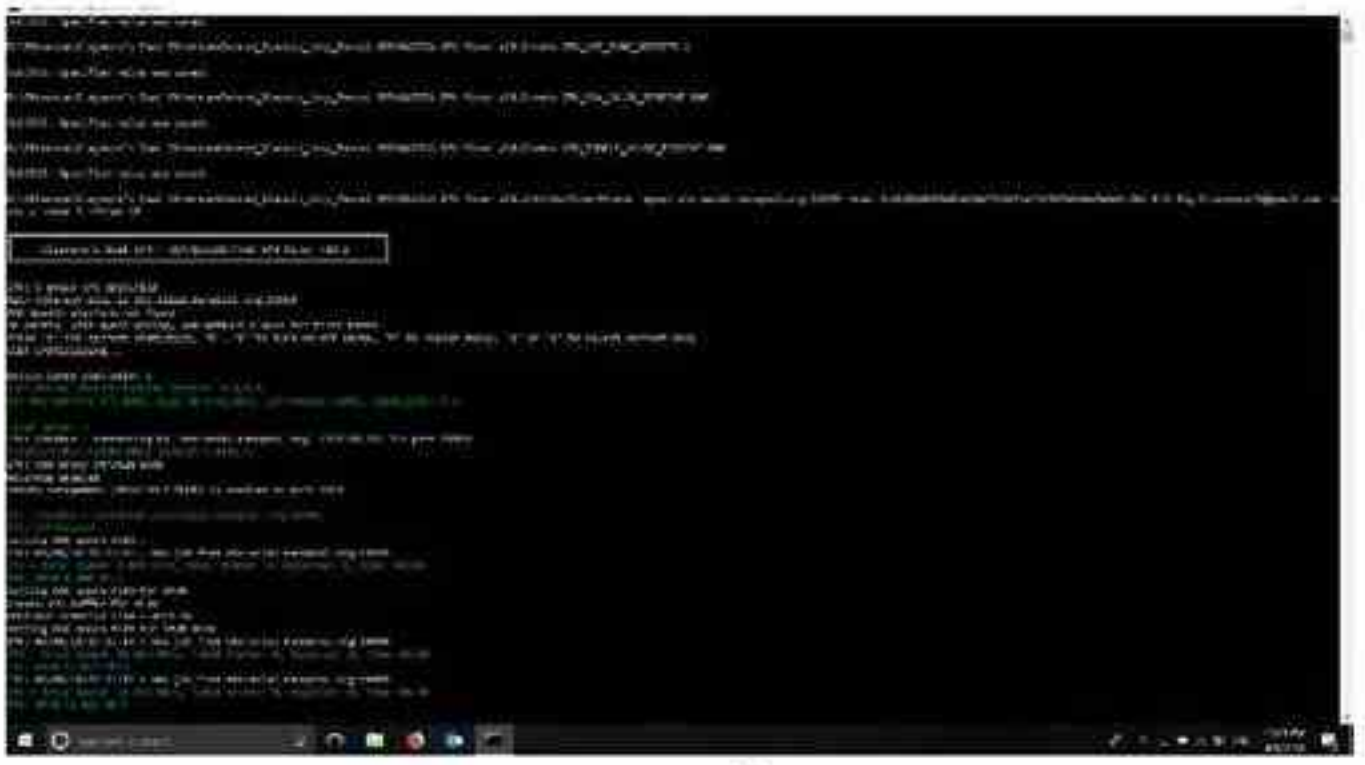


تصویر 8

10. کوئنگ اسٹارٹ میں سرور پر Asia اور کوائن میں ایتھریم کو منتخب کریں۔

تصویر 9

11. کونفگ فائل کو ڈاؤن لوڈ کر کے Clay More کے فولڈر میں کاپی کر کے Start فائل کو Run کریں۔



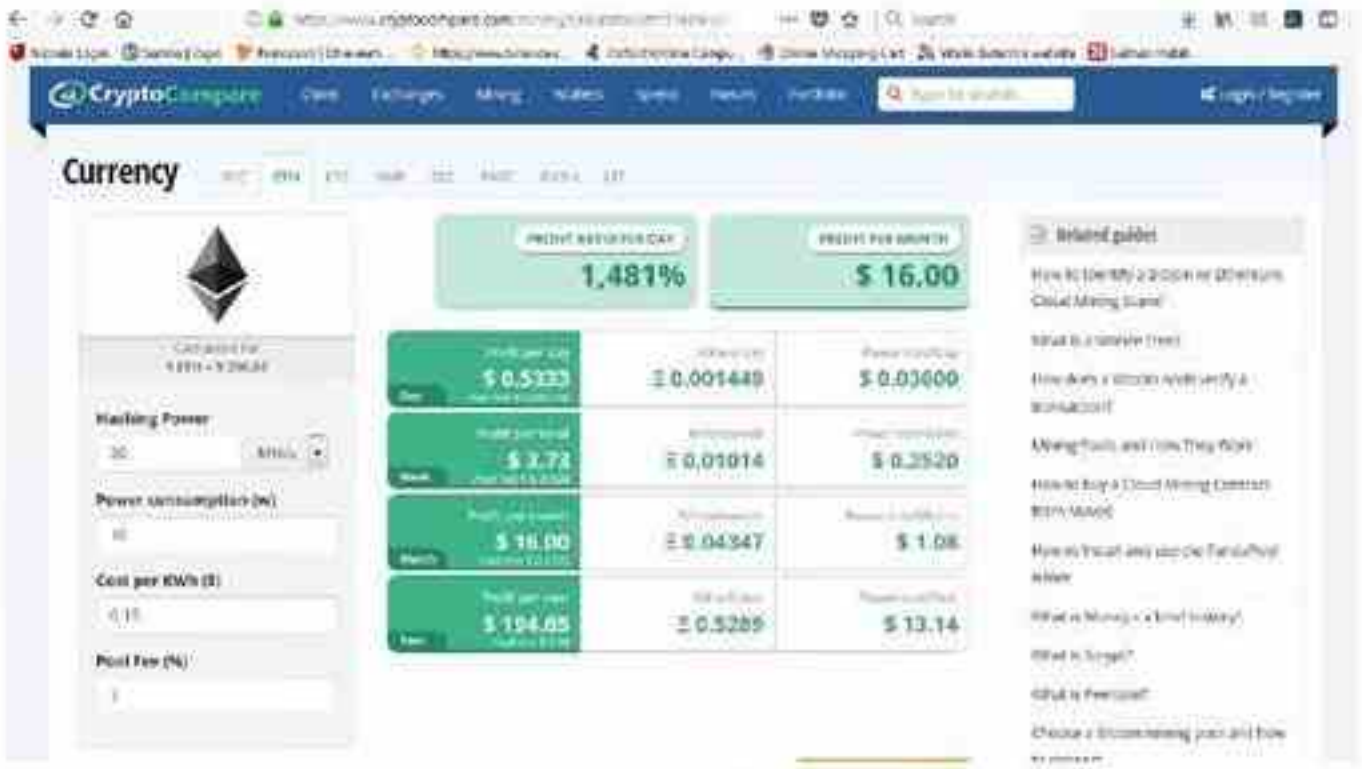
تصویر 10

12. نینوپول میں واپس جاکر ایڈریس بار پر اپنا والٹ ایڈریس ڈالیں۔

تصویر 11

13. آپ مائننگ کر رہے ہیں۔ کسی اور کوائن کی مائننگ کے لئے نینو پول سے وہ والا کوائن منتخب کر کے کونفگ فائل بنالیں۔

اگر آپ بہت سی مشینوں سے مائننگ فارم بنانا چاہتے ہیں تو پہلے Crypto Compare ویب سائٹ کے مائننگ سیکشن میں جا کر یہ دیکھ لیں کی یہ آپ کو منافع بخش بھی رہے گا یا نہیں۔ عمومی طور پر اگر آپ کی بجلی کی قیمت 6 روپے یونٹ سے زیادہ ہے تو آپ کو مائننگ سے کوئی خاطر خواہ فائدہ نہیں ہو گا۔ پاکستان میں 15 روپے تک کا یونٹ ہے۔



تصویر 12

تصویر 13

مندرجہ ذیل تصویریں میرے مائننگ فارم کی ہیں مگر یہ امریکہ میں ہے جہاں بجلی سستی ہے۔
آپ 12 GPU کارڈز کے ساتھ (قریباً 200 MHZ) پر آج کل
0.4- 0.5 ایتھریم ہر ماہ مائن کر سکتے ہیں اور اس پر لاگت 7 لاکھ آتی ہے۔

تصویر14

تصویر15

تصویر16

ایتھریم(Ethereum)پر قرطاسِ ابیض

اگلی نسل کا ذہین معاہدہ اور عدم مرکزیت کا اطلاقی پلیٹ فارم

از: ویٹالک بیوٹیرِن

جنوری 2009ء میں، جب ساتوشی ناکاموتو نے پہلی بار "بِٹ کوائن بلاک چین" کو رُوبہ عمل کیا، انہوں نے بیک وقت دو بنیادی اور غیر آزمودہ تصورات متعارف کروائے: ایک "بِٹ کوائن" (BitCoin)، جو عدم مرکزیت کی حامل، کمپیوٹروں کے مابین (P2P) منتقل ہونے والی آن لائن کرنسی تھی جو اپنی قدر کو کسی پشت پناہی، اندرونی (تفویض کردہ) قدر، یا جاری کرنے والے کسی مرکزی ادارے (یا فرد) کے بغیر برقرار رکھتی ہے۔ اب تک ایک سکے (کرنسی) کی حیثیت سے "بِٹ کوائن" عوام کی بہت زیادہ توجہ حاصل کر چکی ہے، نہ صرف سیاسی نقطۂ نگاہ سے ایک ایسی کرنسی کی حیثیت سے جسے کسی مرکزی بینک کی سرپرستی حاصل نہ ہو، بلکہ اپنی قیمت میں انتہائی نوعیت کے اتار چڑھاؤ کی وجہ سے بھی۔ تاہم، ساتوشی کے اس غیر معمولی تجربے کا ایک اور حصہ بھی ہے، جو یکساں طور پر اہمیت رکھتا ہے: ثبوتِ کار (proof-of-work) پر مبنی "بلاک چین" کا تصور، یہ اجازت دیتا ہے کہ منتقلی (ٹرانزیکشن) کی ترتیب پر عوامی اتفاقِ رائے ہو۔ اور اگر ایک اطلاقیے (اپلی کیشن) کے طور پر بات کی جائے، تو بٹ کوائن کی وضاحت ایک "پہل پر مبنی نظام" (first-to-file system) کے طور پر کی جاسکتی ہے: یعنی اگر کسی کے پاس 50 بٹ کوائنز ہیں، اور وہ بیک

وقت ان 50 بٹ کوائنز کو دو الگ الگ وصول کنندگان، A اور B کی طرف بھیجے، تو ان میں سے جس منتقلی کی پہلے تصدیق ہو گی، اسی پر کام کیا جائے گا (یا اسے "پروسیس" کیا جائے گا)۔ ایسا کوئی داخلی طریقہ نہیں جس سے یہ معلوم ہو سکے کہ ان دونوں میں سے کونسی ٹرانزیکشن سب سے پہلے پہنچی، اور اس مسئلے نے عشروں سے ایک غیر مرکزی ڈیجیٹل کرنسی پر پیش رفت کو روکے رکھا تھا۔ ساتوشی کی "بلاک چین" پہلا قابلِ بھروسہ، غیر مرکزی حل تھی۔ اور اب، زیادہ توجہ بڑی تیزی سے بٹ کوائن ٹیکنالوجی کے دوسرے حصے کی طرف منتقل ہو رہی ہے، اور وہ یہ ہے کہ بلاک چین کے تصور کو کس طرح صرف پیسے (کی لین دین) سے ہٹ کر بھی استعمال کیا جا سکتا ہے۔

بلاک چین کے وہ اطلاق جن کا زیادہ تذکرہ کیا جاتا ہے ان میں "من پسند کرنسیوں" (کسٹم کرنسیز) اور مالیاتی آلات ("رنگین سکّوں") کا ڈیجیٹل اثاثوں کے طور پر اظہار، کسی پس پردہ طبیعی آلے (اسمارٹ پراپرٹی) کی ملکیت، کبھی خراب نہ ہونے والے اثاثے جیسے کہ ڈومین نیمز (نیم کوائن)؛ اور ان ہی کے ساتھ، جدید تر اطلاقات بھی جیسے کہ غیر مرکزی ایکسچینج، مالیاتی ماخوذات، کمپیوٹر سے کمپیوٹر تک براہِ راست (P2P) جوا اور بلاک چین شناخت اور ساکھ پر مبنی نظام وغیرہ۔ تحقیق کا ایک اور اہم میدان "ذہین معاہدے" (smart-contracts) بھی ہو سکتا ہے؛ یعنی ایسے نظام جو ڈیجیٹل اثاثوں کو پہلے سے طے شدہ، خودکار اصولوں کی مطابقت میں از خود حرکت دے سکیں۔ مثلاً شخص ایک ایسا مالیاتی معاہدہ بھی کر سکتا ہے جو اس طرح سے ہو: "A روزانہ کرنسی کے X یونٹ تک نکلوا سکتا ہے، B روزانہ کرنسی کے Y یونٹ تک نکلوا سکتا ہے، A اور B دونوں مل کر کچھ بھی رقم نکلوا سکتے ہیں، اور A کے پاس اختیار ہے کہ وہ B کی کرنسی نکلوانے کی صلاحیت کو ختم کر دے۔" اس میں منطقی توسیع "غیر مرکزی خود مختار تنظیمیں" (DAOs) ہیں، یعنی ایسے طویل مدتی ذہین

معاہدے جو نہ صرف اثاثے رکھتے ہوں بلکہ پوری تنظیم کیلئے قوانین کی بھی رمز کاری (encoding) کریں۔ ایتھریم جو کچھ فراہم کرنے کا ارادہ رکھتا ہے وہ ایک بلاگ چین ہے جس میں ایک بھرپور ''ٹیورنگ کمپلیٹ'' پروگرامنگ لینگویج ہو جسے ایسے ''معاہدے'' تخلیق کرنے میں استعمال کیا جاسکے جو کیفیت میں تقلیب (transition) کیلئے خود اختیاری تفاعلات (فنکشنز) کی رمز کاری کر سکیں، صارفین کو سہولت دے سکیں کہ وہ مذکورہ بالا نظاموں میں سے کسی کو بھی تخلیق کر سکیں، اور ایسے بہت سے دوسرے اطلاق جن کا تصور اب تک نہیں کیا گیا؛ اور وہ بھی صرف سادہ منطق (لاجک) کو صرف چند سطروں پر مشتمل کوڈ کی شکل میں لکھ کر۔

فہرستِ مضامین

تاریخ

بٹ کوائن بطور ''اسٹیٹ ٹرانزیشن سسٹم'' (کیفیتی تقلیبی نظام)

مائننگ (کان کنی)

مرکل شجر (مرکل ٹریز)

بلاک چین کے متبادل اطلاقات

اسکرپٹنگ

ایتھریم

ایتھریم اکاؤنٹس

پیغامات اور منتقلیاں (ٹرانزیکشنز)

ایتھریم کے تحت کیفیتی تقلیب (اسٹیٹ ٹرانزیشن) کا تفاعل
کوڈ پر عملدرآمد (کوڈ ایگزیکیوشن)
بلاک چین اور مائننگ

اطلاقات

ٹوکن سسٹمز
مالیاتی ماخوذات
شناخت اور ساکھ سے متعلق نظام
ڈی سینٹرلائزڈ فائل اسٹوریج (فائلوں کی عدم مرکزیت پر مبنی ذخیرہ کاری)
ڈی سینٹرلائزڈ آٹونومس آرگنائزیشنز (عدم مرکزیت پر مبنی خود مختار تنظیمیں)

مزید اطلاقات

متفرقات اور خدشات

ترمیم شدہ GHOST اطلاق کاری
فیس
حساب کاری اور ٹیورنگ تکمیل پذیری (Turing-Completeness)
کرنسی اور اجراء
مائننگ میں مرکزیت
بڑے پیمانے پر استعمال کی صلاحیت (Scalability)
اس سب کا مجموعہ: ڈی سینٹرلائزڈ اپلی کیشنز (عدم مرکزیت پر مبنی اطلاقیے)

حرفِ آخر

تاریخ

عدم مرکزیت پر مبنی ڈیجیٹل کرنسی اور متبادل اطلاقات جیسے کہ پراپرٹی رجسٹریز کا تصور عشروں سے موجود ہے۔ 1980ء اور 1990ء کے عشروں میں گمنام ای کیش پروٹوکولز نے، جو کرپٹوگرافی کی ابتدائی شکل "چاؤمیئن بلائنڈنگ" (Chaumian-blinding) پر انحصار کرتا تھا، اعلیٰ درجے کے تخلیے (پرائیویسی) والی کرنسی فراہم کی، لیکن یہ پروٹوکول وسیع پیمانے پر توجہ حاصل کرنے میں ناکام ہو گیا کیونکہ اس کا انحصار ایک مرکزی ثالث (بااختیار درمیانی فریق) پر تھا۔ 1998ء میں وی ڈائی کی "بی منی" (b-money) وہ پہلی تجویز بنی جس میں حسابی معمے حل کر کے دولت تخلیق کرنے کا خیال پیش کیا گیا تھا جبکہ عدم مرکزیت پر مبنی اتفاقِ رائے پر بھی بات کی گئی تھی۔ البتہ، اس تجویز میں اس امر کی کچھ خاص تفصیلات نہ تھیں کہ عدم مرکزیت پر مبنی اتفاقِ رائے کی عملی اطلاق پذیری کیونکر ممکن بنائی جاسکے گی۔ 2005ء میں ہال فنی نے "بار بار استعمال کے قابل ثبوت ہائے کار" (reusable proofs of work) کا تصور پیش کیا۔ یہ ایک ایسا نظام ہے جو "بی منی" کو ایڈم بیک کے "ہیش کیش معموں" کے ساتھ (جنہیں حسابی طور پر حل کرنا بہت مشکل ہے) استعمال کرتا ہے۔ یہ دراصل کرپٹو کرنسی ہی کا تصور تھا لیکن، ایک بار پھر، بھروسہ مند کمپیوٹنگ پر استوار ہونے کے باعث یہ بھی اپنے اصل ہدف یعنی مثالی مقام کو حاصل کرنے میں ناکام رہا۔

چونکہ یہ کرنسی پہلے فائل ہونے والی (first-to-file) اپیلی کیشن ہے، جہاں منتقلی کی ترتیب اکثر کلیدی اہمیت رکھتی ہے، اس لئے عدم مرکزیت والی کرنسیوں کو عدم مرکزیت پر مبنی اتفاقِ رائے والے حل کی بھی ضرورت ہوتی ہے۔ بٹ کوائن سے پہلے کے تمام کرنسی پروٹوکولز (قواعد و ضوابط) کی راہ میں یہ حقیقت ہی سب سے بڑی رکاوٹ تھی؛ اور اگرچہ

محفوظ ''بائزنٹائن فالٹ ٹالرینٹ''(Byzantine-fault-tolerant) کثیر فریقی اتفاقِ رائے کے نظاموں پر کئی سال تک تحقیق بھی ہو چکی تھی، لیکن بیان کردہ تمام پروٹوکولز صرف آدھا مسئلہ ہی حل کر رہے تھے۔ ان پروٹوکولز میں یہ فرض کیا گیا تھا کہ نظام کے تمام شرکاء معلوم ہیں، اور حفاظت (سکیوریٹی) کیلئے کچھ اس طرح سے گنجائش پیدا کی گئی تھی ''اگر N فریقین حصہ لیں، تو نظام N/4 کی تعداد میں بے ایمان کرداروں (شرکاء) کو سہار سکتا ہے۔'' البتہ، یہ مسئلہ ہے کہ، کہ ایک گمنام ترتیب میں ایسی حفاظتی گنجائشوں کی وجہ سے (نظام پر) ''سائبل (Sybil) حملوں'' کا خدشہ بڑھ جاتا ہے، جن میں ایک حملہ آور کسی ایک سرور یا بوٹ نیٹ پر ہزاروں نقلی مقاماتِ اتصال (نوڈز) تخلیق کر سکتا ہے؛ اور پھر ان نوڈز کو استعمال کرتے ہوئے یک طرفہ طور پر اکثریتی حصہ حاصل کر سکتا ہے۔

ساتوشی کی جدت طرازی سے ایک ایسا تصور بہم آیا جس میں عدم مرکزیت پر مبنی بہت ہی سادہ پروٹوکول کو، جس کا دارومدار اُن نوڈز پر تھا جو ہر دس منٹ میں ٹرانزیکشنز کو ایک ''بلاک'' میں یکجا کرتے ہوئے مسلسل بڑھتی ہوئی ایک بلاک چین تخلیق کرتی تھیں، ثبوتِ کار کے عملی نظام سے مربوط کر دیا گیا تھا جس کے ذریعے نوڈز کو نظام میں شراکت کا حق حاصل ہوتا ہے۔ اگرچہ یہاں بھی کمپیوٹر کی وسیع تر طاقت والی نوڈز اسی تناسب سے زیادہ اثر پذیری رکھتی ہیں، لیکن پورے نیٹ ورک کے مقابلے میں زیادہ کمپیوٹیشنل پاور (کمپیوٹر کی طاقت) کا استعمال، لاکھوں جعلی نوڈز بنانے کے مقابلے میں کہیں زیادہ مشکل ہے۔ باوجودیکہ بٹ کوائن بلاک چین ماڈل بہت خام اور سادہ ہے، لیکن پھر بھی یہ کافی حد تک بہتر ثابت ہو چکا ہے؛ اور آئندہ پانچ سال کے دوران دنیا بھر میں دو سو سے زائد (کرپٹو) کرنسیوں اور پروٹوکولز کیلئے ٹھوس بنیاد کا کام کرے گا۔

بٹ کوائن بطور کیفیتی تقلیبی نظام(Stat Transition System) تکنیکی نقطۂ نگاہ سے، بٹ کوائن کے کھاتے(ledger)کوایک کیفیتی تقلیبی نظام(اسٹیٹ ٹرانزیشن سسٹم) تصور کیا جاسکتا ہے، جس میں ایک ''کیفیت''(state)ہو جو تمام موجودہ بٹ کوائنز کی ملکیت کی حیثیت پر مشتمل ہو؛ اور ایک ''کیفیتی تقلیبی تفاعل''(اسٹیٹ ٹرانزیشن فنکشن) بھی ہو جو ایک کیفیت اور ٹرانزیکشن وصول کرے(اِن پُٹ لے)اور ایک نئی کیفیت کو بطور نتیجے کے آؤٹ پٹ میں دے۔ مثلاً روایتی بینکاری نظام میں یہ کیفیت ایک ''بیلنس شیٹ'' ہوتی ہے، ٹرانزیکشن ایک درخواست ہوتی ہے جس کے تحت X ڈالر رقم، A سے B تک پہنچائی جاتی ہے(منتقل کی جاتی ہے)، جبکہ اسٹیٹ ٹرانزیشن فنکشن A کے اکاؤنٹ میں سے X ڈالر کی قدر کم کرتا ہے اور X ڈالر کی قدر B کے اکاؤنٹ میں بڑھا دیتا ہے۔ اگر A کے اکاؤنٹ میں پہلے ہی X ڈالر سے کم رقم موجود ہے، تو اسٹیٹ ٹرانزیشن فنکشن غلطی(ایرر)لوٹائے گا۔ یہ بات فارمولے کے طور پر کچھ اس طرح بھی لکھی جاسکتی ہے:

APPLY(S,TX) –> S' or ERROR

مذکورہ بالا بینکاری نظام میں:

APPLY({ Alice: $50, Bob: $50 },"send $20 from Alice to Bob") = { Alice: $30, Bob: $70 }

لیکن:

APPLY({ Alice: $50, Bob: $50 },"send $70 from Alice to Bob") = ERROR

بٹ کوائن کے تحت ''کیفیت'' (اسٹیٹ) دراصل سکّوں (کوائنز) کا مجموعہ ہوتی ہے (تکنیکی الفاظ میں: ''غیر خرچ شدہ منتقلی پر مبنی آؤٹ پٹ'' یا UTXO) جو ڈھالی گئی ہوں اور جنہیں اب تک خرچ نہ کیا گیا ہو، جبکہ ہر UTXO میں ایک مقدار (denomination) اور مالک (کی معلومات) ہوں (جنہیں 20 بائٹ والے ایک ایڈریس سے بیان کیا جاتا ہے جو بنیادی طور پر ایک کرپٹو گرافک پبلک کی ہوتی ہے[1])۔ ایک ٹرانزیکشن میں ایک یا زیادہ اُن پٹ ہو سکتے ہیں، جن میں سے ہر ایک کسی موجودہ UTXO اور ایسے کرپٹو گرافک دستخط کا حوالہ موجود ہوگا جسے پرائیویٹ کی رکھنے والے متعلقہ مالک نے پتے (ایڈریس) سے تیار کیا گیا ہوگا؛ اور ایک یا زیادہ آؤٹ پٹ بھی ہو سکتے ہیں، جن میں سے ہر ایک آؤٹ پٹ ایک نئی UTXO پر مشتمل ہوگا جسے کیفیت میں جمع کیا جائے گا۔

اسٹیٹ ٹرانزیشن فنکشن یعنی APPLY(S,TX) > S' ایسی استعمال کیا جا سکتا ہے:

1۔ TX میں ہر اِن پُٹ کیلئے:

اگر UTXO جس کا حوالہ دیا گیا ہے وہ S نہ ہو، تو ایرر لوٹائے۔

اگر فراہم کردہ دستخط UTXO کے مالک سے مطابقت نہ رکھتا ہو، تو ایرر لوٹائے۔

2۔ اگر ان پُٹ کئے گئے تمام UTXO کی مقداروں (ڈینومی نیشنز) کا مجموعہ، UTXO کی آؤٹ پُٹ کی گئی تمام مقداروں کے مجموعے سے کم ہو، تو ایرر لوٹائے۔

3۔اِن پُٹ کئے گئے تمام UTXO ہٹا کر اور تمام آؤٹ پُٹ کئے گئے UTXO جمع کرتے ہوئے S لوٹائے۔

پہلے مرحلے کا نصف اوّل، ارسال کنندگان کو وہ کوائنز خرچ کرنے سے باز رکھے گا جو وجود ہی نہیں رکھتیں؛ پہلے مرحلے کا نصفِ دوم، ارسال کنندگان کو دوسرے لوگوں کی کوائنز خرچ کرنے سے باز رکھے گا؛ اور دوسرا مرحلہ قدر کی حفاظت کو (یعنی اس قدر میں ردوبدل نہ ہونے کو) عملاً یقینی بنائے گا۔ اسے ادائیگی میں استعمال کرنے کیلئے پروٹوکول کچھ یوں ہے۔ فرض کیجئے ایلس چاہتی ہے کہ وہ باب کو 11.7 BTC (بٹ کوائنز) بھیجے۔ سب سے پہلے ایلس اُن UTXO کا پتا لگائے گی جو اُس کی ذاتی ملکیت ہیں اور معلوم کرے گی کہ وہ مجموعی طور پر کم از کم 11.7 BTC کے برابر ہیں۔ حقیقت میں ایلس ٹھیک ٹھیک 11.7 بٹ کوائنز حاصل نہیں کر پاتی؛ کیونکہ، فرض کیجئے، اس کے پاس 12=2+4+6 یعنی 12 بٹ کوائنز ہیں۔ اب وہ ایک ٹرانزیکشن تخلیق کرے گی جس میں تین اُن پُٹ اور دو آؤٹ پُٹ ہوں گے۔ پہلا آؤٹ پُٹ 11.7 BTC ہوگا جس پر باب کا پتا بطور مالک درج ہوگا، جبکہ دوسرا آؤٹ پُٹ 0.3 BTC ہوگا جو دراصل "کھلا" (ارسال کرنے کے بعد بچ رہنے والی معمولی رقم) ہوگا، جس کی ملکیت کے طور پر ایلس کا نام لکھا ہوگا۔

مائننگ

اگر ہمارا واسطہ قابلِ بھروسہ مرکزی سروس سے ہوتا، تو اس نظام کا اطلاق کوئی خاص اہمیت نہ رکھتا؛ اسے ٹھیک اسی طرح کوڈ کر دیا جاتا جیسا کہ بتایا گیا ہے۔ البتہ، جیسا کہ بٹ کوائن کے ساتھ ہم غیر مرکزیت پر مبنی ایک کرنسی کا پورا نظام وضع کرنے کی کوشش کر رہے ہیں، لہٰذا ہمیں اسٹیٹ ٹرانزیشن سسٹم کو اکثریتی اتفاقِ رائے والے نظام کے ساتھ ملانا ہوگا تاکہ (اس

میں شریک) ہر کوئی ٹرانزیکشنز کی ترتیب پر متفق ہو سکے۔ بِٹ کوائن کے غیر مرکزی اکثریتی اتفاقِ رائے والے عمل کیلئے نیٹ ورک میں ایسے مقاماتِ اتصال (نوڈز) کی ضرورت ہوتی ہے جو ٹرانزیکشنز کیلئے پیکیجز تیار کر سکیں جنہیں "بلاکس" کہا جاتا ہے۔ یہ نیٹ ورک ہر دس منٹ میں لگ بھگ ایک بلاک تیار کرتا ہے، جبکہ ایسے ہر بلاک میں مہرِ وقت (ٹائم اسٹیمپ)، ایک "نونس" (nonce یا صرف ایک بار استعمال کے قابل عدد)، پچھلے بلاک کا حوالہ (یعنی اس کا "ہیش") اور پچھلے بلاک کی تشکیل سے اب تک ہو جانے والی ٹرانزیکشنز کی ایک فہرست موجود ہوتے ہیں۔ (یہ عمل) وقت گزرنے کے ساتھ ساتھ ایک مضبوط، ہمہ وقت بڑھتی رہنے والی "بلاک چین" تخلیق کرتا ہے جو بٹ کوائن کھاتے کی تازہ ترین کیفیت ظاہر کرنے کیلئے مسلسل اپ ڈیٹ ہوتی رہتی ہے۔

اس مجموعۂ اُصول (پیراڈائم) کے تحت، کسی بلاک کی درستگی کو جانچنے والا الگورتھم یہ ہے:

1۔ جانچ کرو کہ موجودہ بلاک میں پچھلے بلاک کا حوالہ دیا گیا ہے یا نہیں، اور وہ درست ہے یا نہیں۔

2۔ جانچ کرو کہ موجودہ بلاک کی ٹائم اسٹیمپ (اپنی قدر میں) پچھلے بلاک کی ٹائم اسٹیمپ سے بڑی ہے [2] اور مستقبل میں دو گھنٹے سے کم وقت پر محیط ہے۔

3۔ جانچ کرو کہ بلاک سے متعلق ثبوتِ کار درست ہے۔

4۔ فرض کیجیے کہ S[0] پچھلے بلاک کے اختتام پر کیفیت ہے۔

5۔ فرض کیجئے کہ TX بلاک کے تحت ٹرانزیکشنز کی فہرست ہے جس میں n ٹرانزیکشنز ہیں اور:

For all i in 0...n-1, setS[i+1] = APPLY(S[i],TX[i])

اگر کوئی ایپلی کیشن بھی ایرر لوٹائے تو باہر نکل آؤ(exit)اور ''جھوٹ''(false)لوٹاؤ۔

6۔سچ(true)لوٹاؤ،اور S[n] کو اس بلاک کے اختتام پر بطور کیفیت رجسٹر کر دو۔

بنیادی طور پر، بلاک میں ہر ٹرانزیکشن کو ایک ایسی اسٹیٹ ٹرانزیشن لازماً فراہم کرنی ہوتی ہے جو درست ہو۔ دھیان رہے کہ بلاک میں کسی بھی طرح سے ''کیفیت'' (اسٹیٹ) کی رمزکاری نہیں ہوتی؛ یہ خالصتاً ایک تجرید ہے جسے توثیق کرنے والی نوڈ پر یاد رکھا جاتا ہے اور جس کا حساب کسی بلاک کیلئے صرف (بحفاظت) لگایا جاسکتا ہے جس کا آغاز پیدائشی کیفیت (genesis state)سے ہوتا ہے اور جسے یکے بعد دیگر ہر بلاک کی ہر ٹرانزیکشن پر اطلاق پذیر کیا جاتا ہے۔ مزید یہ دھیان بھی رہے کہ وہ ترتیب اہمیت رکھتی ہے جس میں ایک کان کن (مائنر)، بلاک میں ٹرانزیکشنز شامل کرتا ہے؛ اگر ایک بلاک میں دو ٹرانزیکشنز یعنی A اور B اس طرح کی ہوں کہ B وہ UTXO خرچ کرے جو A نے تخلیق کئے ہیں، تو بلاک صرف تب ہی درست ہوگا جب A پہلے آئے اور B بعد میں، لیکن بصورتِ دیگر بلاک کو غلط قرار دیا جائے گا۔

بلاک کی توثیق کرنے والے الگورتھم کا دلچسپ حصہ ''ثبوتِ کار''(proof of work)کا تصور ہے: شرط یہ ہے کہ ہر بلاک کا SHA256 ہیش، جسے 256 بٹ والے عدد کے طور پر برتا جاتا ہے، متحرک انداز سے متعین کئے گئے ایک ہدف سے لازماً کم ہونا چاہئے، جو یہ تحریر لکھتے وقت تقریباً 2^{190} ہے۔ اس کا مقصد بلاک تخلیق کرنے کے عمل کو حسابی نقطہ نگاہ سے ''مشکل'' بنانا ہے، تاکہ سائبل حملہ آوروں کو اپنے حق میں پوری بلاک چین از سرِ نو بنانے سے باز رکھنا ہے۔

چونکہ SHA256 کو مکمل طور پر ناقابل پیش گوئی سُوڈو رینڈم فنکشن بنایا گیا ہے، اس لئے ایک درست بلاک بنانے کا واحد طریقہ صرف ''سعی و خطا'' (ٹرائل اینڈ ایرر) ہے۔ یعنی بار

بار ایک نانس (nonce) کا اضافہ کر کے دیکھنا کہ آیا وہ نئے ہیش سے میل کھاتا ہے یا نہیں۔ 2192 کے موجودہ ہدف کا مطلب یہ ہوا کہ اوسطاً 264 کوششیں درکار ہوں گی؛ بالعموم نیٹ ورک کے ذریعے ہدف کو ہر 2016 بلاکس کے بعد پھر سے متعین کیا جاتا ہے، اس طرح کہ نیٹ ورک میں شامل کچھ نوڈز سے ہر دس منٹ بعد ایک نیا بلاک تیار ہوتا رہے۔ کانکنوں (مائنرز) کی اس حسابی مشقت کا ازالہ کرنے کیلئے ہر بلاک کے مائنر کو ایک ایسی ٹرانزیکشن شامل کرنے کا اختیار دیا جاتا ہے جس کے ذریعے ان کیلئے 25 بِٹ کوائنز، عدم سے وجود میں آجاتی ہیں، جن کے وہ خود مالک ہوتے ہیں۔ مزید یہ کہ اگر کسی ٹرانزیکشن کے ان پٹ میں مقداروں (ڈینومی نیشنز) کی تعداد اس کے آؤٹ پُٹ سے زیادہ ہو، تو یہ فرق بھی کان کن ہی کو بطور "ٹرانزیکشن فیس" جاتا ہے۔ سوئے اتفاق کہ یہ وہی طریقہ بھی ہے کہ جس کے تحت بٹ کوائنز جاری کی جاتی ہیں؛ آغاز کی کیفیت میں کوئی کوائن بالکل بھی نہیں ہوتی۔

مائننگ کے مقصد کو بہتر طور پر سمجھنے کیلئے ہم یہ تجزیہ کرتے ہیں کہ اُس وقت کیا ہوتا ہے جب ایک بد طینت حملہ آور دخل اندازی کرتا ہے۔ چونکہ بٹ کوائن کی بنیادوں میں کرپٹو گرافی ثابت شدہ طور پر محفوظ ہے، حملہ آور بٹ کوائن نظام کے کسی ایسے حصے کو نشانہ بنائے گا جسے براہِ راست کرپٹو گرافی کا تحفظ حاصل نہ ہو: یعنی ٹرانزیکشنز کی ترتیب کو۔ حملہ آور کی حکمتِ عملی بہت سادہ ہے:

1۔ ایکسچینج میں کسی تاجر کو 100 BTC بھیجے جائیں جو کسی چیز کیلئے ہوں (ترجیحی طور پر، فوری فراہم کی جانے والی کسی ڈیجیٹل چیز کیلئے)۔

2۔ اس چیز کی فراہمی (ڈیلیوری) کا انتظار کیا جائے۔

3۔ ایک اور ٹرانزیکشن تیار کی جائے جس میں خود کو وہی 100 BTC بھیج دیئے جائیں۔

4۔نیٹ ورک کو قائل کرنے کی کوشش کی جائے کہ خود کو بھیجی گئی ٹرانزیکشن ہی وہ تھی جو پہلے پہنچی تھی۔

پہلا مرحلہ (1) واقع ہوچکا ہے، چند منٹ بعد کوئی مائنر اس بلاک میں ٹرانزیکشن شامل کردے گا، فرض کیجئے کہ وہ ایک عدد 270000 ہے۔ایک گھنٹہ گزرنے پر،اس بلاک کے بعد والی زنجیر میں مزید پانچ بلاک شامل ہوچکے ہوں گے، جن میں ہر ایک بالواسطہ طور پر ٹرانزیکشن کی طرف اشارہ کررہا ہوگا یعنی اس کی ''تصدیق'' کررہا ہوگا۔اس موقعے پر تاجر اس ادائیگی کو حتمی قرار دیتے ہوئے قبول کرلے گا اور طلب کردہ چیز بھجوادے گا؛ چونکہ ہم یہ فرض کررہے ہیں کہ یہ کوئی ڈیجیٹل چیز ہوگی، لہٰذا فراہمی بھی فوراً ہوجائے گا۔اب حملہ آور ایک اور ٹرانزیکشن تخلیق کرتا ہے جس کے ذریعے وہ خود کو BTC 100 بھیجتا ہے۔اگر حملہ آور اسے (نئی ٹرانزیکشن کو) کھلے میں چھوڑ دے گا، تو ٹرانزیکشن پر عمل کاری (پروسیسنگ) نہیں ہوگی؛ مائنرز APPLY(S,TX) کو چلانے کی کوشش کریں گے اور دیکھیں گے کہ TX ایک ایسے UTXO کو استعمال کررہا ہے جو کیفیت (اسٹیٹ) میں موجود ہی نہیں رہا۔ لہٰذا، حملہ آور اس کے بجائے بلاک چین کی ایک ''فورک'' تخلیق کرے گا،اس طرح کہ وہ بلاک 270000 کے ایک اور ورژن پر مائننگ سے آغاز کرے گا جو اسی بلاک 269999 کی طرف (اپنے) پیشرو کی حیثیت سے اشارہ تو کررہا ہوگا لیکن پرانی کی جگہ نئی ٹرانزیکشن کے ساتھ۔ چونکہ بلاک کا ڈیٹا مختلف ہے،اس کیلئے ثبوتِ کار انجام دینے کی لازمی ضرورت ہوگی۔ علاوہ ازیں، حملہ آور بلاک 270000 کا نیا ورژن ایک مختلف ہیش رکھتا ہے، لہٰذا اصل بلاکس جو 270001 سے 270005 تک ہوں گے اس (جعلی) ٹرانزیکشن کی طرف ''اشارہ'' نہیں کررہے ہوں گے؛ پس، اصل زنجیر اور حملہ آور کی بنائی ہوئی (جعلی) زنجیر ایک دوسرے سے مختلف ہوں گی۔اصول یہ ہے کہ ''فورک'' میں طویل

ترین بلاک چین (یعنی وہ کہ جس کے پسِ پشت ثبوتِ کار کی سب سے بڑی تعداد موجود ہے) درست کے طور پر قبول کی جاتی ہے، اور یوں درست اور دیانتدار کانکن ہی 270005 والی زنجیر پر کام کر رہے ہوں گے جبکہ حملہ آور اکیلا ہی 270000 والی زنجیر پر کام کر رہا ہو گا۔ حملہ آور کیلئے اپنی بلاک چین کو طویل ترین بنانے کا صرف ایک ہی طریقہ ہے، اور وہ یہ کہ اسے سارے نیٹ ورک کی مجموعی حسابی طاقت (کمپیوٹیشنل پاور) کے مقابلے میں زیادہ حسابی طاقت درکار ہو گی تاکہ ساتھ رہ سکے (لہٰذا، "51 فیصد حملہ")۔

مرکل اشجار (Merkle Trees)

بائیں: کسی شاخ کی درستگی کو ثابت کرنے کیلئے مرکل شجر میں نوڈز کی صرف تھوڑی سی تعداد پیش کرنا ہی کافی رہے گا۔

بائیں: مرکل شجر کے کسی بھی حصے کو تبدیل کرنے کی کوئی بھی کوشش، بالآخر زنجیر میں کسی نہ کسی مقام پر عدم مطابقت کے طور پر ظاہر ہو جائے گی۔

بٹ کوائن کی ایک اہم وسعت پذیر خاصیت (scalability feature) یہ ہے کہ بلاک کو ایک کثیر سطحی (ملٹی لیول) ڈیٹا اسٹرکچر میں محفوظ کیا جاتا ہے۔ بلاک کا "ہیش" صرف اس کے بلاک ہیڈر کا ہیش ہوتا ہے، تقریباً 200 بائٹ والے ڈیٹا کا ٹکڑا جس میں ٹائم اسٹیمپ، نونس، پچھلے بلاک کا ہیش اور ڈیٹا اسٹرکچر کا "روٹ ہیش" جسے مرکل شجر (مرکل ٹری) کہا جاتا جو بلاک میں تمام ٹرانزیکشنز کا ذخیرہ رکھتا ہے۔

مرکل ٹری، دراصل "ثنائی شجر" (binary tree) کی ایک قسم ہے، جو نوڈز کے ایک ایسے سیٹ پر مشتمل ہوتا ہے جس کے ساتھ، نچلے حصے میں، شجر (ٹری) کی لیف نوڈز ہوتی ہیں جن میں متعلقہ ڈیٹا موجود ہوتا ہے، اور درمیانی نوڈز کا ایک سیٹ ہوتا ہے جہاں ہر نوڈ اپنے دو

بچوں (children) کا ہیش ہوتی ہے، اور آخر میں ایک "روٹ نوڈ" ہوتی ہے جو خود بھی اپنے دو بچوں کے ہیش سے بنی ہوتی ہے، جو اس شجر (ٹری) کی "چوٹی" (top) کو ظاہر کر رہی ہوتی ہے۔ مرکل شجر کا مقصد ایک بلاک میں ڈیٹا کی جستہ جستہ فراہمی کی سہولت فراہم کرنا ہے: ایک نوڈ صرف ایک ہی بلاک کا ہیڈر، صرف ایک ماخذ سے ڈاؤن لوڈ کر سکتی ہے، جو بجائے خود شجر کا ایک ایسا چھوٹا حصہ ہوتا ہے جو ایک اور ماخذ سے متعلق ہوتا ہے، اور پھر بھی یہ یقین دہانی کرتا ہے کہ ڈیٹا درست ہے۔ یہ کیوں کام کرتا ہے؟ اس کی وجہ یہ ہے کہ ہیشز (hashes) اوپر کی طرف پھیلتے ہیں: اگر کوئی بدطینت صارف، مرکل شجر کی تہہ میں کوئی جعلی ٹرانزیکشن داخل کرنے کی کوشش کرے، تو یہ تبدیلی اوپر والی نوڈ میں تبدیلی لائے گی، اور پھر اس سے بھی اوپر والی نوڈ بھی تبدیل ہو جائے گی؛ اور یوں، بالآخر، اس شجر کی جڑ تک میں تبدیلی آجائے گی یعنی اس بلاک کا ہیش بھی بدل کر رہ جائے گا۔ نتیجتاً اس کا پروٹوکول ایک بالکل ہی مختلف بلاک کو رجسٹر کر رہا ہوگا (جو کم و بیش یقینی طور پر ایک غیر درست ثبوتِ کار ہوگا)۔

مرکل ٹری پروٹوکول مدلل طور پر طویل مدتی پائیداری کیلئے بنیاد ہے۔ بٹ کوائن نیٹ ورک میں ایک "مکمل نوڈ" یعنی وہ جو ہر بلاک کو مکمل طور پر محفوظ کرتی ہو اور اس کی عمل کاری (پروسیسنگ) بھی کرتی ہو، بٹ کوائن نیٹ ورک میں 15 گیگا بائٹ جتنی ڈسک اسپیس گھیر لیتی ہے (اپریل 2014ء کے مطابق)، اور اس میں ہر ماہ ایک گیگا بائٹ کا اضافہ ہو رہا ہے۔ سرِ دست یہ صرف چند ڈیسک ٹاپ کمپیوٹروں ہی کیلئے قابلِ عمل ہے، اسمارٹ فونز کیلئے نہیں؛ اور مستقبل قریب میں صرف کاروباری و تجارتی ادارے اور صاحبِ حیثیت شوقیہ افراد ہی اس میں حصہ لینے کے قابل رہ جائیں گے۔ ایک پروٹوکول جسے "ادائیگی کی سادہ توثیق" (simple payment verification) یا مختصراً "ایس پی وی" (SPV) بھی

کہا جاتا ہے، ایک اور قسم کی نوڈز کیلئے اجازت فراہم کرتا ہے، جنہیں ''ہلکی (لائٹ) نوڈز'' کہا جاتا ہے، جو بلاک ہیڈرز ڈاؤن لوڈ کرتی ہیں، ان بلاک ہیڈرز پر ثبوتِ کار کی تصدیق کرتی ہیں، اور پھر صرف وہی ''شاخیں'' (branches) ڈاؤن لوڈ کرتی ہیں جو ان سے تعلق رکھتی ہوں۔ اس طرح ''لائٹ نوڈز'' مضبوط تحفظ (سکیوریٹی) کی ضمانت دیتے ہوئے، کسی بھی بٹ کوائن ٹرانزیکشن کی کیفیت اور ان کا حالیہ بیلنس (موجودہ قدر) معلوم کرتی ہیں، جبکہ یہ سب کرنے کیلئے وہ پوری بلاک چین کا صرف ایک چھوٹا سا حصہ ڈاؤن لوڈ کرتی ہیں۔

بلاک چین کے دیگر اور متبادل اطلاقات

بلاک چین کا بنیادی تصور استعمال کرتے ہوئے اس کا اطلاق دیگر امور پر کرنے کا خیال بھی ایک طویل تاریخ رکھتا ہے۔ 2005ء میں نک ژابو نے ''مالک کے اختیار کے ساتھ محفوظ اثاثہ جاتی عنوانات'' (secure property titles with owner authority) کا تصور پیش کیا، جس کی دستاویز میں وضاحت کی گئی تھی کہ کس طرح ''ہو بہو نقل شدہ (replicated) ڈیٹا بیس ٹیکنالوجی میں ہونے والی جدید ترقی'' بلاک چین پر مبنی ایک ایسے نظام کو ممکن بنائے گی جو کسی کی ملکیت میں موجود اراضی (کی تمام تفصیلات) کی رجسٹری محفوظ کرے گا، (جس کیلئے) ایک مفصل فریم ورک تخلیق کرے گا جس میں ہوم اسٹیڈنگ، ایڈورس پزیشن (نقصاندہ ملکیت) اور جیار جیسن لینڈ ٹیکس جیسے تصورات شامل ہوں گے۔ تاہم، بدقسمتی سے اُس وقت کوئی مؤثر ہو بہو نقل شدہ ڈیٹا بیس موجود نہیں تھا، لہٰذا یہ پروٹوکول عملاً کبھی استعمال ہی نہیں کیا جا سکا۔ البتہ، 2009ء کے بعد سے، جبکہ بٹ کوائن کا عدم مرکزیت پر مبنی اتفاقِ رائے وضع کیا جا چکا تھا، متعدد متبادل اطلاقات بڑی تیزی سے سامنے آنا شروع ہو گئے:

نیم کوائن: 2010ء میں تخلیق کیے گئے ''نیم کوائن'' (Namecoin) کی بہترین وضاحت ایک غیر مرکزی، نام رجسٹر کرنے والے ڈیٹابیس کے طور پر کی جاتی ہے۔ عدم مرکزیت پر مبنی پروٹوکولز جیسے کہ ''دی انیئن راؤٹر'' (ToR)، بٹ کوائن اور بِٹ میسیج وغیرہ میں اکاؤنٹس شناخت کرنے کے کسی ایسے طریقے کی ضرورت ہوتی ہے تاکہ دوسرے لوگ بھی متعلقہ افراد سے دو طرفہ رابطہ رکھ سکیں، لیکن تمام موجودہ حلوں میں شناخت کی غرض سے

1LW79wp5ZBqaHW1jL5TCiBCrhQYtHagUWy

جیسی شناختیں ہی دستیاب ہیں جو اپنے آپ میں ''سُوڈورینڈم ہیش'' ہوتی ہیں۔ مثالی طور پر، کوئی بھی یہ چاہے گا کہ اس کے پاس ایک ایسا اکاؤنٹ ہو جس کا نام، مثلاً، ''جارج'' (george) ہو۔ لیکن مسئلہ یہ ہے کہ اگر ایک شخص ''جارج'' نامی اکاؤنٹ تخلیق کر سکتا ہے تو کوئی دوسرا بھی یہی طریقہ اختیار کرتے ہوئے، اپنے لیے ''جارج'' کے نام سے دوسرا اکاؤنٹ بنا کر خود ہی جارج کا بہروپ بھر سکتا ہے۔ اس (مسئلے) کا واحد ہی ''پہلے فائل ہونے والی'' (first-to-file) پیراڈائم ہے، جہاں پہلے رجسٹر ہونے والا (فرسٹ رجسٹرانٹ) کامیاب اور دوسرا ناکام ہو جاتا ہے — یعنی یہ مسئلہ بٹ کوائن کے ''اتفاقِ رائے'' (concensus) والے پروٹوکول کیلئے موزوں ترین ہے۔ نیم کوائن، اس تصور سے استفادہ کرتے ہوئے نام کی رجسٹریشن کا سب سے پرانا اور کامیاب ترین اطلاق بھی ہے۔

رنگین (Colored) کوائنز: رنگین یا ''کلرڈ کوائنز'' کا مقصد ایک ایسے پروٹوکول کی پاسداری کرنا ہے جو لوگوں کو اپنی، ذاتی، ڈیجیٹل کرنسیز تخلیق کرنے کی سہولت دیتا ہے۔ یا

انہیں صرف ایک یونٹ پر مبنی، اہم لیکن معمولی کرنسی یعنی ''ڈیجیٹل ٹوکن'' کو بِٹ کوائن بلاک چین پر تشکیل دینے کے قابل بناتا ہے۔ کلرڈ کوائنز پروٹوکول میں، ایک فرد عوامی طور پر ایک نئی کرنسی اس طرح ''جاری'' کرتا ہے کہ وہ کسی خاص بِٹ کوائن UTXO کو ایک خاص رنگ (کلر) تفویض کرتا ہے، اور یہ پروٹوکول تکراری انداز سے ایک اور UTXO کا رنگ وہی کر دیتا ہے جو انہیں خرچ شدہ طور پر تخلیق کرنے والی ٹرانزیکشن سے متعلق اِن پُٹس کا رنگ ہوتا ہے (مخلوط رنگوں یعنی مکسڈ کلرز والی اِن پُٹس کے معاملے میں کچھ خصوصی اصول لاگو ہوتے ہیں)۔ اس سے صارف کو ایسے (مجازی) بٹوے رکھنے کی سہولت حاصل ہوتی ہے جن میں صرف ایک خاص رنگ ہی کے UTXO ہوتے ہیں اور جنہیں کم و بیش باضابطہ بِٹ کوائنز ہی کی طرح بھیجا (اور وصول کیا) جا سکتا ہے، جس میں بلاک چین کے ذریعے سابقہ کارگزاریوں کا جائزہ لیتے ہوئے (یعنی ''بیک ٹریکنگ'' کرتے ہوئے) وصول ہونے والے کسی بھی UTXO کا رنگ معلوم کیا جاتا ہے۔

میٹا کوائنز (Metacoins): میٹا کوائنز کے پسِ پشت ایک ایسے پروٹوکول کا تصور ہے جو بِٹ کوائن پر استوار ہو، یعنی جو میٹا کوائن کی ٹرانزیکشنز محفوظ کرنے کیلئے بٹ کوائن ٹرانزیکشنز استعمال کرے لیکن اس کا اسٹیٹ ٹرانزیشن فنکشن مختلف، 'APPLY' ہو۔ چونکہ میٹا کوائن کا اپنا پروٹوکول، غیر درست میٹا کوائن ٹرانزیکشنز کو بٹ کوائن بلاک چین میں ظاہر ہونے سے نہیں روک سکتا، اس لئے ایک اصول کا اضافہ کیا گیا ہے کہ اگر APPLY'(S,TX) ایرر لوٹائے، تو پروٹوکول ڈیفالٹ APPLY'(S,TX) = S پر منتقل ہو جائے۔ اس سے کوئی آزاد اور خود مختار (arbitrary) کرپٹو کرنسی پروٹوکول تخلیق کرنے کا نظام میسر آجاتا ہے، جس میں ایسے جدید تر فیچرز بھی شامل کرنے کی استعداد ہوتی ہے جنہیں بٹ کوائن کے اندر اطلاق پذیر نہیں کیا جا سکتا، لیکن انہیں وضع کرنے کی

لاگت بہت کم ہوتی ہے کیونکہ مائننگ اور نیٹ ورکنگ کی تمام پیچیدگیاں پہلے ہی بٹ کوائن پروٹوکول نے سنبھالی ہوتی ہیں۔

تو معلوم ہوا کہ، بالعموم، اکثریتی اتفاقِ رائے کا پروٹوکول وضع کرنے کے حوالے سے دو تدابیر ہیں: ایک آزاد نیٹ ورک بنایا جائے، اور بٹ کوائن کی بنیاد پر استوار پروٹوکول تخلیق کیا جائے۔ مؤخر الذکر تدبیر، جو "نیم کوائن" جیسے اطلاقات کے معاملے میں مناسب حد تک کامیاب ہے، عملدرآمد میں مشکل ہے؛ (کیونکہ ایسے میں) ہر انفرادی عملدرآمد (کے اقدام) میں نئے سرے سے ایک آزاد بلاک چین کی ضرورت ہوتی ہے، جبکہ تمام ضروری اسٹیٹ ٹرانزیشن اور نیٹ ورک کوڈ کی وضع کاری سے لے کر آزمائش تک کی ضرورت بھی رہتی ہے۔ مزید برآں، ہم پیش گوئی کرتے ہیں کہ عدم مرکزیت پر مبنی اتفاقِ رائے کی ٹیکنالوجی سے متعلق اطلاقات ایک "قوت نمائی قانونِ تقسیم" (power law distribution) کی پیروی کریں گی جہاں اطلاقیوں (اپیلی کیشنز) کی بھاری اکثریت اپنی ذاتی بلاک چین کو جواز فراہم کرنے کیلئے بہت ہی چھوٹی ہو گی؛ اور ہم یہ بھی واضح دیکھتے ہیں کہ عدم مرکزیت پر مبنی اطلاقیوں کی بڑی جماعتیں موجود ہیں، خصوصاً غیر مرکزی خود مختار تنظیمیں، جنہیں آپس میں ربط ضبط رکھنا ضروری ہے۔

بٹ کوائن پر مبنی اندازِ نظر (approach) میں، دوسری جانب، یہ خامی ہے کہ اس میں بٹ کوائن کے تحت ادائیگی کی تصدیق کے سادہ فیچرز موروثی طور پر موجود نہیں۔ ایس پی وی (SPV)، بٹ کوائن کیلئے کام کرتا ہے کیونکہ یہ بلاک چین کی گہرائی کو توثیق کیلئے بطور پراکسی (proxy) استعمال کرتا ہے؛ کسی مقام پر، جبکہ کسی ٹرانزیکشن کے اجداد کافی پیچھے تک پہنچ چکے ہوں، یہ کہنا محفوظ رہے گا کہ وہ جائز طور پر کیفیت (اسٹیٹ) کا حصہ رہے تھے۔ دوسری جانب، بٹ کوائن پر استوار میٹا پروٹوکولز، بلاک چین کو اس پر مجبور نہیں کر سکتے کہ وہ ایسی

ٹرانزیکشنز کو شامل نہ کرے جو اُن کے اپنے پروٹوکول کے سیاق و سباق (context) میں درست یا توثیق شدہ نہ ہوں۔ لہٰذا، ایک مکمل محفوظ ایس پی وی (SPV) میٹاپروٹوکول کے اطلاق کو اُلٹی سمت میں، بِٹ کوائن بلاک چین کی ابتدا تک، نظر رکھنے اور جانچ پڑتال کرنے کی ضرورت ہوگی تاکہ بعض ٹرانزیکشنز کے درست ہونے یا نہ ہونے کا پتا چلایا جاسکے۔ سرِدست، بِٹ کوائن پر استوار میٹاپروٹوکولز کے تمام "ہلکے" عملی اطلاقات کا انحصار، ڈیٹا کی فراہمی کیلئے، ایک بھروسہ مند سرور پر ہوتا ہے، جو اپنے آپ میں انتہائی کم تر درجے کا نتیجہ دیتا ہے، خاص کر اُس وقت جب کرپٹو کرنسی کا بنیادی مقصد ہی اس درمیانی "بھروسے" (کی ضرورت) ختم کرنا ہو۔

اسکرپٹنگ

کسی توسیع (ایکسٹینشن) کے بغیر بھی، بِٹ کوائن پروٹوکول دراصل "ذہین معاہدوں" کے ایک کمزور ورژن میں سہولت پیدا کرتا ہے۔ بِٹ کوائن میں UTXO صرف عوامی کلید (پبلک کی) کے ذریعے ہی ملکیت میں نہیں لیا جاسکتا بلکہ یہی کام ایک زیادہ پیچیدہ اسکرپٹ سے بھی لیا جاسکتا ہے جسے سادہ "تھاک پر منحصر" (stack-based) پروگرامنگ لینگویج میں لکھا گیا ہو۔ اس پیراڈائم میں UTXO خرچ کرنے والی ٹرانزیکشن کو لازماً وہ ڈیٹا فراہم کرنا پڑتا ہے جو اسکرپٹ کی تسلی کرتا ہو (یعنی اسکرپٹ کی مطابقت میں ہو)۔ دراصل، بنیادی عوامی کلید (پبلک کی) کی ملکیت کا نظام بھی ایک اسکرپٹ کے ذریعے ہی لاگو کیا جاتا ہے: یہ اسکرپٹ ایک "بیضوی منحنی دستخط" (elliptic curve signature) کو بطور ان پُٹ لیتا ہے، ٹرانزیکشن اور UTXO کی ملکیت ظاہر کرنے والے پتے (ایڈریس) کے مدمقابل اس کی توثیق کرتا ہے؛ اور اگر توثیقی عمل کامیاب ہو جائے تو 1 لوٹاتا ہے، بصورتِ دیگر 0 لوٹاتا ہے۔

کئی اضافی اُمور کے لیے دوسرے، کہیں زیادہ پیچیدہ، اسکرپٹ موجود ہیں۔ مثلاً کوئی شخص ایک ایسا اسکرپٹ تیار کر سکتا ہے جسے توثیق ("multisig") کیلئے، دی گئی تین نجی کلیدوں (پرائیویٹ کیز) میں سے دو کی جانب سے دستخطوں کی ضرورت ہو جبکہ تجارتی (کارپوریٹ) اکاؤنٹس کیلئے قابل استعمال سیٹ اپ (نظامِ کار)، محفوظ سیونگ اکاؤنٹس اور کچھ تاجرانہ ثالثی (merchant escrow) حالات بھی درکار ہوں۔ حسابی مسائل حل کرنے کے معاوضے یا انعام دینے کیلئے بھی اسکرپٹس استعمال کئے جا سکتے ہیں، اور ایسا اسکرپٹ بھی تیار کیا جا سکتا ہے جو کچھ یوں کہے: ''یہ بِٹ کوائن UTXO آپ کا ہے اگر آپ ایک یہ SPV ثبوت فراہم کر سکیں کہ آپ نے اس مقدار کی ڈوگی کوائن (Dogecoin) ٹرانزیکشن مجھے بھیجی ہے،'' اس طرح کا اسکرپٹ بنیادی طور پر ایک کرپٹو کرنسی کے دوسری کرپٹو کرنسی میں غیر مرکزی تبادلے کو ممکن بناتا ہے۔

البتہ، بٹ کوائن میں استعمال کی گئی اسکرپٹنگ لینگویج کی متعدد اہم حدود و قیود ہیں:

''ٹیورنگ تکمیل'' (Turing-completeness) کا فقدان: اس کا مطلب یہ ہے کہ بِٹ کوائن اسکرپٹنگ لینگویج اگرچہ حسابی عمل (کمپیوٹیشن) کی وسیع تر اقسام کی بڑی تعداد کیلئے معاون ہے، لیکن یہ ہر چیز کیلئے معاون و مددگار ہر گز نہیں۔ وہ مرکزی زمرہ جو اِس میں موجود نہیں، وہ ''چکر'' (loops) ہیں۔ دراصل یہ ٹرانزیکشن کی توثیق کے دوران لامتناہی چکروں (infinite loops) سے بچنے کیلئے کیا جاتا ہے؛ نظری طور پر یہ رکاوٹ اسکرپٹ پروگرامرز کیلئے قابلِ عبور ضرور ہے کیونکہ کسی بھی چکر (لوپ) کی نقل نہایت سادگی سے، اس کے تحت موجود کوڈ کو ''if'' اسٹیٹمنٹ کی مدد سے کئی بار دوہرا کر تیار کی جا سکتی ہے، لیکن اس سے وہ اسکرپٹ حاصل ہوتے ہیں جو جگہ کے معاملے میں کمتر کارکردگی کے حامل ہوتے ہیں۔ مثلاً، ایک ''متبادل بیضوی منحنی دستخط'' الگورتھم اطلاق پذیر کرنے میں لگ بھگ 256

مرتبہ دوہرائے گئے تمام ضربی مرحلوں میں سے ہر ایک کو انفرادی طور پر کوڈ میں شامل کرنا ضروری ہوگا۔

قدری نابینا پن (Value-blindness): اس کا مطلب یہ ہے کہ کسی UTXO اسکرپٹ کیلئے ایسا کوئی طریقہ نہیں کہ وہ انتہائی باریک حد تک جا کر، نکالی جانے والی رقم پر کنٹرول فراہم کرے۔ مثلاً "اوریکل کنٹریکٹ" (oracle contract) کی ایک طاقتور عملی صورت، شراکت داری کا خصوصی معاہدہ (hedging contract) ہو سکتا ہے، جس میں A اور B مشترکہ طور پر 1000 ڈالر مالیت کی بِٹ کوائنز لیں اور اسکرپٹ 30 دن بعد 1000 ڈالر مالیت کی بِٹ کوائنز A کو بھیجے جبکہ باقی تمام رقم (بِٹ کوائنز کی شکل میں) B کو بھیج دے۔ اس کیلئے اوریکل کو یہ لازماً معلوم کرنا ہوگا کہ 1 BTC (ایک بِٹ کوائن) کی قدر، ڈالر میں کتنی ہے۔ تب بھی یہ بھروسے اور انفرااسٹرکچر کی ضروریات کے ضمن میں مکمل طور پر مرکزیت پر مبنی حلوں کے مقابلے میں، جو آج کل موجود ہیں، ایک بہت نمایاں بہتری ہے۔ البتہ UTXO چونکہ "سب کچھ یا کچھ بھی نہیں" ہوتے ہیں، لہٰذا اسے حاصل کرنے کا واحد اور خام طریقہ صرف یہی ہے کہ مختلف رقوم والے بہت سارے UTXO کا ایک انبار لیا جائے (مثلاً ہر k کیلئے، تیس k تک، ایک UTXO لیا جائے جو 2^k والا ہو) اور پھر اوریکل کو یہ انتخاب کرنے دیا جائے کہ ان UTXO میں سے کونسا A کو بھیجا جائے اور کونسا B کو۔

کیفیت کی کمی (Lack of state): UTXO یا تو خرچ شدہ ہو سکتا ہے یا پھر غیر خرچ شدہ؛ ان سے ہٹ کر کثیر مرحلوں (ملٹی اسٹیج) پر مشتمل معاہدوں یا اسکرپٹس کیلئے جو کوئی بھی دوسری اندرونی کیفیت (اسٹیٹ) رکھتے ہوں، کوئی سہولت موجود ہی نہیں۔ اس طرح کثیر مرحلوں پر مشتمل آپشنز والے معاہدے تشکیل دینا، غیر مرکزی تبادلے (ایکسچینج) کی پیشکش

کرنا یا دو مرحلوں والے "کرپٹو گرافک کمٹمنٹ پروٹوکولز (جو محفوظ حسابی انعامات کیلئے ضروری ہوتے ہیں) وضع کرنا مشکل ہو جاتا ہے۔ اس کا مطلب یہ بھی ہے کہ UTXO کو صرف سادہ اور ایک بار ہی استعمال کے قابل (one-off) معاہدوں کی تشکیل میں استعمال کیا جاسکتا ہے جبکہ زیادہ پیچیدہ "کیفیات سے بھرپور" (stateful) معاہدوں کی تیاری، جیسے کہ غیر مرکزی تنظیموں کی تیاری (اس کے ذریعے) ممکن نہیں؛ اور میٹاپروٹوکولز لاگو کرنا بھی اس کے تحت مشکل ہو جاتا ہے۔ قدری نابینا پن والی ثنائی کیفیات (بائنری اسٹیٹس) کا مطلب یہ ہوا کہ ایک اور اہم اطلاق، یعنی (رقم) نکلوانے یا دست برداری کی حد بندی، بھی ناممکن ہو جاتا ہے۔

بلاک چین کا نابینا پن (Blockchain-blindness): UTXO بلاک چین ڈیٹا، جیسے کہ نونس اور پچھلے ہیش کی جانب سے بالکل بے خبر یا "نابینا" ہوتے ہیں۔ اس سے اطلاقات (اپلی کیشنز) کے جوئے میں یا ایسے دوسرے زمروں میں استعمال کئے جانے کی صلاحیت محدود ہو جاتی ہے کیونکہ (ان کی وجہ سے) اسکرپٹنگ لینگویج، جذافیت (randomness) کے ایک ممکنہ قابل قدر ماخذ سے محروم ہو جاتی ہے۔

لہٰذا، ہم کرپٹو کرنسی کی بنیاد پر جدید تر اطلاقات (اپلی کیشنز) کی تیاری میں تین جداگانہ عملی تدابیر دیکھتے ہیں: ایک نئی بلاک چین کی تیاری، بٹ کوائن کے اوپر اسکرپٹنگ کا استعمال، اور بٹ کوائن کے اوپر ایک میٹاپروٹوکول کی وضع کاری۔ نئی بلاک چین کی تیاری سے مطلوبہ خصوصیات کے مجموعے (فیچر سیٹ) کی تشکیل میں بے انتہاء آزادی حاصل ہوتی ہے، لیکن وضع کاری میں (زائد) وقت اور "بوٹ اسٹریپنگ" (bootstrapping) کی زیادہ کوششوں کی قیمت پر۔ اسکرپٹنگ کا استعمال عملی اطلاق کے نقطۂ نگاہ سے آسان ہے اور معیار کا درجہ بھی رکھتا ہے، لیکن یہ اپنی صلاحیتوں کے اعتبار سے بہت محدود ہے؛ اور میٹاپروٹوکولز،

آسان ہونے کے باوجود، پیمانہ سازی (یعنی بڑے پیمانے پر اطلاق پذیری) میں خامیوں کا شکار ہو جاتے ہیں۔ ایتھریم کے ذریعے ایک ایسا عمومی فریم ورک تیار کرنا ہے جو ان تینوں پیراڈائمز کے فوائد بیک وقت فراہم کر سکے۔

ایتھریم

ایتھریم کا مقصد اسکرپٹنگ، آلٹ کوائنز (altcoins) اور آن چین میٹا پروٹوکولز (on-chain meta-protocols) کے تصورات کو یکجا کرتے ہوئے خوب تر بنانا ہے؛ اور ڈیویلپرز (کمپیوٹر پروگرامرز) کو اس قابل بنانا ہے کہ وہ اکثریتی اتفاقِ رائے پر مبنی، ایسی ایپلی کیشنز تیار کر سکیں جو بڑے پیمانوں پر استعمال کے قابل (scalable) ہوں، معیاری (standardized) ہوں، خواص میں مکمل ہوں، وضع کرنے میں آسان ہوں اور مذکورہ تمام پیراڈائمز کے تحت فراہم کردہ، مختلف حالات کے تحت کام کرنے کے کی صلاحیت (interoperability) سے بیک وقت استفادہ کرنے کے قابل ہوں۔ ایتھریم یہ مقصد ایک "حتمی تجریدی اساسی پرت" (ultimate abstract foundational layer) وضع کر کے حاصل کرتا ہے: ایک ایسی بلاک چین جس میں اندرونی طور پر ہی ایک "ٹیورنگ مکمل" (ٹیورنگ کمپلیٹ) پروگرامنگ لینگویج ہو، جو کسی کو بھی ذہین معاہدے اور غیر مرکزیت پر مبنی ایپلی کیشنز لکھنے کی سہولت دے، اور جہاں وہ ملکیت کیلئے اپنے من پسند قوانین، ٹرانزیکشن فارمیٹ اور اسٹیٹ ٹرانزیشن فنکشنز تخلیق کر سکیں۔ نیم کوائن کا ایک بہت ہی بنیادی ورژن صرف دو سطروں والے کوڈ سے لکھا جا سکتا ہے، اور کرنسیوں یا ساکھ پر مبنی نظام (ریپیوٹیشن سسٹمز) وغیرہ جیسے دوسرے پروٹوکولز بھی صرف بیس سطروں (والے کوڈ) میں سموئے جا سکتے ہیں۔ ذہین معاہدے (اسمارٹ

کنٹریکٹس)، یعنی وہ کرپٹو گرافک ''ڈبے'' جن میں کوئی قدر محفوظ ہو اور جو صرف اسی وقت غیر مقفل (ان لاک) ہوں کہ جب کچھ مخصوص شرائط پوری ہو جائیں، انہیں بھی ہمارے اس پلیٹ فارم (کی بنیاد) پر تیار کیا جاسکتا ہے۔ یہ پلیٹ فارم بِٹ کوائن اسکرپٹنگ کے مقابلے میں کہیں زیادہ اور وسیع تر طاقت پیش کرتا ہے کیونکہ اس میں ٹیورنگ تکمیل پذیری، قدر سے آگاہی، بلاک چین اور کیفیت سے آگاہی کی قوتیں اضافی طور پر شامل ہیں۔

ایتھریم اکاؤنٹس

ایتھریم میں کیفیت (اسٹیٹ) جن اشیاء (آبجیکٹس) سے بنتی ہے انہیں ''اکاؤنٹس'' (accounts) کہا جاتا ہے، جبکہ ہر اکاؤنٹ کے ساتھ ایک 20 بائٹ کا ایڈریس ہوتا ہے اور اسٹیٹ ٹرانزیشنز اپنے آپ میں اکاؤنٹس کے درمیان قدر (ویلیو) اور اطلاع (انفارمیشن) کے تبادلے پر مشتمل ہوتی ہیں۔ ایک ایتھریم اکاؤنٹ میں چار فیلڈز ہوتی ہیں:

- نونس (nonce)، ایک کاؤنٹر جسے یہ یقینی بنانے کیلئے استعمال کیا جاتا ہے کہ ہر ٹرانزیکشن صرف ایک مرتبہ ہی پروسیس ہو سکے۔
- اکاؤنٹ کا موجودہ بیلنس۔
- اکاؤنٹ کا کنٹریکٹ کوڈ، اگر موجود ہو۔
- اکاؤنٹ کی اسٹوریج (جو اصلاً خالی ہوتی ہے)۔

''ایتھر'' (Ether) ہی وہ دراصل ایتھریم کا مرکزی رمزی ایندھن (کرپٹو فیول) ہے، اور ٹرانزیکشن فیس کی ادائیگی میں اسی کو استعمال کیا جاتا ہے۔ بالعموم، دو طرح کے اکاؤنٹس ہوتے

ہیں: بیرونی ملکیت والے اکاؤنٹس، جو ''پرائیویٹ کیز'' سے کنٹرول کیے جاتے ہیں؛ اور کنٹریکٹ اکاؤنٹس، جو اپنے کنٹریکٹ کوڈ سے کنٹرول ہوتے ہیں۔ ایک بیرونی ملکیت والے اکاؤنٹ کا کوئی کوڈ نہیں ہوتا، اور کوئی فرد بیرونی ملکیت والے اکاؤنٹ سے پیغامات بھیج سکتا ہے جس کیلئے ایک ٹرانزیکشن تخلیق کر کے اس پر دستخط کئے جاتے ہیں؛ ایک کنٹریکٹ اکاؤنٹ میں، ہر بار جب کوئی کنٹریکٹ اکاؤنٹ کوئی پیغام وصول کرتا ہے تو وہ اپنے کوڈ کو سرگرم (ایکٹیویٹ) کرتے ہوئے اسے اندرونی اسٹوریج میں پڑھنے اور لکھنے کی اجازت دیتا ہے اور دیگر پیغامات بھیجنے یا نتیجتاً کنٹریکٹ تخلیق کرنے کی اجازت دیتا ہے۔

پیغامات اور ٹرانزیکشنز

ایتھریم میں ''پیغامات'' (messages) لگ بھگ بٹ کوائن میں ''ٹرانزیکشنز'' ہی کی طرح ہوتے ہیں، لیکن تین اہم حوالوں سے مختلف بھی ہوتے ہیں۔ پہلا، ایک ایتھریم پیغام کسی بیرونی وجود (فرد یا پروگرام) یا ایک کنٹریکٹ کے ذریعے تخلیق کیا جاسکتا ہے، جبکہ بٹ کوائن ٹرانزیکشن صرف بیرونی طور پر ہی تخلیق کی جاسکتی ہے۔ دوسرا، ایتھریم پیغامات میں ڈیٹا رکھنے کیلئے ایک نمایاں اختیار (آپشن) ہوتا ہے۔ آخر میں، ایتھریم پیغام کے وصول کنندہ کے پاس، اگر وہ ایک کنٹریکٹ اکاؤنٹ ہے تو، ردِ عمل (رسپونس) لوٹانے کا اختیار موجود ہوتا ہے؛ جس کا مطلب یہ ہوا کہ ایتھریم پیغامات ''فنکشنز'' کے تصور پر بھی محیط ہوتے ہیں۔

ایتھریم میں ''ٹرانزیکشن'' کی اصطلاح، ڈیٹا کے ایسے دستخط شدہ پیکیج کیلئے استعمال ہوتی ہے جو بیرونی ملکیت والے اکاؤنٹ کی جانب سے بھیجنے کیلئے تیار کسی پیغام کو محفوظ کرتا ہے۔ ٹرانزیکشنز میں پیغام وصول کرنے والے کی معلومات، بھیجنے والے کی شناخت بتانے کیلئے دستخط، ایتھر کی مقدار اور بھیجا جانے والا ڈیٹا موجود ہوتے ہیں، جبکہ STARTGAS اور

GASPRICE نامی دو مزید قدریں بھی ہوتی ہیں۔ قوت نمائی افراط (exponential blowup)اور کوڈ میں لامتناہی لوپس سے بچنے کیلئے، ضروری ہوتا ہے کہ ہر ٹرانزیکشن یہ حد متعین کرے کہ وہ کوڈ پر عملدرآمد (کوڈ ایگزیکیوشن) میں کتنے حسابی مرحلے (تکراری انداز سے) تخلیق کر سکتی ہے؛ اس میں ابتدائی پیغام اور اضافی پیغامات جو عملدرآمد کے دوران وجود پذیر ہوتے ہیں، دونوں شامل ہیں۔ STARTGAS اسی کی حد ہے، اور GASPRICE وہ فیس ہے جو ہر مرحلے (step) کی انجام دہی پر مائنر کو ادا کی جائے گی۔ اگر ٹرانزیکشن پر عملدرآمد میں "گیس ختم ہو جائے" تو کیفیت میں کی گئی تمام تبدیلیاں (state changes) واپس پلٹ جائیں گی، سوائے ان کے جو فیس کی ادائیگی کیلئے ہوں، اور اگر ٹرانزیشن ایگزیکیوشن تب ہی رُک جائے کہ کچھ "گیس" باقی ہو تو فیس کا بچا ہوا حصہ، ارسال کنندہ کو واپس کر دیا جاتا ہے۔ ایک معاہدہ (کنٹریکٹ) تخلیق کرنے کیلئے ٹرانزیکشن کی ایک علیحدہ قسم بھی ہے، اور متعلقہ پیغام کی ایک قسم بھی؛ معاہدے کے پتے کا حساب، اکاؤنٹ نونس کے ہیش اور ٹرانزیکشن ڈیٹا کی بنیاد پر لگایا جاتا ہے۔

پیغام کے اس نظام کا ایک اہم نتیجہ، ایتھریم کی "درجہ اوّل شہری" والی خاصیت ہے—یعنی یہ خیال کہ معاہدوں میں بھی بیرونی اکاؤنٹس جتنی ہی طاقت ہے، جس میں پیغام بھیجنے اور دیگر معاہدے تخلیق کرنے کی صلاحیت بھی شامل ہے۔ یہ پہلو معاہدوں کو بیک وقت کئی کردار نبھانے کے قابل بناتا ہے: مثلاً، کوئی فرد ایک غیر مرکزی تنظیم (معاہدے) کا ایسا رکن (ممبر) بھی رکھ سکتا ہے جو مخصوص کوانٹم پروف لیمپورٹ دستخطوں (تیسرے معاہدے) کو استعمال کرنے والے شکی مزاج فرد اور ایک شریک دستخطی وجود کے (جو بذاتِ خود ایک ایسا اکاؤنٹ (چوتھا معاہدہ) استعمال کر رہا ہو جس میں سکیوریٹی کیلئے پانچ کلیدیں ہوں) مابین ایک ثالثی اکاؤنٹ (دوسرے معاہدے) کا اضافی کردار بھی ادا کرے۔ ایتھریم پلیٹ فارم کی مضبوطی یہ

ہے کہ غیر مرکزی تنظیم اور ثالثی معاہدے(escrow contract) کو یہ خیال رکھنے کی کوئی ضرورت نہیں کہ ہر فریق کے اکاؤنٹ کا معاہدہ کس نوعیت کا ہے۔

ایتھریم اسٹیٹ ٹرانزیشن فنکشن

ایتھریم کا اسٹیٹ ٹرانزیشن فنکشن، APPLY(S,TX) -> S' درج ذیل کے مطابق بیان کیا جا سکتا ہے:

1۔ یہ جانچ کرے کہ ٹرانزیکشن اچھی حالت میں ہے (یعنی قدروں کے درست نمبر رکھتی ہے)، دستخط درست ہے، اور (وصول شدہ) نونس، ارسال کنندہ کے اکاؤنٹ والی نونس سے مماثل ہے۔ اگر ایسا نہ ہو تو یہ "ایرر" لوٹائے۔

2۔ ٹرانزیکشن فیس کا حساب STARTGAS*GASPRICE کے طور پر لگائے، اور دستخط کے ذریعے بھیجنے والے کا پتا معلوم کرے۔ بھیجنے والے (ارسال کنندہ) کے اکاؤنٹ بیلنس میں سے فیس منہا کرے اور ارسال کنندہ کے نونس میں اضافہ کر دے۔ اگر خرچ کرنے کیلئے کافی بیلنس نہ ہو، تو "ایرر" لوٹائے۔

3۔ کچھ ایسے ابتداء کرے GAS = STARTGAS، اور ٹرانزیکشن میں موجود (تمام) بائٹس کیلئے فی بائٹ "گیس" کی ایک مخصوص مقدار کی تخفیف کر لے۔

4۔ ارسال کنندہ کے اکاؤنٹ سے ٹرانزیکشن کی قدر لے کر اسے وصول کنندہ اکاؤنٹ میں منتقل کر دے۔ اگر وصول کرنے والا اکاؤنٹ اب تک موجود نہیں، تو اسے تخلیق کرے۔ اگر وصول کنندہ اکاؤنٹ ایک کنٹریکٹ ہے تو کنٹریکٹ کا کوڈ یا تو تکمیل ہو جانے تک چلائے یا پھر مزید عملدرآمد کیلئے درکار گیس ختم ہو جانے تک (کوڈ چلاتا رہے)۔

5۔ اگر ارسال کنندہ کے پاس کافی رقم نہ ہونے کے باعث قدر کی منتقلی (کا عمل) ناکام ہو جائے، یا کوڈ ایگزیکیوشن کیلئے گیس ختم ہو جائے تو، سوائے فیس کی ادائیگی کے، اسٹیٹ میں ہونے والی تمام تبدیلیوں کو پلٹا دے؛ اور فیس کو مائنر کے اکاؤنٹ میں جمع کر دے۔

6۔ بصورتِ دیگر، باقی رہ جانے والی گیس کیلئے تمام فیس ارسال کنندہ کو واپس کر دے اور استعمال شدہ گیس کی مطابقت میں مائنر کو ادا کردہ فیس بھجوا دے۔

مثلاً، فرض کیجئے کہ کنٹریکٹ کا کوڈ ہے:

```
if !contract.storage[msg.data[0]]:
contract.storage[msg.data[0]] = msg.data[1]
```

دھیان رہے کہ حقیقت میں کنٹریکٹ کوڈ ایک نچلی سطح کے ای وی ایم کوڈ (low-level EVM code) میں لکھا جاتا ہے؛ جبکہ یہ مثال وضاحت کی غرض سے "سرپنٹ" (Serpent) میں لکھی گئی ہے جو ہماری اعلیٰ سطحی (ہائی لیول) لینگویج ہے، اور جسے EVM کوڈ میں کمپائل کیا جا سکتا ہے۔ فرض کیجئے کہ کنٹریکٹ کی ذخیرہ گاہ (اسٹوریج) خالی ہونے لگتی ہے، اور بھیجی گئی ٹرانزیکشن کے ساتھ 10 ایتھر جتنی قدر، 2000 گیس، 0.001 ایتھر GASPRICE اور دو ڈیٹا فیلڈز: ['CHARLIE', 2][3] موجود ہیں۔

ایسی صورت میں اسٹیٹ ٹرانزیشن فنکشن کا پروسیس کچھ یوں ہو گا:

1۔ جانچ کرو کہ ٹرانزیکشن درست اور اچھی حالت میں ہے۔

2۔ جانچ کرو کہ ٹرانزیکشن ارسال کنندہ کے پاس کم از کم 2 = 2000*0.001 یعنی 2 ایتھر ہیں۔ اگر ایسا ہے تو ارسال کنندہ کے اکاؤنٹ میں سے 2 ایتھر منہا کر دو۔

3۔ابتداء کرو2000 = gas؛یہ فرض کرتے ہوئے کہ ٹرانزیکشن 170 بائٹس طویل ہے اور (فی) بائٹ فیس 5 (گیس جتنی) ہے، 850 نفی کردو، اس طرح کہ 1150 گیس باقی رہ جائے۔

4۔ارسال کنندہ کے اکاؤنٹ سے مزید 10 ایتھر منہا کرو، اور انہیں کنٹریکٹ کے اکاؤنٹ میں جمع کردو۔

5۔ کوڈ چلاؤ (رَن کرو)۔ اس مثال میں یہ کام سادہ ہے: یہ جانچ کرتا ہے کہ انڈیکس 2 پر کنٹریکٹ کی اسٹوریج استعمال ہو چکی ہے یا نہیں، معلوم کرتا ہے کہ ایسا نہیں، اور پھر یہ انڈیکس 2 پر اسٹوریج کو قدر CHARLIE پر سیٹ کردیتا ہے۔ فرض کیجئے کہ اس میں 187 گیس صرف ہو جاتی ہے، تب گیس کی باقی ماندہ مقدار 963 = 187 - 1150 یعنی 963 گیس ہو گی۔

6۔ارسال کنندہ کے اکاؤنٹ میں 0.963 = 0.001*963 یعنی 0.963 ایتھر واپس جمع کرو، اور نتیجے میں ملنے والی اسٹیٹ لوٹاؤ۔

اگر ٹرانزیکشن وصول کرنے والے کی جانب کوئی کنٹریکٹ نہ ہوا، تو مجموعی ٹرانزیکشن فیس، فراہم کردہ GASPRICE اور بائٹس میں ٹرانزیکشن کی لمبائی کے سادہ حاصل ضرب کے برابر ہو جائے گی، اور ٹرانزیکشن کے ساتھ بھیجا گیا ڈیٹا غیر متعلق ہو جائے گا۔ مزید یہ بھی دھیان رہے کہ کنٹریکٹ سے شروع کئے جانے والے (contract-initiated) پیغامات اُس حسابی عمل کیلئے گیس کی حد (gas limit) مقرر کر سکتے ہیں جو انہوں نے انجام دیا ہے، اور اگر ذیلی حسابی عمل میں گیس ختم ہو جاتی ہے تو وہ پلٹ کر اس مقام تک پہنچ جائے گا کہ جب پیغام بھیجا گیا تھا۔ لہٰذا، بالکل ٹرانزیکشن کی طرح، کنٹریکٹس بھی اپنے انجام

دیئے ہوئے ذیلی حسابات کی سخت حدود مقرر کرتے ہوئے اپنے محدود حسابی وسائل بچا سکتے ہیں۔

کوڈ پر عملدرآمد (کوڈ ایگزیکیوشن)

ایتھریم معاہدوں (کنٹریکٹس) میں کوڈ ایک نچلے درجے کی، اسٹیک پر مبنی (stack-base) بائٹ کوڈ لینگویج میں لکھا جاتا ہے جو ''ایتھریم ورچوئل مشین کوڈ'' یا ''EVM کوڈ'' کہلاتا ہے۔ یہ کوڈ، بائٹس کے سلسلے پر مشتمل ہوتا ہے، جس میں ہر بائٹ ایک کارروائی (آپریشن) کو ظاہر کرتا ہے۔ بالعموم، کوڈ ایگزیکیوشن ایک لامتناہی چکر (لوپ) ہوتی ہے جس میں بار بار ایک ہی آپریشن، حالیہ پروگرام کاؤنٹر پر (جو صفر سے شروع ہوتا ہے) انجام دیا جاتا ہے اور پھر پروگرام کاؤنٹر کو ایک کے بقدر بڑھا دیا جاتا ہے، یہاں تک کہ کوڈ کا اختتام آن پہنچے یا پھر ایرر یا STOP یا RETURN کی ہدایت سامنے آجائے۔ یہ آپریشنز تین قسم کی جگہ (اسپیس) تک رسائی رکھتے ہیں کہ جس میں ڈیٹا ذخیرہ (اسٹور) کیا جانا ہوتا ہے:

- اسٹیک (stack): ایک ''آخر اندر، پہلے باہر'' (last-in-first-out) کنٹینر جس تک 32 بائٹ والی قدریں (ویلیوز) دھکیلی جاسکتی ہیں اور (اسی سے یہ ویلیوز) برآمد بھی ہو سکتی ہیں۔
- یادداشت (میموری): بائٹس کی ایک ایسی قطار (byte array) جو لامحدود طور پر پھیلائی جاسکے۔
- کنٹریکٹ کا طویل مدتی (long-term) ذخیرہ: ایک کلید/قدر (key/value) کا ذخیرہ جہاں کلیدیں اور قدریں، دونوں ہی 32 بائٹس والی ہوتی ہیں۔ اسٹیک اور میموری کے برعکس، جو حسابی عمل ختم ہو جانے کے بعد ''ری سیٹ''

(ابتدائی حالت میں بحال) ہو جاتے ہیں، ذخیرہ (اسٹوریج) لمبے عرصے تک برقرار رہتا ہے۔

کوڈ کسی آنے والے پیغام کی قدر، ارسال کنندہ اور ڈیٹا کے علاوہ بلاک ہیڈر ڈیٹا تک بھی رسائی رکھ سکتا ہے، اور کوڈ ڈیٹا کی ایک بائٹ قطار (byte array) بھی بطور آؤٹ پُٹ لوٹا سکتا ہے۔

EVM کوڈ کا باضابطہ ایگزیکیوشن ماڈل حیرت انگیز طور پر بہت سادہ ہے۔ جب ایتھریم کی ورچوئل مشین چل رہی ہو، تو اس کی پوری حسابی کیفیت ایک "ٹپل" (tuple) یعنی کئی حصوں والی ڈیٹا اسٹرکچر (block_state، ٹرانزیکشن، پیغام، کوڈ، میموری، اسٹیک، پی سی، گیس) سے بیان کی جا سکتی ہے، جہاں block_state ایک ہمہ گیر کیفیت (گلوبل اسٹیٹ) ہے جس میں تمام اکاؤنٹس موجود ہوتے ہیں اور جس میں کئی بیلنس اور ذخیرہ (اسٹوریج) بھی شامل ہوتے ہیں۔ ایگزیکیوشن کے ہر پھیرے (راؤنڈ) میں حالیہ ہدایت معلوم کرنے کیلئے کوڈ کی pc ویں بائٹ (pc^{th} byte) لی جاتی ہے، اور ہر ہدایت خود اپنی وضاحت رکھتی ہے جو اس انداز کی ہوتی ہے کہ وہ کس طرح ٹپل (tuple) پر اثر ڈالے گی۔ مثلاً، ADD ایک اسٹیک سے دو آئٹم برآمد کرواتا ہے اور اُن کے مجموعے (sum) کو آگے دھکیلتا ہے، گیس کو 1 کے بقدر کم کرتا ہے اور pc کو 1 کے بقدر بڑھاتا ہے، اور SSTORE سب سے اوپر والے دو آئٹمز کو اسٹیک سے باہر دھکیلتا ہے اور کنٹریکٹ کی اسٹوریج میں دوسرے آئٹم کو پہلے آئٹم کے صراحت کردہ اشاریے (انڈیکس) میں شامل کرتا ہے، جبکہ ساتھ ہی گیس میں 200 تک کی کمی کرتا ہے اور pc میں 1 کا اضافہ کر دیتا ہے۔

اگرچہ "عین وقت پر" (just-in-time) کمپائلیشن کے ذریعے ایتھریم کو آپٹیمائز کرنے

کے کئی طریقے ہیں، تاہم ایتھریم کی بنیادی اطلاق کاری کیلئے صرف چند سو سطروں کا کوڈ کافی ہوتا ہے۔

بلاک چین اور مائننگ (Blockchain and Mining)

ایتھریم بلاک چین کئی اعتبار سے بِٹ کوائن بلاک چین سے مشابہت رکھتی ہے، تاہم ان دونوں میں کچھ فرق بھی ہیں۔ ایتھریم اور بِٹ کوائن میں سب سے بڑا فرق بلاک چین آرکیٹیکچر کے حوالے سے یہ ہے کہ، بِٹ کوائن کے برعکس، ایتھریم بلاکس بیک وقت ٹرانزیکشن لسٹ اور حالیہ ترین کیفیت (اسٹیٹ)، دونوں کی ایک ایک نقل رکھتے ہیں۔ اس سے ہٹ کر دو اور قدریں، بلاک نمبر اور مشکل، بھی بلاک ہی میں محفوظ ہوتی ہیں۔ ایتھریم میں بلاک کی توثیق (block validation) کا الگورتھم یہ ہے:

1۔ جانچ کرو کہ حوالہ دیا گیا پچھلا بلاک موجود ہے اور درست ہے۔

2۔ جانچ کرو کہ بلاک کی ٹائم اسٹیمپ، حوالہ دیئے گئے پچھلے بلاک سے بڑی ہے اور مستقبل کے مقابلے میں 15 منٹ کم ہے۔

3۔ جانچ کرو کہ بلاک نمبر، مشکل، ٹرانزیکشن رُوٹ، انکل رُوٹ اور گیس لمٹ (یعنی ایتھریم سے مخصوص متعدد تصورات) درست ہیں۔

4۔ جانچ کرو کہ بلاک پر موجود ثبوتِ کار درست ہے۔

5۔ متعین کرو کہ S[0] پچھلے بلاک کی STATE_ROOT ہے۔

6۔ متعین کرو کہ TX بلاک کی ٹرانزیکشن لسٹ ہے، n ٹرانزیکشنز کے ساتھ۔ تمام n-0 ... 1 کیلئے مقرر کرو کہ S[i+1] = APPLY(S[i],TX[i])۔ اگر کوئی سی بھی

اپلی کیشنز ایر رلوٹائیں، یا اگر بلاک کے درمیان ہی مجموعی گیس ختم ہو جائے جبکہ وہ مقام GASLIMIT سے بڑھ جائے، تو ایر رلوٹاؤ۔

7۔S_FINAL کو S[n] متعین کرو، لیکن یہ اضافہ کرتے ہوئے کہ بلاک کا انعام مائنر کو ادا کیا جائے۔

8۔جانچ کرو کہ کیا S_FINAL عین وہی ہے جیسا STATE_ROOT ہے۔اگر ایسا ہے، تو بلاک درست ہے؛ بصورتِ دیگر یہ درست نہیں۔

پہلی نظر میں یہ عملی تدبیر انتہائی ناقص کارکردگی کی حامل نظر آسکتی ہے، کیونکہ اسے ہر بلاک کے ساتھ پوری کیفیت (اسٹیٹ) محفوظ کرنا پڑتی ہے، لیکن حقیقت میں اس کی کارکردگی بِٹ کوائن (کی کارکردگی) سے قابلِ موازنہ ہے۔ وجہ یہ ہے کہ اسٹیٹ کو شجری ساخت (ٹری اسٹرکچر) میں محفوظ کیا جاتا ہے، اور ہر بلاک کے بعد اس شجر کے ایک چھوٹے سے حصے کو تبدیل کرنے کی ضرورت پڑتی ہے۔ لہٰذا، بالعموم، دو متصل بلاکس کے درمیان اس شجر کی بڑی اکثریت یکساں رہنی چاہئے اور، اسی بناء پر، ڈیٹا ایک مرتبہ محفوظ کرنے کے بعد، پوائنٹرز (یعنی ہیشز اور سب ٹریز) استعمال کرتے ہوئے، دو مرتبہ اس کا حوالہ دیا جاسکتا ہے۔ایک خاص قسم کا شجر جو "پیٹریشیاٹری" کہلاتا ہے، اس کام کی انجام دہی کیلئے استعمال کیا گا ہے، جبکہ اس میں مرکل ٹری سے متعلق تصورات بھی، اپنی ترمیم شدہ حالت میں، شامل کئے گئے ہیں جو نوڈز کو شامل اور حذف (ڈیلیٹ) کرنے کی سہولت دیتے ہیں؛ اور صرف تبدیلی ہی نہیں بلکہ کارکردگی میں بھی اضافہ کرتے ہیں۔ مزید برآں، کیونکہ کیفیت کی بابت تمام معلومات (اسٹیٹ انفارمیشن) پچھلے بلاک کا حصہ ہوتی ہے، اس لئے ساری بلاک چین کی تاریخ محفوظ کرنے کی کوئی ضرورت نہیں ہوتی — یہ ایک ایسی حکمت عملی ہے کہ جسے اگر بِٹ کوائن پر استعمال کیا جائے، تو تخمیناً یہ 5 سے 20 گنا تک گنجائش (اسپیس) میں بچت کرتی ہے۔

اطلاقات (اپلی کیشنز)

ایتھریم کی بنیاد پر بالعموم تین اقسام کی اپلی کیشنز موجود ہیں۔ پہلا زمرہ مالیاتی اپلی کیشنز کا ہے، جو صارفین کو ایسے زیادہ طاقتور طریقے فراہم کرتے ہیں کہ جن کی بدولت وہ اپنی رقم استعمال کرتے ہوئے معاہدوں میں داخل ہو سکتے ہیں اور ان کی انتظام کاری بھی کر سکتے ہیں۔ ان میں ذیلی کرنسیاں (سب کرنسیز)، مالیاتی ماخوذات (فائنانشیل ڈیریویٹیوز)، ہیجنگ (hedging) معاہدے، بچت (سیونگز) بٹوے، وصیتیں، اور بالآخر بھرپور نوعیت کے ملازمتی معاہدوں کی بعض جماعتیں تک شامل ہیں۔ دوسرا زمرہ نیم مالیاتی اپلی کیشنز کا ہے، جہاں پیسہ تو شامل ہوتا ہے لیکن کئے جانے والے کام کا ایک اہم غیر مالیاتی حصہ بھی ہوتا ہے۔ آخر میں، آن لائن ووٹنگ اور عدم مرکزیت پر مبنی طرزِ حکمرانی (گورننس) جیسی اپلی کیشنز ہیں جو مالیاتی نوعیت کی ہرگز نہیں ہوتیں۔

ٹوکن سسٹمز

بلاک چین پر مبنی (on-blockchain) ٹوکن سسٹمز کے بہت سے اطلاقات ہیں جو امریکی ڈالر، سونے یا کسی کمپنی کے حصص جیسے اثاثہ جات کو ظاہر کرنے والی ذیلی کرنسیوں سے لے کر انفرادی ٹوکنز تک محیط ہیں جو ذہین جائیداد کی اور جعل سازی سے محفوظ کوپنز کی نمائندگی کرتے ہیں، حتیٰ کہ ایسے ٹوکن سسٹمز بھی ہیں جو روایتی قدر سے بالکل بھی تعلق نہیں رکھتے، جنہیں ترغیب کاری میں پوائنٹ سسٹمز کے طور پر استعمال کیا جاتا ہے۔ ایتھریم میں ٹوکن سسٹمز کو لاگو کرنا حیرت انگیز طور پر بہت آسان ہے۔ سمجھنے والا کلیدی نکتہ یہ ہے کہ کوئی کرنسی یا ٹوکن سسٹم بنیادی طور پر ایک آپریشن والا ڈیٹا بیس ہوتا ہے: A میں سے X یونٹ منہا کرو اور B کو X یونٹ دے دو، اس شرط کے ساتھ کہ (اوّل) ٹرانزیکشن سے پہلے A کے پاس

کم از کم X یونٹ تھے اور (دوم) وہ ٹرانزیکشن A کی منظور کردہ ہو۔ ٹوکن سسٹم لاگو کرنے کیلئے صرف اتنا کرنا ہوتا ہے کہ کسی معاہدے میں کسی مخصوص منطق (لاجک) کا اطلاق کر دیا جائے۔

Serpent میں ٹوکن سسٹم لاگو کرنے کا بنیادی کوڈ کچھ یوں ہے:

```
from = msg.sender
to = msg.data[0]
value = msg.data[1]

if contract.storage[from] >= value:
contract.storage[from] = contract.storage[from]
value
contract.storage[to] = contract.storage[to] + value
```

ملاحظہ کیجئے کہ یہ بنیادی طور پر بالکل "بینکنگ سسٹم" اسٹیٹ ٹرانزیشن فنکشن ہی کی مانند ہے جسے اسی دستاویز میں پہلے بیان کیا جا چکا ہے۔ سب سے پہلے کرنسی یونٹوں کی تقسیم کی سہولت میسر کرنے کیلئے کوڈ کی چند اضافی سطریں شامل کرنا ہوں گی اور کچھ دوسرے انتہائی معاملات (بھی)؛ اور مثالی طور پر ایک مزید فنکشن شامل کیا جائے گا جو کسی ایڈریس کا بیلنس معلوم کرنے کیلئے دوسرے معاہدوں کی طرف سے آنے والے استفسار (query) کو سنبھال سکے۔ لیکن بس یہی سب کچھ کرنا ہوگا۔ نظری طور پر، ایتھریم پر مبنی ٹوکن سسٹمز میں، جو سب کرنسیز

کے طور پر برتاؤ کر رہے ہوں، ایک اور ایسا اہم فیچر بھی شامل ہو سکتا جو آن چین بِٹ کوائن پر مبنی بیٹا کرنسیز میں نہیں ہوتا: ٹرانزیکشن فیس کی براہِ راست اسی (دوسری) کرنسی میں ادائیگی کی صلاحیت۔ یہ کچھ اس طرح لاگو کیا جائے گا کہ کنٹریکٹ ایک ایتھر بیلنس برقرار رکھے گا جس کے ذریعے وہ ارسال کنندہ کو فیس ادا کرنے کیلئے ایتھر واپس لوٹائے گا (ری فنڈ کرے گا)، اور وہ اندرونی کرنسی یونٹوں کو جمع کرتے ہوئے، جو اس نے فیس کے طور پر کمائے ہیں، وہ اس بیلنس کو واپس بھرے گا؛ اور انہیں ایک مسلسل جاری نیلامی میں دوبارہ فروخت بھی کرے گا۔ لہٰذا، صارفین کو اپنے اکاؤنٹس کو ایتھر کے ساتھ ''ایکٹیویٹ'' کرانے کی ضرورت ہو گی، لیکن ایک بار ایتھر وہاں آگیا تو وہ بار بار استعمال کے قابل ہو گا کیونکہ معاہدہ ہر بار اسے واپس لوٹاتا رہے گا۔

مالیاتی ماخوذات اور قیام پذیر قدر والی کرنسیاں

ذہین معاہدے کا سب سے عام اطلاق، مالیاتی ماخوذات ہیں، جنہیں لاگو کرنے کیلئے لکھا جانے والا کوڈ بھی سادہ ترین ہے۔ مالیاتی معاہدوں کو لاگو کرنے میں اہم ترین چیلنج یہ ہے کہ ان کی اکثریت کو قیمت کے ایک بیرونی ٹِکر (ticker) کا حوالہ درکار ہوتا ہے۔ مثلاً ایک بہت ہی پسندیدہ اطلاق ایک ایسا ذہین معاہدہ ہے جو ایتھر (یا کسی اور کرپٹو کرنسی) میں شدید اُتار چڑھاؤ کے خلاف انتظامِ تلافی (hedge) کرتا ہے جو امریکی ڈالر کے حساب سے ہو، لیکن ایسا کرنے کیلئے اس معاہدے کا یہ جاننا ضروری ہے کہ ETH/USD کی قدر کیا ہے۔ ایسا کرنے کا سادہ ترین طریقہ ایک ''ڈیٹا فیڈ'' کنٹریکٹ کا استعمال ہے جسے کسی مخصوص فریق (مثلاً NASDAQ) کے ذریعے برقرار رکھتے ہوئے اس طرح ڈیزائن کیا جائے گا کہ وہ فریق اس معاہدے کو ضرورت پڑنے پر اپ ڈیٹ (تازہ) کرنے کے قابل ہو، جبکہ ایک ایسا مواجہ

(انٹر فیس) بھی فراہم کرنا ہوگا جو دیگر معاہدوں کو یہ سہولت دے کہ وہ (مذکورہ) معاہدے کو پیغام بھیج سکیں جس کے جواب میں انہیں قیمت فراہم کی جائے۔

ان اہم اجزاء کی موجود گیمیں، ہیجنگ (hedging) معاہدہ کچھ ایسا دکھائی دے گا:

1۔ فریق A کے 1000 جمع کرانے کا انتظار کرو۔

2۔ فریق B کے 1000 ایتھر جمع کرانے کا انتظار کرو۔

3۔ 1000 ایتھر کی امریکی ڈالر میں قدر معلوم کرو، جسے ذخیرے (اسٹوریج) میں ڈیٹا فیڈ کنٹریکٹ سے کویری (query) کر کے حاصل کیا جائے گا؛ اور وہ (قدر) x امریکی ڈالر ہے۔

4۔ تیس دن بعد، A یا B کو کنٹریکٹ میں "پنج" (ping) کرنے کی اجازت دو، تاکہ A کو x امریکی ڈالر کے بقدر ایتھر بھیجے جا سکیں (جن کا حساب ڈیٹا فیڈ کنٹریکٹ کو ایک بار پھر کویری کر کے نئی قیمت حاصل کرتے ہوئے کیا جائے گا) اور باقی ایتھر B کو بھیج دو۔

ایسے کسی معاہدے کی "کرپٹو کامرس" میں بڑی اہمیت ہوگی۔ کرپٹو کرنسی کے بارے میں بیان کئے جانے والے مسائل میں سے مرکزی مسئلہ اس میں شدید نوعیت کے اتار چڑھاؤ (volatility) ہیں؛ اگرچہ بہت سے صارفین اور تاجر اپنے کرپٹو کرنسی اثاثوں میں سہولت اور سکیوریٹی کو پسند کر سکتے ہیں، مگر اکثر یہ نہیں چاہیں گے کہ (کرنسی کی) قدر میں صرف ایک میں 23 فیصد کمی سے وہ اپنے سرمائے کے بڑے حصے سے محروم ہو جائیں۔ اب تک سب سے عام مجوزہ حل "جاری کنندہ کی پشت پناہی رکھنے والے" (issuer-backed) اثاثے رہے ہیں۔ اس تصور کے مطابق ایک جاری کنندہ کوئی ذیلی کرنسی (سب کرنسی) تخلیق کرتا ہے جس میں وہ (کرنسی) جاری کرنے اور یونٹس واپس لینے کا حق رکھتا ہے؛ اور کسی ایسے فرد کو اس کرنسی کا ایک یونٹ فراہم کرتا ہے جو اسے (آف لائن) کسی وضاحت کردہ اثاثے (مثلاً سونے یا امریکی ڈالر) کا ایک یونٹ دیتا ہے۔ اجراء کنندہ (issuer) تب کسی

اور فرد کو اس وضاحت کردہ اثاثے کی فراہمی کا وعدہ کرتا ہے بشرطیکہ وہ اسے کرپٹو اثاثے (crypto-asset) کا ایک یونٹ واپس فراہم کردے۔ یہ نظام سہولت دیتا ہے کہ کسی بھی نان کرپٹو گرافک اثاثے کو کرپٹو گرافک اثاثے میں "اوپر اٹھایا" (uplift) جائے، بشرطیکہ اجراء کنندہ پر بھروسہ کیا جاسکے۔

تاہم، اجراء کنندہ عملاً ہمیشہ قابل بھروسہ نہیں ہوتے، اور بعض معاملات میں ایسی سروسز کی وجود پذیری کیلئے بینکنگ انفرااسٹرکچر بہت ہی کمزور، یاانتہائی مخالفانہ ہوتا ہے۔ ایسے میں مالیاتی ماخوذات ایک متبادل فراہم کرتے ہیں۔ یہاں، کسی اثاثے کی پشت پناہی میں (مطلوبہ) فنڈز فراہم کرنے والے ایک اجراء کنندہ کے بجائے اندازے لگانے والوں (speculators) کی ایک عدم مرکزیت والی منڈی یہی کردار ادا کرتی ہے، جو اس پر شرطیں لگاتی ہے کہ فلاں کرپٹو گرافک اثاثے کی قیمت اوپر جائے گی یا نہیں۔ اجراء کنندہ کے برعکس، اندازے لگانے والوں کے نادہندہ ہونے کا کوئی امکان نہیں ہوتا کیونکہ ہیجنگ کنٹریکٹ ان کے فنڈز کو صرف ثالثی کیلئے ہی رکھتا ہے۔ دھیان رہے کہ یہ طریقہ کار مکمل طور پر عدم مرکزیت کا علمبردار نہیں کیونکہ قابل بھروسہ ماخذ کو اب بھی قیمت کا ٹِکر (ticker) فراہم کرتے رہنا پڑتا ہے۔ اس کے باوجود، یہ انفرااسٹرکچر کی ضروریات کم کرنے کے نقطۂ نگاہ سے ایک بڑی اور مثبت پیش رفت ہے (اجراء کنندہ ہونے کے برعکس، پرائس فیڈ جاری کرنے کیلئے کسی لائسنس کی ضرورت نہیں ہوتی اور اسے ممکنہ طور پر "آزادئ تقریر" یعنی فری اسپیچ کے طور پر زمرہ بند کیا جاسکتا ہے) جبکہ ساتھ ہی ساتھ اس سے دھوکہ دہی کے امکان میں بھی نمایاں کمی واقع ہوتی ہے۔

شناخت اور ساکھ کے نظام (Identity and Reputation Systems)

اوّلین متبادل کرپٹو کرنسی، نیم کوائن نے بِٹ کوائن جیسی بلاک چین استعمال کرتے ہوئے نام کی رجسٹریشن کا نظام (نیم رجسٹریشن سسٹم) وضع کرنے کی کوشش کی تھی، جس میں صارفین اپنے ناموں کو کسی عوامی ڈیٹابیس میں دیگر ڈیٹا کے ساتھ رجسٹر کروا سکتے ہیں۔ اس کے استعمال کی سب سے زیادہ مثال ''ڈی این ایس سسٹم'' سے دی جاتی ہے جو کسی ڈومین نیم، مثلاً ''bitcoin.org'' (یا، نیم کوائن کے معاملے میں ''bitcoin.bit'') کی میپنگ ایک خاص آئی پی ایڈریس پر کرتا ہے۔ دیگر عملی مثالوں میں ای میل کی تصدیق (authentication) اور ممکنہ طور پر زیادہ جدید ''ریپیوٹیشن سسٹمز'' ہیں۔ ذیل میں ایک بنیادی معاہدہ ہے جو ایتھریم پر نیم کوائن جیسا ''نیم رجسٹریشن سسٹم'' فراہم کرتا ہے:

```
if !contract.storage[tx.data[0]]:
    contract.storage[tx.data[0]] = tx.data[1]
```

یہ معاہدہ بہت ہی سادہ ہے جو دراصل ایتھریم نیٹ ورک میں ایک ڈیٹابیس ہے جسے اس میں شامل تو کیا جا سکتا ہے لیکن نہ تو تبدیل کیا جا سکتا ہے اور نہ ہی ختم کیا جا سکتا ہے۔ کوئی بھی یکساں قدر کے ساتھ نام رجسٹر کروا سکتا ہے، اور وہ رجسٹریشن ہمیشہ کیلئے وہاں چپک کر رہ جائے گی۔ قدرے نفیس اور پیچیدہ ''نیم رجسٹریشن کنٹریکٹ'' میں ''فکشن کلاز'' بھی ہو گی جو دوسرے معاہدوں کو اس سے کویری کرنے کی سہولت دے گی، جبکہ خاص نام والے ''مالک'' (یعنی پہلے رجسٹرار) کیلئے بھی ایک پورا عملی نظام مہیا کرے گی جس کے تحت وہ ڈیٹا تبدیل کر سکے گا یا پھر ملکیت منتقل کر سکے گا۔ اسی کی بنیاد پر ساکھ (ریپیوٹیشن) اور ''ویب آف ٹرسٹ'' فعالیت کا اضافہ بھی کیا جا سکتا ہے۔

عدم مرکزیت پر مبنی فائل کا ذخیرہ(Decentralized File Storage)

پچھلے چند سال میں آن لائن فائل اسٹوریج کی بہت سی مشہور اسٹارٹ اپ کمپنیاں سامنے آچکی ہیں، جن میں سے نمایاں ترین ''ڈراپ باکس'' ہے، جس کا مقصد صارفین کو یہ سہولت دینا ہے کہ وہ اپنی ہارڈ ڈرائیو کے بیک اپ کو اپ لوڈ کر کے اس سروس پر محفوظ کر سکیں اور ضرورت پڑنے پر اس تک رسائی بھی حاصل کر سکیں؛ جبکہ اس کے عوض وہ سروس کو ماہانہ فیس ادا کریں۔ البتہ، آن لائن فائل اسٹوریج کی مارکیٹ فی الحال نسبتاً ناقص کارکردگی کی حامل ہے۔ ایسی ہی دوسری خدمات کے سرسری جائزے سے معلوم ہوتا ہے کہ ایک خاص اور ''ان دیکھی وادی'' میں، 20 سے 200 گیگا بائٹ کی ایک ایسی سطح ہے جہاں پہنچ کر نہ تو مفت کوٹے دستیاب ہیں اور نہ ہی اینٹرپرائز لیول (بڑے ادارہ جات کی سطح) پر رعایتوں کی سہولت موجود ہے۔ فائل اسٹوریج کی ایسی مشہور سروسز میں قیمتیں کچھ ایسی ہوتی ہیں کہ آپ صرف ایک ماہ میں پوری ہارڈ ڈرائیو سے بھی زیادہ خرچ کر رہے ہوتے ہیں۔ ایتھریم معاہدے، اس ضمن میں، غیر مرکزیت پر مبنی ایسا اسٹوریج ماحول فراہم کر سکتے ہیں جس میں انفرادی صارفین، ذاتی کمپیوٹروں کی ہارڈ ڈرائیو کا کچھ غیر استعمال شدہ حصہ کرائے پر دے سکتے ہیں اور اپنی فائل اسٹوریج کی لاگت کم کر سکتے ہیں۔

اس حوالے سے کلیدی حصہ ایک ایسا آلہ ہے جسے ہم نے ''غیر مرکزی ڈراپ باکس معاہدے'' کا نام دیا ہے۔ یہ معاہدہ کچھ یوں کام کرتا ہے: پہلے کوئی شخص مطلوبہ ڈیٹا کو ''بلاکس'' میں تقسیم کرتا ہے، پرائیویسی کی غرض سے ہر بلاک کو اینکرپٹ کرتا ہے، اور اس سے ایک ''مرکل ٹری'' بناتا ہے۔ پھر وہ ایک معاہدہ تشکیل دیتا ہے جس میں یہ اصول ہوتا ہے کہ، ہر N بلاکس کیلئے، معاہدہ اپنے متعلقہ مرکل ٹری سے ایک جزافی (random) انڈیکس اٹھائے گا (جس کیلئے وہ پچھلے بلاک کا ہیش استعمال کرے گا، جو کنٹریکٹ کوڈ کے ذریعے قابل

رسائی ہوگا،اور جو مذکورہ جزافیت یعنی ''رینڈ منیس''کا ماخذ ہوگا)،اور پہلے وجود(entity) کوXایتھر فراہم کرے گا تاکہ ٹرانزیکشن کو ادائیگی کی سادہ توثیق جیسا ثبوتِ ملکیت تفویض کیا جائے جس کا تعلق اس (مرکل)ٹری میں کسی خاص انڈیکس سے ہو۔ جب کوئی صارف اپنی فائل دوبارہ ڈاؤن لوڈ کرنا چاہے، تو وہ ''مائیکروپیمنٹ چینل پروٹوکول'' استعمال کر سکتا ہے (مثلاً 1 زابو فی 32 کلوبائٹس ادا کرو) تاکہ اپنی فائل دوبارہ حاصل کر سکے۔ رقم دہندہ (payer) کیلئے مؤثر ترین طریقہ یہ ہے کہ وہ تب تک ٹرانزیکشن شائع نہ کرے کہ جب تک وہ مکمل ہو کر ختم نہ ہو جائے، بجائے اس کے کہ وہ ہر 32 کلوبائٹس کے بعد ٹرانزیکشن کو ایسی نئی ٹرانزیکشن سے تبدیل کرے جو (پہلے والی کے مقابلے میں) زیادہ پرکشش ہو اور جس کی نونس (nonce) بالکل وہی ہو۔

اس پروٹوکول کی ایک اہم خاصیت یہ ہے کہ اگرچہ ایسا لگتا ہے جیسے کوئی فرد، فائل کو نہ بھولنے کا فیصلہ کرنے کیلئے بہت سی جزافی نوڈز (random nodes) پر بھروسہ کر رہا ہے، لیکن وہ (اسی پروٹوکول کی مدد سے) خفیہ شیئرنگ کے ذریعے کئی ٹکڑوں میں توڑ کر اپنے لئے خدشات کو تقریباً صفر کر سکتا ہے؛ اور دیکھ سکتا ہے کہ معاہدوں (کنٹریکٹس) نے ہر حصے پر نظر رکھی ہوئی ہے کہ آیا وہ اب تک کسی نوڈ کے قبضے میں ہے یا نہیں۔ اگر کوئی معاہدہ اب بھی رقم ادا کر رہا ہے، تو اس سے یہ کرپٹو گرافک ثبوت ملتا ہے کہ باہر کوئی ایسا فرد ہے جو اب بھی فائل ذخیرہ کرنے میں مصروف ہے۔

عدم مرکزیت پر مبنی خودکار تنظیمیں(Decentralized Autonomous Organizations)

''عدم مرکزیت پر مبنی تنظیم'' کا عمومی تصور ایک ایسے مجازی وجود کا ہے جو ارکان (ممبرز) یا شیئر ہولڈرز کی ایک خاص تعداد رکھتا ہو جو، غالباً 67 فیصد اکثریت کے ساتھ، یہ حق رکھتے

ہوں کہ اس وجود کے فنڈز خرچ کر سکیں اور اس کے کوڈ میں ترمیم کر سکیں۔ ارکان اجتماعی طور پر یہ فیصلہ کر سکتے ہیں کہ تنظیم کس طرح فنڈز تفویض کرے گی۔ عدم مرکزیت پر مبنی خودکار تنظیم (DAO) میں فنڈز کی تفویض کاری کے طریقے متعدد اقسام کے معاوضوں کا احاطہ کرتے ہیں: تنخواہوں سے لے کر کسی کام پر بطور انعام دینے کیلئے کسی اندرونی کرنسی سے متعلق کہیں زیادہ عجیب غریب نظاموں تک۔ بنیادی طور پر یہ کسی روایتی کمپنی یا غیر منفعت پسند ادارے کی قانونی جکڑ بندیوں ہی کی نقل ہے جس میں (قواعد و ضوابط کی) پابندی کیلئے صرف کرپٹو گرافک بلاک چین ٹیکنالوجی استعمال کی گئی ہے۔ سرِ دست عدم مرکزیت پر مبنی خودکار تنظیموں سے متعلق گفتگو کا بیشتر حصہ "عدم مرکزیت کی حامل خود مختار کارپوریشن" (DAC) کے سرمایہ دارانہ ماڈل ہی پر مرکوز رہا ہے جس میں سالانہ منافع (dividend) وصول کرنے والے شیئر ہولڈرز اور قابلِ تجارت حصص (شیئرز) شامل ہوں۔ اس کے ایک ممکنہ متبادل میں، جسے "عدم مرکزیت والی خود مختار کمیونٹی" بھی کہا جا سکتا ہے، فیصلہ سازی کیلئے تمام ارکان کے پاس یکساں حصہ (شیئر) ہو گا اور موجودہ ارکان کے 67 فیصد اتفاقِ رائے سے کسی رُکن کو شامل کرنے یا نکال باہر کرنے کا فیصلہ کیا جا سکے گا۔ یہ تقاضا کہ ہر فرد کے پاس صرف ایک ہی رکنیت (ممبر شپ) ہو، گروپ کی جانب سے اجتماعی فیصلہ کر کے ہی پورا کیا جائے گا، اور اس پر عملدرآمد کیا جائے گا۔ غیر مرکزیت پر مبنی تنظیم (DO) کا کوڈ لکھنے کا عمومی انداز، اجمالی طور پر، ذیل میں بتایا گیا ہے۔ اس کا سادہ ترین ڈیزائن تو صرف ایسے کوڈ کا ایک حصہ ہے جو خود کو تبدیل کرنے کے قابل ہو، اور اس وقت تبدیل ہو کہ جب دو تہائی (67 فیصد) ارکان اس تبدیلی پر متفق ہوں۔ اگرچہ نظری طور پر یہ کوڈ ناقابلِ ترمیم ہوتا ہے، لیکن جداگانہ معاہدوں میں کوڈ کے ٹکڑے شامل کر کے اس میں خصوصی نوعیت کی ترمیم پذیری (mutability) کا اضافہ کرتے ہوئے یہ مسئلہ بہ آسانی حل کیا

جاسکتا ہے؛ اور یہ ایڈریس بھی دیا جاسکتا ہے کہ قابل ترمیم اسٹوریج میں (اس مقصد کیلئے) کون کونسے معاہدوں (کنٹریکٹس) سے رابطہ کرنا ہے۔ ایسے کسی ڈی اے او (DAO) کنٹریکٹ کی سادہ انداز سے اطلاق پذیری کیلئے تین طرح کی ٹرانزیکشنز ہوں گی، جنہیں ٹرانزیکشن میں فراہم کردہ ڈیٹا کی بنیاد پر شناخت کیا جائے گا:

- سب سے پہلی [0,i,K,V] جو کسی پروپوزل کو انڈیکس i کے رجسٹر کرتے ہوئے اسٹوریج انڈیکس K پر ایڈریس تبدیل کرکے اس کی قدر V کردے۔
- دوسرے نمبر پر [0,i] ہے جو پروپوزل i کے حق میں ووٹ رجسٹر کرے۔
- اور تیسری [2,i] جو پروپوزل i کو حتمی شکل دے بشرطیکہ کافی ووٹ دیئے جاچکے ہوں۔

اس کے بعد معاہدے کو ان میں سے ہر ایک کیلئے شقیں تفویض کی جائیں گی۔ یہ اسٹوریج میں کی جانے والی تمام آزادانہ تبدیلیوں کا ریکارڈ رکھے گا، جس کے ساتھ یہ فہرست بھی ہوگی کہ ان کیلئے کس کس نے ووٹ دیا۔ اس میں تمام ارکان کی فہرست بھی ہوگی۔ جب اسٹوریج میں ہونے والی کسی بھی تبدیلی کے حق میں دو تہائی ارکان کے ووٹ آجائیں، تو حتمی طور پر وجود میں آنے والی ٹرانزیکشن اس تبدیلی پر عملدرآمد کروا سکے گی۔ اس سے پیچیدہ اور نفیس ڈھانچے میں دوسرے فیچرز جیسے کہ ٹرانزیکشن بھیجنا، رکن شامل کرنا اور رکن نکالنا وغیرہ کیلئے بھی اندرونی طور پر پہلے ہی سے (بلٹ اِن) ووٹنگ کی صلاحیت موجود ہوگی؛ اور یہ مائع جمہوریت (Liquid Democracy) کی طرز پر (کسی دوسرے فرد کو) ووٹ تفویض کرنے کی سہولت تک فراہم کرے گی (یعنی کوئی شخص کسی دوسرے فرد کو اپنی طرف سے ووٹ کرنے کی ذمہ داری تفویض کرسکتا ہے، اور اس تفویض کاری کی نوعیت عبوری (transitive) ہوگی کہ اگر A تفویض کرتا ہے B کو اور B تفویض کرتا ہے C کو تو پھر

C سے A کے ووٹ کا تعین ہوگا)۔ یہ ڈیزائن عدم مرکزیت کی حامل تنظیم کو جاندار انداز سے نشوونما پا کر ایک عدم مرکزیت پر مبنی کمیونٹی بننے کی سہولت دے گا جس سے افراد کو، حتمی طور پر، یہ اختیار ہوگا کہ وہ اس بات کا تعین کرنے کا کام (کسی اور کو) تفویض کر سکیں کہ کون کونسے ارکان ماہرین (specialists) ہیں؛ تاہم یہ عمل "موجودہ نظام" کی طرح نہیں ہوگا کہ جس میں کمیونٹی کے انفرادی ارکان کے اپنی اپنی ترتیب تبدیل کرنے پر ماہرین بار بار بہ آسانی وجود میں آسکتے اور غائب بھی ہو سکتے ہیں۔

عدم مرکزیت پر مبنی کارپوریشن کا ایک متبادل ماڈل کچھ ایسا بھی ہو سکتا ہے کہ جس میں کسی بھی اکاؤنٹ کے پاس صفر یا زیادہ حصص (شیئرز) ہو اور کوئی فیصلہ کرنے کیلئے کم از کم دو تہائی حصص درکار ہوں۔ (اس کارپوریشن کے) تفصیلی ڈھانچے میں اثاثوں کی انتظام کاری کی فعالیت (asset management functionality)، حصص خریدنے یا بیچنے کیلئے پیشکش (آفر) کرنے کی قابلیت، اور پیشکشیں قبول کرنے کی صلاحیت شامل ہیں (ترجیحی طور پر معاہدے کے اندر ایک "آرڈر میچنگ" نظام کی مدد سے)۔ اختیار کی تفویض کاری (delegation) کا وجود بھی مائع جمہوریت کے انداز میں ہوگا، جو "بورڈ آف ڈائریکٹرز" کے تصور کی عمومی شکل ہوگا۔

مستقبل میں تنظیمی بندوبست (گورننس) کیلئے زیادہ جدید نظام لاگو کئے جا سکیں گے؛ البتہ اس موقعے پر ایک غیر مرکزیت پر مبنی تنظیم (DO) کی ابتدائی وضاحت ایک "غیر مرکزیت پر مبنی خود مختار تنظیم" (DAO) کے طور پر کی جا سکتی ہے۔ DO اور DAO کے مابین فرق بہت مبہم ہے، لیکن عمومی خطِ تقسیم یہ ہے کہ آیا تنظیمی بندوبست، بالعموم، کسی سیاسی قسم کے عمل سے کیا جاتا ہے یا پھر کسی "خودکار" عمل کے ذریعے۔ البتہ ایک بدیہی آزمائش "غیر مشترکہ زبان" (no common language) کی کسوٹی ہے: کیا کوئی تنظیم اس

وقت کام کر سکتی ہے کہ جب اس کے کوئی سے بھی دو ارکان یکساں زبان نہ بولتے ہوں؟ ظاہر ہے کہ ایک سادہ، شیئر ہولڈر طرز کی کارپوریشن (ایسے حالات میں) ناکام ہو جائے گی، جبکہ بِٹ کوائن پروٹوکول جیسی کسی چیز کے کامیاب ہونے کا امکان بہت زیادہ ہے۔ رابن ہینسن کا futarchy، جو پیش گوئی کی منڈیوں کے ذریعے تنظیمی بندوبست کا ایک نظام ہے، ایک حقیقی "خود مختار" بندوبست کے ممکنہ خدوخال کی ایک اچھی مثال ہے۔ دھیان رہے کہ یہ فرض کرنا ضروری نہیں کہ تمام DAOs، تمام DOs پر فوقیت رکھتے ہوں؛ خود کاریت (آٹومیشن) سادہ طور پر ایک ایسی پیراڈائم ہے جو بعض مخصوص مقامات پر بہت زیادہ ممکنہ فوائد دے سکتی ہے جبکہ دیگر میں شاید اس کی کوئی عملی حیثیت نہ ہو، اور بہت سی "نیم عدم مرکزیت پر مبنی تنظیمیں" (semi-DAOs) ممکنہ طور پر موجود ہو سکتی ہیں۔

مزید اطلاقات

1۔ بچت بٹوے (savings wallets): فرض کیجئے کہ ایلس اپنے فنڈز کو محفوظ رکھنا چاہتی ہے لیکن اس طرف سے پریشان بھی ہے کہ کہیں کوئی اس کی "پرائیویٹ کی" ہیک نہ کر لے۔ وہ باب کے ساتھ معاہدے کیلئے ایتھر استعمال کرتی ہے جبکہ باب ایک بینک ہے۔ معاہدہ کچھ یوں ہو سکتا ہے:

ایلس اکیلی زیادہ سے زیادہ اپنے فنڈز کا 1 فیصد روزانہ نکلوا سکتی ہے۔

باب اکیلا ان فنڈز کا زیادہ سے زیادہ 1 فیصد روزانہ نکلوا سکتا ہے، لیکن ایلس کو اختیار ہے کہ وہ اپنی "کی" استعمال کرتے ہوئے کوئی ٹرانزیکشن کرے جبکہ اس صلاحیت کو منسوخ کر دے۔

ایلس اور باب، دونوں مل کر کچھ بھی نکلوا سکتے ہیں۔

عام حالات میں ایلس کیلئے 1 فیصد یومیہ کافی ہے، اور اگر ایلس زیادہ نکلوانا چاہتی ہے تو وہ مدد کیلئے باب سے رابطہ کر سکتی ہے۔ اگر ایلس کی ''کی'' ہیک ہو جائے، تو وہ باب کے پاس جاتی ہے تاکہ فنڈز ایک نئے معاہدے کے تحت لائے جائیں۔ اگر ایلس کی ''کی'' گم ہو جائے، تو بالآخر باب سارے فنڈز نکلوالے گا۔ اگر باب بے ایمان ہو جائے، تو پھر ایلس اس کی (فنڈز) نکلوانے کی صلاحیت کو ختم (آف) کر سکتی ہے۔

2۔ فصل کا انشورنس: مالیاتی ماخوذات پر مشتمل معاہدہ بھی اس کے ذریعے بہ آسانی بنایا جا سکتا ہے جس میں پرائس انڈیکس کی جگہ موسم اور آب وہوا سے متعلق ڈیٹا فیڈ استعمال کی گئی ہو۔ مثلاً آیووا کا ایک کسان کوئی ایسا ماخوذہ (derivative) خرید سکتا ہے جو آیووا میں بارش کی بنیاد پر معکوس ادائیگی کرے؛ یعنی اگر خشک سالی ہو تو کسان کو خود بخود رقم موصول ہو جائے اور اگر بارش زیادہ ہو، تو کسان خوشی خوشی رقم (خود کار انداز سے) ادا کرے گا کیونکہ تب اس کی فصل اچھی ہو گی۔

3۔ غیر مرکزیت پر مبنی (decentralized) ڈیٹا فیڈ: مختلف نوعیت کے مالیاتی معاہدوں کیلئے، حقیقتاً یہ ممکن ہے کہ ایک پروٹوکول ''شیلنگ کوائن'' (SchellingCoin) کے ذریعے ڈیٹا فیڈ کو عدم مرکزیت پر مبنی بنا دیا جائے۔ شیلنگ کوائن کچھ ایسے کام کرتی ہے: تمام N فریقین ایک نظام میں کسی اطلاع کے ایک حصے (datum) کو کچھ قدر دیتی ہیں (مثلاً ETH/USD کی قیمت)، یہ قدریں (ویلیوز) ترتیب وار ہوتی ہیں، اور ہر وہ شخص 25 ویں سے لے کر 75 ویں فیصد کے درمیان ہے، وہ ایک ٹوکن بطور انعام حاصل کرتا ہے۔ ہر ایک کیلئے یہ ترغیب بھی ہے کہ وہ ویسا ہی جواب دے جیسا کوئی دوسرا بھی دے گا؛ اور وہی قدر حتمی طور پر طے شدہ (ڈیفالٹ) قرار پائے گی کہ جس پر کھیلنے والوں کی بڑی تعداد، حقیقی معنوں میں متفق ہو گی، یعنی اسی قدر کو درست

(truth) تسلیم کیا جائے گا۔ یہ تدبیر عدم مرکزیت پر مبنی ایک پروٹوکول تخلیق کرتی ہے جو نظری طور پر کسی بھی تعداد میں قدریں فراہم کر سکتا ہے، بشمول ETH/USD، برلن کا درجہ حرارت اور کسی مخصوص و مشکل حسابی عمل کے نتائج بھی۔

4۔ذہین کثیر دستخطی ثالثی (Smart multi-signature escrow): بٹ کوائن ایسی کثیر دستخطی ٹرانزیکشن سے متعلق معاہدوں کی سہولت دیتی ہے جن میں، مثلاً پانچ میں سے تین "کیز" فنڈز کو خرچ کر سکیں۔ ایتھریم میں اس سے کہیں زیادہ باریکی (granularity) فراہم کرتا ہے، یعنی یہ کہ پانچ میں سے چار (کیز) کچھ بھی خرچ کر سکیں، پانچ میں سے تین (کیز) 10 فیصد تک (فنڈز) روزانہ خرچ کر سکیں، جبکہ پانچ میں سے دو (کیز) ہر روز 0.5 فیصد تک (فنڈز) خرچ کر سکیں۔ مزید برآں، ایتھریم کے تحت کثیر دستخطی (multisig) کی سہولت غیر ہم عصر (asynchronous) ہوتی ہے۔ یعنی دو فریقین اپنے اپنے دستخط، ایک ہی بلاک چین پر، مختلف اوقات میں رجسٹر کروا سکتے ہیں جبکہ آخری دستخط خود بخود ٹرانزیکشن بھیج دے گا۔

5۔کلاؤڈ کمپیوٹنگ: ای وی ایم (EVM) ٹیکنالوجی ایک قابل توثیق ماحول تخلیق کرنے میں بھی استعمال کی جا سکتی ہے، جو صارفین کو سہولت دیتی ہے کہ وہ دوسروں سے حسابات کرنے کیلئے کہہ سکیں اور پھر، اختیاری طور پر، اٹکل سے منتخب کئے گئے کچھ مخصوص جانچ کاری مقامات (چیک پوائنٹس) پر انجام دیئے گئے ان حسابات کے درست ہونے کے ثبوت بھی مانگ سکیں۔ اس سے کلاؤڈ کمپیوٹنگ مارکیٹ کی تشکیل میں بھی سہولت پیدا ہوتی ہے جہاں کوئی بھی صارف اپنے ڈیسک ٹاپ، لیپ ٹاپ یا خصوصی سرور کے ساتھ شرکت کر سکے، اور سکیوریٹی ڈپازٹس کے ساتھ اسپاٹ چیکنگ استعمال کرتے ہوئے، نظام کے قابل بھروسہ ہونے کی یقین دہانی کی جا سکے (یعنی نوڈز منفعت بخش انداز میں دھوکہ نہ دے سکیں)۔ تاہم یہ

نظام ہر طرح کے کام کیلئے موزوں نہیں رہے گا؛ مثلاً وہ کام جن میں اعلیٰ سطح کی انٹر پروسیس کمیونی کیشن کی ضرورت ہوتی ہے، نوڈز کے بڑے کلاؤڈ پر بہ آسانی نہیں کئے جاسکتے۔ البتہ دیگر اُمور، جنہیں متوازی انداز سے انجام دینا نسبتاً آسان ہیں، جیسے کہ سیٹی ایٹ ہوم، فولڈنگ ایٹ ہوم اور جینیٹک الگورتھم وغیرہ آسانی سے اس طرح کے کسی پلیٹ فارم پر انجام دیئے جاسکتے ہیں۔

6۔ ہمسر تاہمسر جوا (P2P Gambling): پی ٹو پی جوئے سے متعلق پروٹوکولز کی کوئی سی بھی تعداد، جیسے کہ فرینک استاہانو اور رچرڈ کلیٹن کی "سائبر ڈائس" (Cyberdice)، ایتھریم بلاک چین پر لاگو کی جاسکتی ہے۔ جوئے کا سادہ ترین پروٹوکول دراصل ایک معاہدہ ہی ہوتا ہے جو اگلے بلاک ہیش سے فرق کیلئے ترتیب دیا جاتا ہے، اور جدید تر پروٹوکولز یہیں سے تیار کئے جاسکتے ہیں، جو تقریباً صفر فیس والی گیمبلنگ سروسز (جوئے کی خدمات) تخلیق کرتے ہیں جن میں دھوکہ دہی کی کوئی صلاحیت بالکل بھی نہیں ہوتی۔

7۔ پیش گوئی کی مارکیٹ: کسی اوریکل یا "شیلنگ کوائن" کی فراہمی پر، پیش گوئی کی منڈیاں بھی لاگو کرنا آسان ہے، جبکہ پیش گوئی کی مارکیٹیں اور شیلنگ کوائن یکجا ہو کر مرکزی دھارے میں futarchy کا ایسا اطلاق ثابت ہو سکتی ہیں جس میں غیر مرکزی تنظیموں کیلئے بندوبستی (گورنینس) پروٹوکول سے استفادہ کیا گیا ہو۔

8۔ آن چین ڈی سینٹر لائزڈ مارکیٹ پلیسز، جن میں شناخت اور ساکھ سے متعلق نظاموں کو بطور بنیاد استعمال کیا گیا ہو۔

ترمیم شدہ GHOST نفاذ

یوناتن سومپولنسکی اور ابیب زوہر نے دسمبر 2013ء میں پہلی بار "مشاہدہ کردہ ثقیل ترین ذیلی شجر" (Greedy Heaviest Observed Subtree) یا مختصراً GHOST نامی ایک جدید پروٹوکول پیش کیا۔ GHOST کے پسِ پشت یہ تحریک تھی کہ تیز رفتار تصدیقی اوقات والی بلاک چینز اپنی بلند شرحِ فرسودگی (stale rate) کی بناء پر، حالیہ طور پر کم تر سکیوریٹی کا شکار ہیں؛ کیونکہ بلاکس کسی نیٹ ورک میں پھیلنے کیلئے ایک خاص وقت لیتے ہیں۔ یعنی اگر ایک مائنر A ایک بلاک کی مائننگ کرتا ہے اور مائنر B ایک اور بلاک کی مائننگ A کے بنائے ہوئے بلاک کے B تک پہنچنے سے پہلے کر لیتا ہے، تو مائنر B کا بنایا ہوا بلاک ضائع ہو جائے گا اور نیٹ ورک کی سکیوریٹی میں کوئی حصہ نہیں لے گا۔ مزید یہ کہ مرکزیت کا مسئلہ بھی ہے: اگر مائنر A ایک ایسا مائننگ پُول ہے جس کی ہیش پاور 30 فیصد ہے جبکہ B کی ہیش پاور 10 فیصد ہے، تو A کیلئے خدشہ ہو گا کہ وہ 70 فیصد وقت میں فرسودہ بلاک تیار کر رہا ہو گا (کیونکہ باقی 30 فیصد وقت میں A نے پچھلا بلاک تیار کیا ہو گا اور وہ مائننگ ڈیٹا فوراً حاصل کر لے گا) جبکہ B کیلئے فرسودہ بلاک بنانے کا خدشہ 90 فیصد وقت کیلئے موجود ہو گا۔ لہٰذا، اگر بلاک کا درمیانی وقفہ شرحِ فرسودگی کے بلند ہونے کیلئے بہت مختصر ہوا تو A صرف اپنی جسامت (سائز) کی بدولت نمایاں طور پر زیادہ کارکردگی کا حامل ہو گا۔ ان دونوں اثرات کے یکجا ہونے پر قوی امکان ہے کہ وہ بلاک چینز جو زیادہ تیزی سے بلاکس بنا رہی ہوں گی، وہ ایک ایسا مائننگ پول بنا لیں گی جس کے پاس نیٹ ورک ہیش پاور کی کافی بڑی فیصد ہو گی، جس سے وہ مائننگ کے عمل پر حقیقتاً قابض ہو جائیں گی۔

جیسا کہ سومپولنسکی اور زوہر نے وضاحت کی، GHOST نیٹ ورک سکیوریٹی میں کمی کے پہلے مسئلے کو اس طرح حل کرتا ہے کہ ''طویل ترین'' زنجیر کا تعین کرتے دوران وہ فرسودہ بلاکس کو بھی حساب میں شامل رکھتا ہے۔ مطلب یہ کہ وہ صرف کسی بلاک کے والد (پیرنٹ) اور مزید اجداد ہی کو نہیں بلکہ بلاک کے اجداد کے فرسودہ بچوں کو بھی حساب میں شامل رکھتا ہے (جنہیں ایتھریم کی اصطلاح میں ''انکلز'' (uncles) کہا جاتا ہے) اور یہ معلوم کرتا ہے کہ کس بلاک کی پشت پر ثبوتِ کار کی سب سے بڑی تعداد موجود ہے۔ دوسرا مسئلہ، یعنی مرکزیت کی جانبداری (centralization bias) حل کرنے کیلئے، ہم سومپولنسکی اور زوہر کے بیان کردہ پروٹوکول سے بھی آگے بڑھتے ہیں، اور فرسودہ بلاکس کو مرکزی زنجیر (مین چین) میں رجسٹر ہو کر بلاک کا انعام حاصل کرنے کی اجازت دیتے ہیں: ایک فرسودہ بلاک اپنے بنیادی انعام کا 93.75 فیصد حاصل کرے گا جبکہ ''بھتیجا'' جو فرسودہ بلاک میں شامل ہے، وہ بقیہ 6.25 فیصد حاصل کرے گا۔ البتہ، ٹرانزیکشنز فیس ''انکلز'' کو نہیں دی جائیں گی۔

ایتھریم میں GHOST کے ایک سادہ ورژن کا اطلاق کیا گیا ہے جو صرف پانچ سطحوں (لیولز) تک نیچے جاتا ہے۔ زیادہ واضح طور پر کہا جائے تو ایک فرسودہ بلاک صرف ایک ''انکل'' کی حیثیت سے، اس کے والد سے دوسری اور پانچویں نسل والے بچے کے ذریعے ہی شامل کیا جاسکتا ہے، جبکہ اس سے زیادہ دور کا رشتہ رکھنے والا کوئی بلاک (مثلاً کسی والد سے چھٹی نسل کا بچہ، یا دادا سے تیسری نسل کا بچہ) شامل نہیں کیا جاسکتا۔ ایسا کئی وجوہ سے کیا جاتا ہے۔ اوّل یہ کہ لامحدود GHOST اس حساب میں بہت زیادہ پیچیدگی شامل کردے گا کسی بلاک کیلئے کون کونسے ''انکلز'' درست ہیں۔ دوم یہ کہ ایتھریم میں جس طرح سے ''تلافی'' (compensation) رائج ہے، اسے لامحدود GHOST سے ملا دینے کے نتیجے میں

کسی بھی مائنر کیلئے یہ ترغیب ختم ہو جائے گی کہ وہ مرکزی زنجیر کی مائننگ کرتا رہے اور ایک عوامی حملہ آور کی زنجیر پر کام نہ کرے۔ آخر میں، تخمینے سے معلوم ہوتا ہے کہ پانچ سطحوں والا GHOST جس میں ترغیب کاری بھی شامل ہو، وہ 95 فیصد سے بھی زیادہ کارکردگی کا حامل ہوتا ہے، چاہے اس کا بلاک ٹائم 15 سیکنڈ ہی کیوں نہ ہو، اور 25 فیصد ہیش پاور والے مائنرز کیلئے مرکزیت کے فوائد (centralization gains) تین فیصد کم ہو جاتے ہیں۔

فیس

کیونکہ بلاک چین پر شائع کی گئی ہر ٹرانزیکشن، نیٹ ورک پر اس امر کی لاگت بھی عائد کرتی کہ اسے ڈاؤن لوڈ کر کے اس کی تصدیق کی جائے، لہٰذا اس کیلئے کسی انضباطی نظام (ریگولیٹری مکینزم) کی بھی ضرورت ہوتی ہے، جس میں بالعموم ٹرانزیکشن فیس بھی لگانی پڑتی ہے تاکہ غلط استعمال سے بچا جا سکے۔ مشکل تدبیر، جو بٹ کوائن میں استعمال کی جاتی ہے، خالصتاً رضاکارانہ فیس رکھنے کا عمل ہے، جس میں مائنروں کو صرف چوکیداروں کے طور پر کام کرنا پڑتا ہے جبکہ حرکت پذیری (ڈائنامک) کو کم ترین سطح پر رکھا جاتا ہے۔ یہ تدبیر بٹ کوائن کمیونٹی میں بڑی گرم جوشی سے قبول کی گئی، خصوصاً اس لئے کیونکہ یہ "مارکیٹ پر مبنی" ہے، جو مائنر اور ٹرانزیکشن بھیجنے والوں کے مابین طلب و رسد سے قیمت کا تعین کرتی ہے۔ مذکورہ استدلال میں مسئلہ یہ ہے کہ، بہر حال، ٹرانزیکشن پروسیسنگ کوئی مارکیٹ نہیں۔ تاہم یہ وجدانی طور پر ٹرانزیکشن پروسیسنگ کو ایک ایسی خدمت (سروس) کے طور پر بیان کرتا ہے جو کوئی مائنر کسی ارسال کنندہ کو فراہم کر رہا ہو۔ درحقیقت، ہر ٹرانزیکشن جسے مائنر شامل کرتا ہے، اس کا نیٹ ورک میں شامل ہر نوڈ پر پروسیس ہونا ضروری ہوتا ہے، لہٰذا ٹرانزیکشن پروسیسنگ پر آنے والی

لاگت کا بڑا حصہ تیسرے فریقین کی نذر ہو جاتا ہے جبکہ مائنر، جو یہ فیصلہ کر رہا ہوتا ہے کہ اسے شامل کیا جائے یا نہیں، وہ بہت کم حاصل کر پاتا ہے۔ پس، ''عوام کا المیہ'' جیسے مسائل رونما ہونے کا قوی امکان ہے۔

تاہم، جونہی یہ پتا چلتا ہے کہ خامی مارکیٹ پر انحصار کرنے والے نظام کی وجہ سے ہے، تو جب کوئی غیر درست سادہ کاری کا مفروضہ دیا جاتا ہے، تو وہ جادوئی طور پر خود کو منسوخ کر دیتا ہے۔ متعلقہ استدلال کچھ یوں ہے۔ فرض کیجئے:

1۔ ایک ٹرانزیکشن k آپریشنز کو جنم دیتی ہے، اسے شامل کرنے والے کسی بھی مائنر کو kR انعام سے نوازتی ہے جبکہ R کی قیمت ارسال کنندہ مقرر کرتا ہے اور k اور R پہلے ہی سے (خام حیثیت میں) مائنر کیلئے نمایاں ہوتے ہیں۔

2۔ کسی بھی نوڈ پر ایک آپریشن کی پروسیسنگ لاگت C ہے (یعنی تمام نوڈز یکساں کارکردگی کی حامل ہیں)۔

3۔ مائننگ نوڈز کی تعداد N ہے، جن میں سے ہر ایک کی بالکل مساوی پروسیسنگ پاور ہے (یعنی مجموعی طور پر 1/N)۔

4۔ مائننگ نہ کرنے والی کوئی مکمل نوڈ موجود ہی نہیں۔

ایک مائنر تب ہی کسی ٹرانزیکشن کو پروسیس کرنا چاہے گا کہ جب متوقع انعام، لاگت سے زیادہ ہو۔ لہٰذا، متوقع انعام kR/N ہوا کیونکہ مائنر کے پاس اگلے بلاک کی پروسیسنگ کرنے کا 1/N امکان ہے، اور مائنر کی پروسیسنگ لاگت سادہ طور پر kC ہے۔ پس، مائنرز وہ ٹرانزیکشنز شامل کریں گے کہ جن میں kR/N > kC یا R > NC ہو۔ دھیان رہے کہ R وہ فی آپریشن فیس ہے جو ارسال کنندہ کی مقرر و فراہم کردہ ہے، اور اسی لئے یہ منافعے کی نچلی حد (lower bound) ہے جو ارسال کنندہ اس ٹرانزیکشن سے اخذ کرتا ہے؛ اور

NC ایک آپریشن کو انجام دینے کیلئے پورے نیٹ ورک کی جانب سے مجموعی طور پر ہونے والی پروسیسنگ کی لاگت ہے۔ لہٰذا، مائنرز کو صرف وہی ٹرانزیکشنز شامل کرنے کی ترغیب ملے گی جن سے ہونے والا فائدہ، لاگت سے زیادہ ہو۔

البتہ، حقیقت میں ان مفروضات سے کئی ایک انحرافات موجود ہیں:

1۔ مائنر عملاً کسی ٹرانزیکشن کو پروسیس کرنے کیلئے دیگر تصدیقی نوڈز کے مقابلے میں زیادہ لاگت ادا کر رہا ہوتا ہے، کیونکہ تصدیق میں اضافی وقت سے بلاک کے پھیلاؤ میں تاخیر ہوتی ہے اور یوں اس بات کا امکان بڑھ جاتا ہے کہ وہ بلاک فرسودہ ہو جائے گا۔

2۔ مائننگ نہ کرنے والی مکمل نوڈز بھی موجود ہوتی ہیں۔

3۔ مائننگ پاور کی تقسیم عملاً مکمل طور پر عدم مساوات کی حیثیت سے اختتام پذیر ہو سکتی ہے۔

4۔ مفروضات گھڑنے والے، سیاسی دشمن اور سر پھرے بھی وجود رکھتے ہیں جن کی فعال شراکت سے نیٹ ورک کو نقصان پہنچ سکتا ہے، اور وہ بڑی مکاری سے ایسے معاہدے تشکیل دے سکتے ہیں جن کی لاگت دوسری تصدیقی نوڈز کی ادا کردہ لاگت سے بہت کم ہو۔

مذکورہ بالا نکتہ نمبر 1 اس رجحان کی آبیاری کرتا ہے کہ مائنر کم تعداد میں ٹرانزیکشنز شامل کرے، اور نکتہ نمبر 2 سے NC میں اضافہ ہوتا ہے؛ پس یہ دونوں اثرات، کم از کم جزوی طور پر، ایک دوسرے کو منسوخ کر دیتے ہیں۔ نکتہ 3 اور 4 ہی اصلی مسائل ہیں، جنہیں حل کرنے کیلئے ہم ایک ''تیرتا ڈھکنا'' (floating cap) لگاتے ہیں: کوئی بلاک BLK_LIMIT_FACTOR اور طویل مدتی قوت نمائی متحرک اوسط کے حاصل ضرب سے زیادہ آپریشنز نہیں کر سکتا۔ صراحت کچھ یوں ہے:

blk.oplimit = floor((blk.parent.oplimit *
(EMAFACTOR - 1) + floor(parent.opcount *
BLK_LIMIT_FACTOR)) / EMA_FACTOR)

یہاں BLK_LIMIT_FACTOR اور EMA_FACTOR مستقل ہیں جنہیں وقتی طور پر بالترتیب 65536 اور 1.5 رکھا جائے گا لیکن مزید تجزیئے کے بعد انہیں تبدیل بھی کیا جاسکتا ہے۔

حساب کاری اور "ٹیورنگ مکملیت" (Computation and Turing-Completeness)

ایک اہم نکتہ یہ بھی ہے کہ ایتھریئم ورچوئل مشین "ٹیورنگ مکمل" (ٹیورنگ کمپلیٹ) ہے۔ یعنی کہ EVM کوڈ ایسے کسی بھی حساب کو انکوڈ (encode) کر سکتا ہے جو قابل فہم طور پر انجام دیا جاسکتا ہو، بشمول لامتناہی چکروں (loops) کے۔ EVM کوڈ، لوپنگ کی سہولت دو طریقوں سے دیتا ہے۔ اوّل، اس میں ایک JUMP نامی ہدایت ہے جو پروگرام کو اس کے کوڈ میں پچھلے مقام پر پلٹ کر واپس جانے کی اجازت دیتی ہے، اور JUMPI ہدایت جو مشروط جست (conditional jump) انجام دینے کیلئے while x < 27: x = x * 2 جیسے بیانات کی اجازت دیتی ہے۔ دوم، معاہدے دوسرے معاہدوں کو "کال" (call) کر سکتے ہیں، جس سے تکرار کے ذریعے لوپنگ کی سہولت حاصل ہوتی ہے۔ اس سے فطری طور پر ایک مسئلہ پیدا ہوتا ہے: کیا بدطینت صارفین بنیادی طور پر مائنرز اور مکمل نوڈز کو لامتناہی لوپ میں داخل ہونے کیلئے مجبور کر کے بند کروا سکتے ہیں؟ یہ معاملہ کمپیوٹر سائنس میں ایک مسئلے کی پیداوار ہے جسے "رُک جانے کا مسئلہ" (ہالٹنگ پرابلم) کہتے

ہیں: عمومی معاملات کیلئے ایسا کوئی طریقہ موجود نہیں جو یہ بتا سکے کہ دیا گیا کوئی پروگرام کبھی رکے گا یا نہیں۔

جیسا کہ اسٹیٹ ٹرانزیشن والے حصے میں بتایا گیا، ہمارا حل اس طرح کام کرتا ہے کہ اسے زیادہ سے زیادہ حسابی مراحل طے کرنے کیلئے، کہ جن کی یہ اجازت دے، ایک ٹرانزیکشن کی ضرورت ہوتی ہے، اور اگر عملدرآمد میں زیادہ وقت لگ جائے تو حسابی عمل تو واپس پلٹ جاتا ہے لیکن فیسیں بہر حال ادا کی جاتی ہیں۔ پیغامات بھی اسی طرح کام کرتے ہیں۔ ہمارے حل کے پس پشت تحریک کو واضح کرنے کیلئے درج ذیل مثالیں ملاحظہ کیجئے:

ایک حملہ آور ایک ایسا کنٹریکٹ (معاہدہ) تخلیق کرتا ہے جو ایک لا متناہی لوپ چلاتا ہے، اور پھر اس لوپ کو سرگرم کرنے سے متعلق ایک ٹرانزیکشن، مائنر کو بھیجتا ہے۔ مائنر اس ٹرانزیکشن کو پروسیس کرے گا، اور لا متناہی لوپ چلا دے گا، اور گیس کے ختم ہو جانے تک انتظار ہی کرتا رہ جائے گا۔ اگرچہ عملدرآمد (ایگزیکیوشن) کے بیچوں بیچ ہی گیس ختم ہو جاتی ہے اور پروسیسنگ بھی درمیان میں رک جاتی ہے، لیکن ٹرانزیکشن اب بھی درست ہو گی اور مائنر تب بھی حملہ آور سے ہر حسابی مرحلے کیلئے اپنے معاوضے کا مطالبہ کر سکتا ہے۔

حملہ آور ایک بہت ہی طویل لا متناہی لوپ تخلیق کر کے، انٹرنیٹ کے ذریعے، مائنر اتنے لمبے وقت تک کیلئے کمپیوٹنگ کرتے رہنے پر مجبور رکھتا ہے کہ حسابی عمل ختم ہونے کا وقت آنے پر چند ایک زیادہ بلاک ہی باہر آسکیں گے اور مائنر کے پاس اتنا وقت ہی نہیں بچے گا کہ وہ فیس کا مطالبہ کرنے کیلئے ٹرانزیکشن شامل کر سکے۔ تاہم، حملہ آور کیلئے STARTGAS کی ایک قدر جمع کرانا ضروری ہو گا جس سے ایگزیکیوشن کیلئے درکار حسابی مرحلوں کی تعداد محدود ہو جائے گی؛ لہٰذا مائنر کو پہلے ہی معلوم ہو جائے گا کہ کمپیوٹیشن (حسابی عمل) میں بہت زیادہ مرحلے ہوں گے۔

حملہ آور ایک معاہدہ دیکھتا ہے جس کا کوڈ send(A,contract.storage[A]); contract.storage[A] = 0 جیسا ہو گا، اور ایک ایسی ٹرانزیکشن بھیجتا ہے جس کی گیس صرف پہلا مرحلہ کرنے کیلئے کافی ہو لیکن دوسرے کیلئے نہ ہو (یعنی رقم ضرور نکلوائے لیکن اپنے بیلنس کو نیچے نہ جانے دے)۔ معاہدے کے مصنف کو ایسے حملہ آوروں سے بچاؤ کی طرف سے فکر مند ہونے کی کوئی ضرورت نہیں، کیونکہ اگر ایگزیکیوشن درمیان ہی میں کہیں رُک گئی تو اس دوران کی گئی ساری تبدیلیاں واپس پلٹ جائیں گی۔

فرض کیجئے کہ ایک مالیاتی معاہدہ ایسا ہے جو 9 مختلف ملکیتی ڈیٹا (پروپرائٹری ڈیٹا) فیڈز کا وسطانیہ (median) لیتا ہے تاکہ خدشات کم کئے جا سکیں۔ حملہ آور ان میں سے ایک ڈیٹا فیڈ پر قابض ہو جاتا ہے، جسے "ویری ایبل ایڈریس کال" نظام کے ذریعے قابلِ ترمیم بنایا گیا ہے۔ اس نظام کی وضاحت DAOs والے سیکشن میں کی جا چکی ہے۔ اب وہ اس ڈیٹا فیڈ کو لامتناہی لوپ چلانے کیلئے تبدیل کر دیتا ہے، اور اس طرح کوشش کرتا ہے کہ فنڈز کا مطالبہ کرنے والی کسی بھی کوشش کے نتیجے میں اس مالیاتی معاہدے کی گیس ختم ہو جائے۔ تاہم، یہ مالیاتی معاہدہ متعلقہ پیغام کے ساتھ گیس کی حد مقرر کر سکتا ہے تاکہ اس مسئلے سے بچ سکے۔

ٹیورنگ مکملیت کا متبادل "ٹیورنگ غیر مکملیت" (Turing-incompleteness) ہے، جس میں JUMP اور JUMPI موجود نہیں ہوتے اور کال اسٹیک (call stack) میں کسی بھی وقت ہر کنٹریکٹ کی صرف ایک نقل ہی کے موجود ہونے کی اجازت ہوتی۔ اس نظام کے ساتھ، فیس کا نظام واضح ہوتا ہے اور ہمارے حل کے اطراف بے یقینی کی کیفیات بھی شاید ضروری نہ رہیں، کیونکہ معاہدے پر عملدرآمد (ایگزیکیوشن) کی لاگت کی بالائی حد اس کی جسامت کی پابند ہو گی۔ مزید یہ کہ ٹیورنگ غیر مکملیت بھی کوئی بہت بڑی خامی ہیں؛ معاہدے کی وہ تمام مثالیں جو ہم نے اندرونی طور پر سمجھی ہیں، ان سب میں سے اب تک

صرف ایک ہی کو لوپ کی ضرورت ہے، اور یہ لوپ بھی کسی کوڈ کے یک سطری حصے کو 26 تکراروں کے بعد ختم کیا جا سکتا ہے۔ ٹیورنگ مکملیت کے سنجیدہ نتائج و عواقب، اور محدود فائدے کے پیشِ نظر، کیوں نہ سادہ طور پر ایک ''ٹیورنگ نامکمل'' زبان استعمال کر لی جائے۔ بہر حال، حقیقت میں ٹیورنگ غیر مکملیت اس مسئلے کے صاف ستھرے حل سے بہت دُور ہے۔ ایسا کیوں ہے؟ یہ سمجھنے کیلئے درج ذیل کنڑیکٹس دیکھئے:

C0: call(C1); call(C1);

C1: call(C2); call(C2);

C2: call(C3); call(C3);

...

C49: call(C50); call(C50);

C50: پروگرام کا ایک مرحلہ چلاؤ اور اسٹوریج میں تبدیلی ریکارڈ کرو، اب A کو ایک ٹرانزیکشن بھیجئے۔ پس، 51 ٹرانزیکشنز میں، ہمارے پاس ایسا معاہدہ ہو گا جو 2^{50} حسابی مراحل کا متقاضی ہو گا۔ مائنرز ایسے منطقی بموں کو وقت سے پہلے ہی دریافت کرنے کی کوشش کر سکتے ہیں؛ ہر کنڑیکٹ کے ساتھ ایک قدر (ویلیو) قائم رکھتے ہوئے جو یہ بتائے کہ وہ زیادہ سے زیادہ کتنے حسابی مراحل کی متحمل ہو سکتی، جبکہ اس کا حساب لگانے کیلئے وہ دوسرے معاہدوں کو بار بار کال کرتا رہے، لیکن اس کیلئے مائنرز کو ایسے معاہدوں سے دور رہنا ہو گا جو دوسرے معاہدے تخلیق کرتے ہیں (کیونکہ 50 معاہدوں کی تخلیق اور ایگزیکیوشن بڑی

آسانی سے صرف ایک ہی معاہدے میں سموئی جاسکتی ہے)۔ایک اور مشکل نکتہ یہ ہے کہ کسی میسج کی ایڈریس فیلڈ متغیر (ویری ایبل) ہوتی ہے،اس لئے بالعموم یہ شاید یہ بتانا تک ممکن نہ ہو کہ دیا گیا کوئی معاہدہ،وقت سے پہلے، کونسے دوسرے معاہدوں کو کال کرے گا۔ لہٰذا، بطورِ مجموعی، ہمارے پاس ایک حیرت انگیز نتیجہ ہے: ٹیورنگ مکملیت کی انتظام کاری حیرت انگیز حد تک آسان ہے، جبکہ ٹیورنگ مکملیت کی قلت کو سنبھالنا، یکساں حیرت انگیز طور پر، انتہائی مشکل ہے، جب تک کہ بالکل ایک جیسے کنٹرولز موجود نہ ہوں۔ لیکن اس معاملے میں کیوں نہ پروٹوکول ہی کو "ٹیورنگ مکمل" بنالیا جائے؟

کرنسی اور اجراء

ایتھریم نیٹ ورک کی اپنی اندرونی (بلٹ اِن) کرنسی ہے: ایتھر، جو دوہرا مقصد رکھتی ہے۔ یہ کئی اقسام کے ڈیجیٹل اثاثوں کے مابین تبادلے کو مؤثر بنانے کیلئے بنیادی "لیکویڈیٹی لیئر" (liquidity layer) فراہم کرتی ہے اور، اس سے بھی زیادہ اہم، ٹرانزیکشن فیس ادا کرنے کیلئے ایک نظام فراہم کرتی ہے۔ مستقبل میں مزید بحث سے بچنے اور سہولت کی غرض سے (بِٹ کوائن میں mBTC/uBTC/satoshi کی حالیہ بحث ملاحظہ کیجئے)، ہر مالیت کو پہلے ہی لیبل (pre-labeled) کر دیا جائے گا:

- 1: wei
- 10^12: szabo
- 10^15: finney
- 10^18: ether

اسے ''ڈالر''اور ''سینٹ'' یا''BTC''اور''satoshi''کا پھیلا ہوا ورژن سمجھنا چاہئے۔ مستقبل قریب میں، ہمیں امید ہے کہ ''ether''کو عام ٹرانزیکشنز کیلئے استعمال کیا جائے گا، ''finney''کو مائیکرو ٹرانزیکشنز کیلئے،اور ''szabo''اور ''wei''کو فیس اور پروٹوکول کے نفاذ سے متعلق تکنیکی مباحث میں استعمال کیا جائے گا۔

اجرائی ماڈل(issuance model)کچھ ایسا ہو گا:

ایتھر کو کرنسی کے طور پر فروخت کیلئے 1337 تا 2000 ایتھر فی بِٹ کوائن کی شرح سے جاری کیا جائے گا، اس نظام کا مقصد ایتھریم آرگنائزیشن کو ڈیویلپمنٹ کے اخراجات پورے کرنے کے قابل بنانا ہے جبکہ یہی حکمتِ عملی دوسرے کئی کرپٹو گرافک پلیٹ فارمز پر بڑی کامیابی سے استعمال کی جاچکی ہے۔ اوّلین خریداروں کو زیادہ رعایتیں دے کر فائدہ پہنچایا جائے گا۔ اس فروخت سے حاصل ہونے والی بِٹ کوائنز صرف اور صرف ڈیویلپرز، تحقیق کاروں اور کرپٹو کرنسی کے ماحول میں تنخواہوں اور معاوضوں کی ادائیگی ہی میں استعمال کی جائیں گی۔

فروخت سے حاصل شدہ مجموعی رقم کا 0.099x ان اوّلین افراد کو دیا جائے گا جنہوں نے بٹ کوائن فنڈنگ سے پہلے ڈیویلپمنٹ میں حصہ لیا یا پھر فنڈنگ کی یقین دہانی ممکن بنائی؛ اور مزید 0.099x طویل مدتی تحقیقی منصوبوں کیلئے وقف کیا جائے گا۔

فروخت سے حاصل شدہ مجموعی رقم کا 0.26x سالانہ بنیادوں پر، اس مقام کے بعد، مائنرز کیلئے مختص کیا جائے گا۔

اجرائی تقسیم(Issuance Breakdown)

مسلسل خطی رسد میں نشوونما کا ماڈل اس خدشے کو کم کرتا ہے جسے بعض لوگ بِٹ کوائن میں حد سے زیادہ ارتکازِ دولت کے طور پر دیکھتے ہیں، اور حال اور مستقبل کے زمانوں میں رہنے

والے افراد کو کرنسی یونٹ حاصل کرنے کیلئے منصفانہ مواقع فراہم کرے گا۔ جبکہ، ساتھ ہی ساتھ، ایتھر کی قدر میں کمی کی حوصلہ شکنی بھی کرے گا کیونکہ ''رسدی نمو کی شرح'' (سپلائی گروتھ ریٹ) بطور فیصد، لمبے عرصے تک صفر کے قریب ہی رہے گی۔ ہم نے یہ نظریہ بھی تشکیل دیا ہے کہ سکے (کوائنز) چونکہ ہمیشہ ہی وقت گزرنے پر لاپرواہی یا موت وغیرہ کے باعث گم ہوتے رہتے ہیں، اس لئے کوائن کے خسارے (کمی) کو سالانہ مجموعی سپلائی کے فیصد کے طور پر ماڈل کیا جاسکتا ہے۔ یعنی زیرِ گردش کرنسی کی فراہمی، درحقیقت، ایک ایسی قدر پر قیام پذیر ہو جائے گی جو سالانہ اجراء کو کمی کی شرح سے تقسیم کرکے حاصل ہو گی۔ (مثلاً 1 فیصد خسارے کی شرح پر، جب سپلائی 26X پر پہنچ جائے گی تو ہر سال 0.26X کرنسی کی مائننگ کی جارہی ہو گی جبکہ ہر سال 0.26X کرنسی ہی کم ہو رہی ہو گی؛ اس طرح توازن قائم رہے گا۔)

گروپ	لانچ کے وقت	1 سال بعد	5 سال بعد
کرنسی یونٹ	1.198X	1.458X	2.498X
خریدار	83.5%	68.6%	40.0%
اوّلین حصہ لینے والوں میں تقسیم	8.26%	6.79%	3.96%
طویل مدتی وقف	8.26%	6.79%	3.96%
مائنرز	0%	17.8%	52.0%

کرنسی کے خطی اجراء کے باوجود، بالکل بِٹ کوائن کی طرح، طویل مدتی بنیاد پر رسدی نمو کی شرح صفر کے قریب پہنچ جائے گی۔

مائننگ میں مرکزیت

بِٹ کوائن کا مائننگ الگورتھم کچھ اس طرح کام کرتا ہے کہ یہ مائنرز سے معمولی ترمیم شدہ بلاک ہیڈر والے SHA256 کا حساب لاکھوں مرتبہ، بار بار لگواتا ہے، یہاں تک کہ بالآخر کوئی ایک نوڈ ایسا ورژن لوٹاتی ہے جس کا ہیش (hash) ہدف سے کم ہوتا ہے (جو اس وقت تقریباً 2^{190} ہے)۔ تاہم، یہ مائننگ الگورتھم دو طرح کی مرکزیت (سینٹرلائزیشن) کا شکار ہو سکتا ہے۔ اوّل، مائننگ کے ماحول میں ''ایپلی کیشن اسپیسفک انٹیگریٹڈ سرکٹس'' (ASICs) کی اجارہ داری قائم ہو چکی ہے، جو ایسی کمپیوٹر چپس ہیں جنہیں بطورِ خاص اسی مقصد کیلئے بنایا گیا ہے اور اسی لئے وہ بِٹ کوائن پر کوئی مخصوص کام انجام دینے میں (عام کمپیوٹر چپس کے مقابلے میں) ہزاروں گنا زیادہ کارکردگی کی حامل ہیں۔ اس کا مطلب یہ ہوا کہ بِٹ کوائن مائننگ اب بہت زیادہ عدم مرکزیت اور مساوات کی علمبردار نہیں رہی، کیونکہ اب اس میں مؤثر شراکت کیلئے لاکھوں ڈالر سرمائے کی ضرورت ہوتی ہے۔ دوم یہ کہ بیشتر مائنرز درحقیقت مقامی (انفرادی) طور پر بلاک کی توثیق (block validation) کا کام نہیں کرتے؛ بلکہ بلاک ہیڈرز کی فراہمی کیلئے وہ مرکزی ''مائننگ پُول'' پر انحصار کرتے ہیں۔ غور کیا جائے تو یہ مسئلہ واقعتاً انتہائی سنگین ہے: اس وقت جبکہ یہ تحریر (قرطاسِ ابیض) لکھی جا رہی ہے، چوٹی کے دو مائننگ پولز بالراست طور پر بِٹ کوائن نیٹ ورک کی تقریباً 50 فیصد پروسیسنگ پاور کنٹرول کر رہے ہیں، تاہم اس کا ازالہ اس حقیقت سے ہو جاتا ہے کہ مائنرز

دوسرے مائننگ پُولز کی طرف متوجہ ہو سکتے ہیں اگر کوئی پول یا اتحاد (coalition) 51 فیصد حملے کی کوشش کرے۔

ایتھریم کا حالیہ مقصد مائننگ الگورتھم کو اس بنیاد پر استعمال کرنا ہے کہ اٹکل سے ایک منفرد ہیش فنکشن، ہر 1,000 نونسز (nonces) کیلئے بنایا جائے، جبکہ مناسب حد تک وسیع الاقسام حسابات استعمال کرتے ہوئے خصوصی ہارڈویئر کو حاصل ہونے والا ختم کیا جائے۔ یہ حکمتِ عملی یقیناً مرکزیت کو ہونے والے فوائد کو مکمل طور پر ختم تو نہیں کر سکے گی لیکن اسے ایسا کرنے کی ضرورت بھی نہیں۔ دھیان رہے کہ ہر انفرادی صارف، اپنے نجی لیپ ٹاپ یا ڈیسک ٹاپ کمپیوٹر پر، مائننگ کی ایک مخصوص مقدار تقریباً مفت میں انجام دے سکتا ہے؛ اسے صرف بجلی کا خرچ اُٹھانا پڑتا ہے، لیکن 100 سی پی یو (کمپیوٹر کی ساری حسابی صلاحیت یا پروسیسنگ پاور) استعمال ہو جانے کے بعد اسے مزید مائننگ کے تقاضے پورے کرنے کیلئے بجلی کے ساتھ ساتھ (اضافی) ہارڈویئر کا خرچ بھی اُٹھانا پڑتا ہے۔ ASIC مائننگ کمپنیوں کو پہلے ہیش کا آغاز ہوتے ہی بجلی اور ہارڈویئر کا خرچہ (مستقل بنیادوں پر) برداشت کرنا پڑتا ہے۔ لہٰذا، اگر مرکزیت کا مفاد اس تناسب، (E + H) / E، سے کم رہے، تو ایسی صورت میں بھی ASICs کی اجارہ داری قائم ہو جانے کے باوجود بھی عام مائنرز کیلئے گنجائش رہے گی۔

مزید برآں، ہمارا ارادہ اس طرح سے مائننگ الگورتھم بنانے کا ہے کہ مائننگ کیلئے پوری بلاک چین تک رسائی کی ضرورت رہے، تاکہ مائنرز مجبور ہوں کہ وہ پوری بلاک چین کو محفوظ کریں اور کم از کم اس قابل تو ہوں کہ ہر ٹرانزیکشن کی تصدیق کر سکیں۔ اس سے مرکزی مائننگ پُولز کی ضرورت ختم ہو جائے گی؛ تاہم اس صورت میں بھی مائننگ پُولز اپنا جائز کردار ادا کرتے ہوئے، انعام کی تقسیم میں جزافیت (randomness) کو ہموار رکھنے کا کام کر سکتے ہیں۔ یہ تفاعل (فنکشن) مساوی خوبی کے ساتھ P2P پول کے ذریعے پورا کیا جا سکتا ہے کہ جہاں

کوئی مرکزی کنٹرول نہ ہو۔ یہ اضافی طور پر مرکزیت کے خلاف لڑنے میں بھی مدد دیتا ہے، اس طرح کہ نیٹ ورک میں مکمل نوڈز کی تعداد بڑھا دیتا ہے تاکہ نیٹ ورک معقول حد تک عدم مرکزیت کا حامل رہے، چاہے بیشتر عام صارفین ہلکے کلائنٹس ہی کو کیوں نہ ترجیح دے رہے ہوں۔

پیمانے میں وسعت پذیری (Scalability)

ایتھریم کے بارے میں ایک عام تشویش اس کے پیمانے میں وسعت پذیری ہے۔ بِٹ کوائن کی طرح ایتھریم بھی اسی خامی کا شکار ہے کہ ہر ٹرانزیکشن کو نیٹ ورک کی ہر نوڈ سے پروسیسنگ ہونا ضروری ہوتا ہے۔ بِٹ کوائن میں بلاک چین کا موجودہ سائز 20 گیگا بائٹس پر ہے، جس میں ہر ایک گھنٹے کے دوران 1 میگا بائٹ کا اضافہ ہو رہا ہے۔ اگر بِٹ کوائن نیٹ ورک کو "ویزا" (کریڈٹ کارڈ سروس) کی 2,000 ٹرانزیکشنز ہر ایک سیکنڈ میں پروسیس کرنا پڑیں، تو اس میں ہر تین سیکنڈ کے دوران 1 میگا بائٹ کا اضافہ ہونے لگے گا (یعنی 1 گیگا بائٹ فی گھنٹہ، اور 8 ٹیرا بائٹس سالانہ)۔ ایتھریم بھی ممکنہ طور پر اسی طرح کے افزائشی نمونے (growth pattern) کا شکار بن سکتا ہے۔ یہ متوقع صورتِ حال اس حقیقت کے باعث اور بھی سنگین ہو سکتی ہے کہ، ایتھریم بلاک چین کی بنیاد پر متعدد ایپلی کیشنز ہوں گی۔ یہ کیفیت بِٹ کوائن سے کہیں مختلف ہو گی کیونکہ وہ صرف کرنسی ہی کیلئے ہے۔ البتہ، اس پریشانی کا ازالہ اس حقیقت سے ہو جاتا ہے کہ ایتھریم کی مکمل نوڈز کو پوری بلاک چین ہسٹری کے بجائے صرف "اسٹیٹ" محفوظ کرنے کی ضرورت ہوتی ہے۔

اتنے بڑے بلاک چین سائز کا ایک اہم مسئلہ مرکزیت قائم ہو جانے کا خدشہ ہے۔ اگر بلاک چین کا سائز بڑھتے بڑھتے (مثلاً) 100 ٹیرا بائٹس تک جا پہنچتا ہے، تو ممکنہ منظر نامہ یہ ہو گا کہ

بڑے تجارتی وکاروباری اداروں کی ایک بہت ہی قلیل تعداد مکمل نوڈز (full nodes) چلارہی ہوگی، جبکہ معمول کے صارفین ہلکی SPV نوڈز ہی استعمال کررہے ہوں گے۔ ایسی صورت میں ایک اور اہم خدشہ یہ بھی ہے کہ مکمل نوڈز آپس میں اتحاد کرتے ہوئے کسی خاص منافع بخش انداز میں دھوکہ دہی پر متفق ہوسکتی ہیں (مثلاً یہ کہ بلاک سے متعلق انعامات تبدیل کرتے ہوئے خود ہی کوبِٹ کوائن سے نوازنا شروع کردیں)۔ ایسا کوئی طریقہ نہیں کہ جس کے ذریعے ہلکی نوڈز اس بات کا فوری سراغ لگا سکیں۔ بجا طور پر کم از کم ایک دیانتدار مکمل نوڈ، ممکنہ طور پر، ضرور موجود ہوگی اور چند گھنٹوں کے بعد Reddit یا ایسے کسی چینل کے ذریعے اس فراڈ کی اطلاع بھی نشر ہو جائے گی، لیکن تب تک بہت دیر ہو چکی ہوگی: یہ عام صارفین پر منحصر ہوگا کہ وہ کچھ مخصوص (بے ایمان) بلاکس کو بلیک لسٹ کروانے کی کوشش کریں۔ لیکن بہت وسیع پیمانے پر تعاون واشتراک اتنا ہی مشکل ہوگا کہ جتنا ایک کامیاب 51 فیصد حملہ کرنا ہوسکتا ہے۔ سرِدست بِٹ کوائن میں بھی یہی مسئلہ ہے، لیکن بلاک چین کیلئے پیٹر ٹاڈ کی تجویز کردہ ترامیم بھی موجود ہیں جو اس مسئلے سے نجات دلائیں گی۔

قلیل مدتی بنیاد پر اس مسئلے سے نمٹنے کیلئے کیلئے ایتھریم دو اضافی تدابیر استعمال کرے گا۔ پہلی: بلاک چین پر مبنی مائننگ الگورتھم کی بدولت، کم از کم ہر مائنر کو مکمل نوڈ ہونے پر مجبور کیا جائے گا؛ اور اس طرح مکمل نوڈز کیلئے کم سے کم ہونے کی ایک حد مقرر کی جائے گی۔ دوسری اور زیادہ اہم یہ ہے کہ ہم بلاک چین کے درمیان میں، ہر ٹرانزیکشن کے پروسیس ہو جانے کے بعد، ایک ''اسٹیٹ ٹری رُوٹ'' شامل کردیں گے۔ بلاک کی توثیق (validation) چاہے مرکزیت پر مبنی ہی کیوں نہ ہو جائے، لیکن جب تک دیانتدار توثیقی نوڈز موجود ہیں، تب تک ایک مرکزیت کا یہ مسئلہ ایک توثیقی پروٹوکول کے ذریعے قابو میں رکھا جاسکتا ہے۔ اگر کوئی مائنر ایک غیر درست (غلط) بلاک شائع کرتا ہے، تو وہ بلاک یا تو بری طرح سے فارمیٹ

کیا گیا ہو گا، یا پھر اس کی اسٹیٹ S[n] غلط ہو گی۔ توثیقی نوڈ انڈیکس i فراہم کرے گی، جس کے ساتھ "غیر درستگی کا ثبوت" بھی ہو گا اور جو "پیٹریشیا" ٹری نوڈز کے ذیلی سیٹ پر مشتمل ہو گا جسے APPLY(S[i-1],TX[i]) -> S[i] کو پروسیس کرنا ضروری ہو گا۔ نوڈز اس قابل ہوں گی کہ اِن نوڈز کو حسابی عمل کے جزو کے طور پر چلا سکیں، اور یہ دیکھ سکیں کہ ان سے حاصل شدہ S[i]، فراہم کردہ S[i] سے مماثلت نہیں رکھتا۔

ایک اور، زیادہ پیچیدہ حملے میں بدطینت مائنرز نامکمل بلاکس پبلش کر رہے ہوں گے، لہٰذا یہ پتا لگانے کیلئے پوری معلومات دستیاب ہی نہیں ہوں گی کہ آیا وہ بلاکس درست ہیں یا غلط۔ اس مسئلے کا حل ایک "چیلنج رسپونس" (challenge-response) پروٹوکول ہے: تصدیقی نوڈز "چیلنجز" جاری کریں گی جو ٹارگٹ ٹرانزیکشن انڈیسز (target transaction indices) کی شکل میں ہوں گے، اور ایک نوڈ وصول ہو جانے پر ہلکی نوڈ اس بلاک کو "ناقابلِ بھروسہ" ہی قرار دے گی، جب تک کہ کوئی اور نوڈ، چاہے وہ کوئی مائنر ہو یا کوئی دوسرا توثیق کار، پیٹریشیا نوڈز کا ذیلی سیٹ فراہم کرے جو اس کا ثبوتِ توثیق (proof of validity) ہو۔

سب کچھ ایک ساتھ: عدم مرکزیت پر مبنی ایپلی کیشنز

اوپر واضح کیا گیا "معاہدہ نظام" (کنٹریکٹ مکینزم) یہ سہولت دیتا ہے کہ کوئی بھی ایک بنیادی قسم کی "کمانڈ لائن ایپلی کیشن" تیار کر کے ورچوئل مشین پر چلائے جو بجائے خود پورے نیٹ ورک پر اتفاقِ رائے کے ذریعے رُوبہ عمل ہو گی، اور اسے اجازت دے گی کہ وہ دنیا میں کہیں سے بھی قابلِ رسائی اسٹیٹ میں بطور "ہارڈ ڈرائیو" ترمیم کر سکے۔ البتہ، بیشتر افراد کیلئے، کمانڈ لائن انٹرفیس والا نظام، جو ٹرانزیکشن بھیجتا ہے، اطمینان بخش حد تک صارف دوست نہیں

ہو گا؛ اور یوں عدم مرکزیت کو مرکزی دھارے کے ایک پُر کشش متبادل کا درجہ بھی حاصل نہیں ہو پائے گا۔ اس حوالے سے ایک مکمل ''غیر مرکزی ایپلی کیشن'' کو دونوں چیزوں پر مشتمل ہونا چاہئے: اوّل نچلی سطح کے ''بزنس لاجک'' اجزاء پر، خواہ وہ مکمل طور پر ایتھریم ہی پر، ایتھریم اور دوسرے نظاموں کا مجموعہ استعمال کرتے ہوئے لاگو کئے گئے ہوں (مثلاً ایک P2P میسجنگ لیئر، جسے فی الحال ایتھریم کلائنٹس پر رکھنے کا منصوبہ ہے) یا پھر مکمل طور پر دوسرے نظاموں کے ذریعے اطلاق پذیر کئے گئے ہوں؛ اور (دوم) اعلیٰ سطح کے گرافیکل یوزر انٹرفیس کے اجزاء پر۔ ایتھریم کلائنٹ کا ڈیزائن کسی ویب براؤزر ہی کی طرح کام کرے گا، لیکن اس میں ''eth'' جاوا اسکرپٹ اے پی آئی کی سپورٹ بھی شامل ہو گی، جو نہ صرف خصوصی نوعیت کے ویب پیجز دکھانے میں مدد کرے گا بلکہ (اسی کے ذریعے) کلائنٹ اس قابل بھی ہو گا کہ وہ ایتھریم بلاک چین کے ساتھ دو طرفہ عمل کر سکے۔ ''روایتی'' ویب کے نقطۂ نگاہ سے، یہ ویب پیجز مکمل طور پر ساکن (static) مواد ہوں گے، کیونکہ بلاک چین اور دوسرے عدم مرکزیت پر مبنی پروٹوکولز، صارف کی جانب سے شروع کی گئی درخواستوں کو سنبھالنے کی غرض سے مکمل طور پر کسی سرور کی جگہ پر خدمات انجام دے رہے ہوں گے۔ امید ہے کہ عدم مرکزیت پر مبنی پروٹوکولز، بالآخر، خود ہی کسی نہ کسی انداز میں ایتھریم سے استفادہ کرتے ہوئے، خود بھی ویب پیجز محفوظ کرنے میں استعمال ہو رہے ہوں گے۔

حرفِ آخر

ایتھریم پروٹوکول کو اصلاً کرپٹو کرنسی کے ایک جدید و بہتر نمونے کے طور پر سوچا گیا تھا، جو ایک اعلیٰ پائے کی عمومی پروگرامنگ لینگویج کے ذریعے ترقی یافتہ فیچرز جیسے کہ بلاک چین پر مبنی ثالث (escrow)، مالیاتی معاہدوں کیلئے (رقم) نکلوانے کی حدود، جوئے کی منڈیوں

جیسے اطلاقات کی فراہمی کر سکے۔ ایتھریم پروٹوکول کسی بھی اپلی کیشن کو براہِ راست ''سپورٹ'' نہیں کرے گا، بلکہ ٹیورنگ مکمل پروگرامنگ لینگویج موجود ہونے کا مطلب یہ ہے کہ، نظری طور پر، کسی بھی قسم کے من پسند معاہدے تخلیق کئے جا سکیں جو کسی بھی قسم کی ٹرانزیکشن یا اطلاق کیلئے ہوں۔ ایتھریم کا اس سے بھی دلچسپ پہلو یہ ہے کہ ایتھریم پروٹوکول، کرنسی سے کہیں بڑھ کر ہے۔ (جیسے کہ) عدم مرکزیت پر مبنی فائل اسٹوریج کے گرد پروٹوکولز اور عدم مرکزیت پر مبنی اپلی کیشنز، ڈی سینٹرلائزڈ (عدم مرکزیت پر مبنی) حسابی عمل اور پیش گوئی کی ڈی سینٹرلائزڈ مارکیٹس، اور درجنوں دوسرے تصورات یہ استعداد رکھتے ہیں کہ کمپیوٹیشنل انڈسٹری کی کارکردگی میں اضافہ کریں، اور دیگر P2P پروٹوکولز میں تیز رفتار ترقی کیلئے پہلی بار ایک ''معاشی پرت'' (economic layer) کا اضافہ کریں۔ آخر میں، ایسی اپلی کیشنز کی بھی ایک بڑی تعداد ہے جس کا دولت سے کوئی تعلق نہیں۔

ایک ''آربٹریری اسٹیٹ ٹرانزیشن فنکشن'' (arbitrary state transition function) کا تصور، جبکہ اسے ایتھریم پروٹوکول کے ذریعے لاگو کیا جائے، منفرد استعداد والا ایک پلیٹ فارم مہیا کرتا ہے؛ جو ڈیٹا اسٹوریج، جوئے یا مالیات میں خصوصی اطلاقات کیلئے بند سرے والا (closed-ended)، ایک مقصد کا حامل پروٹوکول نہیں، بلکہ (اس کے برعکس) ایتھریم ایک کھلے سرے والا (open-ended) ڈیزائن ہے؛ اور ہمیں یقین ہے کہ یہ آنے والے برسوں میں مالیاتی اور غیر مالیاتی، دونوں طرح کے پروٹوکولز کی بڑی تعداد کیلئے ایک ''بنیادی پرت'' کی حیثیت سے خدمت انجام دینے کے حوالے سے انتہائی موزوں ہے۔

Notes and Further Reading (Not to be translated)

Notes:

1. A sophisticated reader may notice that in fact a Bitcoin address is the hash of the elliptic curve public key, and not the public key itself. However, it is in fact perfectly legitimate cryptographic terminology to refer to the pubkey hash as a public key itself. This is because Bitcoin's cryptography can be considered to be a custom digital signature algorithm, where the public key consists of the hash of the ECC pubkey, the signature consists of the ECC pubkey concatenated with the ECC signature, and the verification algorithm involves checking the ECC pubkey in the signature against the ECC pubkey hash provided as a public key and then

verifying the ECC signature against the ECC pubkey.

2. Technically, the median of the 11 previous blocks.

3. Internally, 2 and "CHARLIE" are both numbers, with the latter being in big-endian base 256 representation. Numbers can be at least 0 and at most 2^256-1.

Further Reading

1. Intrinsic value: https://tinyurl.com/BitcoinMag-IntrinsicValue

2. Smart property:

https://en.bitcoin.it/wiki/Smart_Property

3. Smart contracts:

https://en.bitcoin.it/wiki/Contracts

4. B-money: http://www.weidai.com/bmoney.txt

5. Reusable proofs of work:

http://www.finney.org/~hal/rpow/

6. Secure property titles with owner authority:

http://szabo.best.vwh.net/securetitle.html

7. Bitcoin whitepaper:
http://bitcoin.org/bitcoin.pdf
8. Namecoin: https://namecoin.org/
9. Zooko's triangle:
http://en.wikipedia.org/wiki/Zooko's_triangle
10. Colored coins whitepaper:
https://tinyurl.com/coloredcoin-whitepaper
11. Mastercoin whitepaper:
https://github.com/mastercoin-MSC/spec
12. Decentralized autonomous corporations,
Bitcoin Magazine:
https://tinyurl.com/Bootstrapping-DACs
13. Simplified payment
verification:https://en.bitcoin.it/wiki/Scalability#Si
mplifiedpaymentverification
14. Merkle trees:
http://en.wikipedia.org/wiki/Merkle_tree
15. Patricia trees:
http://en.wikipedia.org/wiki/Patricia_tree

16. GHOST:
http://www.cs.huji.ac.il/~avivz/pubs/13/btc_scalability_full.pdf
17. StorJ and Autonomous Agents, Jeff Garzik:
https://tinyurl.com/storj-agents
18. Mike Hearn on Smart Property at Turing Festival:
http://www.youtube.com/watch?v=Pu4PAMFPo5Y
19. Ethereum RLP:
https://github.com/ethereum/wiki/wiki/%5BEnglish%5D-RLP
20. Ethereum Merkle Patricia trees:
https://github.com/ethereum/wiki/wiki/%5BEnglish%5D-Patricia-Tree
21. Peter Todd on Merkle sum trees:http://sourceforge.net/p/bitcoin/mailman/message/31709140/

کنسنسیز الگورتھمز(Consensus Algorithms)

جب ہم بلاچین کے بارے میں بات کرتے ہیں تو ہمارے دماغ میں آنے والی پہلی چیز نیٹ ورک کی سیکیورٹی ہوتی ہے جسے ہم بلاک چین کے کنسنسیز(Consensus)(اتفاق رائے)الگورتھم سے حاصل کرتے ہیں۔ جیسے کہ آپ جان گئے ہیں کہ ہم پبلک لیجرز کی تمام ٹرانزیکشنز کو نیٹ ورک میں مطابقت پذیر رکھتے ہیں تاکہ یہ امر یقینی بنائیں کہ لیجرز صرف اُس وقت اپ ڈیٹ ہوگا جب موزوں شرکاء کسی ٹرانزیکشن کی منظوری دیں گے۔اور جب لیجرز کو اپ ڈیٹ کیا جائے تو وہ اسی ترتیب میں اسی ٹرانزیکشنز کے ساتھ اپ ڈیٹ ہوگا۔
یہاں ہم مختلف کنسنسیسز الگورتھم کے بارے میں پڑھیں گے اور جانیں گے کہ وہ کیسے کام کرتے ہیں۔

بے زنٹاین فالٹ ٹولیرانس(Byzantine fault tolerance):

"تصور کریں کہ بازنطینی فوج کے کئی دستے دشمن کے شہر کے باہر گھات لگائے بیٹھیں ہیں اور ہر دستے کا اپنا جنرل ہے۔ تمام جنرلز ایک دوسرے سے بات صرف پیغام رساں کے ذریعے کر سکتے ہیں۔ دشمن پر کڑی نظر رکھنے اور مشاہدے کے بعد انہیں ایک مساوی منصوبے کی کاروائی

پر فیصلہ لینا ہے کہ کیالائحہ عمل اختیار کیا جائے۔ ہو سکتا ہے کہ کچھ جنرلز غدار ہوں اور وفادار جنریلوں کو ایک متفقہ فیصلے پر پہنچنے سے روک رہے ہوں۔ اب تمام جنرلز کو شہر پر حملہ کرنے کا فیصلہ لینا ہے لیکن انہیں حملہ کرنے کے لئے ان کی فوج کی ایک بڑی تعداد کی ضرورت ہے۔ جنریلوں کو ایک الگورتھم کی ضروری ہے جو اس بات کو یقینی بنائے کہ

۱۔ تمام وفادار جنرلز ایک متفقہ لائحہ عمل پر فیصلہ کر لیں۔

۲۔ چند ایک غداروں کی وجہ سے وفادار قائدین کہیں غلط منصوبہ کو اختیار نہ کر لیں۔

وفادار قائدین صرف وہی کریں گے جو الگورتھم انہیں بتائے گا کہ کیا کرنا چاہئیے اور غدار جو مرضی چاہے کرتے رہیں۔ الگورتھم کی یہ ذمہ داری بنتی ہے کہ وہ اس بات کی ضمانت دے کہ ناماسوا غدار کے کاموں کے، وفادار قائدین نہ صرف ایک معاہدے تک پہنچنیں بلکہ مناسب منصوبے پر بھی متفق ہو جائیں۔"

نیٹ ورکز پر حملوں اور غلط سافٹ ویئر کا رجحان بڑھ رہا ہے جس کے نتیجے میں غلط نوڈس بن سکتے ہیں جو کہ غلط رویے کا اظہار کر سکتے ہیں۔ اس کی روک تھام کے لئے بے زنٹاین فالٹ ٹولیرنس الگورتھم بہت اہم کردار ادا کرتا ہے۔ بے زنٹاین کے جنریلوں کے اس مسئلہ کے بہت سے حل ہیں جن میں سے مندرجہ ذیل قابل ذکر ہیں۔

پریکٹیکل بے زنٹاین فالٹ ٹولیرنس(Practical Byzantine Fault Tolerance - PBFT):

1999 میں میگول کاسٹرو(Miguel Castro) اور باربرا لسکوف(Barbara Liskov) نے پریکٹیکل بے زنٹاین فالٹ ٹولیرنس (پی بی ایف ٹی) الگورتھم متعارف کرایا۔ اسے آپ آسان لفظوں میں سمجھنے کیلئے عملی طور پر بیزنٹن غلطی کو برداشت کرنے والا

الگورتھم کہہ سکتے ہیں۔ اس الگورتھم نے بے زنٹاین سٹیٹ مشین کی نقل کرنے میں اعلی کارکردگی کا مظاہرہ کیااور ساتھ ہی ایک سیکنڈ میں ہزاروں درخواستوں کو پرسیس کرتا تھا۔ پی بی ایف ٹی صحیح معنوں میں بے زنٹاین فالٹ ٹولیرنس کا حل دیتا ہے۔

اس میں ہر نوڈ اپنی اندرونی اسٹورتیج برقرار رکھتا ہے۔ جب نیا پیغام نوڈ وصول ہوتا ہے تو وہ پیغام دوسرے نوڈز پر بھیجتا ہے۔ دوسرے نوڈز آنے والے پیغام کی جانچ کرتے ہیں اور درست ہونے پر اس پر دستخط کر کے تصدیق کرتے ہیں۔ جیسے ہی ایک جیسے جوابات اچھی تعداد میں وصول ہوتے ہیں تو یہ متفقہ طور پر مانا جاتا ہے کہ پیغام ایک درست ٹرانزیکشن ہے۔

پی بی ایف ٹی کے بعد، اس کی مضبوطی اور کارکردگی کو اور بہتر بنانے کے لئے بہت سے بی ایف ٹی پروٹوکول متعارف کروائے گئے۔

آئی بی ایم کی ٹیکنالوجی ہائپر لیجر (Hyperledger) کنسنسیز اور ٹینڈرمنٹ کور (TendermintCore) کنسنسیز، دونوں پی بی ایف ٹی کنسنشیز الگورتھم کی مثالیں ہیں۔

پروف آف ورک (Proof of Work):

پروف آف ورک سب سے زیادہ معروف اور عمومی طور پر استعمال ہونے والے کونسنشیز الگورتھمز میں سے ایک ہے اور کرپٹو کرنسی کی دنیا کی سب سے مضبوط کرنسی بٹ کوائن میں استعمال ہو رہا ہے۔ پی بی ایف ٹی کے برعکس، اتفاق رائے تک پہنچے کے لئے اسے نیٹ ورک پر موجود ہر نوڈز سے پیغام نہیں چاہئے ہوتا۔ مگر ہر ایک فرد اتفاق رائے تک پہنچنے کے نتائج جمع کرواسکتا ہے۔

انفرادی طور پر مائینز اپنے بلاک کے ہیڈر کا ہیش نکالتا ہے اور چیک کرتا ہے کہ نتیجہ صحیح ہے کہ نہیں۔ اگر غلط ہے تو مائینز اس میں ردوبدل کر کے پھر سے صحیح نتیجہ نکالنے کی کوشش کرتا ہے ۔جو پہلے اس معمہ کو حل کر لیتا ہے وہی لاٹری جیت جاتا ہے۔ اسے محنت کے انعام کے طور پر 12.5 نئے بٹ کوائنز ملتے ہیں اور ساتھ تھوڑی سی ٹرانزیکشن فیس وصول کرتا ہے۔

اگرچہ پروف آف ورک الگورتھم اپنے آپ میں ایک شاہکار ہے مگر بے مثال نہیں۔ اس پر عام تنقید یہ کی جاتی ہے کہ یہ کمپیوٹنگ توانائی کی بہت زیادہ مقدار استعمال کرتا ہے اور ٹرانزیکشن کی تصدیق میں تقریبا 10 سے 60 منٹ تک لے لیتا ہے۔ اس کی مائیننگ زیادہ ان ممالک میں ہو رہی ہے جہاں بجلی سستی ہے۔ اس وجہ سے مائیننگ مرکزی ہو رہی ہے۔

پروف آف سٹیک (Proof of Stake):

پروف آف سٹیک کو عام طور پر پروف آف ورک کا متبادل سمجھا جاتا ہے۔ اس طرح کے اتفاق رائے الگورتھم میں، بجائے اس کے کہ آپ بلاک مائین کرنے کے لئے کمپیوٹر کے مہنگے آلات پر پیسے لگائیں، آپ وہی پیسے اس سسٹم میں رکھ کر سرمایہ کاری کر سکتے ہیں۔ اس نظام میں کوئی نیا کوائن نہیں بنایا جاتا بلکہ تمام کوائنز پہلے دن سے موجود ہوتے ہیں اور اس کے مالکان نے ایک بڑی رقم محفوظ کر رکھی ہوتی ہے۔ جیسے کہ ہمارے بینکوں میں بچت اکاونٹس ہوتے ہیں۔ مالکان کو صرف ٹرانزیکشن فیس کے ذریعے ہی ادائیگی کی جاتی ہے۔

اس نظام میں اگلے بلاک بنانے کے لئے کس کو منتخب کیا جائے گا یہ مالک کے محفوظ کردہ سکوں پر منحصر ہے۔ اگر ایک شخص کے پاس 300 سکے ہیں اور دوسرے کے پاس 100 سکے ہیں تو تین سو سکوں کے مالک کو منتخب ہونے کے امکان دوسرے شخص سے 3 گنا زیادہ ہیں۔ تاہم، اس کا مطلب یہ بھی ہے کہ امیر صارفین نیٹ ورک کو کنٹرول کر سکتے ہیں۔

بلاک بن جانے کے بعد اگلا مرحلہ اسے بلاک چین کے نیٹ ورک پر لانے کا ہے۔اس پر مختلف پروف آف سٹیک سسٹمز نے مختلف طریقے اختیار کیئے ہیں۔ مثلاً ئینڈرمنٹ کونسنسیز سسٹم پر نیٹ ورک کے ہر نوڈ کو بلاک پر دستخط کرنا پڑتا ہے جب تک کہ بلاک کو اکثریت ووٹ نہ مل جائیں۔اس کے برعکس دیگر نظاموں میں دستخط کرنے کے لئے ایک بے ترتیب گروپ کو منتخب کیا جاتا ہے۔

پیئر کوائن پہلا کرپٹو کرنسی تھی جس نے اس نظام کو نافذ کیا تھا۔ اس کے بعد بلیک کوائن (blackcoin) اور نکسٹ (NXT) کوائن آتے ہیں۔ ایتھریم فی الحال پروف آف ورک کے نظام پر چل رہا ہے لیکن اس سال پروف آف سٹیک پر منتقل ہونے کی منصوبہ بندی کر رہے ہیں۔

پروف آف ایکٹیوٹی(Proof of Activity):

جیسا کہ ہم جانتے ہیں کہ ضروت سے زیادہ کاغذی کرنسی نکالنے سے مہنگائی بہت بڑھ جاتی ہے ۔اس مسئلے سے بچنے کے لئے کرپٹو کرنسیز کی پیداوار پر حد متعین کر دی گئی ہے۔ بٹ کوائن کل 21 ملین پیدا کئے جائیں گے جس کا مطلب ہوا کہ ایک وقت ایسا آئے گا جب بٹ کوائن مائینرز کو نیا بلاک بنانے پر انعام نہیں ملے گا اور وہ صرف ٹرانزیکشن فیس وصول کریں گے۔

یہاں سکیورٹی کا یہ مسئلہ سامنے آتا ہے کہ چونکہ صارفین ذاتی مفاد کے لئے نیٹ ورک پر آتے ہیں تو جب بلاک انعام ختم ہو جائے گا تو شاید وہ نیٹ روک چھوڑ دیں جس سے نظام خراب ہونے کا خدشہ ہے ۔ لہٰذا پروف آف ایکٹیوٹی کو بٹ کوائن کے لئے ایک متبادل کونسنسیز الگوریتھم کے طور پر بنایا گیا تھا۔ پروف آف ایکٹیوٹی ایک ہائبرڈ نظام ہے جو پروف آف ورک اور پروف آف سٹیک دونوں کے ملاپ سے بنا ہے۔

اس نظام میں مائینگ کا طریقہِ کار روایتی پروف آف ورک جیسا ہی ہے جس میں مائینرز کرپٹو گرافک کا معمہ حل کرنے کی کوشش کرتے ہیں۔اس پہلے مرحلے کے مختلف طریقہ کار ہیں جس میں سے ایک یہ ہے کہ اس کے مائینڈ بلاکس میں ٹرانزیکشنل ریکاڈز نہیں ہوتے۔یہ صرف اس کا خاکہ ہوتا ہے۔لہذا جیتنے والا بلاک صرف ہیڈر اور انعام کے ایڈریس پر مشتمل ہوتا ہے۔

اس کے بعد یہ سسٹم پروف آف سٹیک پر چلا جاتا ہے۔ہیڈر میں موجود معلومات کی بنیاد پر نئے بلاک پر دستخط کرنے کے لئے ایک غیر مخصوص گروہ کا انتخاب کرتا ہے۔اب گروہ کے افراد کا انتخاب اس بات پر منحصر ہے کہ وہ کتنے زیادہ سکوں کے مالک ہیں۔جس کے پاس جتنے زیادہ سکے ہوں گے اس کو منتخب کیا جائے گا۔جیسے ہی تمام افراد اس پر دستخط کرتے ہیں بلاک کا سانچا اصل بلاک میں بدل جاتا ہے۔

اگر بلاک کو مکمل کرنے کے لئے جانچ کرنے والے افراد اس وقت موجود نہ ہوں تو نئے گروپ کا انتخاب کر لیا جاتا ہے۔یہ سلسلہ اس وقت تک چلتا رہتا ہے جب تک ایک بلاک قابل قبول دستخط نہ حاصل کر لے۔اس نظام میں ٹرانزیکشن فیس مائینز اور دستخط کرنے والوں کے درمیاں تقسیم ہو جاتی ہے۔

پروف آف ایکٹیوٹی پر بھی تنقید کے طور پر وہی الزامات لگے ہیں جو پروف آف ورک اور پروف آف سٹیک پر لگائے جاتے ہیں۔یہ نظام 51 فیصد حملوں کو روکنے میں موثر ثابت ہوا ہے۔کیونکہ اس میں یہ پیشن گوئی نہیں کی جاسکتی ہے کہ مستقبل میں دستخط کرنے والے کون ہوں گے۔

ڈیکرڈ(Decred)وہ واحد کوائن ہے جو پروف آف ایکٹیوٹی کی مختلف صورتوں کو استعمال کر رہا ہے۔

پروف آف برن(Proof of Burn):

اس نظام میں بھی بجائے اس کے کہ سارے پیسے کمپیوٹر کے مہنگے آلات پر لگا دیے جائیں، صارف اپنے سکے ایک ایسے پتے پر بھیجتے ہیں جہاں سے وہ کبھی واپس نہیں آ سکتے۔ایسی نامعلوم جگہ پر سکے بھیجنے کو جلانے سے تشبیہ دی گئی ہے۔ جیسے ہی صارف سکے بھیجتے ہیں تو اسے ایک غیر مخصوص انتخاب کے عمل کے مطابق زندگی بھر کے لئے اس نظام پر مائین کرنے کی اہلیت مل جاتی ہے۔

مائینرز اس نظام کی مقامی کرنسی کے ساتھ ساتھ دوسری کرپٹو کرنسیز کو بھی استعمال کر سکتے ہیں۔اور یہ طریقہ خاص طور پر اس بات پر منحصر ہے کہ اس نظام کو کن بنیادوں پر کھڑا کیا گیا ہے ۔ صارف جتنے زیادہ سکے جلائے گا اتنے ہی اس کے اگلا بلاک مائین کرنے کے لئے اختیارات ملنے کے امکانات بڑھ جائیں گے۔

گزرتے وقت کے ساتھ اس نظام پر صارف کا حصہ کم سے کم تر ہوتا جاتا ہے اس لئے اسے وقت کے ساتھ ساتھ اور سکے جلانے پڑھتے ہیں تاکہ لاٹری میں منتخب ہونے کے امکانات بڑھ جائیں۔

پروف آف بُرن ایک دلچسپ متبادل کونسنسیز الگوریتھم ہے۔ لیکن یہ بلاوجہ بہت سے وسائل کو ضائع کر دیتا ہے۔اس پر ایک اور تنقید یہ بھی کی جاتی ہے کہ اس میں مائینگ کی اہلیت صرف ان لوگوں کو حاصل ہو جائے گی جو زیادہ پیسہ جلانے کے لئے تیار ہیں۔

سلم کوائن (slimcoin) وہ اکلوتا کوائن ہے جو کنسنسیز کے لئے پروف آف بُرن کی ٹیکنیک کو استعمال کرتا ہے۔ سلم کوائن کو پیئر کوائن کی بنیادوں پر کھڑا کیا گیا ہے۔ یہ کوائن پروف آف ورک، پروف آف سٹیک اور پروف آف بُرن تینوں کے مجموعہ کو استعمال کرتا ہے لیکن یہ ابھی تک مکمل طور پر عمل میں نہیں آئی۔

پروف آف کاپیسٹی (Proof of Capacity):

جیسے کہ ابھی تک ہم جان چکے ہیں کہ زیادہ تر متبادل پروٹوکولز ایسے ہیں جن میں پیسے لگا کر کام کیا جا سکتا ہے۔ پروف آف کاپیسٹی پروٹوکول بھی کچھ مختلف نہیں ہے لیکن اس میں صارف ہارڈ ڈرائیو کی جگہ کو ادائیگی کے طور پر استعمال کر کے کام کر سکتے ہیں۔ جتنی زیادہ ہارڈ ڈرائیو میں جگہ ہو گی اتنے ہی آپ کے منتخب ہونے کا امکانات بڑھ جائیں گے تاکہ آپ گلا بلاک مائین کر سکیں اور انعام جیت سکیں۔

پروف آف کاپیسٹی میں مائینگ سے پہلے یہ الگورتھم پہت بڑے ڈیٹا سیٹس بناتا ہے جو کہ 'پلاٹ' کے نام سے جانے جاتے ہیں۔ انہیں صارف اپنی ہارڈ ڈرائیو پر محفوظ کر لیتے ہیں۔ آپ کے پاس جتنے زیادہ پلاٹس ہوں گے، آپ کے لئے اتنے زیادہ چین میں اگلے بلاک کو تلاش کرنے کے امکان زیادہ ہوں گے۔

اگر آپ ٹیرابائیٹس کی ہارڈ ڈرائیوز لے کر سرمایہ کاری کرتے ہیں تو اس کے ذریعے آپ ڈپلیکیڈ (Duplicate) بلاک بنانے اور سسٹم کو منتخب (fork) کرنے کے بہتر موقع خریدتے ہیں۔ لیکن اس نظام میں ابھی بھی چور ڈاکوؤں کے روک تھام کے لئے کوئی لائحہ عمل نہیں اختیار کیا گیا۔

پروف آف کاپیسٹی کی مزید دو اقسام ہیں:

1۔ پروف آف اسٹوریج (Proof of Storage)

2۔ پروف آف سپیس (Proof of Space)

برسٹ کوائن (Brustcoin) واحد کرپٹو کرنسی ہے جو پروف آف کاپیسٹی کو استعمال کر رہی ہے۔

پروف آف ایلیپسڈ ٹائم(Proof of Elapsed Time):

جیسے آپ 'گزرے ہوئے وقت کا ثبوت' بھی کہہ سکتے ہیں۔ انٹیل کمپنی (جو کمپیوٹر کے لئے چِپ سازی کا کام کرتی ہے) نے اپنا ایک متبادل کونسنشیز پروٹوکول بنایا ہے جس کا نام پروف آف آلیپسڈ ٹائم رکھا ہے۔ یہ نظام بالکل پروف آف ورک کی طرح کام کرتا ہے لیکن اس سے کم بجلی کا استعمال ہوتا ہے۔

اس کے علاوہ، صارفین کو کرپٹو گرافی کا کوئی معمہ حل نہیں کرنا پڑتا بلکہ اس کا الگور تھم ایک بااختیار عملدرآمد ماحول(Trusted Execution Environment - TEE) کا استعمال کرتا ہے، جیسا کہ ایس جی ایکس(SGX) یہ ماحول اس بات کو قابلِ عمل بناتا ہے کہ نئے بلاکس غیر مخصوص لاٹری کے طریقہِ کار سے وجود میں آئیں اور اس میں کسی قسم کا کام نہ کرنا پڑے۔

انٹیل کی یہ کاروائی بذریعہ TEE ضمانت شدہ انتظار کے وقت پر مبنی ہے۔ انٹیل کے مطابق یہ الگور تھم باآسانی ہزاروں نوڈز پر چلایا جا سکتا ہے اور یہ اُن انٹیل پروسیسرز پر مؤثر طریقے سے چلیں گے جو ایس جی ایکس کی حمایت کرتے ہیں۔

پروفنز آف سپیس اینڈ ٹائم(Proofs of Space and Time):

کنسنسیز کا یہ الگور تھم اپنی ذات میں منفرد ہے۔ یہ بھی پروف آف ایکٹیوٹی کی طرح ہائبریڈ سسٹم ہے۔ اس میں کنسنسیز کے الگور تھم زپروف آف سپیس اور پروف آف ٹائم دونوں کو اکٹھا استعمال کیا جاتا ہے۔ اس سے بننے والا بلاک چین "چیا" (Chia) کہلاتا ہے۔ بٹ ٹورنٹ کے خالق برام کوہن(Bram Cohen) نے اس نئے بلاک چین کو تخلیق کیا

ہے۔ برام کوہن نے چیانیٹ ورک کے نام سے نئی کمپنی شروع کی ہے جو کہ پروفنز آف سپیس اینڈ ٹائم کی بنیاد پر نئی کرپٹو کرنسی کا اجراء کرے گی۔ برام کوہن کا کہنا ہے کہ اس کا بنیادی مقصد بٹ کوائن کے مرکزی مسائل کو حل کرنا ہے۔

بٹ کوائن کا الگورتھم پروف آف ورک بجلی توانائی زیادہ خرچ کر دیتا ہے اور گزرتے وقت کے ساتھ انعامات جیتنے والے ان مائینرز کو بہت فائدہ پہنچا ہے جہاں بجلی کی قیمت انتہائی کم ہے۔ اگر تصویر کا دوسرا رخ دیکھیں تو تمام ٹرانزیکشنل ڈیٹا صرف چند ہاتھوں میں رہتا ہے۔ ان مسائل کے حل کے لئے چیا بہت مفید اور انتہائی سستا ہے اور یہ ہارڈ ڈرائیو کی غیر استعمال شدہ اسٹوریج کو استعمال کرتے ہوئے بلاک چین کی تصدیق کرتا ہے۔ یہ دو مرحلے میں بلاک کی توثیق کے طریقہ کار پر منحصر ہے۔

پروفنز آف سپیس اینڈ ٹائم کے نظام میں جب ایک نیا بلاک آتا ہے، تو اس کے بارے میں تمام نوڈز پر نشر کیا جاتا ہے اور کسان (Farmer) اس کے اوپر کام کرنے لگتے ہیں۔ دوسرے سسٹمز کے برعکس اس میں مائینرز نہیں کسان ہوتے ہیں۔ جب کسان کو ایک نیا بلاک ملتا ہے تو وہ اسے نیٹ ورک پر شائع کرتے ہے۔ پھر تمام کسان اپنے نیٹ ورک پر موجود بہترین پروف آف سپیس ڈھونڈتے ہیں۔ پھر تین بہترین پروف آف سپیس کے بارے میں پورے نیٹ ورک پر نشر کر دیتے ہیں اور ساتھ ہی پروف آف ٹائم کا سرور اس کے اوپر کام کرنا شروع کر دیتا ہے۔ جیسے ہی پروف آف ٹائم سرور اپنا کام مکمل کرتا ہے یہ تمام معلومات کو مکمل طور پر تصدیق شدہ بلاک کے طور پر نیٹ ورک پر شائع کر دیتا ہے۔

برام کوہن نے 2018 کے آخر میں اس نظام کو استعمال کرتے ہوئے ایک متبادل کرپٹو کرنسی نکالنے کا ارادہ ظاہر کیا ہے۔

1. https://www.coindesk.com/short-guide-blockchain-consensus-protocols/
2. https://blog.knoldus.com/2017/08/13/consensus-algorithms-in-blockchain/
3. https://mastanbtc.github.io/blockchainnotes/consensustypes/
4. https://techcrunch.com/2017/11/08/chia-network-cryptocurrency/
5. https://cointelegraph.com/news/bittorrent-creators-chia-could-fix-bitcoin-with-own-altcoin-by-late-2018
6. http://moneyinc.com/chia-network-scare-every-bitcoin-investor/
7. https://en.wikipedia.org/wiki/Proof-of-space
8. https://bitcoin.stackexchange.com/questions/4737/what-is-the-key-difference-between-the-proof-of-activity-proposal-and-proof-of-s

آئی۔ سی۔او(Initial Coin Offering)

کسی بھی کاروبار یا بزنس کے لئے سرمائے کی ضرورت ہوتی ہے۔ روایتی طور پر اس سرمائے کو حاصل کرنے کے بہت سے طریقے ہیں۔ مثلاً:-

1. آپ اپنی جمع پونجی لگا کر کاروبار کی شروعات کریں۔
2. اپنے اثاثہ جات، سونا، گاڑی وغیرہ بیچ کر کاروبار شروع کریں۔
3. دوستوں، رشتہ داروں، خاندان والوں اور جان پہچان والوں سے پیسے لیں۔
4. بینک سے سود پر قرضہ لیں جو شرعاً جائز ہی نہیں ہے۔
5. اپنی کمپنی کے شئیرز بیچ دیں، اب ہر شئیر خریدنے والا اتنے حصّے کا آپ کی کمپنی میں مالک ہے۔ اگر ٪50 یا اکثریت شئیرز ہولڈرز یہ فیصلہ کریں کہ آپ کمپنی سے نکال دیئے جائیں تو وہ بالکل ایسا کر سکتے ہیں۔ آپ کی تنخواہ تک طے کر سکتے ہیں۔ آپ کے یہ تمام معاملات سیکیورٹی ایکسچینج کمیشن (SEC) سے رجسٹر کروانے ہوتے ہیں۔ اور حکومتی اداروں اور ملکی قانون کی پابندی کرنی ہوتی ہے۔ اِس سارے عمل نے اِس طریقہ کو بہت مشکل بنا دیا ہے۔
6. آپ Crowd Funding کراؤڈ فنڈنگ کر سکتے ہیں۔ اپنے منصوبے یا کمپنی کی تفصیلات، ٹیم کی تعلیم و قابلیت اور تجربہ اور مزید تکنیکی تفصیلات کِک اسٹارٹر Kick Starter یا Go Fund Me جیسی ویب سائٹ پر اَپ لوڈ کر کے آپ دنیا بھر

میں موجود عام عوام سے رقم کی اپیل کرتے ہیں۔ یہ زیادہ تر عطیہ (Donations) کی شکل میں ہوتی ہیں۔ پیسے دینے والے کو یا تو کچھ نہیں ملتا کہ وہ آپ کے کام کو کارِ خیر سمجھتے ہوئے آپ کی مدد کر رہا ہے یا منصوبہ مکمل ہونے پر آپ کی پراڈکٹ کا سیمپل وغیرہ۔ یہاں عموماً اگر آپ مقرر کردہ ہدف کے مطابق رقم جمع کر سکتے ہیں تو یہ رقم آپ کو مل جائے گی۔ (کمپنی اپنا کمیشن کاٹ لے گی، جو عموماً 10 سے 15 فی صد ہوتا ہے)

اگر آپ زیادہ لوگوں کو اپنی طرف متوجّہ نہ کر سکیں اور فنڈنگ کا ہدف حاصل نہ ہو پایا تو سب لوگوں کو ان کی رقم واپس کر دی جائے گی اور آپ کو کچھ نہیں ملے گا۔

7. آئی سی او (Initial Coin Offering) دراصل اوپر بیان کئے ہوئے کراؤڈ فنڈنگ طریقہ کار کی جدید شکل ہے۔ تمام معاملات ویسے ہی ہوتے ہیں مگر آپ یہ سب کچھ بلاک چین پر کرتے ہیں اور عموماً پیسے کسی کرپٹو کرنسی میں ملتے ہیں۔ جواب میں آپ پیسہ لگانے والے کو اپنے پراجیکٹ یا کمپنی کے کچھ ٹوکن دیتے ہیں۔

آئی سی او اگر فنڈنگ کا ہدف پورا کر لیتا ہے تو آپ کو پیسے مل جاتے ہیں ورنہ تمام لوگوں کو ان کی کرپٹو کرنسی واپس مل جاتی ہے۔ آئی سی او لکھتے وقت آپ عموماً ایک وائٹ پیپر لکھتے ہیں، جس میں منصوبے کی تفصیلات، ٹیم کی قابلیت، ٹوکنز کی کل سپلائی اور ڈسٹری بیوشن، پراجیکٹ کی ٹائم لائن وغیرہ ہوتی ہے۔

کراؤڈ فنڈنگ کے برعکس یہاں پیسہ لگانے والوں کو ٹوکنز کی مالیت بڑھنے کی امید ہوتی ہے تاکہ وہ زیادہ منافع کما سکیں۔

ٹوکنز کی 3 بنیادی قسمیں ہیں:-

1. کوئنز :-

ہر پراجیکٹ کی اپنی Native Currency ہوتی ہے۔ مثلاً ایتھریم نے جب آئی سی او کیا تو ایتھریم چالیس سینٹ کا تھا $ 0.4 بعدِ ازاں اِسکی قیمت $1300 تک پہنچی۔ قریباً 4 ہزار گنا منافع۔

2. یوٹیلٹی ٹوکنز :-

یہ یونٹ آف سروس ہوتے ہیں جسے بعدِ ازاں استعمال کیا جا سکتا ہے۔ مثلاً آپ کسی اِسکول کی آئی سی او میں شرکت کریں تو بعد میں آپ اپنے بچوں کو ان ٹوکنز کے عوض تعلیم دلا سکتے ہیں۔ آرٹ اور میوزک انڈسٹری میں اس کی کئی مثالیں موجود ہیں۔

3. سیکیورٹی ٹوکنز :-

یہ بالکل کمپنی شئیرز کی طرح ہوتے ہیں اور آپ کمپنی کے حصّے دار بنتے ہیں۔ اِن کے لئے SEC سے رجسٹر ہونا ضروری ہے۔

یہ معلوم کرنے کے لئے کہ کون سا ٹوکن SEC کے دائرہ کار میں آتا ہے۔ امریکن SEC نے Howey-Test کی شرط رکھی ہے اگر ٹوکن کی خریداری میں کسی بھی قسم کی رقم استعمال ہوتی ہے۔ یہ رقم کسی کمپنی کو دی گئی ہے اور رقم دینے والا بغیر کسی محنت کے صرف رقم کی بنیاد پر منافع کا حقدار ٹھرتا ہے تو یہ عمل سیکیورٹی کہلائے گا اس پر SEC کے تمام قوانین کا اطلاق ہو گا۔

2013 میں N x t کے نام سے ICO ہوا تھا جو 28 ستمبر 2013 سے 8 نومبر 2013 تک چلا تھا۔ اس میں 21 بٹ کوائن جمع کئے گئے تھے 73 سرمائے داروں کی طرف سے جن کی اس وقت کل مالیت صرف 14 ہزار ڈالر تھی۔ کچھ ہی سالوں میں اِن 73 لوگوں کو ملنے والے منافع کی شرح 2 لاکھ فی صد کے قریب تھی۔

ایتھریم(Ethereum)کا ICO ،20 جولائی 2014 سے 2 ستمبر 2014 تک چلا(کوئی 42 دن)اور اس نے ساڑھے اکتیس ہزار بٹ کوائن جمع کئے جو اس وقت کے حساب سے 18 ملین ڈالرز کے تھے۔ یہاں پیسہ لگانے والوں کو 4 ہزار گنا منافع ملا۔

لِسک Lisk کا ICO 22 فروری سے 21 مارچ 2016 میں ہوا۔ 5.7 ملین ڈالر جمع ہوئے اور منافع کی شرح ٪138 رہی۔

ویوز (Waves) نے 16 ملین ڈالرز اور ڈاؤ (DAO) نے 160 ملین ڈالرز کا ICO کیا۔

ابھی تک کوئی ہزار سے اوپر ICO ہو چکے ہیں جس میں 10 ارب ڈالرز سے زیادہ کی سرمایہ کاری ہو چکی ہے۔

آئی سی او کی بڑھتی ہوئی مقبولیت کے پیشِ نظر آپ اسے مستقبل کے سیکیورٹی شئیرز کہہ سکتے ہیں۔

ایتھریم پلیٹ فارم اور ERC20 ٹوکن اسٹینڈرڈ کی مدد سے کوئی بھی شخص کچھ گھنٹوں میں اپنے ٹوکنز جاری کر سکتا ہے۔

آنے والے ٹوکنز میں Human-IQ جس میں غریب لوگوں کو بین الاقوامی معاشی نظام سے جوڑا جائے گا، Aeternity جس میں اسمارٹ کانٹریکٹ لائیو ڈیٹا کے ساتھ کام کر سکیں گے، Internet of Coins ،Cosmos ، Blue Frontiers ، Gnosis ،Etherex اور Akasha قابلِ ذکر ہیں جن میں سرمایہ کاری کر کے اچھے منافع کی توقع ہے۔

کسی بھی ICO میں سرمایے کاری سے پہلے وہاں کے مقامی قانون کو چیک کر لیں۔ مثلاً چائنہ نے ICO کو یکسر منع کر دیا ہے، امریکہ نے بہت سے قوانین کا اطلاق کر دیا ہے۔ کہیں ایسا نہ ہو لاعلمی میں آپ کسی قانونی مشکل میں پھنس جائیں۔

ICO میں بھی مزید جدّتیں متعارف ہو رہی ہیں مثلاً آئی بی او (Initial Bounty Offering)۔ یہاں شروع میں پراجیکٹ کے لئے کام کرنے والے ڈویلپرز کو IBO کے نام پر ٹوکنز ملتے ہیں جب وہ اپنے حصّے کا کام کر لیتے ہیں۔

اوسطاً ایک آئی سی او 12.7 ملین ڈالر جمع کر پاتا ہے اور اوسطاً ICO پر منافع کی شرح 12.8 گنا ہوتی ہے۔

ٹوکن فاؤنڈری اور اس جیسی بہت سی ایپ سائٹس آپ کو ICO کو لانچ کرنے میں مدد دیتی ہیں۔

مزید معلومات کے لئے ٹوکن مارکیٹ، آئی سی او لِسٹ، سمتھ کراؤن، آئی سی او رپورٹ، آئی سی او کاؤنٹ ڈاؤن، آئی سی او رٹینگ، اور کرپٹو کمپیئر جیسی ویب سائٹ کا مطالعہ کریں۔

علمائے کرام سے چند سوالات

جیسا کہ آج کل بلاک چین اور کرپٹو کرنسی کا چرچا ہر جگہ ہو رہا ہے اور لوگوں کی ایک بڑی تعداد اس میں شامل ہو رہی ہے ہم چاہتے ہیں کہ آپ مندرجہ ذیل امور پر ہماری راہنمائی فرما دیں، ہم آپ کا جواب من و عن اگلے ایڈیشن میں شائع کر دیں گے۔

****

کیا فرماتے ہیں مفتیان کرام و علمائے دین اس بارے میں کہ :

1۔ پیسے زر کی شرعی تعریف کیا ہے؟ اسلامی نقطہ نظر سے زر کسے کہتے ہیں؟

2۔ زر اور کرنسی میں کیا فرق ہے؟

3۔ زر کی تعریف قرآن و حدیث میں آتی ہے یا ائمہ کرام اور پہلے لوگوں کی رائے سے نتیجہ اخذ کیا گیا ہے؟

4۔ بلاک چین، رقوم کی منتقلی کا ایک عوامی کھاتا، بذات خود حلال ہے یا حرام؟

5۔ کیا آپ کرپٹو گرافی (پیچیدہ ریاضی) کے ذریعے ڈیجیٹل کرنسی (برقی پیسہ) کو ناجائز قرار دینگے؟

6۔ بٹ کوائن اور اس جیسی دوسری کرپٹو کرنسیز، مثلاً ایتھیریم، لائٹ کوائن، ریپبل، سب بلاک چین اور کرپٹو گرافی کی مدد سے وجود میں آتی ہے اور عوام میں تدریجاً مقبولیت پا رہی ہیں۔ کیا بذات خود ان میں کوئی شرعی قباحت ہے؟

7۔ کچھ لوگ کرپٹو کرنسی کو ناجائز کاموں میں بھی استعمال کرتے ہیں مثلاً نشہ آور چیزوں کی خرید وفروخت یا جرائم کی ادائیگی۔ ایسی صورت میں ان کا یہ مخصوص استعمال ناجائز ہوگا یا خود کرپٹو کرنسی ہی ناجائز ہو جائے گی؟

8۔ اگر آپ لوگوں کی فلاح و بہبود اور لاعلمی کو مد نظر رکھتے ہوئے، کسی مبینہ نقصان کے پیش نظر کرپٹو کرنسی کو ناجائز قرار دیتے ہیں تو اس کی صراحت فرمادیں کہ ایسا عوام کے مفاد کی خاطر کیا جارہا ہے نہ کہ کرنسی بذات خود حرام ہو گئی۔

9۔ اکیسویں صدی بلاشبہ ایجادات اور نت نئی ٹیکنالوجی کی صدی ہے۔ اور ہمیں قرآن سنت یا ائمہ کرام کے اقوال سے اس کی مثالیں نہیں ملتی مثلاً واٹس ایپ، فیس بک، انسٹا گرام، انٹرنیٹ ،آن لائن بینکنگ وغیرہ۔ ایسی صورت میں نئی ٹیکنالوجی کے علم کا حصول کہ انہیں سمجھا جاسکے کہ وہ شریعت کے مزاج کے مطابق ہے یا نہیں، جائز ہوگا یا ناجائز؟

10۔ حکومتوں کی کرپشن، لوٹ مار اور بے راہ روی کی وجہ سے لوگوں کا مرکزی اداروں سے اعتماد اٹھتا جارہا ہے ایسے میں وہ متبادل نظام کی تلاش میں سرگرداں ہیں۔ کرپٹو کرنسی اور بلاک چین وہ نظام مہیا کرتا ہے۔ کیا ہم ظلم برداشت کرتے رہیں یا اپنی زندگی کو بہتر بنانے کے لیے کسی اور نظام کی طرف مائل ہو سکتے ہیں؟

اللہ تعالی آپ کو اجر دیوے۔ رہنمائی فرمادیں، بہت سوں کا بھلا ہو گا۔

****

دارالافتاء ومدارس کی فہرست جن کی خدمت میں یہ سوالنامہ بذریعہ ای میل یاڈاک بھیجا گیا:

1. جامعہ دارالعلوم کراچی، پاکستان
2. جامعہ بنوریہ العالمیہ، کراچی، پاکستان
3. جامعۃ الرشید، کراچی، پاکستان
4. دارلافتااہلسنت، کراچی، پاکستان۔arulifta@dawateislami.net
5. دارالافتاء مدینۃ العلم، کراچیmmadinatulilm@yahoo.com
6. زہرہ اکیڈمی، کراچیinfo@zahraacademy.org
7. جامعہ حوزہ کوثر، اسلام آباد۔info@alkauthar.edu.pk
8. مدرسہ الزہراء، کراچی۔info@madrasafzahra.com

ہمیں جیسے ہی جوابات موصول ہوئے، ہم انہیں کتاب کے اگلے ایڈیشنز میں اور اپنی ویب سائٹ(www.cryptopakistan.org)پر شائع کرتے رہیں گے۔

فی الوقت موصول ہونے والے جوابات ملاحظہ فرمایئے:

جوابات:

منجاب: مفتی اویس پراچہ،
شریک تخصص فی فقہ المعاملات المالیہ، جامعۃ الرشید، کراچی

1. اسلامی نقطہ نظر سے ہر اس چیز کو زر کہا جاسکتا ہے جس کا بطور زر استعمال عام ہو جائے۔ اس بات کی تصریح علامہ ابن عابدین، امام سرخسی، امام مالک رحمہم اللہ اور دیگر کی تحریرات میں ملتی ہے۔ البتہ اس چیز کا موجود ہونا اور جائز ہونا ضروری ہے۔

2. مفتی تقی عثمانی صاحب دامت برکاتہم کی تصریح کے مطابق زر اور کرنسی میں فرق یہ ہے کہ زر کی پشت پر حکومت کا ہونا ضروری نہیں ہوتا جبکہ کرنسی کی پشت پر حکومت ہوتی ہے اور وہ لیگل ٹینڈر ہوتی ہے۔

3. زر کی تعریف تو قرآن کریم یا احادیث میں نہیں ملتی البتہ زر کی کچھ قسموں (مثلاً دراہم و دینار) کا ذکر ان میں ملتا ہے۔

4. کسی ٹیکنالوجی کو اس کے استعمال اور مقاصد کی بنیاد پر حرام یا حلال کہا جاتا ہے۔ بذات خود ٹیکنالوجی کوئی ایسی چیز ہی نہیں ہے جس پر حرام یا حلال کا لفظ بولا جاسکے۔

5. اس سوال کا جواب اس قدر سادہ نہیں ہے۔ ہمیں شرعی اصولوں کے تحت ایک ضابطہ طے کرنا ہوگا اور پھر اس کی روشنی میں ہر کرپٹو کرنسی پر الگ الگ حکم لگانا ہوگا۔ کم از کم میں مطلقا کرپٹو کرنسی ناجائز نہیں کہہ سکتا۔

6. اگر کوئی کرپٹو کرنسی اپنا وجود کسی بھی شکل میں رکھتی ہے اور اس کا سسٹم ضائع ہونے سے محفوظ ہے پھر وہ عوام میں رواج پاتی ہے تو اس کے جواز پر غور کیا جا سکتا ہے۔ سر دست بٹ کوائین ان شرائط کو پورا کرتی ہے۔ لیکن اگر کوئی کرپٹو کرنسی وجود ہی نہیں رکھتی یا اس کا ضائع اور ہلاک ہونا واضح طور پر ممکن ہے تو اس کی ذات میں ہی یہ قباحت موجود ہے۔ ایتھیریم کے بارے میں چونکہ یہ کہا جاتا ہے کہ اس کی آخری حالت محفوظ ہوتی ہے تو عین ممکن ہے کہ یہ ان دو شرائط کو پورا نہ کر سکے۔ بہر حال اس پر تحقیق کی ضرورت ہے۔

7. یہ استعمال ناجائز ہوگا۔

8. جب اس پر فتوی تحریر کیا جائے گا تو وجہ بھی تحریر کی جائے گی۔ فی الحال صرف آراء ہیں۔

9. یہ کام نہ صرف جائز بلکہ مستحسن ہے اور اس حوالے سے ان ٹیکنالوجیز سے واقف حضرات کو مضبوط حوالوں اور دلائل کے ساتھ مفتیان کرام کی مدد کرنی چاہیے تاکہ ان کے سامنے صورت حال واضح ہو سکے۔ بسا اوقات جو چیز آپ حضرات کے سامنے واضح ہوتی ہے وہ مفتیان کرام کے سامنے اس وجہ سے واضح نہیں ہوتی کہ وہ اس فیلڈ کے نہیں ہوتے۔ اس غیر واضح ہونے کی وجہ سے حکم لگانے میں دشواری ہوتی ہے۔

10. ہر مسئلے کو الگ الگ دیکھ کر جواب دیا جا سکتا ہے۔ نہ تو ہر جگہ حکومتوں کا ظلم اور کرپشن ایسی ہے اور نہ ہی ہر جگہ متبادل نظام کا استعمال فائدے مند ہے۔ سرمایہ دارانہ نظام کے خلاف اسی قسم کے دعوے سوشلزم اور کمیونزم کے داعیوں نے کیے تھے جن کا نقصان برسوں عوام نے بھگتا۔ اس لیے صرف ان دعووں پر کوئی فیصلہ نہیں کیا جا سکتا۔

المفتی اویس پراچہ

02-اپریل-2018

جامعۃ الرشید

۱

بسم اللہ الرحمن الرحیم

محترمی ومکرمی!

السلام علیکم ورحمۃ اللہ وبرکاتہ،

ڈیجیٹل کرنسی سے متعلق آپ کا سوال نامہ موصول ہوا، اس بارے میں ابھی دار الافتاء جامعہ دار العلوم کراچی میں تحقیق جاری ہے، فی الحال کوئی حتمی رائے نہیں دی جاسکتی۔ کچھ عرصہ کے بعد دوبارہ معلوم کریں۔

والسلام

محمد شعیب

دار الافتاء جامعہ دار العلوم کراچی

۲۱-۳-۱۴۳۹

۱۰ دسمبر ۲۰۱۷ء

فتاویٰ

دارالعلوم دیوبند، انڈیا۔

سوال #146744

آپ نے بٹ کوئن (bitcoin) کے بارے میں سنا ہوگا، یہ ڈیجیٹل کرنسی ہے اس کی قیمت سونے کی طرح اوپر نیچے ہوتی ہے، پانچ سال پہلے اس کی قیمت صرف پانچ ڈالر تھی اور اب ۷۵۰/ ڈالر ہے۔ اس کے بعد اور بہت ساری ڈیجیٹل کرنسیوں نے مارکیٹ میں جنم لیا جیسے اِتھیریوم (ETHEREUM)، داش (DASH) اور ایسی بیش بہا کرنسیاں وجود میں آئیں، یہ ساری کرنسیاں بٹ کوئن (bitcoin) کے عوض خریدی جاتی ہیں اور اوپر نیچے منافع کم کر کے بیچ دیئے جاتے ہیں۔ کچھ مشہور ویب سائٹس جہاں بٹ کوئن کے بارے میں آپ پڑھ سکتے ہیں وہ ویب سائٹ

https://blockchain.info

https://www.coinbase.com

جہاں بٹ کوئن کے عوض باقی کوئن کی خرید وفروخت ہوتی ہے وہ بھی کافی ہیں، کچھ مثال کے طور پر درج ذیل ہیں:

https://poloniex.com/exchange\nhttps://btc-e.com

اسی سے متعلق میرے دو سوالات ہیں:

(۱) کیا میں اپنی کچھ رقم بٹ کوئن کی صورت میں محفوظ کر سکتا ہوں جیسے کہ لوگ سونا یا مال و زر کی صورت میں محفوظ رکھتے ہیں یا زمین جائداد کی صورت میں، کیونکہ یہ بٹ کوئن کی اپنی قیمت بڑھا رہا ہے، پانچ سال پہلے ۵۰۰/ پاکستانی روپے کا تھا اور آج ۷۰/ہزار روپے کا ہے۔

(۲) کیا اس بٹ کوئن کے عوض میں تجارت کر سکتا ہوں؟ مجھے علم ہے کہ فیروکس (forex) تو حرام ہے، شاید کچھ صورتیں اُس میں حلال ہوں مگر میں شک کی بنیاد پر فیروکس (forex) نہیں کرتا، مگر کیا اس بٹ کوئن کی تجارت بھی حرام ہے جب میرا مقصد بٹ کوئن کے عوض کوئی کوئن خرید کر اس کو اپنے پاس رکھنا ہے اور جب اس کی قیمت بڑھ جائے تو واپس بیچ کر بٹ کوئن کی صورت میں منافع کما لینا ہے۔

میں نے ایکسچینج کے معاملے میں فتویٰ پڑھا ہے اور پوچھا بھی ہے کہ ڈالر اور پاؤنڈ یورو کے بارے میں، میں لوگوں سے سستا لے کر آگے مہنگا بیچتا ہوں، اُن علماء نے کہا کہ ایکسچینج جائز ہے۔ برائے مہربانی میرے بٹ کوئن کے معاملے میں رہنمائی فرمائیں، میں اپنی اضافی رقم بٹ کوئن کی صورت میں سنبھالنا چاہتا ہوں، کیونکہ یہ بھی زر اور زمین کی طرح اپنی مالیت کو بڑھاتا ہے اور منافع کا سبب بنتا ہے۔

Published on: May 16, 2017

جواب #146744

بسم اللہ الرحمن الرحیم

1438/8/N=881-238Fatwa:

(۱، ۲): آج کل دنیا میں جو مختلف کرنسیاں رائج ہیں، وہ فی نفسہ مال نہیں ہیں، وہ محض کاغذ کا ٹکڑا ہیں، ان میں جو مالیت یا عرفی ثمنیت پائی جاتی ہے، وہ دو وجہ سے ہے؛ ایک تو اس وجہ سے

کہ ان کے پیچھے ملک کی اقتصادی چیزیں ہوتی ہیں؛اسی لیے ملک کی اقتصادی ترقی اور انحطاط کا کرنسی کی ویلیو پر اثر پڑتا ہے،یعنی:اقتصاد ہی کی وجہ سے ملک کی کرنسی کی ویلیو گھٹتی بڑھتی ہے۔ اور دوسری وجہ یہ ہے کہ ہر ملک عوام کے لیے اپنی کرنسی کا ضامن وذمہ دار ہوتا ہے؛یہی وجہ ہے کہ جب کوئی ملک اپنی کوئی کرنسی بند کرتا ہے تو کرنسی محض کاغذ کا نوٹ بن کر رہ جاتی ہے اور اس کی کوئی ویلیو یا حیثیت باقی نہیں رہتی۔اب سوال یہ ہے کہ ڈیجیٹل کرنسی کے پیچھے کیا چیز ہے جس کی وجہ سے اس کی ویلیو متعین ہوتی ہے اور اس کی ترقی اور انحطاط سے کرنسی کی ویلیو گھٹتی بڑھتی ہے؟اسی طرح اس کرنسی کا ضامن وذمہ دار کون ہے؟نیز کرنسی کی پشت پر جو چیز پائی جاتی ہے،کیا واقعی طور پر اس پر کرنسی کے ضامن کا کنٹرول ہوتا ہے یا یہ محض فرضی اور اعتباری چیز ہے؟

ڈیجیٹل کرنسی کے متعلق مختلف تحریرات پڑھی گئیں اور اس کے متعلق غور کیا گیا تو معلوم ہوا کہ ڈیجیٹل کرنسی محض ایک فرضی چیز ہے اور اس کا عنوان ہاتھی کے دانت کی طرح محض دکھانے کی چیز ہے اور حقیقت میں یہ فاریکس ٹریڈنگ وغیرہ کی طرح نیٹ پر جاری سٹے بازی اور سودی کاروبار کی شکل ہے،اس میں حقیقت میں کوئی مبیع وغیرہ نہیں پائی جاتی اور نہ ہی اس کے کاروبار میں بیع کے جواز کی شرعی شرطیں پائی جاتی ہیں۔

پس خلاصہ یہ کہ بٹ کوئن یا کوئی اور ڈیجیٹل کرنسی، محض فرضی کرنسی ہے، حقیقی اور واقعی کرنسی نہیں ہے، نیز کسی بھی ڈیجیٹل کرنسی میں واقعی کرنسی کی بنیادیں صفات نہیں پائی جاتیں، نیز ڈیجیٹل کرنسی کے کاروبار میں سٹہ بازی اور سودی کاروبار کا پہلو معلوم ہوتا ہے؛اس لیے بٹ کوئن یا کسی اور ڈیجیٹل کرنسی کی خریداری کرنا جائز نہیں۔اسی طرح بٹ کوئن یا کسی بھی ڈیجیٹل کرنسی کی تجارت بھی فاریکس ٹریڈنگ کی طرح ناجائز ہے؛لہٰذا اس کاروبار سے پرہیز کیا جائے۔

قال اللہ تعالی: وأحل اللہ البیع وحرم الربا الآیۃ (البقرۃ: ۲۷۵)، یاأیھا الذین آمنوا إنما الخمر والمیسر والأنصاب والأزلام رجس من عمل الشیطن فاجتنبوہ لعلکم تفلحون (المائدۃ، ۹۰)، وقال رسول اللہ صلی اللہ علیہ وسلم: إن اللہ حرم علی أمتي الخمر والمیسر (المسند للإمام أحمد، ۲: ۳۵۱، رقم الحدیث: ۶۵۱۱)، ﴿وَلَا تَأْكُلُوٓا أَمْوَالَكُم بَيْنَكُم بِالْبَاطِلِ﴾ أي بالحرام، یعني بالربا، والقمار، والغصب والسرقۃ (معالم التنزیل ۲: ۵۰)، لأن القمار من القمر الذي یزداد تارۃً وینقص أخری۔ وسمی القمار قمارًا؛ لأن کل واحد من المقامرین ممن یجوز أن یذہب مالہ إلی صاحبہ، ویجوز أن یستفید مال صاحبہ، وھو حرام بالنص (رد المحتار، کتاب الحظر والإباحۃ، باب الاستبراء، فصل في البیع، ۹: ۵۷۷، ط: مکتبۃ زکریا دیوبند)۔

واللہ تعالیٰ اعلم

دارالافتاء،

دارالعلوم دیوبند

http://www.darulifta-deoband.com/home/ur/Halal-Haram/146744

تصوراتی دنیا کی تصوراتی کرنسی

یعنی

''بٹ کوئن'' (BITCOIN) کا تعارُف وطریقۂ کار

اوراس کا حکم شرعی

الحمد لله رب العالمين ، والصلوة والسلام على رسوله الكريم أما بعد!

عن عبد الله بن مسعود رضي الله عنه قال : قال رسول الله صلى الله عليه وسلم : " طلب كسب الحلال فريضة بعد الفريضة " . رواه البيهقي في شعب الإيمان . (مشكوة المصابيح : ۲/۱۲۸، رقم : ۲۷۸۱ ، كتاب البيوع)

حضرت عبداللہ ابن مسعود رضی اللہ تعالیٰ عنہ حضور اکرم صلی اللہ علیہ وسلم کا قول نقل کرتے ہیں کہ ''حلال کمائی کا حصول وطلب دیگر فرائض کی ادائیگی کی طرح ایک مستقل فریضہ ہے۔''

حضرت شیخ الاسلام مفتی محمد تقی عثمانی دامت برکاتہم نے اپنی ایک تحریر میں رقم فرمایا ہے کہ موجودہ دور میں اللہ تعالیٰ کے فضل وکرم سے سارے عالم کے مسلمانوں میں ایک شعور پیدا ہورہا ہے، اور وہ شعور یہ ہے کہ جس طرح ہم اپنی عبادتیں شریعت کے مطابق انجام دینا چاہتے ہیں، اسی طرح اپنے معاملات کو بھی شریعت کے سانچے میں ڈھالیں، یہ قدرت کی طرف سے ایک شعور ہے، جو ساری دنیا کے مسلمانوں میں رفتہ رفتہ پیدا ہونا شروع ہوا ہے، اور اس کا نتیجہ یہ ہے کہ بعض ایسے لوگ جن کی ظاہری شکل وصورت اور ظاہری وضع قطع کو دیکھ کر دور دور تک یہ گمان بھی نہیں ہوتا تھا کہ متدین (دین دار) ہوں گے، لیکن اللہ تعالیٰ نے ان کے دل میں حرام مال کی نفرت اور حلال مال کی طرف رغبت پیدا فرمادی۔ اب وہ اس فکر میں ہیں کہ کسی طرح ہمارے معاملات شریعت کے مطابق ہوجائیں، وہ اس تلاش میں ہے کہ کوئی ہماری رہنمائی کرے، لیکن اس میدان (خاص کر حوادث ونوازل/جدید معاملات) میں رہنمائی کرنے والے، ان کے مزاج ومذاق کو سمجھ کر ان کے معاملات اور اصطلاحات کو سمجھ کر جواب دینے والے بہت کم ہوگئے، یعنی اس وقت ضرورت تو بہت بڑی ہے، لیکن اس ضرورت کو پورا کرنے والے افراد بہت کم ہیں۔

آج اگر ایک تاجر تجارت کررہا ہے، اور تجارت میں روزمرہ نئے نئے حالات پیش آتے ہیں، وہ کسی عالم کے پاس جاتا ہے، کہ بھائی میری یہ صورت حال ہے، اس کا حکم بتائیں؟ لیکن صورت حال یہ ہوگئی ہے کہ تاجر عالم کی بات نہیں سمجھتا، اور عالم تاجر کی بات نہیں سمجھتا، کیوں کہ دونوں کے درمیان ایک ایسا فاصلہ قائم ہوگیا ہے کہ ان کی بہت سی اصطلاحات اور بہت سے معاملات میں ان

کے عرف اور طریق کار سے عالم ناواقف ہے، اس کا نتیجہ یہ ہوا کہ جب انہوں نے یہ محسوس کیا کہ علماء کے پاس جا کر ہمیں اپنے سوالات کا پورا جواب نہیں ملتا، تو انہوں نے علماء کی طرف رجوع کرنا ہی چھوڑ دیا۔ اس کی وجہ سے علماء اور کاروبار کرنے والوں کے درمیان اور معاملات کے اندر بہت بڑا فاصلہ پیدا ہوگیا، اور اس کے نتیجے میں خرابی در خرابی پیدا ہوتی چلی گئی۔ (ملخص از انعام الباری: ۹/۴۳، بیر بیر) آخر کوئی تو بات ہوگی کہ امام محمد رحمۃ اللہ علیہ مارکیٹ میں جا کر باقاعدہ تاجروں کے تجارتی حال واحوال دریافت فرمایا کرتے تھے، اور ان کے مسائل کو حل کرنے کی خاطر رات بھر آرام نہیں فرماتے تھے، آج امت کو امام محمد جیسے کئی محمدوں کی ضرورت ہے، لہٰذا اب ضرورت اس بات کی ہے کہ "فقہ المعاملات" کو سمجھا جائے اور پڑھا جائے۔ اور تاجروں سے جدید مسائل ونوازل کی صورتیں معلوم کر کے، انہیں قلم بند کر کے، ان پر حکم شرعی کا انطباق کیا جائے۔

چوں کہ دوستوں کی طرف سے کئی مرتبہ "بٹ کوئن" وغیرہ کرنسیس سے متعلق حکم شرعی پوچھا گیا، لیکن بات وہی تھی کہ نہ ہم اُن کی بات سمجھ پائے تھے، نہ وہ ہماری زبان، ان کو یہی جواب دیا جاتا رہا کہ اون لائن جتنی بھی کرنسیس یا کاروبار آج کل چلتے ہیں، وہ اطمینان بخش نہیں ہوتے ہیں، لہٰذا ان کاروباروں میں مشغول نہ ہونا ہی بہتر ہے، لیکن انہوں نے اصرار کیا کہ "بٹ کوئن" (تصوراتی کرنسی) کے بارے میں جان کاری اور نیٹ پر موجود اس کے تعارف وطریقۂ کار کو ذرا ایک مرتبہ دیکھ لیں، یا سن لیں، کیوں کہ بہت سے مسلمان (خصوصاً نوجوان طبقہ) کم وقت میں زیادہ پیسہ کمانے کے چکر میں اس طرح کی اون لائن کرنسیس کے کاروبار کو فالو کر رہے ہیں، اگر اس طریقۂ کار کی حلت یا حرمت سامنے نہ لائی گئی، اور اگر یہ کاروبار حرام ہوا، تو اشتمال بالحرام کی وجہ سے تجار عوام وعلماء سب ماخوذ ہوں گے، اور اگر حلال ہوا، تو کسی طرح کا کوئی شبہ باقی نہ رہے گا، بلکہ اطمینان کے ساتھ جو چاہے یہ کاروبار کر سکتا ہے۔ چنانچہ بٹ کوئن سے متعلق بنیادی جان کاری حاصل کی گئی، اور حضرت شیخ الاسلام مدظلہ کی مذکورہ تحریر کو پڑھنے کے بعد مزید شوق پیدا ہوا کہ اس معاملہ کا حل جلد از جلد عوام اور تاجروں کے سامنے پیش کیا جائے، لہٰذا بٹ کوئن سے متعلق بنیادی جان کاری، اس کے فوائد، اہمیت اور متوقع خطرات درج ذیل ملاحظہ فرمائیں:

کرنسی کی قسمیں:

دنیا میں دو طرح کی کرنسی چلتی ہیں: (۱) ایک لیگل کرنسی (Legal Currency) جو 180 ممالک میں چلتی ہیں۔
(۲) اور دوسری آلٹرنیٹو کرنسی (Alternative Currency) جو انٹرنیٹ پر، پوری دنیا میں چلتی ہے۔

۱۹۸۳ء میں ڈیجیٹل منی (Digital Mony) کا آئڈیا ایک کمپنی نے دیا، اور پھر ۱۹۹۰ء کے زمانے میں ڈی جی کیش کمپنی (Digi Cash Company) وجود میں آئی، اور مختلف کرنسیاں وجود میں آئیں، جیسے ڈکسی پے (DixiPay)، اسکریل (Skrill)، ایکو پیز (ecoPayz)، پے پال (PayPal)، انٹرو پے (entroPay)، او کے پے (OKPAY)، ایگو پے (EGOPAY)، سولڈ ٹرسٹ پے (SolidTrustPay)، پرفیکٹ منی (Perfect Mony)، ای پیمنٹ (Epayments)، کیو پے زا (Q PAYZA)، نیٹ الر (NETELLER)، وغیرہ یہ سب وہ منی اور کرنسیس ہیں جو انٹرنیٹ پر یوز (Use) کی جاتی ہیں۔

"**بٹ کوئن**" کو ڈیجیٹل کرنسی (Digital Currency)، کرپٹو کرنسی (Crypto Currency)، ڈیجیٹل منی

(Digital Mony)، ڈیجیٹل کیش (Digital Cash)، بایوگرافی (Bayografy) بھی کہتے ہیں۔ان میں سب سے اہم اور قیمتی "بٹ کوئن کرنسی" (Bitcoin Currency) ہے۔ (ع۔م)

"بٹ کوئن" کیسے کام کرتا ھے؟: "بٹ کوئن" کو کرنسی کی ایک نئی قسم کہا جاتا ہے، اگرچہ دیگر کرنسیوں کی طرح اس کی قدر کا تعین بھی اسی طریقے سے ہوتا ہے کہ لوگ اسے کتنا استعمال کرتے ہیں۔ "بٹ کوئن" کی منتقلی کے عمل کے لیے "مینگ" کا استعمال ہوتا ہے، جس میں کمپیوٹر ایک مشکل حسابی طریقۂ کار سے گزرتا ہے، اور ۶۴ ڈیجٹس کے ذریعے مسئلے کا حل نکالتا ہے، ہر مسئلہ جو حل ہو جاتا ہے اس کے نتیجے میں ایک "بٹ کوئن" بنتا ہے۔ اس وقت ڈیڑھ کروڑ "بٹ کوئن" موجود ہیں۔ بٹ کوئن حاصل کرنے کے لیے صارف کے پاس بٹ کوئن کی معلومات ہونی چاہیے جو کہ یہ ۳۴۔۲۷ الفاظ اور ہندسوں کی لڑی ہوتی ہے۔ یہ ہندسے اور لفظ "ورچوول پوسٹ باکس" کی مانند ہوتے ہیں۔ بٹ کوئن کی معلومات کے لیے کوئی رجسٹر نہیں ہوتا، اس لیے لوگ جب ان کی ترسیل کرتے ہیں، تو اپنی شناخت چھپانے کے لیے انہیں استعمال کرتے ہیں۔ یہ ایڈریسز "بٹ کوئن" کے والٹ (Wallet) میں محفوظ ہوتے ہیں جو جمع پونجی کا حساب کتاب رکھتے ہیں۔ "بٹ کوئن" کی ترسیل میں جانچ کے لیے کمپیوٹر کی بہت توانائی استعمال ہوتی ہے۔

"بٹ کوئن" کی قدر پہلی بار سونے سے زیادہ ہوگئی:

ڈیجیٹل ورچوول کرنسی "بٹ کوئن" کے ایک یونٹ کی قدر تاریخ میں پہلی بار ایک اونس سونے کی قیمت سے تجاوز کر گئی ہے، گزشتہ دنوں "بٹ کوئن" کی قدر ایک ہزار ۲۶۸ امریکی ڈالر تھی، جب کہ اس کے مقابلے میں ایک اونس سونے کی قیمت ایک ہزار ۲۳۳ ڈالر رہی۔

"بٹ کوئن" کی قدر میں حالیہ اضافے کی وجہ چین میں اس کی بڑھتی مانگ ہے، تاہم حکام نے خبردار کیا ہے کہ اس کے ذریعے سے ملک سے باہر پیسہ لے جایا جا رہا ہے۔ ۲۰۱۴ء میں بٹ کوئن کی قدر شدید مندی کا شکار ہوئی تھی، تاہم گزشتہ مہینے بٹ کوئن کی قدر میں اضافہ دیکھا گیا تھا۔ ۲۰۰۹ء میں متعارف کروائے جانے کے بعد سے بٹ کوئن کی قدر غیر مستحکم رہی ہے، اور بہت سے ماہرین یہ سوال کرتے رہے ہیں کہ کیا ڈیجیٹل کرنسی زیادہ عرصے تک چل سکے گی؟

رواں سال کے آغاز میں چینی حکام نے بٹ کوئن کے ذریعے تجارت کے خلاف کریک ڈاؤن کیا تھا، جس کی وجہ ملک سے باہر غیر قانونی طور پر رقم کی ترسیل کو روکنا بتایا گیا تھا، تاہم بیجنگ کی جانب سے نگرانی کے سخت طریقۂ کار کے باوجود کرنسی کی قدر میں کچھ ہی دن کے لیے کمی آئی، اور جنوری کے اواخر سے اس کی قدر میں جو اضافہ ہونا شروع ہوا، وہ تا حال جاری ہے۔

رواں سال جنوری میں بٹ کوئن کی قدر میں ریکارڈ اضافے کے بعد اس میں مسلسل استحکام دیکھنے کو مل رہا ہے۔

(بشکریہ انقلاب [بمبئی] مؤرخہ ۹ مارچ ۲۰۱۷ء بروز جمعرات)

بٹ کوئن لیگل کرنسی ھے یا نھیں؟:

(۱) ۱۸۰ ممالک کی کرنسی الگ ہے، جسے سرکیولیٹنگ کرنسی (Circulating Currency) کہتے ہیں، یعنی پیپر کرنسی۔

(۲) الٹرنیٹو کرنسی (Alternative Currency) اس میں پلاسٹک کرنسی زیادہ ہوتی ہے، مثلاً: ٹین کارڈ، سکرین کارڈ،

ویزا کارڈ، اے ٹی ایم کارڈ وغیرہ۔ بٹ کوئن بھی ایک الٹرنیٹو کرنسی (Alternative Currency) ہے۔

الیکٹرانک منی (Electronic Money) یا ای منی (E Money)۔

(۳) بٹ کوئن جاپانی سائنٹسٹ "ستوشی ناکاموتو" نے ۲۰۰۸ء میں ایجاد کیا، اور اوپن سورس یعنی ۲۰۰۹ء میں اسے ریلیز کیا۔

بٹ کوئن ویلیو (BTC): ایک ستوشی: -/1.00000000 = 1btc

-/1satoshi = 0.00000001

فی الحال ایک بی ٹی سی (BTC) کی قیمت -/47,250 (پاکستانی روپیہ) اور قریباً 45000 (ہندوستانی روپیہ) ہے۔

بٹ کوئن ویلیو ہسٹری:

۲۰۰۹، ۲۰۱۰ء میں اس کی کوئی ویلیو نہیں تھی۔ پھر بڑھتے بڑھتے سیل اینڈ ڈیمانڈ کے فارمولے پر یہ کرنسی چلتی ہے۔ ہر آدھے گھنٹے بعد ریٹ چینج ہوتا ہے۔ حتیٰ کہ مئی ۲۰۱۶ء میں ایک بٹ کوئن کا ریٹ -/450 ڈالر تھا۔

مستقبل میں ۲۱ ملین بٹ کوئن بنیں گے۔ 6.12 ملین بن چکے ہیں، جو ٹریڈ ان مارک ہو رہے ہیں۔

بٹ کوئن مرچنٹس: تقریباً ۱۲ ہزار کمپنیاں (مرچنٹس) BTC یوز کر رہی ہیں۔

ٹاپ ٹین بیگیسٹ کمپنیاں (Tpp 10 Biggest Bitcoin Accepting Merchants):

MicroSoft. Dell. Expedia. Airbattic. American Redcross. Wikipedia.

Destinia. Overstock.com. Cnewegg. Reeds.

آل ورلڈ (All World) (پوری دنیا میں) تقریباً ۶ سو کمپنیاں ہیں جو کرپٹو کرنسی کے اوپر کام کر رہی ہیں۔ (۶ سو کرنسیس الگ الگ ہیں، مثلاً: بٹ کوئن (Bit Coin)، بلیک کوئن (Balck Coin)، ڈیش (Dash)، ڈوج کوئن (Doge Coin)، ڈیجیٹل نوٹ (Digital Note) وغیرہ)۔ لیکن BTC کی ویلیو تمام کرپٹو کرنسیس سے زیادہ ہے۔

BTC کی اہمیت: ۱۲۰۰۰ ہزار مرچنٹ مثلاً: Microsoft. Wordpress. Apple app stor. Reddit. Amazon وغیرہ اسے یوز (استعمال) کر رہے ہیں۔

دیگر کرنسیس کے مقابلے BTC کی طاقت: مینکنگ سسٹم کو پیپر کرنسی تک آنے میں 250 سال لگے، ATM مشین 85 سال بعد بینک کے پاس آئے، جب کہ BTC صرف اور صرف ۳ سال میں اتنی فیمس ہوئی کہ اس کے ATM بن گئے۔ ۱۲ سو ڈالر تک اس کا ریٹ بڑھ گیا تھا۔ فی الحال آل ورلڈ ۲۰ ممالک میں BTC کے ATM لگے ہوئے ہیں۔ پہلا BTC اے ٹی ایم (ATM) اکتوبر ۲۰۱۳ء کناڈا (Canada) میں لگا تھا۔

BTC کے استعمال کی وجہ: یہ آپ کی اپنی کرنسی ہے۔ کوئی نہیں جانتا کہ آپ کے پاس کتنے BTC موجود ہیں؟ یعنی نو بینک نو گورنمنٹ (No Bank No Govt)، لین دین کے لیے سب سے محفوظ ترین طریقہ ہے۔ کم از کم ایزی ٹرانسفر اس سے کیا جا سکتا ہے۔ فیس بھی بہت کم، نا کے برابر۔ جب کہ نوٹ بینک کی پراپرٹی ہے، کسی بھی وقت اُسے واپس لے سکتا

ہے، نوٹ ناکارہ ہوجاتا ہے، BTC میں ایسا کچھ بھی نہیں، آنے والے وقت میں ۹۸ر ہزار پانچ سو ڈالر تک انکریز (Increase) کرسکتی ہے، یعنی ایک کروڑ کا ایک BTC ہوگا۔

Start Btc Work, آپ بٹ کوئن کیسے اسٹارٹ کرسکتے ہیں؟ یعنی مائن (Mine) کرنے کا طریقہ :

BTC کی ایک مشین ہوتی ہے، کمپنیاں مختلف سَروَرز (Sarovers) پر BTC کو کور کررہی ہوتی ہیں۔ آپ ان کمپنیوں کی ویب سائٹس پر جاکر بٹ کوئن وغیرہ دیگر ڈیجیٹل کرنسیوں کو مائن کرسکتے ہیں۔

بٹ کوئن مائن (Mine / حاصل کرنے) کے بنیادی طریقے تین ہیں:

(۱) Asic Mining۔ ستوشی ناکاموتو پروگرامر نے جو سافٹ ویئر اور پروگرام بنایا وہاں سے مائن کرنے کو ایزیک مائننگ کہتے ہیں، جیسے پتھر، کوئلہ، سونا اور ہیروں کی مائننگ ہوتی ہے، ایسے ہی بٹ کوئن کی مائننگ ہوتی ہے، کمپیوٹر سسٹم میں بذریعہ سی پی یو (CPU)، یا جی پی یو (GPU) سے ہی ہم بٹ کوئن آن کرسکتے ہیں، پروسیز مشین کو کمپیوٹر سسٹم سے اٹیچ کرنا پڑتا ہے، اور یہ مشین ہائی پاور کے ہوتے ہیں، جو بانگ کانگ وغیرہ سے منگوائے جاسکتے ہیں، یعنی مشین خود ہمیں خریدنا ہوتا ہے۔

(۲) Cloud Mining۔ بڑی بڑی کمپنیوں کے بڑے بڑے ڈاٹا سرورز جو بٹ کوئن کو مائن کرتے ہیں، جس میں مختلف کمپنیاں یہ آفر کرتی ہیں کہ اگر آپ ایزیک مائنر سے اسے آن نہیں کرسکتے، تو ہمارے ساتھ ۳، یا ۵ر سال کا معاہدہ کریں، اس میں ہمارے اکاؤنٹ میں ڈالر وغیرہ یعنی کرنسیز کا ہونا ضروری ہوتا ہے، جس کی بنیاد پر ہمیں بٹ کوئن مائن کی جاتی ہیں، یعنی دی جاتی ہے۔

(۳) Free Websites۔ فری بٹ کوئنس ان ویب سائٹس کے ذریعے حاصل کی جاتی ہیں۔ لیکن کہاوت ہے کہ جتنا گڑ اُتنا میٹھا۔ یعنی جتنی زیادہ کمائی کرنا ہے اس کے لیے پہلے دو طریقوں میں سے کسی ایک کو اپنانا ہوگا۔ Solve Captcha کرنے کے بعد، یعنی فارم پُر کرنے پر کمپنی آپ کو فری بٹ کوئن یعنی کچھ ستوشی دیتی ہے۔ ہر گھنٹے کے بعد کیپچا (Captha) بدلتا رہتا ہے۔

مزید دو طریقے اور ہیں:

(۱) کرپٹو کرنسی (Crypto Currency) کی ٹریڈنگ کے ذریعے۔ (اس طریقہ میں مختلف کرپٹو کرنسی کو بٹ کوئن میں، اور بٹ کوئن کو دوسری کرپٹو کرنسی میں ایکسچینج کرکے بٹ کوئن کمائے جاتے ہیں۔)

(۲) گیم لنگ (Gameling) کے ذریعے۔ (اس طریقہ میں بہت سارے ایسے گیم کھیلے جاتے ہیں جن کی ونگ پرائز میں بٹ کوئن حاصل ہوتے ہیں۔)

مائننگ فی Mining Fee: دالل کو 500 ستوشی انعام میں ملتی ہے۔ جتنی زیادہ ٹرانزیکشن کرے گا اتنی زیادہ Fee ملے گی۔ ایفیشنٹ ہارڈ ویئر اور سافٹ ویئر BTC کے لیے ضروری ہے، نیز بجلی بھی خرچ کرنی پڑتی ہے، جتنا زیادہ انویسٹ کریں گے، اتنا ہارڈ ویئر پاور ہمیں دیں گے۔ یہ عمل رسکی ہے، کہ کچھ کمپنیاں انویسمنٹ لے کر بھاگ جاتی ہیں، بہت کم کمپنیاں اس میں باقی رہتی ہیں۔

بعض اہم شارٹ کٹس (Some Important Shortcuts: یعنی کمپنیاں جو پاور مائنر (Miner)

کو دیتی ہیں، ان کو شارٹ کٹ میں اس طرح لکھا یا کہا جاتا ہے، جو مندرجہ ذیل ہے:

1) 1000 Hash/s= 1 kilo Hash= 1 KH/s

2) 1000 KH/s= 1 Mega Hash= 1 MH/s

3) 1000 MH/s= 1 Giga Hash= 1 KH/s

4) 1000 GH/s= 1 Tera Hash= 1 TH/s

بعض کمپنیاں ایک کلو ہیش یونٹ (Hash Unit) کے ساتھ پاور دیتی ہیں، آہستہ آہستہ میگا ہیش (Mega Hash) کی طرف جاتے ہیں، اسی طرح ہوتے ہوتے ٹیرا ہیش (Tera Hash) تک پہنچتے ہیں، یعنی درجہ بدرجہ بٹ کوئن (BitCoin) کا پاور بڑھتا جاتا ہے۔

رسک لیں یا پیچھے بیٹھیں رہیں؟ (Take Risk Or Stay Back):

سوال یہ پیدا ہوتا ہے کہ اس کرنسی کے حصول کے لیے ہمیں اس کے کاروبار میں شریک ہونا چاہیے یا نہیں؟ فائدہ اٹھائیں یا نہیں؟ تو یاد رکھیں کہ اگر رسک لیں تو سکسیس فل (کامیاب) ورنہ ستوشی ضائع ہوں گے، کامیابی ممکن ہے، اس لیے اگر رسک لے لو تو بہتر ہے، کیوں کہ کرنٹ پوزیشن سے باہر (اونچی) پوزیشن پر جا سکتے ہیں۔

(بحوالہ اون لائن ویڈیو، من جانب جبران علی، Dablio Raja&)

❁.....❁.....❁

تفصیلی رپورٹ بسلسلہ بٹ کوئن

آپ نے پیسے کے کئی رُوپ دیکھے ہوں گے، جیسے بھارتی روپے، امریکی ڈالر، برٹش پاؤنڈ، جاپانی ین، اور یوروپ کا یُورو۔ یہ تمام کرنسیز ہیں۔ ان میں سے زیادہ تر کرنسیز کاغذ سے بنی ہوتی ہیں، جنہیں آپ اپنی آنکھوں سے دیکھ سکتے ہیں، اپنی جیب میں رکھ سکتے ہیں، اور انہیں چھو کر محسوس بھی کر سکتے ہیں۔ آپ جس دیش میں بھی جاتے ہیں، اسی دیش کی کرنسی استعمال کرنی پڑتی ہے، لیکن کیا آپ نے ایسی کرنسی کے بارے میں سنا ہے کہ جو دکھائی نہیں دیتی لیکن پھر بھی وہ دنیا کی سب سے مولیوان (قیمتی) کرنسی ہے۔

ہم بٹ کوئن کی بات کر رہے ہیں، یہ ایک پرکار کی ڈیجیٹل کرنسی ہے، اگر انٹرنیٹ ایک دیش ہوتا تو شاید بٹ کوئن کرنسی انٹرنیٹ کی راشٹریہ کرنسی ہوتی۔ ہوسکتا ہے کہ بٹ کوئن کے بارے میں آپ میں سے بہت سارے لوگوں نے نہیں سنا ہوگا، اور جنہوں نے سنا بھی ہوگا ان میں سے بہت سارے لوگ یہ نہیں جانتے ہیں کہ یہ کیسے کام کرتی ہے؟ بٹ کوئن ہوتا کیا ہے؟ اس لیے آج ہم دنیا کی سب سے قیمتی کرنسی کا تعارف آپ کے سامنے کریں گے، کیوں کہ اس کرنسی کے ایک سکے کی قیمت آج کی تاریخ میں قریب ۴۵۰۰۰ روپے (ہندوستانی) ہیں۔ یہ الگ بات ہے کہ یہ سکہ کسی کو دکھائی نہیں دیتا، کیوں کہ یہ ایک طرح کا ڈیجیٹل سکہ ہے۔

دنیا میں پہلی بار بٹ کوئن کے روپ میں ہوئے لین دین کو ایک بھارتیہ ایجنسی فریز کرنے کی تیاری کر رہی ہے، بٹ کوئن کا استعمال کر کے ڈرگ تسکروں نے پیسے کا لین دین شروع کر دیا ہے، اور اب اس لین دین کی رقم میں سے قریب ۵۰۰ر بٹ کوئنس کو

فریز کرنے کی تیاری بھارت کے نیز کوکس کنٹرول بیورو نے کرلی ہے۔ایک بٹ کوئن کی قیمت قریباً ۴۵ ہزار روپے ہیں، تو ضبط کی جانے والی رقم گویا دو کروڑ ۲۵ لاکھ روپے ہیں۔

آخر بٹ کوئن ہے کیا؟ اور یہ کیسے کام کرتا ہے؟ کیوں دنیا بھر کے لوگ بٹ کوئنس خریدنا چاہتے ہیں؟

بٹ کوئن دنیا کی پہلی ای سینٹرالائز کرپٹو کرنسی (Crypto Currency) ہے، خاص طور پر ڈیجیٹل دنیا کے لیے بنائی گئی ہے، بٹ کوئن کا استعمال پوری دنیا میں کبھی بھی اور کہیں بھی کیا جاسکتا ہے، بٹ کوئن کے ذریعے کوئی بھی ویکتی (شخص) دنیا میں کسی بھی دوسرے ویکتی (شخص) کو رقم بھیج سکتا ہے، پیسہ بھیج سکتا ہے، اور سب سے بڑی بات یہ ہے کہ اس کے لیے کسی بینک یا تھرڈ پارٹی ایجنسی کی مدد نہیں لینی پڑتی، یعنی آپ جو بھی پیسہ کسی کو بھیجنا چاہتے ہیں، اس پیسے کو سیدھے اپنے بٹ کوئن والیوٹ سے کسی دوسرے ویکتی کے بٹ کوئن والیوٹ میں ٹرانسفر کرسکتے ہیں، اس طرح سے پیسہ ٹرانسفر کرنے پر آپ کو صرف ڈھائی سینٹ یعنی قریب ایک روپیہ ۶۷ پیسے کی فیس دینی ہوتی ہے، جو کہ بہت ہی کم ہے، معمولی ہے، دنیا بھر میں اس وقت لاکھوں لوگ سادھارن کرنسی (موجودہ چلن) کی جگہ بٹ کوئن کا استعمال کررہے ہیں، ابھی دنیا میں پیسوں کے قانون لین دین کے لیے بینکوں کا استعمال کرنا پڑتا ہے، یہاں تک کہ کسی دیش (ملک) میں کتنی کرنسی کا سرکولیشن (اجرا) ہوگا یہ بھی بینک اور وہاں کی سرکاریں طے کرتی ہیں، لیکن بٹ کوئن ایک ایسی ووستھا (سہولت) ہے، جس پر کسی ایجنسی، بینک یا سرکار کا نیئنترن (قبضہ) نہیں ہے، بٹ کوئن کے تحت لین دین سیدھے دو لوگوں کے درمیان ہوتا ہے، یہ آرتھک ووستھا کا لین دین پوری طرح سے اَن کرپٹیڈ (رشوت و دھوکہ دہی سے پاک) ہوتا ہے، یعنی سُرکشت و محفوظ طریقہ ہے، لیکن اس لین دین کے معاملے میں آپ کے والیوٹ (کھاتے) میں نوٹ نہیں آتے، کرنسی نہیں آتی، بلکہ کچھ ڈیجیٹل کوڈس آتے ہیں، اور یہی کوڈس آپ تک پہنچی ہوئی رقم ہوتی ہے۔

اب آپ کو بتاتے ہیں کہ بٹ کوئن کی اَرتھ ووستھا (پیسوں کے لین دین کی سہولت) کیسے کام کرتی ہے؟

پانچ سال پہلے تک ایک بٹ کوئن صرف ۶ روپے کا تھا، لیکن آج ایک بٹ کوئن ۴۵۰۰۰ روپے کا ہوگیا ہے، بٹ کوئن کی شروعات آج سے سات سال پہلے ۳ رجنوری ۲۰۰۹ء کو "ستوشی ناکا موتو" (SATOSHI NAKA MOTO) نام کے ایک پروگرامر نے کی تھی، لیکن آپ کو یہ بھی ہم بتادیں کہ ستوشی ناکا موتو کون ہے؟ یہ آج تک کسی کو نہیں پتہ، حالانکہ الگ الگ وقت پر، الگ الگ لوگ ستوشی ناکا موتو ہونے کا دعویٰ کرتے رہے ہیں، لیکن بٹ کوئن کے اصلی جنک (موجد) کے بارے میں ابھی بھی کسی کے پاس کوئی پختہ جان کاری نہیں ہے۔

ستوشی ناکا موتو نے جب بٹ کوئن کی شروعات کی تھی، تب ان کا مقصد اسے کرنسی میں بدلنا نہیں تھا، بلکہ ایسا صرف یہ ثابت کرنے کے لیے کیا گیا تھا کہ بنا کسی تھرڈ پارٹی کی مدد کے بھی آرتھک (پیسوں کا) لین دین کیا جاسکتا ہے، یعنی یہ سیدھے دو لوگوں کے بیچ بھی سنبھو (ممکن) ہے۔

۲۲ رمئی ۲۰۱۰ء کو پہلی بار ایک پیزا (Pizza) کے بدلے ۱۰ ہزار بٹ کوئن دینے کی پیشکش کی گئی تھی، یعنی تب ایک بٹ کوئن کی قیمت صرف دس پیسے تھی، یا دس پیسے سے بھی کم تھی، لیکن آج بٹ کوئن کی قیمت کئی ہزار گنا بڑھ چکی ہے، اس کے مارکیٹ میں آجانے کے بعد زیادہ سے زیادہ لوگ اب اسے خریدنے کی کوشش کررہے ہیں، اور بٹ کوئن کی قیمت لگاتار بڑھتی جارہی ہے۔

دنیا میں الگ الگ دیش ہیں، الگ الگ سنسکرتیاں ہیں، الگ الگ لوگ ہیں، الگ الگ بھاشائیں (زبانیں) ہیں، الگ الگ کھان پان اور الگ الگ طاقتیں ہیں، لیکن پوری دنیا میں ایک چیز ایسی ہے جو سب کو جوڑتی ہے، اور وہ چیز ہے پیسہ، آج لگ بھگ ہر کام کے لیے پیسوں کی ضرورت پڑتی ہے، چاہے وہ کھانا خریدنا ہو، پانی خریدنا ہو، گھر خریدنا ہو، ہتھیار خریدنا ہو، یعنی ہر چیز کے لیے پیسوں کی ضرورت ہوتی ہے، کئی لوگوں کی زندگی اس پیسے کو کمانے کے چکر میں خرچ ہو جاتی ہے، پیسے کے لیے لوگ محنت کرتے ہیں، سنگھرش (انتھک محنت) کرتے ہیں، اپرادھ (جرائم) کرتے ہیں، اور یہاں تک کہ لوگوں کا خون (قتل) بھی کر دیتے ہیں، لیکن کیا آپ نے کبھی سوچا ہے کہ یہ پیسے، یہ کرنسی، اور کاغذ کا وہ ٹکڑا جسے ہم نوٹ کہتے ہیں، اصل میں ہے کیا؟

دراصل جو کاغذ کا نوٹ آپ کی جیب میں ہے، وہ ایک طرح کا وعدہ ہے آپ کو کاغذ کے ٹکڑے پر لکھی گئی رقم کے چکانے کا، جب آپ یہ نوٹ کسی دکان دار کو دیتے ہیں، تو وعدے کا یہ کاغذ اس کے پاس پہنچ جاتا ہے، اور وہ دکان دار بدلے میں آپ کو سامان دے دیتا ہے، یعنی کاغذ کے اس نوٹ کا پورا مولیہ (قیمت/ویلیو) صرف وہ وعدہ ہے جو ریزرو بینک (RBI) نے آپ سے کیا ہے، لیکن جب کاغذ کے یہی نوٹ آپ بینک میں جمع کراتے ہیں، تو بینک اس میں سے ایک بڑی رقم دوسروں کو اُدھار دے دیتا ہے، جب کہ آپ کے اکاؤنٹ میں آپ اپنی جمع کرائی گئی رقم دیکھ پا رہے ہوتے ہیں، حالانکہ اصلیت میں وہ رقم وہاں ہوتی نہیں ہے، ادھار لینے والا ویکتی (شخص) اسی پیسے سے سامان خریدتا ہے، اور وہ پیسہ ایک بار پھر بینک میں پہنچتا ہے، بینک اس پیسے کو پھر ادھار کے طور پر دے دیتا ہے، اور اس پر بیاج بھی وصولتا ہے، اس طرح سے کاغذ کے ٹکڑے پر کیا گیا وعدہ ارتھ ویوستھا (پیسوں کے لین دین) کا سب سے بڑا وعدہ بن جاتا ہے، سچ یہ ہے کہ اگر تین پرتشت (فی صد) لوگ بھی بینکوں میں جمع اپنا پیسہ واپس مانگ لیں، تو بینکوں کے پاس دینے کے لیے کیش (نقد) ہوگا ہی نہیں، کیوں کہ وہ کیش یعنی آپ کے واسطے بینک کو سونپے گئے نوٹ ایک بڑی ارتھ ویوستھا (مالی لین دین) کا حصہ بن گئے ہیں، اور اس پوری ارتھ ویوستھا پر نیئنترن (قبضہ) ہے سرکاروں کا اور بینکوں کا، یعنی سرکار اور بینک کے ستھر (سطح) پر کوئی گڑبڑ ہو جائے، تو آپ کا پورا پیسہ ڈوب سکتا ہے، لیکن بٹ کوئن اسی خطرے اور بینکوں اور سرکار کے اسی نیئنترن (قبضہ) کو دور کرنے کی کوشش ہے۔

بٹ کوئن ایک ڈیجیٹل کرنسی ہے، اور ایک سافٹ ویئر ہے، بٹ کوئن انٹرنیٹ کی دنیا سے جڑے کمپیوٹرس کے ذریعے ونیمے (ادائیگی اجرت) کا نیا طریقہ ہے، بٹ کوئن ایک ایسی ڈیجیٹل کرنسی ہے جو اوپن سورس سافٹ ویئر پر آدھارت (قائم) ہے، جس کا اوشکار (ایجاد) ستوشی ناکاموتو نے کیا تھا، آج دنیا کے ہزاروں پروگرامر بٹ کوئن کے فیچرس کو زیادہ مضبوط اور محفوظ و سرکشت بنا رہے ہیں، جب ہم سامانیہ طور پر سادھارن کرنسی کا استعمال کرتے ہیں، تو اس کی دیکھ ریکھ کا ذمہ بینکوں کا ہوتا ہے، یعنی پیسہ کہاں سے چل کر ان کے پاس پہنچا؟ اس کا پورا ریکارڈ بینک اپنے پاس رکھتے ہیں، اور اس کے بدلے میں فیس کے نام سے اچھی خاصی رقم آپ سے وصولتے ہیں، اور بٹ کوئن پیسوں کے لین دین کے بیچ سے بینک اور مڈل مین کو ہٹا کر اسے زیادہ تیز اور محفوظ و سرکشت بنا دیتا ہے۔

اب سوال یہ ہے کہ ڈیجیٹل کرنسی کے ساتھ تو کافی چھیڑ چھاڑ کی جا سکتی ہے، یا پھر فلموں کی طرح اس کی پائریسی بھی ہو سکتی ہے، تو اس کا جواب ہے کہ ایسا تو سمبھو (ممکن) نہیں ہے، کیوں کہ ستوشی ناکاموتو کی اوشکار کی خاصیت یہ ہے کہ بٹ کوئن عام لوگوں کے بیچ بے باک چینج میں بھیجا جاتا ہے، جیسے بینک آپ کے پیسے کا حساب بکس اور مائنس میں رکھتے ہیں، ویسے ہی بلاک چینج میں ہر

ایک بٹ کوئن کا حساب رکھا جاتا ہے، یعنی دنیا میں کہیں بھی اور کبھی بھی ہوئے کسی بھی بٹ کوئن ٹرانزیکشن کا حساب ہمیشہ بلاک چینج میں موجود رہتا ہے، اور اس بلاک چینج میں سرکشت رکھنے والے لوگوں کو بھی لین دین پر نظر رکھنے کے لیے بلاک چینج کو سرکشت رکھنے کے لیے انعام کے طور بٹ کوئن دیے جاتے ہیں، کیوں کہ ہر ٹرانزیکشن کو ویری فائی کیا جاتا ہے، اور نیٹ ورک اس کا ریکارڈ رکھتا ہے، اس لیے اس میں دھاندلی نہیں کی جاسکتی، اسمت پیسہ (غیر قانونی کالا دھن) گھوٹالوں کو جنم دیتا ہے، اسکیمس کو جنم دیتا ہے، اور آرتھک مندی (پیسوں کے دیوالیہ) کی وجہ بھی بنتا ہے، کسی کو نہیں پتہ کہ اس وقت دنیا میں کتنے ڈالرس ہیں؟ لیکن اگلے ۱۲۵ ورشوں (سالوں) کے دوران بننے والے بٹ کوئنس کی سنکھیا (تعداد) ابھی سے نردھارت (طے) ہے، بینک کئی ایسے لوگوں کو پیسے ادھار دیتے ہیں جن کا ارادہ ہی واپس کرنے کا نہیں ہوتا، یہ لوگ یا تو خود کو دیوالیہ گھوشت (کنگال ہونے کا اعلان) کر دیتے ہیں، یا دیش چھوڑ کر چلے جاتے ہیں، اور اس کا خمیازہ عام آدمی کو ہی بھگتنا پڑتا ہے، لیکن ڈیجیٹل کرنسی پر کسی سرکار کے بینک کا نیئنترن (قبضہ) نہیں ہوتا، یہ ایک ایسی کمپیوٹر کوڈنگ ہے کہ اس کے ساتھ گھوٹالہ بھی نہیں کیا جاسکتا۔

بٹ کوئن کا سب سے زیادہ استعمال رے مینٹنس (حوالہ) کے شیکٹر (شعبے) میں بڑھ رہا ہے، رے مینٹنسیس اس رقم کو کہتے ہیں جو باہر رہنے والے اپنے دیشوں میں بھیجتے ہیں، رے مینٹنسیس حاصل کرنے کے معاملے میں بھارت دنیا کا نمبر ایک دیش (ملک) ہے، ۲۰۱۵ء میں ۴ لاکھ ۶۲ ہزار کروڑ روپے کی رقم رے مینٹس کی تھی، عام طور پر یہ رقم بینکوں کے ذریعے یا منی ٹرانسفر ایجنسیوں کے ذریعے بھیجی جاتی ہے، جس پر ۵ فی صد سے ۳۰ فی صد تک رقم وصول کی جاتی ہے، پوری دنیا میں منی ٹرانسفر پر اوسطاً ۱۰ فی صد کا چارج لگتا ہے، یعنی جو رقم باہر رہنے والے اپنے گھر بھیجتے ہیں اس میں سے اوسطاً ۴۶ ہزار کروڑ روپے اس فیس میں چکائے جاتے ہیں، جو بینکوں کے پاس جمع ہو جاتے ہیں۔

بٹ کوئن کا استعمال دنیا میں ہر دن بڑھ رہا ہے، دنیا کی ہزاروں کمپنیاں اب پیمنٹ کے لیے بٹ کوئن کو سویکار (قبول) کر رہی ہیں، آپ فون خریدنے سے لے کر ہوٹل بک کرانے، کار خریدنے، الیکٹرانک آئٹم خریدنے، یہاں تک کہ کافی خریدنے کے لیے بھی بٹ کوئن کا استعمال کر سکتے ہیں، لیکن ایسا نہیں ہے کہ بٹ کوئن کے ساتھ خطرے نہیں ہیں، سرکار کا نیئنترن نہ ہونے کی وجہ سے اس کرنسی کی ویلیو اوپر نیچے ہوتی رہتی ہے، لوگ غلط کاموں کے لیے ممنوعہ چیزیں خریدنے کے لیے بھی بٹ کوئن کا استعمال کر رہے ہیں، اور دنیا بھر کی کئی سرکاریں اور ریگولیٹرس اسے قانونی مانیتا (منظوری) دینے کے لیے تیار نہیں ہیں، لیکن بٹ کوئن کا سارا حساب وکتاب انٹرنیٹ پر موجود رہتا ہے، یعنی بٹ کوئن کالے دھن کی سمسیا (پریشانی) کو بھی سماپت (ختم) کر سکتا ہے، اور پیسوں کے لین دین میں نئے طریقوں کو متعارف کرا سکتا ہے۔ (بیورو رپورٹ زی میڈیا)

آخر بٹ کوئن یعنی ڈیجیٹل کرنسی کام کیسے کرتی ہے؟ اور بٹ کوئن نکلتے کہاں سے ہیں؟

تو آپ کو بتا دیں کہ بٹ کوئن کا آدان پردان (لین دین) پیئر ٹو پیئر (براہ راست ادائیگی) تکنیک (الیکٹرانک سسٹم) سے ہوتا ہے، یعنی یہ رقم ایک کمپیوٹر سے سیدھے دوسرے کمپیوٹر میں پہنچ جاتی ہے، لیکن اس لین دین کو سرکشت ومحفوظ بناتے ہیں وہ ہزاروں لوگ جو اپنے طاقت ور کمپیوٹرس کی مدد سے ان ٹرانزیکشن پر نظر رکھتے ہیں، اور ان کی جانچ کرتے ہیں، اور جو بھی شخص ایسی کامیابی حاصل کر لیتا ہے، اسے بطور انعام کچھ بٹ کوئنس دیے جاتے ہیں، اسے بٹ کوئن کی مائننگ (Mining) کہا جاتا ہے، دراصل کوڈ لینگویج میں ہونے والے اس

آدان پردان (لین دین) کو ویری فائی کرنے والے ہزاروں لوگ اس پر کریا (طریقۂ کار) میں بینک کے ایک کلرک (اجیر) کی طرح کام کرتے ہیں، اور انہیں مائنرس (Miners) کہا جاتا ہے، یہ لوگ ٹرانزیکشن پر نظر رکھتے ہیں تاکہ اس کا غلط استعمال نہ ہو، اس کے لیے ان مائنرس کو ایک میتھ میٹکل پرابلم (Mathmetical Problum) حل کرنی ہوتی ہے، جو مائنر جتنی جلدی یہ پرابلم سول (حل) کرتا ہے، اس کے بدلے اسے ساڑھے بارہ بٹ کوئن ملتے ہیں، اور اس طرح سے بٹ کوئن ڈیجیٹل بازار میں آجاتے ہیں، نیز بٹ کوئن کی تعداد ایک متعین وقت کے وقت گھٹ کر آدھی رہ جاتی ہے، شروعات میں ایک بلاک سے ۵۰ر بٹ کوئن نکالا کرتے تھے، ہر چار سال میں بٹ کوئن کی تعداد پر تی بلاک گھٹ کر آدھی رہ جاتی ہے، اس لیے آج سے ۱۲۵ر سالوں کے بعد یعنی ۲۱۴۰ر تک نئے بٹ کوئنس کا نرمان (مارکیٹ میں آمد) بالکل بند ہو جائے گا، شمار کے حساب سے تب تک دنیا میں ۲ر کروڑ ۱۰ر لاکھ بٹ کوئنس آچکے ہوں گے۔

بٹ کوئن مستقبل کی کرنسی ہے، اور مستقبل میں ختم بھی ہو جائے گی، اس لیے لوگوں میں زیادہ سے زیادہ بٹ کوئن خریدنے کی ہوڑ مچی ہوئی ہے، اس کا دارومدار ''ڈیمانڈ اینڈ سپلائی'' (Demand & Supply) پر ہے، بھارت میں ۲۰۱۵ء میں ایک بٹ کوئن کی قیمت ۱۴۰۰۰ر روپے تھی، جب کہ مئی ۲۰۱۶ء میں یہ بڑھ کر ۳۰۰۰۰ر روپے فی بٹ کوئن ہو گئی تھی، اور آج کے ریٹ کے حساب سے فی بٹ کوئن قریب ۴۵۰۰۰ر روپے ہیں۔ ایک اندازے کے مطابق ۲۰۱۸ء میں فی بٹ کوئن ۱۰ر ہزار ڈالر تک اس کی قیمت جا سکتی ہے، یعنی آج کے کرنسی ریٹ کے حساب سے ۶ر لاکھ ۶۸ر ہزار روپے۔

دنیا کی بڑی بڑی کمپنیاں اس کو استعمال کر رہی ہیں، کہ آگے چل کر نوٹ کی اہمیت و قیمت کم ہو جائے گی۔ اس وقت دنیا میں قریب ۸ر سو کروڑ موبائل فونس ہیں، جب کہ دنیا کی آبادی سات سو کروڑ ہے، اس کے برعکس دنیا میں ۲ر سو کروڑ لوگ ایسے ہیں جن کے پاس کوئی بینک اکاؤنٹ نہیں ہے، یعنی سبھی موبائل فونس والے بٹ کوئنس کا استعمال کرنے لگیں، تو یہ دنیا کی سب سے بڑی بینکنگ پرنالی بن جائے گی، جس میں کسی بھی سرکار یا ادارے کا دخل نہیں ہوگا، بہر حال سرکشت و محفوظ لین دین کا یہ طریقہ ہونے کے باوجود بٹ کوئن کے اپنے کئی خطرے ہیں، اس لیے بہت سارے دیشوں (ملکوں) نے ابھی تک بٹ کوئن کو قانونی مانیتا (منظوری) نہیں دی ہے۔ اس کے علاوہ اَن کرپٹیڈ (رشوت و دھوکہ دہی سے پاک) ہونے کی وجہ سے ڈرگس (Drugs) اور ہتھیاروں کی تسکری (اسمگلنگ/غیر قانونی سپلائی) کرنے والے مافیا اور دیگر اپرادھک (جرائم پیشہ) لوگ بھی لین دین کے لیے بٹ کوئن کا استعمال کر رہے ہیں، جو کہ خطرناک ہے۔

بٹ کوئنس کا بڑھتا استعمال دیکھ کر کہا جا سکتا ہے کہ آنے والے کچھ ورشوں (سالوں) میں دیوالی کی شام کو ہونے والی لکشمی پوجن (دولت کی پوجا) کا طریقہ بھی، ہو سکتا ہے بدل جائے، اور تب شاید لوگ اپنے کمپیوٹرس اور موبائل فونس پر بٹ کوئن کے وال پیپرس لگا کر اس کی پوجا کرنے لگیں۔ (بیورو رپورٹ زی نیوز Zee News India)

الغرض! ''بٹ کوئن'' (BitCoin) مستقبل کی ایک ایسی عالمی ڈیجیٹل کرنسی کے طور پر اُبھر رہی ہے، جس کا دارومدار ہی ''ڈیمانڈ اینڈ سپلائی'' (Demand & Supply) پر ہے۔ اور دنیا کی تمام بڑی بڑی نام ور کمپنیاں بھی پیمنٹ و لین دین کے لیے اسی کا سہارا لے رہی ہیں، لیکن چوں کہ اب تک اس ڈیجیٹل کرنسی کو کسی ملک نے باقاعدہ قانونی منظوری نہیں دی ہے، اس لیے کہ ہر ایک ملک کو اپنی کرنسی کے ڈاؤن ہونے اور گراوٹ کا خطرہ ہے، حتی کہ امریکہ جیسا سپر پاور ملک بھی اس کرنسی سے دہشت میں ہے۔

یہ ایک ایسی کرنسی ہے جس میں آپ مجبور نہیں بن سکتے، برخلاف لیگل کرنسی کے، کہ اس میں نوٹ بندی کے سرکاری اعلان کے بعد آپ ہاتھ میں پیسے ہوتے ہوئے بھی مجبور و لاچار ہو جاتے ہیں۔

یہ ایک ایسی کرنسی ہے جسے کوئی سرکاری ادارہ (بینک وغیرہ) کنٹرول نہیں کرتا۔ کسی تھرڈ پارٹی یا ایجنسی یا بینک کی اس میں سہارے کی ضرورت نہیں پڑتی۔ اس کرنسی کو ہر کوئی اپنے پاس محفوظ رکھ سکتا ہے، اور خود ہی اس کی جان کاری بھی رکھتا ہے۔ اس پر کم از کم (Minimum) کرنسی بھی ٹرانسفر کی جا سکتی ہے، اور زیادہ سے زیادہ بھی۔ اس پر چارج بھی بہت ہی کم (Very Cheap) لگتا ہے، برخلاف سرکاری اداروں اور بینکوں کے کہ وہاں چارج اور ٹیکس بہت زیادہ لگتے ہیں، جیسا کہ موجودہ سرکاری فیصلے بھی آ چکے ہیں کہ اے ٹی ایم سے چار مرتبہ ٹرانزیکشن پر 150 روپے چارج لگے گا، اور بھی دیگر چارجس وضع کیے جا رہے ہیں۔ نیز بٹ کوئن کے ذریعے اون لائن خریداری بھی کی جا سکتی ہے، من پسند اشیاء دنیا کے کسی بھی کونے سے انسان آرڈر دے کر منگوا سکتا ہے، اور بعض لوگ کہتے ہیں کہ اگر کوئی شخص بٹ کوئن کو لیگل کرنسی میں تبدیل کرنا چاہے، تو کر بھی سکتا ہے۔ الغرض! اس کرنسی کی ایجاد کا مقصد ہی یہ ہے کہ لین دین میں سرکاری اداروں اور بینکوں کے بوجھ سے بچا جائے، یعنی: نو بینک نو سرکار (No Bank No Govt)۔ ایک طرف جہاں لوگوں کے لیے اس میں سہولت ہے وہیں دوسری طرف فراڈ اور دھوکہ دہڑی کرنے والے، مافیا اور جرائم پیشہ افراد، اسی طرح بڑے بڑے سٹہ باز اور جواری و قماری لوگ اور بینک اکاؤنٹس ہیکرس و بلیک میلنگ کرنے والے لوگ بھی اس کے ذریعے اپنے کاروبار یعنی جرائم کو بڑھاوا دے رہے ہیں، جہاں ایک طرف کالے دھن سے نجات کے لیے اس طریقہ کار کو روبہ عمل لایا جا سکتا ہے، ایسے ہی کالے دھن کے ادخار میں یہ ممد و معاون بھی ہو سکتا ہے۔

خلاصہ بشکل سوال وجواب :

سوال: بٹ کوئن کیا ہے؟

جواب: بٹ کوئن ایک ورچوول کرنسی ہے، ایک کوموڈٹی، ایک کرپٹو کرنسی، ایک سافٹ ویئر، میڈیم آف ایکسچینج، اور سب سیٹ آف الیکٹرونک اینڈ ڈیجیٹل کرنسی ہے۔

سوال: بٹ کوئن کو کس نے بنایا؟

جواب: بٹ کوئن کو ۲۰۰۸، ۲۰۰۹ء میں ایک جاپانی انجینئر "ستوشی ناکاموتو" نے تخلیق کیا۔ بٹ کوئن کا مخفف BTC ہے، بٹ کوئن کی ویلیو آٹھ ڈیسیمٹ ڈیسمل پر مشتمل ہے، یعنی بٹ کوئن کو حسابی عمل میں یوں تحریر کیا جاتا ہے۔ 1. 00 00 00 00 بٹ کوئن کی چھوٹی سی چھوٹی اکائی۔ 0. 00 00 00 01 (یونٹ) کو "ستوشی" کہا جاتا ہے، جو اس کے خالق "ستوشی ناکاموتو" کے نام سے منسوب ہے۔

سوال: ہم بٹ کوئن کو کہاں کہاں اسٹور کر سکتے ہیں؟

جواب: بٹ کوئن کو جہاں جمع کر کے رکھا جاتا ہے، اسے بٹ کوئن والیٹ کہا جاتا ہے، سب سے پہلے ایسے والیٹ کی ضرورت ہے، جس سے آپ اپنا بٹ کوئن کا ایک یونیک اور انفرادی ایڈریس تخلیق کر سکیں، یعنی اپنا ایک بٹ کوئن ہیش، جیسے بٹ کوئن اسٹور جس پر آپ کے کمائے ہوئے تمام بٹ کوئن جمع ہوں گے۔ یہ چار قسم کے والیٹ ہوتے ہیں:

(۱)ویب والیٹ(Web Wallet)۔(آن لائن والیٹ)۔(۲)سافٹ ویئر والیٹ(Softwear Wallet)۔

(۳)پیپر والیٹ(Paper Wallet)۔(۴)ہارڈ والیٹ(Hard Wallet)/فزیکل بٹ کوئن)۔

ویب والیٹس(Web Wallets)صرف بٹ کوئن ہی نہیں، بلکہ کرپٹو کرنسی(Crypo Currency)کے تمام کوئنس کو، وصول کرنے، اسٹور کرنے، ان کو کسی اور کوئن/کرنسی میں ایکسچینج کرنے، یا کسی کو ٹرانسفر کرنے کے لیے استعمال کر سکتے ہیں۔ویب والیٹس مثلاً: TC.E.com Coinbase.com Cryptsy.com Bitcoin-central.net Bitstamp.net Bittrex.com وغیرہ۔(اس کے علاوہ اب USB شکل کی کچھ والیٹ ڈیوائس بھی مارکیٹ میں آچکی ہیں)

سوال: بٹ کوئن حاصل کرنے کے کون کونسے طریقے ہیں؟

جواب: بٹ کوئن کمانے کے پانچ طریقے ہیں:

(۱)فری سائٹس(Free Sites)سے۔(اس طریقہ میں مختلف فری ایسی سائٹس پر ایڈ دیو کرتے ہیں، جو اس ایڈ دیو کے بدلے ہمیں فری بٹ کوئن مہیا کرتی ہیں۔)

(۲)کرپٹو کرنسی(Crypto Currency)کی ٹریڈنگ(Trading)کے ذریعے۔(اس طریقہ میں مختلف کرپٹو کرنسی کو بٹ کوئن میں، اور بٹ کوئن کو دوسری کرپٹو کرنسی میں ایکسچینج کر کے بٹ کوئن کماتے ہیں۔)

(۳)فزیکل مائنر سے۔(اس طریقہ میں ہم اپنا خود کا مائنر خرید لیتے ہیں، اور خود مائننگ فارم اپنی بنا لیتے ہیں۔)

(۴)کلاؤڈ مائننگ کے ذریعے۔(اس طریقے میں ہم کلاؤڈ مائننگ فراہم کرنے والی کمپنیوں سے بٹ کوئن کی بدولت، بٹ کوئن مائنرز کی اسپیڈ خرید لیتے ہیں۔)

(۵)گیم لنگ کے ذریعے۔(اس طریقے میں بہت سارے ایسے گیم کھیلے جاتے ہیں، جن کی ونگ پرائز میں بٹ کوئن حاصل ہوتے ہیں۔)

سوال: بٹ کوئن کو کہاں کہاں استعمال کیا جا سکتا ہے؟

جواب: 10,000 یا 12,000 مرچنٹس ایسے ہیں جو اپنے کاروبار میں خرید و فروخت کے لیے بٹ کوئن کو قبول کرتے ہیں، ورڈ پریس، ایمازون، بٹ کوئن نریول، ریڈٹ، پے پال، ای بے وغیرہ، جن کا نام تفصیل میں موجود ہیں۔

ماہانہ 14.19% نئے مرچنٹس اس کرنسی کے استعمال میں شامل ہو رہے ہیں۔

دنیا کی کل 7 ملین آبادی میں سے ابھی تک 1.6 ملین لوگ ہی صرف بٹ کوئن کے مطابق جانتے ہیں۔

ماہانہ 5.46% نئے لوگ اس نظام کا حصہ بن رہے ہیں۔

ان کمپنیوں کے ناموں کی لسٹ جو BTC کو لین دین میں قبول کرتے ہیں، ان کی تفصیل جاننے کے لیے دیکھئے:

http://www.bitcoinvalues.net/who-accepts-bitcoins-payment-companies-stores-take-bitcoins.html

سوال: بٹ کوئن کمانے کا سب سے صحیح/تیز/محفوظ ترین طریقہ کون سا ہے؟

جواب: یوں تو بٹ کوئن کو کمانے/حاصل کرنے کے بہت سے طریقے ہیں، لیکن ایسا طریقہ جس میں ہماری انویسٹمنٹ محفوظ ہو، بٹ کوئن کی ارننگ انتہائی فاسٹ ہو، جو منافع بخش ہو، آسان ہو، بنام کام کیے ہو، وہ ہے اپنا بٹ کوئن مائنر لگا کر بٹ کوئن کی مائننگ کرنا۔ اس طریقہ میں ہم ایک مائننگ مشین خرید لیتے ہیں، اور اسے ایک انٹرنیٹ کی تار، اور بجلی کی تار سے منسلک کر دیتے ہیں، بنا ساتھ کوئی کمپیوٹر چلائے، یا لیپ ٹاپ لگائے بنا، یہ مشین بٹ کوئن بنانا شروع کر دیتی ہے، اور سیکنڈز کے حساب سے آپ کے بٹ کوئن مائن کر رہی ہوتی ہے، روزانہ کی بنیاد پر یہ خود بخود تمام اس دن کے بنائے بٹ کوئن کو آپ کے بٹ کوئن والیٹ میں ٹرانسفر کر دیتی ہے، اور آپ چاہیں تو روزانہ اسے کیش بھی کروالیں، یوں جو مشین آپ نے خریدی، وہ بطور انویسٹمنٹ آپ کا سرمایہ محفوظ ہے، اور آپ روزانہ کی بنیاد پر منافع حاصل کرتے رہیں۔

سوال: بٹ کوئن کو کیش کروانے کے کون کونسے طریقے ہیں؟

جواب: آج دنیا کے تقریباً تمام ہی ممالک میں اس وقت بٹ کوئن کو سرکولیٹنگ کرنسی (ملکی گردشی) کرنسی میں تبدیل کرنے کے لیے ایکسچینج بن چکی ہیں۔ اور تقریباً دنیا کے 20 ممالک ایسے بھی ہیں، جہاں بٹ کوئن کو حاصل کرنے کے لیے ATM مشین تنصیب ہیں۔ آپ بٹ کوئن کو دیگر درجنوں ڈالر میں بھی تبدیل کروا سکتے ہیں۔

کسی ایکسچینجر سے بھی آپ بٹ کوئن کے بدلے پاکستانی یا ہندوستانی کرنسی حاصل کر سکتے ہیں، یا پاکستانی و ہندوستانی کرنسی سے بٹ کوئن خرید سکتے ہیں۔ (بحوالہ تحریر من جانب ڈیبلو راجہ، Dablio Raja)

؟؟؟ استفتاء ؟؟؟

بٹ کوئن ڈیجیٹل کرنسی کے بارے میں مذکورہ تفصیلات پڑھنے کے بعد ذہن میں مختلف سوالات گردش کر رہے ہیں کہ:

(۱) مذکورہ ڈیجیٹل کرنسی کی شرعی حیثیت کیا ہے؟ کیا یہ لیگل (Legal) کرنسی شمار ہوگی؟ یا الٹرنیٹو (Alternative) کرنسی کہلائے گی؟

(۲) کیا مسلمان اون لائن اس ڈیجیٹل کرنسی کو مائن (Mine) کر سکتے ہیں؟

(۳) اگر کسی نے مائن (Mine) کر لیا، تو اب اس کو استعمال کیا جا سکتا ہے یا نہیں؟

(۴) اگر کسی نے اس کے ذریعے مارکیٹ سے اون لائن سامان کی خریداری کی ہے، تو اس کا کیا حکم ہوگا؟

(۵) اگر کوئی شخص اس کے ذریعے پیسہ کماتا ہے، تو کیا اس کا یہ عمل شرعاً درست ہوگا؟

(۶) بعض لوگ بطور دلالی کے اون لائن اس کا کاروبار چلا رہے ہیں، کیا یہ از روئے شرع جائز ہے؟

(۷) بعض لوگ اسے دجالی کرنسی کا نام دے رہے ہیں، اس لیے کہ اس کا موجد (ستوشی ناکاموتو) ابھی تک پردۂ خفا میں ہے، اور بہت قلیل مدت میں یہ کرنسی عالم پر چھا گئی ہے، جس کو فالو کرنے والی تمام بڑی بڑی انٹرنیشنل کمپنیاں بھی اکثر و بیشتر یورپی ممالک و امریکہ وغیرہ سے تعلق رکھتی ہیں، تو کیا اس کے پیچھے عالمی خفیہ دجالی طاقتوں کا ہاتھ ہو سکتا ہے یا نہیں؟

(۸) بھارت کی موجودہ سرکار نے ابھی گزشتہ دنوں نوٹ بندی کا بھیانک کھیل کھیلا، اور پھر اس کے بعد اچانک یہ اعلان کر دیا کہ اب "بھارت" بھی کیش لیس (Cash Lase) ہوگا، کئی جگہوں پر پے ٹی ایم (Paytm) کا طریقہ کار ادائیگی کے لیے

اپنایا جارہا ہے، جس سے یہی سمجھ میں آتا ہے کہ یہ بھی مذکورہ ڈیجیٹل کرنسی کی طرف بڑھتا ہوا ایک قدم ہے۔

(۹) اسی طرح عربی فتویٰ ویب سائٹ، مثلاً: ''اسلام ویب'' کے حوالہ سے ایک ویڈیو یوٹیوب پر اپلوڈ ہے، جس کا عنوان ہے:

'' الربح من الانترنت البيتكوين '' (الحكم الشرعي لتعدين البيتكوين) . جس کا ماحصل یہ ہے:

فقہی اصول: الأصل في المعاملات الإباحة والجواز لا التحريم . کے پیش نظر کہا کہ: فهذا لا شك في جـــوازه . موصوف نے کلاؤڈ مائننگ (Cloud Mining) کو اجارہ کے حکم میں کہہ کر جائز قرار دیا۔ اجرت معلوم ہے جو ثمن طاقہ ہے، اور طرفین راضی ہیں، کہا: فالعقد جائز ولا حرج فيه . نیز کہا کہ اس کو بیع وشراء کا معاملہ بھی قرار دیا جاسکتا ہے، اس اعتبار سے بھی یہ جائز ہے۔

ویڈیو میں موصوف محترم نے اشیاء میں اصل اباحت کا قاعدہ یا اصول تو بیان کردیا، لیکن اس اصول کی تفصیل پر بالکل توجہ نہ دی، کہ اگر اشیاء میں اصل اباحت ہو، اور حرمت کا شبہ پیدا ہوجائے، اور وہ شبہ ناشی عن دلیل بھی ہو، تو اب اس شبہ کے نتیجے میں اس مباح کا ترک کیا جائے گا یا نہیں؟ قطع نظر اس کے کہ ترک مباح واجب ہوگا یا مستحب، جب کہ تقویٰ بھی اس کے ترک کا متقاضی ہو۔ اب موصوف محترم کے ویڈیو کا کیا جواب دیا جائے گا؟ (ع۔م)

(۱۰) اور بھی دیگر عربی فتاویٰ وتحریریں دیکھنے کے بعد معلوم ہوا کہ علمائے عرب کے نزدیک بٹ کوئن کی حیثیت لیگل کرنسی (Legal Currency) کی ہے، اس لیے وہ اس پر بیع صرف کے احکام جاری کرتے ہیں، مثلاً اسلام ویب پر موجود، بٹ کوئن سے متعلق پوچھے گئے ایک سوال کے جواب سے یہی معلوم ہوتا ہے، مزید جان کاری کے لیے عربی فتویٰ وتحریر کی کماحقہٗ عبارات نقل کی جاتی ہیں، ان عربی تحریروں کے بارے میں از روئے شرع ارباب دارالافتاء کا کیا خیال ہے؟ براہ کرام مطلع فرمائیں!

حكم شراء وبيع العملات الإلكترونية (بيتكوين) وحكم عملية التنقيب

(۱) " **السؤال**: أود أولا أن أشكركم على مجهوداتكم ، ونسأل الله عز وجل أن يجعلها في ميزان حسناتكم . منذ خمس سنوات ظهرت عُملة جديدة اسمها البيتكوين ، وهي عملة الكترونية – عملة تشفيرية – يمكن مقارنتها بالعملات الأخرى ، مثل : الدولار ، أو اليورو ، لكن مع عدة فوارق أساسية ، من أبرزها أن هذه العملة هي عملة الكترونية بشكل كامل تتداول عبر الانترنت فقط من دون جود فيزيائي لها ، وتقوم بيتكوين على التعاملات المالية ، وتستخدم شبكة الند للند ، والتوقيع الالكتروني ، والتشفير بين شخصين مباشرة دون وجود هيئة وسيطة تنظم هذه التعاملات ، حيث تذهب النقود من حساب مستخدم إلى آخر بشكل فوري دون وجود أي رسوم تحويل ، ودون المرور عبر أي مصارف ، أو أي جهات وسيطة من أي نوع كان ، وهذه الخدمة متوفرة على مستوى العالم ، ولا تحتاج لمتطلبات ، أو أشياء معقدة لاستخدامها ، وعند الحصول على العملات يتم تخزينها في محفظة الكترونية ، ومن الممكن استخدام هذه العملات في أشياء كثيرة ، منها شراء الكتب والهدايا ، أو الأشياء المتاح شراؤها عن طريق الانترنت ، وتحويلها لعملات أخرى ، مثل : الدولار ، أو اليورو ، بالإضافة إلى شراء المنتجات ، ويستطيع المستخدم تبديل قطع بيتكوين النقدية الموجودة لديه بعملات أخرى حقيقية ، وعملية التبديل هذه تتم بين المستخدمين أنفسهم الراغبين في بيع مبالغ بيتكوين ،

وشراء عملات حقيقية مقابلها ، أو العكس ، ونتيجةً لذلك تمتلك بيتكوين سعر صرف خاص بها ، ويرتفع هذا السعر ، إذ يصل اليوم إلى ٦٠٠ دولار بعد أن كانت تعادل بضعة دولارات فقط قبل عامين ، وعلى عكس العملات التقليدية التي عادةً ما تكون مدعومة بأصول معينة ، مثل : الذهب أو العملات الأخرى ، فإن بيتكوين يتم دعمها وانتاجها من المستخدمين أنفسهم ، ويقصد بالمستخدمين أي مستخدم يرغب في التعامل مع بيتكوين ، ويمتلك جهاز كمبيوتر ، واتصال بالانترنت ، ويتم هذا من خلال عملية تُدعى : التنقيب – وهو عبارة عن تطبيق خاص يقوم المستخدم بتثبيته على أي جهاز كمبيوتر بحيث يقوم التطبيق بعملية إنتاج عملات بيتكوين جديدة ، وبشكل بطيء ، ويستطيع المستخدم من خلال هذه العملية الحصول على قطع بيتكوين النقدية الافتراضية مقابل استخدام التطبيق للقدرة الحسابية التي يقدمها معالج جهاز الكمبيوتر الخاص بالمستخدم في توليد كميات جديدة من العملة ، وعندما يتم توليد مجموعة جديدة من القطع النقدية لدى كل مستخدم ، يتم توزيع هذه المبالغ وفق خوارزمية معينة بحيث لا يمكن أن تصل القيمة الكلية لعملات بيتكوين الموجودة في السوق لأكثر من ٢١ مليون بيتكوين ، كما يحصل المستخدمون أصحاب قوة المعالجة الأعلى على حصة أكبر تتناسب مع مدى إنتاج أجهزتهم من العملات ، ومنذ أسبوعين أقوم بعمليات التنقيب ، وأحصل على أجر مقابل ذلك ، فهل عملية التنقيب حلال أم حرام؟ وهل يجوز لي شراء عملة البيتكوين بثمن وبيعها عند ارتفاع ثمنها ؟

الإجابة : الحمد لله ، والصلاة والسلام على رسول الله ، وعلى آله وصحبه ، أما بعد : فمن ملك شيئًا من تلك النقود الالكترونية بوسيلة مشروعة ، فلا حرج عليه في الانتفاع بها فيما هو مباح ، فقد بينا في فتوى سابقة أن لعملة الرقمية ، أو النقود الالكترنية عملات في شكل الكتروني غير الشكل الورقي ، أو المعدني المعتاد ، وعلى ذلك فشراؤها بعملة مختلفة معها في الجنس ، أو متفقة يعد صرفًا ، ولا بد في الصرف من التقابض ، والتماثل عند اتحاد الجنس ، والتقابض دون التماثل عند اختلاف الجنس ، والقبض قد يكون حقيقيًا ، وقد يكون حكميًا ، كما بينا في الفتوى رقم : ٢٣١٣٦٠ . وعلى كل فالتنقيب أو انتاج تلك العملة وفق ما هو مأذون فيه دون غش ، أو تحايل لا حرج فيه ، وللفائدة انظر الفتوى رقم : ١١٠٧٣ . وإذا جاز عمل التنقيب جاز أخذ الأجرة عليه . والله أعلم .

(اسلام ويب : حكم شراء وبيع العملات الالكترونية (بيتكوين) وحكم عملية التنقيب ، رقم الفتوى : ٢٥١١٧٠)

حكم الكسب عن طريق التجارة بالعملة الإلكترونية (بيتكوين)

(٢) " **السؤال**: ما حكم ربح البيتكوين العملة الرقمية من مواقع تعمل بهذا الشكل الآتي :

هناك مواقع تعطي كمية من العملة البيتكوين ، وهذه العملة رقمية كل ١ بيتكوين يساوي ٢٣٠ دولارًا ، وهي تعطي في اليوم ما يقارب ١ دولارًا ، ويمكن ربح العملة عن طريق الدخول إلى أحد المواقع كل فترة زمنية معينة ، والحصول على كمية من عملة البيتكوين ، لكن هناك بعض المواقع تعطي البيتكوين على شكل معينة من البيتكوين . علمًا أنني لا أدفع شيئًا من المال ؛ لأن تلك المواقع تقدم البيتكوين مجانًا من أجل الحصول

على زوار لمواقعها ، والربح من الإعلانات التي تضعها . فهل هناك شيء محرم ؟

الفتوى : الحمد لله ، والصلاة والسلام على رسول الله ، وعلى آله وصحبه ، أما بعد :

فقد سبق لنا بيان أن الربح بمثل هذه الطريقة لا يظهر لنا فيه حرج ، بشرط كون الاشتراك بها مجانيًا دون مقابل ، وأن يكون محتوى الصفحات والإعلانات مباحًا ، كما سبق في الفتوى : رقم : ٢٩٣٨٩٦ . وراجع للفائدة حول البيتكوين الفتوى رقم : ٢٥١١٧٠ . والله أعلم .

(مترك ويب بحواله اسلام ويب ، حكم الكسب عن طريق التجارة بالعملة الإلكترونية [بيتكوين])

هل تداول بيتكوين أوتعدينه حلال أم حرام ؟

(٣) يوجد العديد من الأشخاص لديهم ارتياب كبير من البيتكوين خصوصًا انها تقنية جديدة عمرها أقل من ست سنوات . وأغلب استفسارات تصب في نطاق واحد هل البيتكوين حلال أم حرام ؟ . توجد فتاوى من موقع موثوق ومحترم عن البيتكوين ، وشرعية تداوله أو تعدينه .

الفتوى الأولى بخصوص التعدين السحابي .

http://fatwa.islamweb.net/fatwa/index.php?page=showfatwa&Option=Fatwaid&Id=276679

الفتوى الثانية بخصوص التعامل بالعملات الرقمية بصفة عامة .

http://fatwa.islamweb.net/fatwa/index.php?page=showfatwa&Option=Fatwaid&Id=251170

هذه فتاوى من موقع جد موثوق . وإذا كان لديكم أي فتاوي رسمية من جهات رسمية كالأزهر أو وزارة أوقاف في أحد الدول العربية أن يقوم بوضعها هنا حتى نزيل هذا اللبس بالنسبة للأعضاء اللذين لديهم شكوك حول العملة الرقمية . تحياتي لكم .

هل تعدين الذهب أو التنقيب عن الذهب حلال أم حرام ؟

هل الاتجار بالذهب والفضة حلال أم حرام ؟

هل استخدام الانترنت حلال أم حرام ؟

هل الاتجار بالنفط حلال أم حرام ؟

هل بيع النفط من خلال العقود حلال أم حرام ؟

هل استخدام العقود التجارية والتراسل المالي عبر الانترنت حلال أم حرام ؟ ما الجواب ؟؟

ما يقاس شرعًا على ما ورد أعلاه ، لا بد أن يقاس على هذه العملة الإلكترونية نفس القواعد والضوابط الشرعية المنطبقة على وارد أعلاه ، أعتقد تصلح للتطبيق على العملة الإلكترونية خصوصًا أنها لا تختلف عن العملة الورقية إلا بما يلي .

١ – عملة لا مركزية ، لا يوجد جهة حكومية أو غيرها تسيطر على انتاجها . (موجودة في العالم الافتراضي بانتظار شخص ما أو هيئة ما تقوم باستخراجها والانتفاع بها) .

٢ – عملة تستخدم أساسًا في التعاملات الرقمية (أي في عالم الانترنت الافتراضي) . مثلها مثل العقود التجارية

٣- لا وجود فيزيائي لها (أوراق .. مثال الدولار فمعنى ما أرادت على سبيل المثال الحكومة الأميركية واحتاجت لسيولة ، فإنها تستطيع طباعة أوراق اسمها دولار ! لا وجود فيزيائي له ولكن تم Maktoob وتسييلها في الأسواق) للتذكير فقط : موقع بيعه لياهو بعدة ملايين كثيرة ! وهو عبارة عن كود برمجي ..... وكل بتكوين ! عبارة عن كود برمجي فريد من نوعه . ..... إذا ما الفرق ؟؟؟

عودة بنا إلى الأحكام الشرعية : فطالما أنها تستخدم من خلال الأوجه الشرعية في عمليات البيع والشراء ، طالما أنه لا يتم استغلالها في عقود ربوية أو تخزينها في بنوك ربوية أو شراء ما هو غير شرعي بها !! وطالما أن ذلك يعود لمن يستخدمها ، فتغدو إذا طريقة الاستخدام وما يتبعها من ضوابط شرعية هي الحكم في حلالها أو حرامها .

ولأن العديد يسأل عن شرعيتها ، فإن الأحق أن نسأل عن شرعية أوراق العملة المتداولة ! لأن الأصل في العملة هما الذهب والفضة ، والباقي قد يعامل على أنه من الممكن أن يتم مقايضتها ، أو يبيعها Assets أصول .

والعديد من الخبراء الاقتصاديين والذين هم على دراية وعلم بماهية ونظام البتكوين يعتبرونها أصل من الأصول يمكن مقايضتها ، مثلها مثل الذي يشتري أو يصمم برنامج ما ، ومن ثم يقرر أن يبيعه أو يبادله بشيء آخر . لأنها محدودة في الانتاج ، لها كمية ثابتة لن تتجاوزها ، وهي تعتبر أصل كل جزء مكون لواحد بتكوين عبارة عن كودات برمجية فريدة غير متشابهه ولكنها متسلسلة ... ولن تتشابه لأنه لو حصل ذلك لتم تزويرها ونسخها . أرجو أن لا يفهم كلامي على أنه فتوى ، ولكن يؤخذ به عند محاولة تفسير نظام البتكوين لأصحاب العلاقة الذين هم أقدر على إصدار فتوى . هذا ما عندي يا أصدقائي ، فإن أحسنت فمن الله ، وإن أسأت أو أخطأت فمن نفسي . والله أعلم . (askbitcoiner.com)

نوٹ:- بٹ کوئن کی مزید تفصیل جاننے کے لیے "بٹ کوئن وکی پیڈیا" سرچ کیجیے! اور عرب علماء کے نزدیک حکم شرعی کی مزید تفصیل کے لیے اون لائن ویب سائٹس پر "الحكم الشرعي لتعدين البيتكوين" لکھ کر سرچ کیجیے!

نیز بٹ کوئن سے متعلق اس تحریر میں ممکن ہے کچھ نقص وکوتاہی ہو، یا معلومات میں کچھ کمی ہو، تو حضرت والا سے عاجزانہ ومؤدبانہ درخواست ہے کہ ماہرین سے جان کاری کے بعد صحیح صورتِ حال اور اس کے حکم شرعی سے آگاہ فرمانے کی زحمت برداشت کی جائے گی، کہ لوگوں کی ایک کثیر تعداد صحیح صورتِ حال اور حکم شرعی کی منتظر ہے۔ ہم آپ کے نہایت مشکور وممنون ہوں گے۔

فجزاكم الله أحسن الجزاء ، وبارك الله في حياتك ، وأطال الله بقاءك علينا ! آمين يا رب العالمين !

﴿راقم ومستفتي : عبد المتين اشاعتي كانڑ گاؤں ، اورنگ آباد ، مهاراشٹر ، الهند﴾

الجواب وباللہ التوفیق :

اصل جواب سے پہلے لیگل کرنسی (زرِ قانونی/نوٹ) کی مختصر تاریخ بیان کرنا مناسب معلوم ہوتا ہے:

اللہ پاک نے لین دین کے لیے خلقۃً سونا چاندی کو پیدا فرمایا، ایک زمانہ تک اسی کے ذریعے سے لین دین ہوتا رہا، پھر سناروں کا سونا اپنے پاس رکھ کر اس کے بدلے رسید جاری کرنے لگے، جس کی پشت پر سونا ہوتا تھا، ہوتے ہوتے یہ رسید کاروبار

میں بنیادی حیثیت اختیار کرگئی، جب حکومتوں نے دیکھا کہ نجی ادارے رسیدیں جاری کررہے ہیں، تو اس نے قانون بنادیا کہ اب نجی بینکوں کو یہ نوٹ یا رسید جاری کرنے کا حق نہیں ہے، صرف حکومت کا بینک ہی نوٹ جاری کرسکتا ہے، ابتداء میں بینکوں پر لازم تھا کہ وہ جتنے نوٹ جاری کرتے ہیں ان کے پاس اتنا سونا ہونا ضروری ہے، لیکن بعد میں یہ قانون ختم کردیا گیا اور یہ کہا گیا کہ پورا سونا ہونا ضروری نہیں، لیکن ایک خاص تناسب سے سونا ہونا چاہیے، یعنی جتنے نوٹ جاری کیے ہیں، اُن کا مثلاً دو تہائی سونا ہونا چاہیے، بعد میں دو تہائی کو کم کرکے ایک تہائی کردیا، ایک چوتھائی کردیا، نسبتیں بدلتی چلی گئیں، یہاں تک کہ ایک وقت ایسا آیا کہ ساری دنیا کے ملکوں کے پاس سونا کم ہوگیا، صرف امریکہ ایک ایسا ملک تھا جس کے پاس سونا وافر مقدار میں موجود تھا، اب جن ممالک کے پاس سونا کم تھا اور نوٹ زیادہ جاری ہوگئے تھے، انہوں نے یہ سوچا کہ ہمارے پاس اتنا سونا تو نہیں ہے، کہ ہم ہر حامل نوٹ کو جو بھی آئے اس کو سونا ادا کریں، اس واسطے انہوں نے آپس میں یہ طے کرلیا کہ اگر ہم کسی وقت یہ سونا ادا نہ کرسکے، تو سونے کے بدلے ہم امریکی ڈالر ادا کریں گے، اور امریکہ یہ کہتا تھا کہ چوں کہ میرے پاس سونا وافر مقدار میں موجود ہے، لہٰذا میں اپنی یہ ذمہ داری قبول کرتا ہوں کہ میرے پاس جو بھی ڈالر لے کر آئے گا، میں اس کے بدلے سونا دوں گا، تو صورت ایسی تھی کہ دنیا کے سارے ممالک نوٹ کی پشت پر ڈالر رکھتے تھے، اور ڈالر کی پشت پر سونا تھا، تو جب ڈالر کی پشت پر سونا ہوا، تو بالواسطہ ان نوٹوں کی پشت پر سونا ہوا، پہلے بلاواسطہ ہوا کرتا تھا، اب بالواسطہ ہوگیا۔ پھر ۱۹۷۱ء میں ایسا ہوا کہ امریکہ میں سونے کا شدید بحران آیا، لوگوں نے محسوس کیا کہ سونے کی کچھ کمی ہورہی ہے، تو امریکہ کے بینکوں کے پاس ہجوم لگ گیا، جس کو دیکھو ڈالر لے کر جارہا ہے، کہ مجھے سونا دو، ہزاروں اور لاکھوں افراد بیک وقت جاکر امریکی بینکوں کے پاس اکٹھے ہوگئے اور کہنے لگے کہ ڈالر کے بدلے سونا دو۔ امریکہ نے محسوس کیا کہ اس طرح تو سونے کے ذخائر ختم ہوجائیں گے، اور میں قلاش ہوجاؤں گا، جو سونا میرے پاس ہے وہ جاتا رہے گا، چنانچہ اس بحران کے موقع پر امریکہ نے بھی یہ اعلان کردیا کہ میں بھی سونا نہیں دیتا، جو چاہو کرلو، اب ڈالر کے بدلے سونا نہیں دوں گا، البتہ جس کے پاس ڈالر ہے وہ اس کے ذریعے بازار سے جو چیز چاہے خریدے، سونا خریدے، چاندی خریدے، لیکن میں سونا دینے کا پابند نہیں ہوں، تو ۱۹۷۱ء میں نوٹ کی پشت پر سے سونا بالکل ختم ہوگیا۔ اب اس کی پشت پر بالواسطہ یا بلاواسطہ سونا نہیں ہے۔ اب اس نوٹ کی حقیقت صرف یہ ہے کہ اس نوٹ میں اتنی طاقت ہے کہ اس کے ذریعے بازار سے کچھ چیزیں خریدی جاسکیں، اور جس ملک کا نوٹ ہے، اسی ملک کے بازار میں خرید سکتے ہیں، باقی دنیا کے کسی ملک میں بھی اب اس کی پشت پر سونا چاندی نہیں ہے۔ (۱)

الغرض! ملکی کرنسی ترقی کرتی گئی اور آج کل اس کے پس پشت سونے کے بجائے ملکی اقتصادیات وصناعات ہوگئیں، ہر ملک کی حکومت اور بینک یہ طے کرتا ہے کہ پورے ملک میں کتنی کرنسی کا اجراء ہو، حکومت اور بینک اس کرنسی اور نوٹ کے حامل شخص سے یہ وعدہ کرتے ہیں کہ وہ اسے اس نوٹ یا کرنسی کے بقدر عین مال دینے کی مکلف وپابند ہے، حکومت اور بینک کے اس وعدہ کی وجہ سے ان کرنسیوں اور نوٹوں میں قوتِ خرید یعنی مالیت پیدا ہوتی ہے، اگر ملک یا بینک کی طرف سے یہ وعدہ نہ ہو، تو یہ کاغذی نوٹ کاغذ کے پُرزے کے سوا کچھ بھی نہیں، جب کہ بٹ کوئن نہ کاغذی نوٹ ہے، اور نہ ہی اس کے پس پشت کسی ملک کی حکومت یا بینک موجود ہے، جو اس کے مالک سے اس طرح کا کوئی وعدہ کرتی ہو، یہ محض ایک "تصوراتی دنیا کی تصوراتی کرنسی" (ڈیجیٹل دنیا کی ڈیجیٹل کرنسی) ہے، جب کہ لین دین کے لیے مال یا ذمہ (عین یا دین) کا ہونا ضروری ہے، جیسے نقد لین دین کی صورت میں جانبین کی

طرف سے مال ہوتا ہے، یا اُدھار لین دین کی صورت میں ایک جانب مال اور دوسری جانب ذمہ ہوتا ہے، جو مبیع یا ثمن کی ادائیگی کا مکلف و پابند ہوتا ہے، یعنی سلم ونسیئہ۔ جب کہ بٹ کوئن میں یہ صورت نہیں پائی جاتی، اس لیے کہ بٹ کوئن فی نفسہٖ نہ ذہب وفضہ (سونا چاندی) کے قبیل سے ہے، اور نہ اس کے پس پشت کسی حکومت یا بینک کا ذمہ ہے۔ (موجودہ دور کے بعض فقہاء نے نوٹ کو حوالہ یعنی مال کی رسید مانا ہے۔ علماء عرب نوٹ وغیرہ کو سونا چاندی کے قائم مقام مانتے ہیں۔ اور اکثر و بیشتر علماء برصغیر اسے فلوس نافقہ میں شمار کرتے ہیں۔ (۲)

بٹ کوئن ودیگر الٹرنیٹیو کرنسیس کی خرابیوں کا جائزہ:

اس تمہید کے بعد اب ہم بٹ کوئن سے متعلق تحصیلی جان کاری کا شرعی جائزہ لیتے ہیں:

۱- اس کرنسی کے حصول میں جوا اور سٹہ کا دخل ہے کہ اگر رسک لیں تو سکسیس فل (کامیاب) ورنہ ستوشی ضائع ہوں گے، اور اگر رسک نہ لو، تو کچھ بھی کما نہیں پائیں گے، یعنی کامیابی وناکامی دونوں پہلو بہم ہیں، اسی کو قمار اور سٹہ کہتے ہیں، جو شرعاً ممنوع ہے۔ (۳)

۲- بٹ کوئن وغیرہ کرنسیس محض تصوراتی دنیا کی تصوراتی کرنسیس ہیں، کاغذی نوٹ وکرنسی کی طرح ان کا کوئی وجود نہیں ہے، نیز ہر ملک کی کرنسی کے پیچھے اس ملک یا بینک ادارے کا وعدہ ہوتا ہے، اس کرنسی کا نہ کوئی ملک ہے اور نہ کوئی بینک ادارہ، جو اس کے پس پشت رہ کر وعدہ پورا کر سکے، اس لیے اس کو ثمن عرفی بھی نہیں کہا جا سکتا، بلکہ یہ صرف تصوراتی کرنسی ہے۔ (۴)

۳- ہر ملک کی کرنسی کا اجرا اُس کی حکومت کی طرف سے ہوتا ہے، اور حکومت یا بینک کی طرف سے اس کرنسی کے پس پشت لین دین میں ادائیگی کا وعدہ ہوتا ہے، جب کہ بٹ کوئن کے ذریعے لین دین میں آپ کے والیوٹ (کھاتے) میں نوٹ یا کرنسی نہیں آتی، بلکہ کچھ ڈیجیٹل کوڈس آتے ہیں، جو آپ تک پہنچی ہوئی رقم ہوتی ہے، بالفرض اگر ڈیجیٹل کوڈس میں غلطی ہو جائے، یا کوئی الیکٹرانک مشین خراب ہو جائے، تو پھر اس کی کیا گارنٹی ہے کہ وہ ضائع نہ ہوں گے۔ (۵)

۴- اس تصوراتی کرنسی کا موجد بھی نامعلوم ومبہم شخص ہے، اس لحاظ سے بھی یہ کرنسی کہلائی جانے کے لائق نہیں ہے۔

۵- اس کرنسی پر کسی سرکار کا قبضہ نہیں ہے، اس کرنسی کی ویلیو کم زیادہ ہوتی رہتی ہے، لوگ غلط کاموں کے لیے ممنوعہ چیزیں خریدنے کے لیے بھی بٹ کوئن کا استعمال کر رہے ہیں، نیز اب تک دنیا کی کسی ملکی حکومت نے اس ڈیجیٹل کرنسی کو سرکاری منظوری نہیں دی ہے، یعنی اس کرنسی کے پس پشت کسی کا کوئی وعدہ نہیں ہے، اس لحاظ سے بھی یہ تصوراتی کرنسی اطمینان بخش نہیں ہے۔

۶- مستقبل میں کچھ سالوں کے بعد یہ کرنسی بالکل بند ہو جائے گی، جب کہ لین دین بین تو حاجات ناس میں سے ہے، اور جب تک دنیا باقی ہے، حاجات ناس کا تحقق ہوتا رہے گا، جس کے لیے کرنسی کی ضرورت پڑتی رہے گی، اور یہ کرنسی جب بند ہو جائے گی، تو پھر حاجات ناس کس ذریعے سے پوری ہوں گی؟

۷- لیگل کرنسی (Legal Currency) میں سرکاری یا نجی اداروں کی طرف سے وعدہ کی بنیاد پر اون لائن ادائیگی کی جاتی ہے، اون لائن کیش پیمنٹ (On Line Cash Payment) کا انتظام ہوتا ہے، لیکن اس میں صرف وہی لوگ

ہوتے ہیں، جو یا تو تعلیم یافتہ ہوتے ہیں یا سرکاری و نجی اداروں کے ملازم ہوتے ہیں، اور جو عوام ہیں وہ یا تو تعلیم یافتہ نہیں کہ اون لائن وعدہ کی ہوئی لیگل کرنسی کا لین دین کر سکیں، یا پھر تعلیم یافتہ ہیں مگر ان کے پاس وہ الیکٹرانک آلات (کمپیوٹر، انڈرائڈ موبائل فون اور انٹرنیٹ کے استعمال کے ذرائع) موجود نہیں ہوتے، جن سے وہ اپنی ضروریات پوری کر سکیں، ظاہری بات ہے ان تمام صورتوں میں حرج لازم آتا ہے، جب کہ الٹرنیٹو کرنسی کا استعمال صرف آن لائن ہی ہوتا ہے، حقیقت میں اس کا کوئی وجود نہیں، نہ اس کے پیچھے کسی سرکاری یا نجی ادارے کا وعدہ ہے، تو پھر اس میں تو حرج عظیم لازم آئے گا، اور لوگوں کی زندگی قفل کا شکار ہو کر رہ جائے گی، بلکہ اس دنیا میں جینا ہی دوبھر ہو جائے گا، اس لحاظ سے بھی بٹ کوئن (BitCoin) وغیرہ کرنسیس میں عدم تحفظ انسانیت کا احساس ہوتا ہے۔[۶]

اگر کوئی یہ سوال کرے کہ غیر تعلیم یافتہ ہوں یا غیر مستطیع ہوں، تو ان کے لیے اس کرنسی پر عمل درآمد کا ایک راستہ اور ہے، وہ یہ کہ جن کے پاس یہ سب سہولیات نہ ہوں، وہ ان سہولیات والوں سے رابطہ کریں، لیکن کیا ہر جگہ یہ سہولیات والے اشخاص میسر ہو جائیں گے، ابھی ماضی قریب میں ہندوستانی سرکار نے لیگل کرنسی پر پابندی لگائی، تو دیہات والوں اور غریب کسانوں کو کتنی پریشانیوں، تکلیفوں اور دقتوں کا سامنا کرنا پڑا، حتی کہ جن لوگوں نے دوسروں کے اکاؤنٹس میں پیسہ جمع کروایا، انہیں سرکاری حکام اور جمع کرنے والے حضرات ہر دو کی طرف سے ذہنی و دماغی اذیتوں کا سامنا کرنا پڑا، ہر طرح سے عوام و خواص کو بڑی بے دردی و بداخلاقی کے ساتھ کرنسی کی بندش میں روندا گیا، جب لیگل کرنسی (Legal Currency)، جس کو ہم اطمینان بخش سمجھتے ہیں، اس کا یہ حال ہے، تو پھر الٹرنیٹو کرنسی (Alternative Currency) جس کے پس پشت کوئی سرکار وغیرہ نہیں، اس میں عوام وغیرہ کا کیا حال ہوگا؟ یہ سمجھنے میں دیر نہیں لگتی۔

پوچھے گئے سوالوں کے جوابات

مختصر تمہید اور بٹ کوئن کی تفصیل سے متعلق شرعی جائزہ کے بعد اب پوچھے گئے سوالات کے جوابات حکم اجتماعی (سد ذرائع) کے طور پر دیے جا رہے ہیں:

(۱) جی نہیں! اسے لیگل کرنسی (Legal Currency) نہیں کہیں گے۔

(۲) مائن (Mine) نہیں کر سکتے۔

(۳) جتنے بٹ کوئن (BitCoin) ہیں، انہیں استعمال کر کے، کسی تدبیر سے اس معاملہ سے نکل جائے۔

(۴) جو سامان خریدا گیا شرعاً وہ حلال ہوگا۔

(۵) جو معاملہ غرر و خطر کا ہو، اس کا کرنا شرعاً درست نہیں ہے۔[۷]

(۶) دلالی کی آمدنی حلال ہے۔[۸]

(۷) ممکن ہے۔

(۸) جی ہاں! لیکن یہ قدم صحیح نہیں ہوگا۔

(۹-۱۰) بعض عربی ویب سائٹس پر، فقہی اصول " الأصل في الأشياء الإباحة " کا سہارا لے کر، اس کرنسی کے جواز کا فتویٰ دیا گیا، لیکن کسی بھی چیز کے جواز کے لیے محض اس کی اباحت کافی نہیں ہوتی ہے، بلکہ یہ بھی دیکھنا ضروری ہوتا ہے کہ یہ شئے مفضی إلی الحرام والفساد نہ ہو، مثلاً: بیع عند أذان الجمعۃ اگرچہ فی نفسہ مباح ہے، لیکن اس کے مخل فی السعي إلی الجمعۃ ہونے کی وجہ سے اسے مکروہ تحریمی قرار دیا گیا۔ اسی طرح حمل سلاح کے ساتھ راستہ پر چلنا اگرچہ فی نفسہ مباح ہے، لیکن اس اندیشہ کی وجہ سے کہ اس سے کسی کو زخم نہ لگ جائے، اُسے منع قرار دیا گیا۔ وجیہ عورتوں کے ساتھ بلا ضرورت گفتگو اور اُن کے ساتھ خلوت اگرچہ فی نفسہ مباح ہے، لیکن مفضی إلی الحرام (زنا) ہونے کی وجہ سے ممنوع قرار دیا۔ معلوم ہوا کہ ذرائع ممنوع بھی ممنوع قرار پاتے ہیں، اگرچہ فی نفسہ ذرائع مباح ہوتے ہیں، اسی کو حضرات فقہائے کرام سدّ ذرائع سے تعبیر کرتے ہیں، جیسا کہ قواعد فقہیہ ہیں: " ما أدى إلى الحرام فهو حرام "(۹)، " الوسيلة إلى الحرام حرام "(۱۰)، "ما أفضى إلى الحرام كان حرامًا "(۱۱)، " إن الوسيلة أو الذريعة تكون محرمة إذا كان المقصد محرما "(۱۲) وغیرہ۔

نیز "الأصل في الأشياء الإباحة" اس اصل میں مزید دو نظریے ہیں: (۱) " الأصل في الأشياء الحظر " عند بعض أصحاب الحديث . (۲) "الأصل في الأشياء الوقف" عند بعض أصحابنا (الأحناف)۔(۱۳)

لہٰذا مذکورہ کرنسی فی نفسہ مباح ہو، تب بھی (جب کہ احقر کے نزدیک اس کا کرنسی ہونا ہی محلِ غور ہے)، اس کے مفاسد، متوقع خطرات اور اندیشوں کی بنا پر اس کو لین دین کا ذریعہ بنانا کسی بھی صورت میں جائز و درست نہیں ہونا چاہیے۔(۱۴)

والحجة على ما قلنا :

(۱) (انعام الباری: ۳۳۲/۲، ۳۳۳، نوٹ کیسے رائج ہوا؟)

(۲) (ملخص از انعام الباری: ۳۲۳/۲، ۳۲۵، نوٹ کی فقہی حیثیت)

(۳) ما في " القرآن الكريم " : ﴿يا أيها الذين امنوا إنما الخمر والميسر والأنصاب والأزلام رجسٌ من عمل الشيطن فاجتنبوه لعلكم تفلحون﴾ . (سورة المائدة : ۹۰)

ما في " أحكام القرآن للجصاص " : ولا خلاف بين أهل العلم في تحريم القمار ، وأن المخاطرة من القمار ، قال ابن عباس : إن المخاطرة قمار ، وأن أهل الجاهلية كانوا يخاطرون على المال والزوجة ، وقد كان ذلك مباحًا إلى أن ورد تحريمه . (۳۹۸/۱)

ما في " جامع الترمذي " : (ونهى النبي ﷺ عن بيع الغرر) عن أبي هريرة رضي الله عنه قال : " نهى رسول الله ﷺ عن بيع الغرر وبيع الحصاة " . (۲۳۳/۱ ، أبواب البيوع ، باب ما جاء في كراهية بيع الغرر ، صحيح مسلم : ۲/۲ ، كتاب البيوع)

ما في " رد المحتار " : القمار من القمر الذي يزداد تارة وينقص أخرى ، وسمي القمار قمارًا لأن كل واحد من المقامرين ممن يجوز أن يذهب ماله إلى صاحبه ، ويجوز أن يستفيد مال صاحبه ، وهو حرام بالنص .

(۵۷۷/۹ ، ۵۷۸ ، الحظر والإباحة ، باب الاستبراء وغيره)

ما في " معجم لغة الفقهاء " : القمار تعليق التملك على الخطر والمال من الجانبين . (ص/۳۶۹)

(۴) (حوالہ بالا) (۵) (حوالہ بالا)

(۶) ما في " القرآن الكريم " : قوله تعالىٰ : ﴿ولا تلقوا بأيديكم إلى التهلكة﴾ . (سورة البقرة : ۱۹۵)

ما في " روح المعاني " : استدل بالآية على تحريم الإقدام على ما يخاف منه تلف النفس . (۱۱۸/۲)

ما في " البحر المحيط لأبي حيان الغرناطي " : والظاهر أنهم نهوا عن كل ما يؤول بهم إلى الهلاك في غير طاعة الله ..... ولا تجعلوا أنفسكم لقى إلى التهلكة فتهلك . (٢/١١٩، ١٢٠)

ما في " الموافقات في أصول الأحكام للإمام الشاطبي " : ومجموع الضروريات خمسة : وهي حفظ الدين ، والنفس ، والنسل ، والمال ، والعقل . (٢/٣ ، كتاب المقاصد ، المسئلة الأولى)

ما في " روضة الطالبين " : ويحرم ما يضر من البدن والعقل . (٣/٢٨١)

(٧) (ديكهيے حواله نمبر : ٣)

(٨) ما في " صحيح البخاري " : باب أجرة السمسرة – ولم ير ابن سيرين وعطاء وابراهيم والحسن بأجر السمسار بأساً ، وقال ابن عباس : لا بأس أن يقول : بع هذا الثوب فما زاد على كذا وكذا فهو لك ، وقال ابن سيرين : إذا قال : بعه بكذا وكذا فما كان من ربح فهو لك أو بيني وبينك فلا بأس به . (١/٣٠٣ ، كتاب الإجارة ، باب أجر السمسار)

ما في " رد المحتار " : قال في " التاتر خانية " : وفي الدلال والسمسار يجب أجر المثل ، وما تواضعوا عليه أن في كل عشرة دنانير كذا فذاك حرام عليهم . وفي " الحاوي " : سئل محمد بن سلمة عن أجرة السمسار ، فقال : أرجو أنه لا بأس به ، وإن كان في الأصل فاسداً لكثرة التعامل ، وكثير من هذا غير جائز فيجوزوه لحاجة الناس إليه كدخول الحمام .

(٩/٧٥ ، كتاب الإجارة ، مطلب في أجرة الدلال)

ما في " الفتاوى البزازية على هامش الهندية " : إجارة السمسار والمنادي والحمامي والصكاك وما لا يقدر فيه الوقت ولا مقدار العمل لما كان للناس به حاجة جاز ويطيب الأجر المأخوذ لو قدر أجر المثل . (٥/٣٠ ، نوع في المتفرقات)

(٩) (بدائع الصنائع : ٦/٣٨٨)

(١٠) (بدائع الصنائع : ١/٢٢٨) .

(١١) (موسوعة قواعد الفقهية : ٩/٣٢) .

(١٢) (المقاصد الشرعية للخادمي : ص/٣٦)

(١٣) ما في " الأشباه والنظائر لإبن نجيم " : قاعدة : ٣٣٨ : هل الأصل في الأشياء الإباحة حتى يدل الدليل على عدم الإباحة ، وهو مذهب الشافعي – رحمه الله – ، أو التحريم حتى يدل الدليل على الإباحة ، ونسبه الشافعية إلى أبي حنيفة (رحمه الله) ..... ٣٤٠ : وفي " شرح المنار " للمصنف : الأصل في الأشياء الإباحة عند بعض الحنفية ، ومنهم الكرخي . وقال بعض أصحاب الحديث : الأصل فيها الحظر . وقال بعض أصحابنا : الأصل فيها الوقف ، بمعنى أنه لا بد لها من حكم ، لكنا لم نقف عليه بالفعل . انتهى . (١/٢٥٣ ، ٢٥٤ ، القاعدة الثالثة : اليقين لا يزول بالشك ، ط : مكتبه فقيه الامت ديوبند)

(١٤) ما في " القواعد الكلية والضوابط الفقهية " : درء المفاسد أولى من جلب المصالح .

(ص/١٨٢ ، الفتاوى الحديثية : ص/٢٠٣ ، مطلب الاجتماع للموالد والأذكار ، الأصول والقواعد للفقه الإسلامي : ص/١٤١ ، قاعدة : ١٢٣ ، الأشباه والنظائر لإبن نجيم : ص/٣٢٢ ، درر الحكام شرح مجلة الأحكام : ١/٣١ ، المادة : ٣٠ ، قواعد الفقه : ص/٨١ ، قاعدة : ١٣٣ ، جمهرة القواعد الفقهية : ٢/٣٣ ، قاعدة : ٨٩١ ، ترتيب اللآلي : ص/٦٩١ ، القواعد الفقهية : ص/١٤٠ ، شرح القواعد : ص/٢٠٥) فقط

والله أعلم بالصواب وعلمه أتم وأحكم

كتبه العبد : مفتي محمد جعفر ملي رحماني

بیٹ کوین اور دیگر ڈیجیٹل کرنسیز کے ثمنیت میں جواز یا عدم جواز کے دلائل اور ان کا تحقیقی جائزہ

دوسرا حصہ
مفتی ثناءاللہ، دارالافتاء دارالعلوم الرحمانیہ، مردان

بٹ کوین اور دیگر ڈیجیٹل کرنسی کے ساتھ خرید وفروخت جائز ہے یا نہیں۔ اس بارے میں معاصرین کے دو رائے ہیں: بعض جواز کے قائل ہے، جب کہ بعض کی رائے میں اس کے ذریعے خرید وفروخت جائز نہیں، جواز اور عدم جواز کے دلائل ذکر کرنے سے پہلے ایک تمہید کا ذکر کرنا ضروری معلوم ہوتا ہے، اس کے بعد جواز اور عدم جواز کے دلائل بیان کرکے ان کا تجزیہ لینے کی کوشش کی جائے گی، جب کہ آخر میں آنے والے حالات میں ضرورت کے وقت ڈیجیٹل کرنسی کو بطور متبادل اختیار کرنے کیا ممکنہ شرعی صورت متوقع ہو سکتی ہے:

تمہید: فطری طور پر اللہ رب العزت نے سونا، چاندی کو بطور زرِ مبادلہ پیدا فرمایا، مگر وقت گزرنے کے ساتھ وقتی مصالح اور انتظامی ضرورتوں کے پیش نظر حکومتوں نے انہیں مہر زدہ بنا کر باقاعدہ ملکی نگرانی میں اسے پیش کیا، بعد میں دیگر وجوہات کی بنا پر سونے چاندی کے درہم ودینار کے ذیلی ریزگاریوں کو دیگر دھاتوں جیسا پیتل، لوہا، چمڑہ اور بعد میں کاغذ کو آپس کے لین دین اور لوگوں کے باہمی تعارف کے ساتھ ملکی حکم نامے کے طور پر رائج کیا گیا، موجودہ حالات میں معاملات کے بدلتے انداز اور انٹرنیٹ کے اکثر کاروباروں میں داخل ہونے کی وجہ سے ملک کے مختلف اطراف اور دنیا کے اردگرد کونے سمیٹتے ہوئے ایک گاؤں کے مانند بن چکے ہیں، جس میں تجارتی معاملات کی آسانی کے لیے براہِ راست تقریباً ہر ملک میں مرکزی بینکوں میں رقوم کی منتقلی ڈاکخانوں، ویسٹرن یونین اور دیگر اداروں کے بغیر ہوتی ہے، تاہم انٹرنیٹ پر خرید وفروخت کے لیے ڈالر، یورو یا ملکی کرنسی کے بدلے پہلے تو ویب اور ماسٹر بنکوں سے جاری کیے گئے، مگر کئی مشکلات اور دیگر خطرات کے پیش نظر الیکٹرک منی کے نام سے ایک کرنسی وجود میں آئی، جو عام طور پر بنکوں اور حکومتوں کے ماتحت ہوتے تھے، مگر وقت گزرنے کے ساتھ شدت سے یہ مرکزی اور ذیلی بنکوں کے مروجہ نظام کو بعض افراد کی جانب سے بوجھ محسوس کیا جانے لگا، تو ان سے نکلنے کے لیے سب سے پہلے ۲۰۰۷ میں ڈیجیٹل کرنسی کا نظریہ پیش کیا گیا، جسے نامعلوم افراد کی جانب سے ۲۰۰۹ میں بیٹ کوین bit coin کے نام ایک غیر محسوس، نظر نہ آنے والی، صرف موبائل میں موجود بیلنس کی طرح نمبرات کی صورت میں ڈیجیٹل کرنسی کے طور پر وجود میں آئی، جس کی بنیاد ریاضی کے شعبہ لوگ رتھم پر مبنی ہے، جس کا مقصد فرضی نمبرات، مشینی ایجاد سے بچاؤ اور ایک نمبر کی وضع کردہ کرنسی کو دوبارہ منظر عام پر نہ آنا تھا۔

بیٹ کوین اور دیگر ڈیجیٹل کرنسیوں کی حفاظت کے لیے بنکوں کی ٹرانزکشن اور رقوم کی منتقلی وغیرہ حسابات کی طرح "بلوک چین" کا نظریہ پیش کیا گیا، جس میں باقاعدہ ایک ضامن ادارے کے ماتحت خرید وفروخت کے بعد مخصوص اجرت کے عوض آن لائن چوری اور دیگر خطرات سے محفوظ کیا جاتا ہے، کرنسی کی قیمت کا تعین طلب ورسد کی آزادی کے سپرد کیا گیا، جس کی وجہ سے ابتداء میں اس کی قیمت ایک ڈالر سے بہت کم، مگر بعد میں اتار، چڑھاؤ سے گزرتے ہوئے اب اس کی قیمت پانچ ہزار ڈالر تک پہنچ چکی ہے۔

بعض مغربی ممالک میں ٹیکسوں کی حصولی، نجی حسابات اور اس کرنسی کی نگرانی کے لیے جزوی طور پر تسلیم کیا گیا ہے، جب کہ دیگر بعض ممالک مثلاً چین اور سعودی عرب وغیرہ میں اس پر پابندی عائد کی گئی، کسی بھی ملک کی باقاعدہ نگرانی نہ ہونے اور اس کرنسی اتار چڑھاؤ کی وجہ سے بین الاقوامی طور پر اس کرنسی کے تحت طے پائے جانے والے معاملات کرنے والے اداروں کو کئی بار تنبیہ کی جا چکی ہے۔

اگرچہ عرب ممالک میں بہت سے حضرات مفتیانِ کرام نے اس کے تحت کی جانے والی معاملات کے جواز کا فتویٰ دیا ہے، مگر دیگر بعض مفتیانِ کرام نے باقاعدہ حکومت کی تسلیم نہ کرنے تک محتاط رہنے کا فتویٰ دیا ہے، جب کہ محققین مفتیانِ کرام نے اس بارے میں اب تک توقف کا قول اختیار کیا ہے۔

یہی وجہ ہے کہ بعض عالمی اداروں مثلاً البدی وغیرہ نے اس کرنسی کے تحت معاملات کو اگرچہ جائز کہا ہے، مگر غرر اور دیگر غیر شرعی معاملات کی وجہ سے خود اس سے تحرز کا مشورہ دیا ہے، جب کہ ملکی سطح پر جامعۃ العلوم الاسلامیہ علامہ بنوری ٹاؤن اور جامعۃ الرشید نے تعامل اور حکومتی حکم نامے کے بغیر اس کرنسی کو کاروباری یا سرمایہ کاری کے طور پر اختیار کرنا ناجائز کہا ہے۔

جواز کے دلائل:

پہلی دلیل: اس دلیل کی وضاحت سے پہلے دو قاعدوں کا جاننا ضروری ہے:

پہلا قاعدہ: "الحکم علی الشئ فرع عن تصورہ" اس قاعدہ کا مطلب یہ ہے کہ کسی بھی مسئلہ میں اس وقت تک فتویٰ دینے درست نہیں، جب تک اس مسئلے کی پوری ماہیت اور اس کے عمل کا مکمل طریقہ کار اس کے سامنے واضح نہ ہو۔ جیسا کہ اللہ تعالیٰ کا فرمان ہے: ولا تقف مالیس لک بہ علم [الاسراء:۳۶] اور (اے بندے) جس چیز کا تجھے علم نہیں اس کے پیچھے نہ پڑ۔

دوسرا قاعدہ: "الأصل فی المعاملات الاباحۃ والجواز لا التحریم" معاملات میں اباحت اور جواز اصل ہے جب کہ حرمت کے لیے باقاعدہ کسی دلیل شرعی کا ہونا ضروری ہے۔ جیسا کہ حدیث مبارک میں ہے: (ما أحل اللہ فی کتابہ فھو حلال وما حرم فھو حرام، وما سکت عنہ فھو عافیۃ فاقبلوا من اللہ عافیتہ فإن اللہ لم یکن نسیا)[1] ان دو قاعدوں کے بعد واضح رہے کہ بیٹ کوین اور دیگر ڈیجیٹل کرنسیز کا وجود چونکہ کسی آلہ[2] کے بغیر نہیں ہوتا، اس لیے آلہ کو خریدنے کا حکم دیگر آلات کی طرح ہے یعنی جس طرح دوسرے آلات صنعت و تجارت مثلاً کارپینٹنگ اور ٹیلرنگ کے لیے مشینیں وغیرہ خریدنا اور ان سے کام کرنا جائز ہے اسی طرح ڈیجیٹل کرنسیز کے لیے الیکٹرک پریس، یو ایس بی اور کمپیوٹر وغیرہ خریدنا جائز ہے۔

دوسری دلیل: وہ معاملات وبیوعات جو فاسد و باطل امور کی وجہ سے ناجائز ہوتے ہیں اگر بیع کو ان امور سے پاک کیا جائے، تو بیع میں عدم جواز کی کوئی وجہ باقی نہیں رہے گی، جن میں اشیاء محرمہ کی خرید و فروخت، غرر، سوم علی سوم غیرہ، صفقتان فی صفقۃ، شروط فاسدہ، بیع صرف اور ربا وغیرہ کی خرابیوں نہ ہو، تو وہ بیع جائز ہوتی ہے، چونکہ بیٹ کوین اور دیگر ڈیجیٹل کرنسیز میں ان مذکورہ خرابیوں میں سے کوئی ایک خرابی بھی نہیں پائی جاتی، لہذا ان کا کاروبار شرعاً جائز ہونا چاہیے۔[3]

تیسری دلیل: کرنسی ہونے کے لیے عوام کا کسی جنس کی زیر معاملہ ہونے پر اتفاق کرنا لازم ہوتا ہے، جو بیٹ کوین میں پایا جاتا ہے، کیونکہ عوام اس کے ذریعے سے خرید و فروخت کرتے ہیں اور اب تو بعض ممالک میں اے ٹی ایم مشینیز، آن لائن خریداری، بلوں کی ادائیگی وغیرہ کئی معاملات میں اس کا عمل دخل زیادہ ہوتا جارہا ہے، تو جیسا کاغذی نوٹ ثمن ہے اسی طرح بٹ کوین اور دیگر ڈیجیٹل کرنسیز جن پر تعامل ہوتا جارہا ہے وہ بھی ثمن شمار ہوگا۔

---

[1] کشف الأستار عن زوائد البزار، کتاب الأطعمۃ، باب فیما أحل وما حرم، رقم:۲۸۵۵، ج۳ص۳۲۵۔

[2] نوٹ: ڈیجیٹل کرنسیز کے لیے آلات کی حیثیت ایسی ہے جیسے کاغذی نوٹ کی صحیح اور غیر صحیح ہونے کو معلوم کرنے والے مشین ہوتا ہے یا پھر اصلی اور نقلی سونا چاندی کے درمیان فرق کرنے کے لیے سنار اور صراف کے پاس موجود آلہ اور اس کا تجربہ ہوتا ہے، لیکن اس کے ساتھ ساتھ ان آلات کے بغیر ان کرنسی کا وجود اگر ہو بھی، تو پھر خارج میں اس کا اندازہ آلات کے بغیر ناممکن ہے۔

[3] مزید تفصیل کے لیے دیکھئے: نبیل السحابی onecoinbilaraby@gmail.com

چوتھی دلیل: کسی بھی چیز کی مالیت سے اس کی حیثیت معلوم ہوتی ہے اور مالیت کا مدار طلب ورسد کی آزاد قوتوں سے متعین ہوتا ہے، جو بٹ کوین کی قیمت کی مقرر ہونے میں بنیادی کردار ادا کر رہا ہے۔ ابتدا میں جب اس کی طلب کم تھی اور رسد زیادہ تو اس کی قیمت کم تھی اور جب اس کی طلب بڑھ گئی تو اس وجہ سے اس کی قیمت بھی بڑھ گئی۔ اس سے معلوم ہوتا ہے کہ بٹ کوین باقاعدہ ایک کرنسی ہے۔

پانچویں دلیل: جرمنی اور کینیڈا اور دیگر ممالک نے اس کی ثمنیت تسلیم کرلی ہے۔ بلکہ بعض حلقوں سے یہ باتیں بھی سننے میں آتی ہے کہ بیٹ کوین کو آدھی دنیا نے تسلیم کرلیا ہے۔

چھٹی دلیل: فقہی اعتبار سے ہر وہ چیز جس کی طرف لوگوں کا میلان ہو، یا جس کی ذخیرہ اندوزی ممکن ہو، اسی طرح اس کی حفاظت ہو سکتی ہو، تو اس کو مال کہا جاسکتا ہے، بٹ کوین اور دیگر ڈیجیٹل کرنسیز پر مال کی مذکورہ تینوں تعریفات صادق آرہی ہے، لہذا اسے مال تسلیم کرنا اور اس کے ذریعے باقاعدہ کاروبار کرنا جائز نہیں۔

عدم جواز کے دلائل:

اس کے مقابلے میں دیگر محققین کی رائے یہ ہے کہ بیٹ کوین حرام کا استعمال حرام ہے اور اس کے ساتھ خرید وفروخت اور کاروبار جائز نہیں۔

پہلی دلیل:

اللہ تعالی نے آلۂ تبادلہ کے لیے جس چیز کو حقیقی ثمن بنایا وہ سونا اور چاندی ہے، جس کی ثمنیت کو سنتِ نبویہ کے دور سے بھی در حقیقت تائید حاصل ہوئی، لیکن بعد کے زمانوں میں حالات کے تغیر کی وجہ سے سونا چاندی کے ساتھ ساتھ فلوس کی ترتیب کو اسلامی اور غیر اسلامی حکومتوں میں وقتی ضرورت کے طور پر رواج حاصل ہوا، مگر آلۂ تبادلہ کی اصل نمائندگی کا سہرا پھر بھی سونا چاندی کے سر رہا اور فلوس کے ساتھ سونا اور چاندی کے درا ہم ودنانیر بطور اصل اور فلوس کی حیثیت فرع کے طور پر جاری رہی۔

بیٹ کوین اور دیگر ڈیجیٹل کرنسیز[4] کو اگر اس تناظر میں دیکھا جائے، تو یہ بات کافی بآسانی واضح ہوتی ہے کہ مالیت کے لیے حقیقی چیز کا ہونا ضروری ہے، جس کی پشت پر سونا چاندی یا اس کے علاوہ دوسرے کسی قابل اعتماد چیز کی ضمانت موجود ہو، اس کے علاوہ کسی ایسی چیز کا ثمن مقرر کرنا جس کی حیثیت وہمی اور غیر اصل ہو، جو محض سافٹ ویئر کے کسی دقیق عمل کے نتیجے میں سامنے آتا ہو اور صرف ریاضی حسابات اور تکنیکی مہارت کے طور پر متعارف ہو، جس کی ثمنیت کی قوت سافٹ ویئر کی مضبوطی پر موقوف ہو، یعنی جس ڈیجیٹل کرنسی کا سافٹ ویئر جتنا زیادہ قوی ہو اور وائرس وغیرہ سے خراب نہ کرنا ممکن ہو، تو وہ قیمت کے اعتبار سے زیادہ ہوتا ہے۔

---

[4] اس سے یہ اعتراض بھی ختم ہو جاتا ہے کہ جب ثمنیت میں اصل سونا چاندی ہے تو پھر کاغذی نوٹ اور بنک کی رسید یا دیگر مروجہ الیکٹرک رقوم کو پھر کیوں بطور زرِ مبادلہ عام عرف میں اور حکومتی سطح پر قابل قبول تسلیم کیا گیا ہے۔ تو اس کا جواب اس تشریح سے بخوبی سامنے آگئی کہ کاغذی نوٹ اگرچہ مالِ حقیقی نہیں مگر ابتداء میں سونا اور چاندی کا قائم مقام تھا اور آج کل کے دور میں درآمدات وبرآمدات وغیرہ دیگر امور اس کے پیچھے کارفرما ہے۔ اسی طرح حکومتی اتحاد اور مرکزی بنک کی ضمانت نے بھی اس کی توثیق مزید مستحکم کردی ہے۔ اسی طرح بنک رسید اور دیگر الیکٹرک رقوم کی حیثیت بھی دراصل کاغذی نوٹ کے مرہون منت ہے جس سے کوئی اشکال باقی نہیں رہتا۔

اس سے معلوم ہوا کہ زرِ مبادلہ کے لیے ثمنیت اور قابل ضمانت ہونا لازمی ہے اس کے بغیر کسی سافٹ وئیر اور محض وہمی چیز سے ثمنیت ثابت نہیں ہوتی اور چونکہ بٹ کوین میں نہ تو ثمنیت ہے اور نہ قابل ضمانت کوئی شئ، اس وجہ سے بیٹ کوین سے مالیت ثابت نہیں ہوتی۔

کاغذی کرنسی ابتداء میں چونکہ سونا چاندی کی رسید ہوتی تھی جس کی وجہ سے اس زمانے کے محققین نے اس کے کرنسی کی حیثیت کو قبول کر دیا اور بعد میں جب ۱۹۷۰ کی دہائی میں فرانس اور امریکہ کا ڈالر کے عوض سونے کے مطالبہ پر معاملہ گھمبیر ہو گیا اور امریکہ نے ڈالر کے بدلے سونا دینے سے انکار کر دیا، تو اس کے بعد کرنسی کی حیثیت بالکل آزاد ہو گئی، مگر پھر درآمدات و برآمدات اور دیگر کئی عوامل کرنسی کے اتار چڑھاو میں متاثر کن کردار ادا کر رہی ہے، جس کی وجہ سے کاغذی نوٹ کو بعض محققین نے ثمنِ حقیقی قرار دیا، تاہم ثمن عرفی سے گرانا کسی کے نزدیک بھی درست نہیں۔

اس سے واضح ہوا کہ ثمنیت کے لیے یا تو سونا چاندی کا ہونا ضروری ہے اور یا پھر اس کی رسید جیسے فلوس اور کاغذی نوٹ کی حیثیت ۱۹۷۰ تک اور تیسری صورت یہ ہے کہ ملکی اور قانونی سطح اس کی باقاعدہ اجازت ہو، جو باقاعدہ مرکزی بنک یا بین الاقوامی مرکزی بنک کی منظور شدہ کرنسی ہو، اس کے علاوہ کوئی کرنسی ثمنیت کے طور پر قابل قبول نہیں ہونی چاہیے۔

دوسری دلیل: گذشتہ دلیل سے یہ بات واضح ہوئی کہ کرنسی ہونے کے لیے کم از کم قابل ضمانت ہونا لازمی ہے، جو بٹ کوین اور دیگر ورچوئل کرنسیز میں نہیں ہے، کیونکہ قابل ضمانت ہونے سے مراد یہ ہے کہ مرکزی بینک جو کسی حکومت کے ماتحت ہو اور اپنے صارفین کی آسانی کے لیے زرِ مبادلہ کے طور پر کوئی کرنسی لاگو کریں، وہی لوگوں کے لیے قابل اعتماد ہو گا اس کے علاوہ کوئی دوسرا طریقہ جس میں مرکزی حکومت کا عمل دخل نہ ہو، درست نہیں ہونا چاہیے۔

تیسری دلیل: کرنسی کی قیمت کی تقرری حکومتی جانب سے مقرر ہوتی ہے یا پھر کسی حکومت کی زیادہ پیداوار اور مضبوط معیشت کی وجہ سے اس کی کرنسی دوسرے کمزور معیشت والے ممالک کے مقابلے میں زیادہ وزنی ہوتی ہے۔ طلب و رسد کی وجہ سے کرنسی کی قیمت کا تعین نہیں ہو سکتا، جب کہ بٹ کوین اور دیگر کرنسیز کی قیمت کا تعین طلب و رسد کرتا ہے ہاں دیگر اشیاء استعمال و خورد و نوش کی قیمت کا تقرر طلب و رسد کر سکتا ہے۔

اب چونکہ بٹ کوین میں قیمت کی تقرری طلب و رسد کی وجہ سے ہے، لہٰذا اسے زیادہ سے زیادہ عرض اور سامان کہہ سکتے ہیں، ثمن نہیں کہا جا سکتا۔

چوتھی دلیل: کرنسی حکومتی ادارے کی نمائندہ متصور ہوتی ہے اب اگر کوئی ادارہ حکومتی سرپرستی کے بغیر اپنے طور پر کوئی کرنسی جاری کریں تو اس میں حکومتی نمائندگی ظاہر نہیں ہوتی، اس وجہ سے اس کو کرنسی کی حیثیت دینا دانشمندی نہیں، کیونکہ جب بھی زرِ مبادلہ کی ضرورت ہو گی سافٹ وئیر میں مزید ارقام اور نمبرات داخل کر کے کرنسی کو زیادہ کیا جانا ممکن ہو سکتا ہے۔

پانچویں دلیل: اگر بٹ کوین اور دیگر ورچوئل کرنسیز کی ثمنیت کو تسلیم کر لیا جائے، تو اس طرح ہر ایک ادارے کو یہ اختیار حاصل ہو گا کہ وہ اپنی کرنسی جاری کریں اور یوں ایک ہی ملک میں متعدد کرنسیز کا اجراء ہو گا جو ملکی خانہ جنگی کو مقتضی ہو گا اور اس کا سبب یہی تھا کہ ہم نے اس کے جواز کا حکم دیا۔ لہٰذا اس کو تسلیم کرنا، وقتی پروپیگنڈا سے متاثر ہو کر اس کی تسلیم کرانے کی تگ و دو کرکے اس کرنسی کو دوسری غیر اسلامی چیزوں کی طرح اسلامی بنانے کی کوشش کرنا کئی خطرات کو جنم دے گی، اسی کے بارے میں عالم اسلام کے اقتصادیات کے مشہور محقق اور عظیم مؤرخ و مصنف "علامہ مقریزی" "مصر میں قحط دو بالا اور خانہ جنگی کے اسباب کے بارے افراط زر کے بارے میں دنیا کے سب سے پہلے لکھے گئے کتاب "اغاثۃ الامۃ بکشف الغمۃ" میں لکھتے ہیں:

"قحط کے اسباب میں سب سے بڑا سبب یہ ہے کہ کثرت سے فلوس رائج ہوں گے"۔ ص ۴۰۔

عصر حاضر میں ہر ملک کی الگ الگ کرنسی ہونے کے بعد ورچوئل کرنسیز کثرت سے رواج پا رہی ہے اور ہر ملک میں کرنسی کے ذیل بائنڈز، ڈیبٹ اور ماسٹر

کارڈز، موبائل کارڈز وغیرہ کے علاوہ ڈیجیٹل کرنسی کا تصور ختم ہونے والا تاثر باندھ دیا گیا ہے، جب کہ قحط اور وبا کے لیے کثرت زر کے ساتھ ساتھ اشیاء کا مہنگا اور عام دسترس سے نکلنا ہے اور کرنسی کے پیچھے مال اور درآمدات وغیرہ کا نہ ہونے کے ساتھ مہنگے سے مہنگے تر ہونے سے کرنسی کو اپنے گرفت میں لینے کی بات عام فہم سی ہے۔

چھٹی دلیل: اصل ثمن تو سونا چاندی ہے کاغذی نوٹ کی ثمنیت بھی ضرورت کی وجہ سے ہوئی اور ضرورت کے بارے میں فقہائے کرام کا مشہور قاعدہ ہے: الضرورۃ تقدر بقدرھا کہ ضرورت بقدر ضرورت ہی نکالی جائے گی ضرورت سے زیادہ نکالنے کی اجازت نہیں ہوگی، جب کہ آن لائن کاروبار کے مشکلات کے لیے ویزٹ کارڈ، ماسٹر کارڈ اور بنکوں سے دیگر جاری ہونے والے کارڈز سے بھی ضرورت پوری ہو سکتی ہے، اسی طرح الیکٹرک کرنسی بھی اس کے متبادل کے طور پر جدید کاروبار میں ایک پیش رفت ہے، جس کے بعد مزید ایک کرنسی کو تسلیم کرنا ایک غیر ضروری فعل کو شرعی حکم کے طور پر تسلیم کرنا ہوگا۔

ساتویں دلیل: کرنسی نے کاغذی مطبع سے سفر کرتے کرتے تھک کر غیر حقیقی وجود کے حامل کمپیوٹر کے سافٹ ویئرز کی صورت کو اگر صحیح مانا جائے تو اس کا مطلب یہ ہوگا کہ صیہونی یہودی اور عیسائی کرنسی چھاپنے سے تنگ آکر مزید انتظار نہیں کر سکتے، بلکہ اب اگر انہیں پیسوں کی ضرورت ہو، تو چھاپ خانے کے بجائے سافٹ ویئرز کا سہارا لیں گے اور میڈیا کے ذریعے تشہیر کر کے عوام کو اس کی جانب راغب کریں گے تاکہ حکومتوں کو پھنسانا آسان ہو جائیں۔

آٹھویں دلیل: کرنسی عوام کی سہولت کے لیے ہوتی ہے کہ ہر پڑھا لکھا اور ناخواندہ سب آسانی کے ساتھ اپنی ضرورت کی چیزوں کو خرید سکیں اور ضرورت سے زائد اشیاء کو فروخت کریں، کرپٹ کوین اور دیگر ڈیجیٹل کرنسی کا معاملہ اس سے کہیں زیادہ مختلف ہے کیونکہ اس میں تو ایک بجلی اور دوسرا انٹرنٹ کی ضرورت ہوتی ہے اور پھر ہر جگہ اس کا میسر ہونا بھی مشکل ہے، لیکن اس کے استعمال میں ہر ناخواندہ کو کسی ماہر تعلیم یافتہ کے بغیر کسی چیز کے خریدنے کا سہولت مہیا نہیں ہوگا۔

نویں دلیل: دجال کے فتنے سے کی شدت بیٹ کوین کی اجراء سے محسوس ہونے لگی کیونکہ دجالی نظام کے لیے راستہ ہموار کرنے کے لیے دجال کے ہر کارے ابھی سے ساری دنیا کی تجارت کنٹرول کرنے کے بعد ماحولیات اور خوراک کے قبضہ کے متصل بعد ایک عالمی کرنسی وضع کرنے کے لیے بطور تمہید بیٹ کوین اور دیگر ڈیجیٹل کرنسیز کا جال بچھا کر آسانی اور سہولت کا جھانسہ دے کر انفرادی اور اجتماعی مالیت کو محض انٹرنٹ اور بادلوں کے تابع کرنے کے درپے ہیں ابھی سے اس منصوبے کی تکمیل میں اگر رخنے نہ ڈال گئی اور دیگر شعبوں کی طرح اس کی بھی منظوری دے دی گئی اور ساتھ اکثر امور کی طرح اس کرنسی کے لیے بھی بغیر سوچے سمجھے جواز کے حیلے بہانے تراشنے کی سعی پیہم کرنے لگیں، تو وہ وقت دور نہیں کہ یہ اعلان ہو جائے: "عالمی ہیکروں نے ڈیجیٹل کرنسی کو ہیک کر کے سارا نظام تباہ کر دیا اور نامعلوم افراد کے خلاف رپورٹ درج کر دیا گیا ہے" ان جیسے چکنی چپڑی باتوں سے عوام کو بہلا کر عالمی ایجنڈے میں مانع لوگوں کے کرنسیز کو منجمد کر کے اپنے پیروکاروں میں نوازنے کی روش اپنائیں گے، تاکہ کانے دجال" اسرائیل کے سپر مین منتظر" کے سامنے سب کو مجبور و مقہور کر دیا جائے۔

جواز اور عدم جواز کے دونوں دلائل کا محاکمہ:

جواز کے دلائل کا تجزیہ: دوسری دلیل کے ضمن میں یہ بات ذکر کی گئی کہ جس بیع میں عدم جواز کی وجوہات میں سے کوئی وجہ نہ ہو تو وہ جائز ہے اور اگر عدم جواز کی کوئی صورت ہو، تو وہ ناجائز ہو گی جب کہ بیٹ کوین اور دوسرے ڈیجیٹل کرنسیز میں عدم جواز کی وجوہات میں سے کوئی وجہ نہیں لہذا اس کا کاروبار جائز ہے۔

اس دلیل میں دو باتیں محل نظر ہیں:

پہلی بات: یہ ہے کہ اس میں عدم جواز کی وجوہات میں سے کوئی ایک وجہ نہیں، یہ بات ہمیں تسلیم نہیں، کیونکہ بیع کے ناجائز ہونے کے وجوہات میں سے ایک اہم وجہ یہ ہے کہ مال نہ ہو اور بیٹ کوین بھی مال نہیں، کیونکہ مال یا تو شئی مرغوب اور قابل ذخیرہ چیز کا نام ہے جب کہ اس میں یہ وصف نہیں پائی جا رہی اور اس کی وجہ یہ ہے کہ اعیان و منافع پر مال کا اطلاق ہوتا ہے اور بیٹ کوین نہ تو اعیان میں سے ہے اور نہ منافع میں۔ لہذا یہ مال نہیں ہوا تو جو حکم غیر مال کی خرید و فروخت کا ہوتا ہے وہی اس کا بھی ہو گا۔

اور اگر بعض لوگوں کے ہاں یہ شئی مرغوب اور قابل ذخیرہ ہو، تو بھی جو لوگ جو اس کو شئی مرغوب اور قابل ذخیرہ نہیں مانتے ان نزدیک یہ مال نہیں ہوا اور جس طرح جو چیز بعض کے نزدیک غیر مال ہو اور بعض کے نزدیک مال جیسے شراب وغیرہ تو اس کی بیع فاسد ہوتی ہے۔ لہذا یہی حکم بیٹ کوین کا بھی ہو گا۔

دوسری بات: اس دلیل میں پوری توجہ بیٹ کوین کے کاروبار میں شرعی خامی پر مرکوز کی گئی ہے جب کہ ہمارا موضوع اس کی کرنسیت کا ثبوت ہے جب اس کی کرنسیت ثابت ہو جائے، تب ہم اس کے کاروبار کے جواز و عدم جواز کے احکام پر بحث کریں گے۔ یعنی دعویٰ ایک ہے اور دلیل دوسرا۔ دعویٰ ہے بیٹ کوین کی کرنسیت و عدم کرنسیت اور دلیل ہے بیٹ کوین کے کاروبار میں شرعی خامی نہیں۔

عدم جواز کے دلائل کا تجزیہ:

عدم جواز کی پہلی دلیل کا تجزیہ:

۱۔ اس دلیل کا حاصل یہ ہے کہ ثمنیت کے لیے اصل سونا چاندی ہے یا پھر اس کی رسید اور تیسری صورت میں قابل ضمانت حکومت۔

اس کے جواب میں یہی کہا جا سکتا ہے کہ ثمن شرعی میں تو اصل یہی ہے کہ سونا چاندی یا اس کی رسید ہو اور یا پھر قابل ضمانت حکومت جیسا کہ فلوس وغیرہ، لیکن عرفی ثمن میں اس کے لیے تعامل اور حکومت کی اجازت بھی کافی معلوم ہوتی ہے۔ اس وجہ سے یہ کہا جا سکتا ہے کہ ہم بھی بیٹ کوین کو ثمن شرعی نہیں کہہ رہے بلکہ ہم اس کو ثمن عرفی کہہ سکتے ہیں۔

۲۔ جہاں تک یہ بات ہے کہ بیٹ کوین اور ڈیجیٹل کرنسیز میں سافٹ ویئر کی مضبوطی پر قوت ثمن کا اعتبار ہے یعنی جو سافٹ ویئر قوی ہوتا ہے اس کی قیمت زیادہ ہوتی ہے تو یہی بات عام کاغذی کرنسی میں بھی ہے کہ جس کرنسی کے عوام اور حکومت مضبوط ہو تو ان کی کرنسی بھی مضبوط ہوتی ہے۔

۳۔ اور یہ بات کہ بیٹ کوین وغیرہ ڈیجیٹل کرنسیز میں ہیکنگ وغیرہ کا خطرہ ہے، تو یہی خطرہ کاغذی نوٹ کے غصب میں اور اس کی نقلی کاپی تیار کرنے میں بھی ہے، جب وہ جائز ہے تو اس میں کیا حرج ہے؟

بٹ کوینز اور دیگر ڈیجیٹل کرنسیز کے ویب سائٹس دیکھنے سے معلوم ہوا ہے کہ معاملہ اس طرح نہیں بلکہ کرنسی کا اجرا ہر ایک کے بس کا روگ نہیں کر سکتا، بلکہ اس کے لیے باقاعدہ سرٹیفکیٹ ہوتی ہے اور وہی ادارے کامیاب ہو گا جس کے ساتھ bloc chain یعنی ٹرانزکشن بھی ہو اور اس کا ہاتھ آجانبر ادارے کا

کام نہیں۔اسی طرح کرنسی کے ابتداء سے ہی اس کی تعداد متعین ہوتی ہے مثلاً بٹ کوین کی تعداد ۲۱ ملین کوینز ہے اور دیگر کوینز کی بھی تعداد متعین ہے۔لہذا "چوتھی دلیل" دراصل اس سسٹم سے ناواقفیت کی بناء پر ہے کوئی تحقیق اس کے پشت پر نہیں۔

ہاں البتہ یہ ہے کہ ٹرانزکشن ملنا بھی ممکن ہے اور تعداد کا مقرر ہو جانا بھی کوئی ایسی ٹھوس ثبوت نہیں جس کی بناء پر ہم یہ کہے کہ اس سے زیادہ نہیں ہو سکتا اور نہ ہی یہ ٹرانزکشن سافٹ ویئر کوئی نہیں بنا سکتا اور نہ ہی ان اداروں کی انسان دشمنی کسی پر مخفی ہے۔

عدم جواز کے دلائل میں "چوتھی دلیل" سے یہ بات معلوم ہوتی ہے کہ ہر ایک ادارے کو ڈیجیٹل کوینز بنانے کی اجازت حاصل ہوگی اور یوں ہر ادارہ اپنے اختیار سے ضرورت کے مطابق جب چاہے کوینز بنا سکتا ہے۔

جواز و عدم جواز کے مندرجہ بالا دلائل اور ان پر کیے گئے تجزیے کی روشنی میں چند باتیں معلوم ہوئیں:

پہلی بات:

۱۔بٹ کوین اور دیگر ڈیجیٹل کرنسیز کی حیثیت کا بغور مطالعہ کیا جائے، تو یہ بات بخوبی سامنے آتی ہے کہ اس کی مدار صرف ڈیجٹس اور اقام اور نمبرات میں وہی ہے، جو کاغذی کرنسی پر لکھی ہوئی ہے، یعنی جس طرح کاغذی کرنسی کے اوپر لکھے گئے نمبرات اگر ہو، تو وہ کرنسی شمار ہوتی ہے اگرچہ نوٹ کیسی گھسی پٹی پرانی کیوں نہ ہو جائے اور دکان دار اسے قبول نہ کرے، تو بنک اس کا ذمہ دار ہے، کہ وہ اسے تبدیل کرا کے نیا نوٹ جاری کرے، لیکن اگر کوئی نوٹ کتنا ہی نیا کیوں نہ ہو، لیکن اس کے نمبرات نظر نہ آتے ہوں، تو یہ نہ تو بازار میں مقبول ہے اور نہ ہی بنک میں اس کا تبادلہ ہو سکتا ہے، لہذا ثمن عرفی کی کرنسیت ملکی اجازت کے ساتھ نمبرات سے مقید ہو گئی، جو بٹ کوین اور دیگر ڈیجیٹل کرنسی میں بطریقہ اولی نظر آتے ہیں کیونکہ اس میں بھی یہی نمبرات موجود ہوتے ہیں۔

۲۔ جس طرح ڈیبٹ کارڈ اور دوسرے کارڈز کی طرح موبائیل کمپنیوں کے موبائیل کارڈز اور ایزی لوڈ کو حکومتی سرپرستی حاصل ہونے کے ساتھ لوگوں کو اس کے ذریعے معاملہ کرنے کی اجازت ہے، کیونکہ اس میں حساب کتاب کے لیے نمبرات وغیرہ موجود ہے اور اس کے ذریعے کی جانے والی باتوں کا معتد بہ ریکارڈ ادارے کے ساتھ موجود ہوتا ہے، اسی طرح بٹ کوین اور دیگر ڈیجیٹل کرنسیز میں بھی یہی علت اگر پائی جائے، مثلاً حکومتی سرپرستی اور عوام کی قبولیت ہو، تو پھر اس کے ذریعے معاملات کے درست ہونے کے بارے میں سوچا جا سکتا ہے، کیونکہ ریکارڈ اور حساب، کتاب وغیرہ اب اس کرنسی میں ممکن ہو گئی۔

دوسری بات:

بیٹ کوین اور دیگر ڈیجیٹل کرنسیز کے مال اور ثمن یا سامان اور عرض ہونے یا نہ ہونے کے لحاظ سے صرف فقہی طور پر انتظامی اور مصلحتی مفاسد سے قطع نظر اسے بطورِ ثمن استعمال کرنے میں بظاہر کوئی اشکال نہیں نظر آتا، ہاں البتہ سونا چاندی، اس کی رسید یا ضامن حکومتی یا ان کے مسلم ادارے اور تعامل نہ ہونے کی وجہ سے اسے بطورِ کرنسی استعمال کرنا درست معلوم نہیں ہوتا۔

تیسری بات:

بعض صوفیا کے مکاشفات کے بارے میں سنا ہے (واللہ اعلم کہ صحیح بات ہے یا نہیں) کہ آخری زمانے میں امام مہدی علیہ الرضوان کی مخالفت کرنے والے اکثر فقہاء ہوں گے، جب کہ سعودیہ کے مفتیان کرام نے تو یہ بات تقریباً کہہ دی کہ اسرائیل کے مقابلے میں لڑنا درست نہیں، مگر بہر حال اس مکاشفے کے صدق و کذب سے قطع نظر اگر ڈیجیٹل کرنسی کے بارے میں ہر عاقل، بالغ ذی شعور اپنے فہم سے بآسانی یہ ادراک کر سکتا ہے کہ یہ کرنسی

حقیقتاً میں دجال کی چلائی ہوئی سازش کے نتیجے میں ہی وجود میں آئی ہوئی ایک ہتھیار کی شکل ہے، مگر عصر حاضر میں جواز وعدم جواز کے دلائل کا تذکرہ اور ان کے مابین مقارنہ کے بعد راجح ومرجوح کے لیے نظائر وامثلہ کا نہ ختم ہونے والا تانتا لگا کر مختلف نام نہاد محققین، حدیث الأسنان اور سفہاء الاعلام کا کردار ادا کرتے ہوئے معمر اور تجربہ کار اکابر کے برعکس غیر محتاط انداز میں فتوی دے کر بلا معاوضہ، غیر شعوری انداز میں مدعی ست اور گواہ چست کا کردار ادا کرتے ہوئے عالمی برادری کی خدمت کرتے ہوئے نظر آتے ہیں، جن میں بعض عرب محققین پیش پیش ہیں۔ اللہ تعالی سے دعا ہے کہ وہ ہمیں قرب قیامت کے ظاہری وباطنی فتنوں سے نجات عطاء فرمائیں۔ اللھم ارنا الحق حقا وارزقنا اتباعہ وارنا الباطل باطلا وارزقنا اجتنابہ

ڈیجیٹل کرنسی اورون کوائن (Onecoin) کمپنی کا کاروبار!

ادارہ

علمائے کرام سے ایک اہم مسئلے کے بارے میں رہنمائی مطلوب ہے:

آج کل انٹرنیٹ پر ڈیجیٹل کرنسی کی کئی کمپنیاں کام کررہی ہیں، بقول ان کے ایک ایسا دور آنے والا ہے یا آچکا ہے جب دنیا میں کاغذ کے نوٹ ختم ہوجائیں گے اور اس کی جگہ ڈیجیٹل کرنسی لے لے گی اور واقعی دنیا کے بڑے بڑے بینکوں نے اس کرنسی کو قبول بھی کرلیا ہے اور وورجسٹرڈ ہوچکی ہے۔ان کمپنیوں میں ایک کمپنی ون کوائن (Onecoin) کے نام سے کام کررہی ہے جو اپنی ایک ڈیجیٹل کرنسی متعارف کروارہی ہے اور بہت سارے لوگ نفع کمانے کی غرض سے دھڑا دھڑ اس کمپنی کے ممبر بنتے جارہے ہیں۔

اس کمپنی کا ماننا ہے کہ ڈیجیٹل کرنسی تبھی عام ہوگی جب لوگ اس کو استعمال کرنا شروع کردیں گے، اس لیے اس کمپنی نے لوگوں کی توجہ حاصل کرنے کے لیے اس میں سرمایہ کاری کرنے پر کئی منافع بخش طریقے فراہم کیے ہیں۔

پہلا طریقہ

منافع حاصل کرنے کا پہلا طریقہ یہ ہے کہ جو اس کمپنی کی رکنیت حاصل کرنا چاہتا ہے تو اسے ۱۰۰ یورو سے لے کر ۲۸۰۰۰ یورو تک میں کوئی ایک پیکج حاصل کرنا ہوتا ہے۔ کمپنی ان پیکجز کو (ایجوکیشن یا تعلیمی پیکجز کا نام دیتی ہے) اس کے ساتھ ساتھ ان پیکجز کے بدلے کمپنی اس ممبر کو ٹوکن بھی دیتی ہے، ان ٹوکنوں کی تعداد ہر پیکج کے حساب سے الگ الگ ہے۔ پھر کچھ ٹوکن عرصہ تقریباً ۹۰ دن گزرنے کے بعد کمپنی ان ٹوکنوں کو دگنا کردیتی ہے۔ ٹوکن دگنا ہونے کے بعد ممبر ان کو اختیار حاصل ہوتا ہے کہ وہ ان ٹوکنوں کو ڈیجیٹل کوائنز (سکوں) میں تبدیل کروالیں جو کمپنی فری میں کرکے دیتی ہے۔ ڈیجیٹل کوائنز حاصل کرنے کے بعد ہر صارف کو اختیار ہوتا ہے کہ وہ ان کوائنز کو بیچ سکے۔ اس طرح صارف کو تقریباً

ڈگنا فائدہ حاصل ہوتا ہے، کیونکہ کوائنز اچھی قیمت میں بک جاتے ہیں۔

دوسرا طریقہ

منافع حاصل کرنے کا دوسرا طریقہ ''Compensation plan'' کا ہے جو کہ اختیاری ہے، لازمی نہیں، یعنی اگر کسی کو فائدہ حاصل کرنا ہو تو وہ اس طریقے کو اختیار کرے، ورنہ نہیں۔ پھر اس کی بھی تین صورتیں ہیں: پہلی صورت ''Direct Sale'' کی ہے، یعنی جو بندہ کمپنی کی رکنیت حاصل کرلے اور اس کے بعد کسی کو بھی کمپنی کے بارے میں بتائے اور وہ بندہ اس کے اکاؤنٹ کے تحت کمپنی کا ممبر بن جائے تو وہ نیا آنے والا ممبر جتنے پیسوں کی سرمایہ کاری کرتا ہے، اس کا دس فیصد (10%) کمپنی پہلے والے ممبر کو دیتی ہے جو اس کے آنے کا سبب بنا اور یہ ادائیگی ایک دفعہ ہوتی ہے۔

دوسری صورت ''Network Bounus'' (نیٹ ورک بونس) کی ہے، اس صورت میں کسی بھی ممبر کے تحت دائیں اور بائیں جانب جتنے بھی لوگ بالواسطہ یا بلاواسطہ ممبر بنتے ہیں، ان کی ہفتہ وار مجموعی سرمایہ کاری کا دس فیصد حصہ کمپنی اس پہلے درجے والے ممبر کو ادا کرتی ہے، جن کے نیچے ان کی رکنیت واقع ہوئی اور یہ ادائیگی کمپنی ہفتے میں ایک دفعہ کرتی ہے۔

تیسری صورت ''Matching Bounus'' کی ہے۔ اس کی تفصیل یہ ہے کہ کوئی ممبر رکنیت حاصل کرنے کے بعد جن لوگوں کو ڈائریکٹ سپانسر کرکے کمپنی کا ممبر بنواتا ہے تو اس کو کمپنی کی اصطلاح میں ''First generation'' (پہلی نسل) کہتے ہیں اور پہلی نسل یا درجے والے جن لوگوں کو ڈائریکٹ سپانسر کرکے کمپنی میں لاتے ہیں، وہ پہلے والے ممبر کی دوسری نسل کہلاتے ہیں۔ اسی طرح تیسری اور پھر چوتھی نسل تک سلسلہ ہوتا ہے۔ تو پہلی نسل یا درجے کے ممبر ہفتہ وار ''Bounus'' سے جتنا کماتے ہیں، اس کا دس فیصد پہلے والے ممبر کو ملتا ہے، اسی طرح دوسری، تیسری اور چوتھی نسل والوں کی ہفتہ وار کمائی کے حساب سے پہلے والے رکن کو ملتا رہتا ہے اور یہ ''Matching Bounus'' ہفتے میں ایک دفعہ اور چار نسلوں یا درجوں تک دس فیصد کے حساب سے ملتا ہے، چار سے زیادہ نہیں۔ اس کے علاوہ کمپنی کبھی کبھار ڈیجیٹل کرنسی (Coins) کے حامل ممبران کے لیے ایک اور اضافی پیشکش بھی کرتی ہے کہ کمپنی میں ان کے جتنے بھی کوائنز موجود ہیں، مقررہ تاریخ کو وہ تعداد دُگنی ہو جائے گی۔ اس کے ساتھ ساتھ کئی ایک قسم کے بونس اور ایوارڈ مختلف ممبران کو وقتاً فوقتاً ان کی کارکردگی کے حساب سے دیتی ہے۔

برائے مہربانی اس ساری تفصیل کی روشنی میں چند سوالات کے جوابات مرحمت فرمائیں:

سوال نمبر۱: اس کمپنی میں منافع حاصل کرنے کا جو پہلا طریقہ مذکور ہے، اس کی شرعی حیثیت کیا ہے؟

سوال نمبر۲: منافع حاصل کرنے کے دوسرے طریقے کی تین صورتیں ہیں، ہر ہر صورت کا

شرعی حکم کیا ہے؟

سوال نمبر۳: تمام ممبران کے کوائنز کو کسی مقررہ تاریخ پر دگنا کرنے کی شرعی حیثیت کیا ہے؟

سوال نمبر۴: اہم سوال یہ ہے کہ اگر کوئی اس کمپنی میں صرف کوائنز حاصل کرنے کے لیے رکنیت حاصل کرلے اور "Networking" کے ذریعے مزید لوگوں کو رکن نہ بنائے تو کیا شرعاً ایسا کرنا صحیح ہوگا؟

سوال نمبر۵: عمومی طور پر اس کمپنی میں سرمایہ کاری کرنا شریعتِ اسلامیہ کی نظر میں کیسا ہے؟

نوٹ: برطانیہ میں مقیم کافی علماء اور مفتیان کرام اس کمپنی کی رکنیت حاصل کر کے اس بزنس کو اختیار کر چکے ہیں اور ان کے پاس برطانیہ کے کسی مفتی صاحب کا فتویٰ بھی ہے، جس کے تحت وہ اس بزنس کو بالکل جائز کہہ رہے ہیں۔

مستفتی: گلاب خان، کراچی

الجواب حامداً ومصلیاً

واضح رہے کہ کسی بھی قدری (Valueable) چیز کے کرنسی بننے کے لیے ضروری ہے کہ اس مقامی حکومت اور اسٹیٹ کی جانب سے اس کرنسی کو سکہ اور ثمن تسلیم کر کے اس کو عام معاملات (لین دین) میں زرِ مبادلہ کا درجہ دے دیا گیا ہو، ایسی کرنسی کو لوگ رغبت ومیلان کے ساتھ قبول کرنے کے لیے آمادہ بھی بن جائیں اور اُسے رواجِ عام مل جائے۔

۱:..... مذکورہ ڈیجیٹل کرنسی نہ تو کسی حکومت کی طرف سے تسلیم شدہ کرنسی (ثمن) ہے اور نہ ہی تمام لوگوں میں اس کا رواج ہے، لہٰذا اس کی ثمنیت قابلِ اعتبار نہیں ہے اور محض چند ٹوکن جن کی کوئی واقعی مالی حیثیت نہیں ہے، اس کی قیمت ۱۰۰ یورو سے ۲۸۰۰۰ تک مقرر کرنا درست نہیں ہے۔ نیز اگر مجوزہ ڈیجیٹل کرنسی کو بالفرض قانونی واصطلاحی کرنسی تسلیم کرلیا جائے تو ڈیجیٹل کرنسی کا مبادلاتی عمل (لین دین) شرعی لحاظ سے بیع صرف (نقدی کا لین دین) کہلائے گا، جبکہ نقدی کا آپس میں تبادلہ کرتے وقت ایک ہی مجلس میں قبضہ ضروری ہے، جبکہ مذکورہ کمپنی ٹوکن دینے کے ۹۰ دن بعد ان ٹوکنوں کو دگنا کر کے ڈیجیٹل کوائنز (سکوں) میں تبدیل کر کے دیتی ہے تو یہ بھی بیع صرف میں اُدھار کی ایک صورت ہونے کی وجہ سے ناجائز ہی ہے، لہٰذا سوال میں مذکور منافع کا پہلا طریقہ بھی ناجائز ہے۔ فتاویٰ شامی میں ہے:

''والمالية تثبت بتمول الناس كافة أو بعضهم والنقود يثبت بها وبإباحة الانتفاع به شرعاً۔'' (ج:۴،ص:۵۰۱،ط:۱ ایچ ایم سعید)

وفیہ ایضاً:

''هو مبادلة شئ مرغوب فيه بمثله على وجه مفيدٍ مخصوصٍ۔''

(ج:۴،ص:۵۰۶،ط:۱ ایچ ایم سعید)

بدائع الصنائع میں ہے:

ترک دنیا سے مراد یہ ہے کہ نہ کسی چیز کے آنے کی خوشی ہو اور نہ جانے کا غم۔ (حضرت مجدد الف ثانی رحمۃ اللہ علیہ)

''وأما الشرائط (فمنها) قبض البدلين قبل الافتراق لقوله عليه الصلاة والسلام في الحديث المشهور والذهب بالذهب مثلاً بمثل يداً بيد والفضة بالفضة مثلاً بمثل يداً بيد، الحديث۔'' (فصل فی شرائط الصرف، ج:۵، ص:۲۱۵)

۲..... مذکورہ کمپنی کے منافع حاصل کرنے کا دوسرا طریقہ جس کی تین صورتیں ہیں، یہ تینوں صورتیں دراصل کمیشن کے تحت آتی ہیں اور کمیشن کی اسلامی قانونِ تجارت اور تبادلہ میں مستقل تجارتی حیثیت نہیں ہے، اس لیے کہ جسمانی محنت (جو کہ تجارت کا ایک اہم جزء ہے) کے غالب عنصر سے خالی ہونے کی بنا پر فقہاء کرام نے اصولاً اس کو ناجائز قرار دیا ہے، لیکن لوگوں کی ضرورت اور تعامل کی وجہ سے اس کی محدود اور مشروط اجازت دی ہے، بظاہر مذکورہ کمپنی کا مقصد زیادہ سے زیادہ لوگوں کا سرمایہ اپنے کاروبار میں لگا کر اور ممبر در ممبر سازی کر کے زیادہ سے زیادہ رقم حاصل کرنا اور اس حاصل ہونے والی رقم سے لوگوں کو کمیشن فراہم کرنا ہے، لہٰذا اس کمپنی سے معاملہ کرنا اور اس میں سرمایہ کاری کر کے منافع حاصل کرنا جائز نہیں ہے، چونکہ اس کمپنی کے کوائنز اور ٹوکن خریدنا جائز نہیں ہے، اسی طرح اس کمپنی کے ممبر بن کر مذکورہ تینوں صورتوں ''Direct Sale''، ''Network Bounus'' اور ''Matching Bounus'' کے ذریعے کمیشن حاصل کرنا بھی درست نہیں ہے۔ فتاویٰ شامی میں ہے:

''والربح إنما يستحق بالمال أو بالعمل أو بالضمان۔''

(فتاویٰ شامی، کتاب المضاربۃ، ج:۵، ص:۶۴۶، ط: ایچ ایم سعید)

وفیہ ایضاً:

''سئل عن محمد بن سلمة عن أجرة السمسار: فقال: أرجو أنه لا بأس به وإن كان في الأصل فاسداً لكثرة التعامل وكثير من هذا غير جائزة فجوزوه لحاجة الناس إليه۔''

(فتاویٰ شامی، مطلب فی أجرۃ الدلال، ج:۶، ص:۶۳، ط: ایچ ایم سعید)

الأشباہ والنظائر میں ہے:

''ما أبيح للضرورة يقدر بقدرها۔'' (الأشباہ والنظائر، القاعدۃ الخامسۃ: الضرر یزال، ص:۸۸، قدیمی)

وفیہ ایضاً:

''وصرح به في فتاوى قاري الهداية ثم قال والعقد إذا فسد في بعضه فسد في جميعه۔'' (الأشباہ والنظائر، القاعدۃ الثانیۃ، ص:۱۱۷، قدیمی)

۳..... مذکورہ کمپنی کے کوائنز (سکوں) کا حصول اور ان کی خرید و فروخت چونکہ ناجائز ہے، اسی طرح ان کوائنز کو دگنا کر کے بیچنا بھی ناجائز ہے۔ البنایہ شرح الہدایہ میں ہے:

''إن فساد العقد في البعض إنما يؤثر في الباقي إذا كان المفسد

مقارناً۔" (البنایہ شرح الہدایہ، ج:۸، ص:۱۷۷)

نیز ان کوائنز (سکوں) کی زیادتی بلاعوض ایک عقد میں لازم ہونے کی وجہ سے بھی جائز نہیں ہے۔

فتاویٰ شامی میں ہے:

"باب الربا هو لغةً مطلق الزيادة وشرعاً (فضل) ولو حكماً فدخل ربا النسيئة والبيوع الفاسدة فكلها من الربا فيجب رد عين الربا ولو قائمًا لارد ضمانه لأنهٗ يملك بالقبض قنية وبحر (خال عن عوض) ..... مشروط ذلك الفضل لأحد العاقدين۔" (فتاویٰ شامی، ج:۵، ص:۱۶۸، ۱۶۹، ط:ایچ ایم سعید)

۴، ۵..... مذکورہ کمپنی کا ٹوکن اور کوائنز کا لین دین کرنا چونکہ ناجائز ہے، اس لیے اگر کوئی اس کمپنی میں صرف کوائنز حاصل کرنے کے لیے رکنیت حاصل کرے اور نیٹ ورکنگ (Networking) کے ذریعے اگرچہ ممبر سازی نہ کرے، تب بھی ان کوائنز کو خریدنا جائز نہیں ہے۔

نیز اس طرح کی مشکوک کمپنی کے کاروبار میں سرمایہ کاری کرنا بھی درست نہیں ہے، اس لیے کہ شریعتِ اسلامی میں کاروبار اور لین دین کا مدار معاملات کی صفائی اور دیانت وامانت پر ہے اور فرضی چیزوں کے بجائے اصلی اور حقیقی چیزوں کی خرید وفروخت اور حقیقی محنت پر زور دیتی ہے اور استفتاء کے ساتھ منسلکہ فتویٰ سے یہ بھی بات واضح ہوتی ہے کہ "One Coin" (ون کوائن) کمپنی کے معاملات صاف اور واضح نہیں ہیں، لہٰذا ان سے اجتناب کرنا ضروری ہے، کیونکہ یہ بظاہر دوسروں کا مال، غیر واضح، مبہم اور ناجائز طریقے سے ہتھیانے کے مترادف ہے، جسے شرعی اصطلاح میں "اکل باطل" کہتے ہیں۔ تفسیر کبیر میں ہے:

"قال بعضهم: اللّٰه تعالى إنما حرم الربا حيث أنه يمنع الناس عن الاشتغال بالمكاسب..... فلايكاد يتحمل مشقة الكسب والتجارة والصناعات الشاقة۔"

(التفسیر الکبیر للرازی، سورۃ البقرۃ، ج:۷، ص:۹۱، ایران)

"بعض علماء فرماتے ہیں: اللہ تعالیٰ نے اس لیے سود کو حرام قرار دیا ہے کہ یہ لوگوں کو اسباب معاش اختیار کرنے سے روکتا ہے ..... لہٰذا لوگ کمائی، تجارت اور سخت محنتوں کے بوجھ برداشت کرنے سے کتراتے ہیں۔"

احکام القرآن میں ہے:

"نهى لكل أحد عن أكل مال نفسه ومال غيره بالباطل وأكل مال نفسه بالباطل إنفاقهٗ في معاصي اللّٰه وأكل مال الغير بالباطل قد قيل: فيه وجهان: أحدهما ما قال السدي وهو أن يأكل بالربا والقمار والبخس والظلم وقال ابن عباسؓ رضي اللّٰه تعالى عنه والحسن رحمه اللّٰه تعالى أن يأكلهٗ بغير عوض۔"

(احکام القرآن، ج:۳، ص:۲۱۹، دار الکتب العلمیہ، بیروت)

''ہر ایک کو اپنا مال اور دوسروں کا مال ناحق طور پر کھانے سے منع کیا گیا ہے۔ اپنے مال کو ناحق طور پر کھانا یہ ہے کہ اس کو اللہ تعالیٰ کی نافرمانی میں خرچ کیا جائے اور دوسرے کے مال کو ناحق طور پر کھانے کے متعلق آیا ہے اس کی دو صورتیں ہیں: پہلی صورت: سدیؒ فرماتے ہیں: اس کو سود، جوا، کمی (ناپ تول میں) اور ظلم کے ذریعہ کھائے۔ حضرت ابن عباسؓ اور حسنؒ فرماتے ہیں کہ: اس کو بغیر عوض کے کھائے (سودی معاملہ کرے)۔''

الجواب صحیح	الجواب صحیح	الجواب صحیح	کتبہٗ
ابوبکر سعید الرحمٰن	محمد شفیق عارف	رفیق احمد بالاکوٹی	محمد طیب حیدری
			تخصص فقہِ اسلامی

جامعہ علوم اسلامیہ علامہ بنوری ٹاؤن کراچی

نوٹ: زیر نظر سوال وجواب مولانا مفتی محمود اشرف صاحب دامت برکاتہم کی خدمت میں پیش کیا گیا تھا، استادِ محترم کی رائے تھی کہ مال کا "عین" ہونا ضروری ہے، اور BITCOIN اعیان میں سے نہیں ہے بلکہ اعراض میں سے ہے، اس لئے اس پر مال کی تعریف صادق نہیں آتی۔ اس کے بعد یہ مسئلہ شیخ الاسلام حضرت نائب صدر صاحب دامت برکاتہم کی خدمت میں پیش کیا گیا، حضرت نے فرمایا کہ ابھی اس کی صورتحال پوری طرح واضح نہیں ہے، اسلئے فی الحال اس کا جواب دینے سے توقف کیا جائے۔

حررہ: العبد محمد عزیر قاسم

4/صفر/1438ھ

5/نومبر/2016ء

بٹ کوئن: تعارف

آزاد دائرۃ المعارف، وکیپیڈیا سے

بٹ کوئن) انگریزی (bitcoin :ایک ڈیجیٹل کرنسی اور پیئر ٹو پیئر پیسٹ نیٹ ورک ہے جو آزاد مصدر دستور پر مبنی ہے[8] اور عوامی نوشتہ سودا کا استعمال کرتی ہے۔ بٹ کوئن کمانے یا حاصل کرنے میں کسی شخص یا کسی بینک کا کوئی اختیار نہیں۔ یہ مکمل آزاد کرنسی ہے، جس کو ہم اپنے کمپیوٹر کی مدد سے بھی خود بنا سکتے ہیں۔

بٹ کوئن کرنسی کا دیگر رائج کرنسیوں مثلاً ڈالر اور یورو سے موازنہ کیا جاسکتا ہے، لیکن رائج کرنسیوں اور بٹ کوئن میں کچھ فرق ہے۔ سب سے اہم فرق یہ ہے کہ بٹ کوئن مکمل طور پر ایک ڈیجیٹل کرنسی ہے جس کا وجود محض انٹرنیٹ تک محدود ہے، خارجی طور پر اس کا کوئی جسمانی وجود نہیں۔ اسی طرح بٹ کوئن کرنسی کے پیچھے کوئی طاقتور مرکزی ادارہ مثلاً مرکزی بینک نہیں ہے اور نہ ہی کسی حکومت نے اب تک اسے جائز کرنسی قرار دیا ہے، اسی وجہ سے ریاستہائے متحدہ امریکہ کے وزارت خزانہ نے اسے غیر مرکزی کرنسی (decentralized currency) قرار دیا ہے[9]، کیونکہ اس کرنسی کو ایک شخص براہ راست دوسرے شخص کو منتقل کر سکتا ہے، اس کے لیے کسی بینک یا حکومتی ادارہ کی ضرورت نہیں ہوتی۔ تاہم انٹرنیٹ کے ذریعہ بٹ کوئن کو دیگر رائج کرنسیوں کی طرح ہی استعمال کیا جاسکتا ہے۔

بٹ کوئن کا آغاز 2009ء میں کازب نام ستوشی ناکاماتو نے کیا۔[10] اسے کرپٹو کرنسی کہتے ہیں کیونکہ یہ پبلک کی کرپٹوگرافی کے اصولوں پر مبنی ہے۔[11]

یہ کرنسی حسابی عمل لوگرتھم کی بنیاد پر کام کرتی ہے، جس کے لئے کمپیوٹر کو انٹرنیٹ سے منسلک کر کے، کمپیوٹر کے پروسیسر سے کام لیا جاتا ہے۔ جس کمپیوٹر کا پروسیسر جتنا طاقتور ہوتا ہے، اتنی جلد وہ حسابی عمل لوگرتھم کا سوال حل کر کے بٹ کوئن بناتا ہے۔

بٹ کوئن خاصی تحقیق و تجسس کا موضوع بھی رہا ہے، کیونکہ کرپٹوگرافی کرنسی ہونے کی وجہ سے اس کے مالکان اور صارفین پتہ لگانا خاصا مشکل ہے، اس وجہ سے اس کا غیر قانونی استعمال بھی کیا جاسکتا ہے۔ 2013ء میں غیر قانونی سرگرمیوں میں ملوث ویب سائٹ سلک روڈ کو امریکی ایف بی آئی نے بند، اور 144,000 بٹ کوئنز کو منجمد کر دیا، اس وقت اس کی قیمت 28.5 ملین ڈالرز تھی۔[12] جبکہ امریکی حکومت بٹ کوئن کے معاملہ میں دیگر حکومتوں سے زیادہ فراخ دلی سے کام لیتی ہے۔[13] چین میں یوان کے ساتھ بٹ کوئن کی فروخت پر پابندی ہے، نیز بٹ کوئن منڈیاں (exchanges) کے لیے بینک اکاؤنٹ رکھنے کی اجازت نہیں۔

کرپٹو کرنسی[ترمیم]

بٹ کوئن کو ایک کرپٹو کرنسی) انگریزی (cryptocurrency : سمجھا جاتا ہے، اس کا مفہوم یہ ہے کہ یہ کرنسی بنیادی طور پر رازداری کے اصولوں کو ملحوظ رکھتی ہے۔ نیز اسے اپنی نوعیت کی واحد کرنسی سمجھا جاتا ہے، لیکن درحقیقت اس طرح کی کم از کم 60 کرپٹو کرنسیاں انٹرنیٹ پر موجود ہیں، جن میں سے 6 کرنسیاں اصل ہیں۔ چونکہ بٹ کوئن ایک آزاد مصدر کرنسی ہے، اس لیے اس کی نقل

اور اس میں کچھ اصلاحات کر کے دوسری نئی کرنسی بنائی جا سکتی ہے، اس لیے اس وقت موجود تمام کرپٹو کرنسیاں (باستثناء ریپل) انگریزی: Ripple) بٹ کوئن کی طرح ہی کام کرتی ہیں۔[14]

http://www.ittaleem.com/urdu-tutorials/340103-1576-1657-1705-1608-1574-1606-1705-1740-1575-1729-1746-1567-a.html

السلام علیکم

موجودہ دور کی سب سے اہم کرنسی بٹ کوئن کے مطابق میں آج کچھ باتیں آپ کو بتانا چاہوں گا۔

بٹ کوئن پہلی ڈیجیٹل کرنسی ہے۔ جس کو کمانے میں یا حاصل کرنے میں کسی شخص یا کسی بینک کا کوئی اختیار نہیں۔
یہ مکمل آزاد کرنسی ہے، جس کو ہم اپنے کمپیوٹر کی مدد سے بھی خود جنریٹ کر سکتے ہیں۔
اس کرنسی کو بنانے کا خیال سب سے پہلے 2009 میں تب آیا، جب معاشی بحران کے سبب امریکہ کے کئی بینک دوالیہ ہو گئے، اور لوگوں کا کئی بلین ڈالرز کا نقصان ہوا۔
اس کرنسی کو کرپٹو کرنسی کا نام دیا گیا۔ یہ کرنسی حسابی عمل لوگرا تھم کی بنیاد پر کام کرتی ہے۔
جس کے لئے ہم اپنے کمپیوٹر کو انٹرنیٹ سے منسلک کر کے، کمپیوٹر کے ان حصوں کو کام میں لاتے ہیں جو حسابی عمل میں بھرپور حصہ لیتے ہیں۔
جیسا کہ ہمارے کمپیوٹر کا پروسیسر۔
اس حسابی عمل کی بدولت کمپیوٹر ایک لوگرا تھم کا سوال حل کرتا ہے۔

کرپٹو کرنسی مائننگ

کرپٹو کرنسی مائننگ کی اصطلاح اس کام کے لئے استعمال کی جاتی ہے، جس کی بدولت ہمارا کمپیوٹر کسی کرپٹو کرنسی کو کھود کر نکالتا ہے۔
لوگرا تھم کے ایک مشکل سوال کو حل کرنے کے لیئے ہم اپنے کمپیوٹر کو کسی ایک پول سے منسلک کر دیتے ہیں، جہاں ہمارے کمپیوٹر جیسے ہزار ہا کمپیوٹر اس کام کو کرنے میں جتے ہوتے ہیں۔
اور جیسے ہی ایک بلاک حل ہوتا ہے، تو اس سے برآمد ہونے والی کرنسی کو ان تمام کمپیوٹرز میں ان کی اسپیڈ اور کام کرنے کی صلاحیت کے

حساب سے تقسیم کر دی جاتی ہے۔

کرپٹو کرنسی کا خاندان

اسکی 2 بنیادی اقسام ہیں، جس میں ایک کا نام سکرپٹ کوئن ہے جبکہ دوسرے کو شاو256 کے نام سے جانا جاتا ہے۔

دونوں کوئنز کے مابین بنیادی فرق

ان دونوں اقسام کے کوئنز کا تعلق گو کہ کرپٹو کرنسی سے ہی ہے، مگر ان دونوں میں بے انتہا فرق ہے۔
جیسے سکرپٹ کوئن کو ہم کم ہیش پاور سے مائن کر سکتے ہیں، جیسے اپنے سی پی یو سے، جبکہ شاو کوئن، سی پی یو کے بس کی بات نہیں۔
سکرپٹ کوئن کی مشکلات کم ہوتی ہیں، جس کے سبب وہ جلدی بر آمد کیا جا سکتا ہے، جبکہ شاو کوئن کی مشکلات انتہائی زیادہ ہوتی ہیں اس لئے اسے کسی عام سی پی یو سے مائنن نہیں کیا جا سکتا۔
سکرپٹ کوئن کو سی پی یو سے بھی مائن کیا جا سکتا ہے، جبکہ شاو کوئن کے لئے ہمیں کمپیوٹر میں الگ سے ایک گرافکس کارڈ لگانا پڑتا ہے۔

کرپٹو کوئن کی اقسام

کرپٹو کوئن کی سب سے پہلی قسم بٹ کوئن کو جاپانی ریاضی دان ستوشی ناکاموٹو نے 2009 میں متعارف کروایا۔ اسی لیے کسی بھی کوئن کی ماں، یا مائنر و قیمت کو ستوشی کہا جاتا ہے۔
بٹ کوئن کے علاوہ اس وقت کئی اور کوئن مارکیٹ میں آ چکے ہیں۔
جن میں لائٹ کوئن، ہائیر کوئن، فیدر کوئن، ورلڈ کوئن، مون کوئن، ڈیجیٹل کوئن۔۔۔۔ وغیرہ

مزید دیکھیے

http://dailypakistan.com.pk/special-report/31-Mar-2014/88187

English Articles

Cryptocurrency

virtual currencies.

Digital currencies

UK: Bitcoin is treated as **'private money'**. When bitcoin is exchanged for sterling or for foreign currencies, such as euro or dollar, no VAT will be due on the value of the bitcoins themselves. However, in all instances, VAT will be due in the normal way from suppliers of any goods or services sold in exchange for bitcoin or other similar cryptocurrency. Profits and losses on cryptocurrencies are subject to capital gains tax.[1]

Hong Kong SAR	Yes	On 16 November 2013, Norman Chan, the chief executive of Hong Kong Monetary Authority (HKMA) said that bitcoins is only a virtual commodity. He also decided that bitcoins will not be regulated by HKMA. However, the authority will be closely watching the usage of bitcoins locally and its development overseas.[93]
Germany	Yes	On 19 August 2013, the German Finance Ministry announced that bitcoin is now essentially a "unit of account" and can be used for the purpose of tax and trading in the country. It is not classified as a foreign currency or e-money but stands as "private money"

United States Bitcoin and other currencies were received generally positively, with it being stated that bitcoin was a "legal means of exchange" and that "online payment systems, both centralized and decentralized, offer legitimate financial services" by US officials such as Peter Kadzik and Mythili Raman [94][95] It was noted, however, that the Justice Department's Criminal Division has seen an increased use of virtual currencies for illegal purposes such as drugs and child pornographyThe U.S. Commodity Futures Trading Commission stated in March 2014 it was considering regulation of digital currenciesAs of November 2014, there are no final rules at the U.S. state level yet.

http://en.wikipedia.org/wiki/Cryptocurrency

Fraud[edit]

On August 6, 2013 Magistrate Judge Amos Mazzant of the Eastern District of Texas federal court ruled that because cryptocurrency (expressly bitcoin) can be used as money (it can be used to purchase goods and services, pay for individual living expenses, and exchanged for conventional currencies), it is a currency or form of money. This ruling allowed for the SEC to have jurisdiction over cases of securities fraud involving cryptocurrency.[96]

GBL, a Chinese bitcoin trading platform suddenly shut down, and up to $5 million worth of bitcoin disappeared with it.[83] Subscribers were unable to log into the Chinese bitcoin platform on October 26, 2013.

In February 2014 cryptocurrency made national headlines due to the world's largest bitcoin exchange, Mt. Gox, declaring bankruptcy. The company stated that it had lost nearly $473 million of their customer's bitcoins likely due to theft. This was equivalent to approximately 750,000 bitcoins, or about 7% of all the bitcoins in existence. Due to this crisis, among other news, the price of a bitcoin fell from a high of about $1,160 in December to under $400 in February.[84]

List of cryptocurrencies[edit]

This is a list of some of the well-known cryptocurrencies. There were more than 530 cryptocurrencies available for trade in online markets as of 7 November 2014 but only 10 of them had market capitalizations over $10 million.[85]

Release	Currency	Symbol	Founder	Hash Algorithm	Timestamping
2009	Bitcoin[86][a]	BTC[87][88]	Satoshi Nakamoto[86][89][b]	SHA-256d[c][90][91]	POW[c][92][93]
2011	Namecoin[86][d]	NMC	Vincent Durham[94][95][96]	SHA-256	POW
2011[97]	Litecoin[86][e]	LTC	Charles Lee[98]	scrypt[99]	POW
2012[100]	Peercoin	PPC	Sunny King (pseudonym)[101]	SHA-256[102]	POW & POS
2013	Ripple[86] [103][104][105]	XRP[106]	Chris Larsen & Jed McCaleb[107]	ECDSA[f][5]	"Consensus"

Release	Currency	Symbol	Founder	Hash Algorithm	Timestamping
2013	Mastercoin	MSC	J. R. Willett[55]	SHA-256d[53]	N/A
2013	Primecoin	XPM	Sunny King (pseudonym)[63]	1CC/2CC/TWN[64]	POW[64]
2013	Dogecoin[64][65]	DOGE	Jackson Palmer & Billy Markus[66]	scrypt[52]	POW
2014[67]	Darkcoin[64][7]	DRK	Evan Duffield & Kyle Hagan[68]	X11	POW & POS[64][8]
2014	Auroracoin	AUR	Baldur Odinsson (pseudonym)[69]	scrypt	POW
2014	BlackCoin	BC, BLK			POS

http://www.coindesk.com/information/is-bitcoin-legal/

Legislative branch

The SEC case has forced the legislative branch of government to consider bitcoin's legal status. Shavers had claimed that he could not be prosecuted for securities fraud, as bitcoin wasn't money. However, Judge Amos Mazzant issued a memorandum arguing that bitcoin can be used as money.....

The Department of Homeland Security was the most worried about the

criminal threat from illicit use of bitcoin, while the Department of Justice, the Federal Reserve and the Department of Justice all acknowledged the legitimate uses of virtual currencies. The SEC argued that "any interests issued by entities owning virtual currencies or providing returns based on assets such as virtual currencies" were considered securities and thus fell under its remit.....

What this means to you

The legality of bitcoin depends on who you are, and what you're doing with it.

There are three main categories of bitcoin stakeholder. Someone may fall under more than one of these categories, and each category has its own legal considerations.

Users

These are individuals that obtain bitcoins, and either hoard them or spend them. Under the FinCEN guidance, users who simply exchange bitcoins for goods and services are using it legally.

FinCEN: "A person that creates units of this convertible virtual currency and uses it to purchase real or virtual goods and services is a user of the convertible virtual currency and not subject to regulation as a money transmitter."

Miners

According to the FinCEN guidance, people creating bitcoins and exchanging them for fiat currency are not safe.

FinCEN: "By contrast, a person that creates units of convertible virtual currency and sells those units to another person for real currency or its equivalent is engaged in transmission to another location and is a money transmitter."

Miners seem to fall into this category, which could theoretically make them liable for MTB classification. This is a bone of contention for bitcoin miners, who have asked for clarification. This issue has not to our knowledge been tested in court.

Exchanges

Exchanges are defined as MTBs.

FinCEN: "In addition, a person is an exchanger and a money transmitter if the person accepts such de-centralized convertible virtual currency from one person and transmits it to another person as part of the acceptance and transfer of currency, funds, or other value that substitutes for currency."

www.en.wikipedia.org/wiki/Money

Money is any item or verifiable record that is generally accepted as payment for goods and services and repayment of debts in a particular country or socio-economic context.[1][2][3] The main functions of money are distinguished as: a medium of exchange; a unit of account; a store of value; and, perhaps, a standard of deferred payment.[4][5] Any item or verifiable record that fulfills these functions can be considered money.

Money is historically an emergent market phenomenon establishing a commodity money, but nearly all contemporary money systems are based on fiat money.[6] Fiat money, like any check or note of debt, is without intrinsic use value as a physical commodity. It derives its value by being declared by a government to be legal tender; that is, it must be accepted as a form of payment within the boundaries of the country, for "all debts, public and private".[citation needed] Such laws in practice cause fiat money to acquire the value of any of the goods and services that it may be traded for within the nation that issues it.

Links

http://dailyanarchist.com/2013/01/30/is-bitcoin-sharia-compliant

الجواب باسم ملہم الصواب

Bitcoin اور اس کی ہم مثل دیگر مجازی / غیر حسی crypto currencies اور فقہ اسلامی میں مذکور مال اور ثمن کی تفصیلات پر تفصیلی غور کرنے کے بعد Bitcoin کی شرعی حیثیت ہماری رائے میں درج ذیل ہے:

1. Bitcoin شرعی لحاظ سے "مال" کے زمرے میں آتا ہے۔ مال کی تعریف فقہاء نے یہ کی ہے: "جس چیز کی طرف طبیعت (سلیمہ) مائل ہو، اور بوقت حاجت اسے محفوظ کرنا ممکن ہو۔" دور حاضر میں ایسی بیسیوں اشیاء ہیں جنہیں غیر حسی ہونے کے باوجود شرعاً بھی مال تسلیم کیا گیا ہے۔ Bitcoin بھی مال کی تعریف میں بیان کردہ ان دونوں شرائط پر پورا اترتا ہے:

   i. اس وقت ہزاروں لوگ اس کے ذریعہ تبادلہ کر رہے ہیں، کرنسیوں کے باہم تبادلے کے ریٹ بتانے والی معروف ویب سائٹس Bitcoin کا ایکسچینج ریٹ بھی بتاتی ہیں، جس سے یہ بات واضح ہوتی ہے کہ اس کا عرف عام قائم ہو چکا ہے۔

   ii. اسے کسی بھی برقی آلہ (Electronic Device) میں محفوظ کیا جا سکتا ہے۔ اگر کوئی شخص اسے کسی آلہ میں محفوظ کر کے سالوں استعمال نہ بھی کرے تو وہ محفوظ رہتے ہیں۔ یہ ضائع اسی وقت ہوں گے جب وہ برقی آلہ گم ہو جائے یا خراب ہو جائے۔ ضائع ہونے کی صورت میں حکومت یا کوئی اور اتھارٹی اس کی ضامن نہیں اور اس کا بدل ادا کرنے کی پابند نہیں، اس سے یہ ثابت ہوا کہ یہ بذات خود مال ہے چیک یا ڈرافٹ کی طرح کسی اور کی رسید نہیں ہے۔ ﴿فقہی مقالات، کرنسی نوٹ کی شرعی حیثیت﴾ میں ہے: **"ثمن عرفی کی ہلاکت کے وقت حکومت اس کا بدل ادا نہیں کرتی ہے۔"**

2. پھر یہ شرعی لحاظ سے ثمن بھی ہے۔ شریعت میں ہر اس چیز کو ثمن رائج کہا جاتا ہے جس کی لوگوں کے عرف میں مالیت ہو اور لوگ اسے بطور ذریعہ مبادلہ (کرنسی) کے طور پر استعمال کرنا شروع کر دیں۔ مختلف ادوار میں کرنسی مختلف مراحل سے گزرتی رہی ہے، ان تمام اقسام کی کرنسیوں کے ساتھ تبادلے کو فقہاء نے جائز کہا ہے، چاہے اس کی مالیت کسی حکومت کے جاری کرنے سے پیدا ہوئی ہو جیسے کرنسی نوٹ جسے Legal tender کہا جائے یا محض لوگوں کے استعمال سے رائج

0303 6406067 PDF Book Company

ہوئی ہو، دونوں صورتوں میں وہ شرعاً کرنسی کہلائے گی۔ لہٰذا Bitcoins اور دیگر ڈیجیٹل / Virtual کرنسیاں شرعی لحاظ سے فلوس رائجہ کے حکم میں ہیں۔ ان میں اکثر علامات کرنسی نوٹ کی ہیں اور ان کے تمام احکام وہی ہونگے جو کرنسی نوٹ کے ہیں۔ جیسے: جریان الربا، وراس مال المضاربہ، والشرکۃ، والسلم بہا، والاستقراض، ووجوب الزکاۃ۔ (البتہ ان دونوں میں فرق یہی ہے کہ کرنسی نوٹ کی ثمنیت حکومت کی مرہون منت ہوتی ہے، حکومت اگر ثمنیت باطل کردے تو ان کی کوئی قیمت باقی نہیں رہے گی، [کرنسی نوٹ کی شرعی حیثیت: ص25] جبکہ غیر حسی کرنسیوں کی ثمنیت باصطلاح الناس قائم ہوتی ہے، لہٰذا جب تک یہ عرف قائم ہے ثمنیت بھی باقی رہے گی، عرف ختم ہونے کے بعد یہ سلعہ کے حکم میں ہوگا۔ فقہ میں اس کی مثال نبھرجہ یا زیوف کی ہوگی)

الدر المختار وحاشية ابن عابدين (رد المحتار) (5/ 233)

مطلب في النبهرجة والزيوف والستوقة وفي التتارخانية الدراهم أنواع أربعة: جياد، ونبهرجة، وزيوف، وستوقة. واختلفوا في تفسير النبهرجة، قيل هي التي تضرب في غير دار السلطان والزيوف: هي المغشوشة. والستوقة: صفر مموه بالفضة. وقال عامة المشايخ: الجياد فضة خالصة تروج في التجارات وتوضع في بيت المال. والزيوف ما زيفه بيت المال: أي يرده، ولكن تأخذه التجار في التجارات لا بأس بالشراء بها، ولكن يبين للبائع أنها زيوف. والنبهرجة: ما يرده التجار. والستوقة: أن يكون الطاق الأعلى فضة والأسفل كذلك وبينهما صفر وليس لها حكم الدراهم اهـ.

3. اس کے استعمال کے جواز کا مدار اس بات پر ہے کہ مستعمل کس ملک میں اسے استعمال کر رہا ہے۔
   a. بعض ممالک نے اسے قانونی طور پر تسلیم کیا ہے اور اس پر دیگر کرنسیوں کی طرح ٹیکس بھی لگایا ہے، جیسے امریکا، جرمنی، ہالینڈ اور اکثر ترقی یافتہ ممالک۔
   b. بعض نے اس سے منع نہیں کیا اور نہ ہی اس کے استعمال کے ضوابط Regulations بنائے ہیں، جیسے ہانگ کانگ۔
   c. بعض ممالک اس معاملے میں بالکل ساکت ہیں جیسے پاکستان۔

/http://www.coindesk.com/information/is-bitcoin-legal

اس قسم کے ممالک میں Bitcoins کو بطور کرنسی استعمال کرنا جائز ہے۔

جن ممالک میں اس کو ذریعہ تبادلہ بنانا قانونی طور پر منع ہے (ایسے ممالک بہت ہی کم ہیں) ان میں اس حکم حاکم کی وجہ سے اس کا استعمال جائز نہیں ہو گا۔

==========

http://en.wikipedia.org/wiki/Cryptocurrency

http://en.wikipedia.org/wiki/Bitcoin

--(البحر الرائق شرح كنز الدقائق 277/5 ط دار الكتاب الإسلامي)--

وفي الكشف الكبير المال ما يميل إليه الطبع ويمكن ادخاره لوقت الحاجة والمالية إنما ثبت بتمول الناس كافة أو بتقوم البعض والتقوم يثبت بها وبإباحة الانتفاع له شرعا فما يكون مباح الانتفاع بدون تمول الناس لا يكون مالا كحبة حنطة ما يكون مالا بين الناس ولا يكون مباح الانتفاع لا يكون متقوما كالحر

(منحة الخالق على البحر الرائق) لأن المال ما يميل إليه الطبع ويدخر لوقت الحاجة أو ما خلق لمصالح الآدمي ويجري فيه الشح والضنة اهـ أنواع الأموال من حيث الثمنية:

الموسوعة الفقهية، مصطلح: ثمن، 27/15

8- ذهب الحنفية إلى أن الأموال أربعة أنواع: (2)

أ- ثمن بكل حال، وهو النقدان، صحبه الباء أو لا، قوبل بجنسه أو بغير جنسه؛ لأن الثمن ما يثبت دينا في الذمة عند العرب، كذا ذكره الفراء، (3) والنقود لا تستحق بالعقد إلا دينا في الذمة، فكانت ثمنا بكل حال.

ب - مبيع بكل حال، كالدواب ونحوها من الأعيان غير المثلية والعدديات المتفاوتة؛ لأن العروض لا تستحق بالعقد إلا عينا فكانت مبيعة.

ج - ثمن من وجه نظرا إلى أنها مثلية ثبتت في الذمة فأشبهت النقد، ومبيع من وجه، نظرا إلى الانتفاع بأعيانها فأشبهت العروض. وذلك كالمثليات غير النقدين من المكيل والموزون والعددي المتقارب كالبيض. فإنه إن كان معينا في العقد كان مبيعا، وإن لم يكن معينا وصحبه الباء، وقوبل بالمبيع فهو ثمن. وإن لم يصحبه حرف الباء ولم يقابله ثمن فهو مبيع؛

لأن المكيل والموزون غير النقدين يستحق بالعقد عينا تارة، ودينا أخرى، فكان ثمنا في حال، مبيعا في حال.

د- ثمن بالاصطلاح، وهو سلعة في الأصل كالفلوس.

فإن كان رائجا كان ثمنا، وإن كان كاسدا فهو سلعة متمن.

فتح القدير للكمال ابن الهمام(169/6)

وأما الفلوس النافقة فلأنها تروج رواج الأثمان فالتحقت بها. قالوا: هذا قول محمد لأنها ملحقة بالنقود عنده حتى لا تتعين بالتعيين، ولا يجوز بيع الثمن بواحد بأعيانها على ما عرف، أما عند أبي حنيفة وأبي يوسف رحمهما الله تعالى لا تجوز الشركة والمضاربة بها لأن ثمنيتها لتبدل ساعة فساعة وتصير سلعة. وروي عن أبي يوسف مثل قول محمد، والأول أقيس وأظهر، وعن أبي حنيفة صحة المضاربة بها....؛ لأنها وإن خلقت للتجارة في الأصل لكن الثمنية تختص بالضرب المخصوص؛ لأن عند ذلك لا تصرف إلى شيء آخر ظاهرا إلا أن يجري التعامل باستعمالها ثمنا فتنزل التعامل بمنزلة الضرب فيكون ثمنا ويصلح رأس المال.

فتح القدير للكمال ابن الهمام(21/7)

وصورة أربع: أن يبيع فلسا بغير عينه بفلسين بغير أعيانهما لا يجوز لأن الفلوس الرائجة أمثال متساوية قطعا لاصطلاح الناس على سقوط قيمة الجودة منها فيكون أحدهما فضلا خاليا مشروطا في العقد وهو الربا.

وأن يبيع فلسا بعينه بفلسين بغير عينهما لا يجوز، وإلا أمسك البائع الفلس المعين وطالبه بفلس آخر. أو سلم الفلس المعين وقبضه بعينه منه مع فلس آخر لاستحقاقه فلسين في ذمته فيرجع إليه عين ماله ويبقى الفلس الآخر خاليا عن العوض.

وكذا لو باع فلسين بأعيانهما بفلس بغير عينه، لأنه لو جاز لقبض المشتري الفلسين ودفع إليه أحدهما مكان ما استوجب عليه فيبقى الآخر فضلا بلا عوض استحق بعقد البيع، وهذا على تقدير إن رضي بتسليم المبيع قبل قبض الثمن. والرابع أن يبيع فلسا بعينه بفلسين بعينهما فيجوز خلافا لمحمد. وأصله أن الفلس لا يتعين بالتعيين ما دام رائجا عند محمد، وعندهما يتعين، حتى لو هلك أحدهما قبل القبض بطل العقد. وجه قول محمد أن الثمنية ثبتت باصطلاح الكل فلا تبطل باصطلاحهما وإذا بقيت أثمانا لا تتعين فصار كما لو كانا بغير عينهما

الدر المختار وحاشية ابن عابدين (رد المحتار)(300/2)

[فرع] في الشرنبلالية: الفلوس إن كانت أثمانا رائجة أو سلعا للتجارة تجب الزكاة في قيمتها وإلا فلا. اهـ.

الدر المختار و حاشیۃ ابن عابدین (رد المحتار) (180/5)

تنبیہ] سئل الحانوتي عن بیع الذهب بالفلوس نسیئة. فأجاب: بانه یجوز إذا قبض أحد البدلین لما في البزازیة لو اشتری مائة فلس بدرهم یکفي التقابض من أحد الجانبین قال: ومثله مالو باع فضة أو ذهبا بفلوس کما في البحر عن المحیط قال: فلا یغتر بما في فتاوی قاری الهدایة من أنه لا یجوز بیع الفلوس إلی أجل بذهب أو فضة لقولهم لا یجوز إسلام موزون في موزون وإلا إذا کان المسلم فیه مبیعا کزعفران والفلوس غیر مبیعة بل صارت ثمانا اهـ.

واللہ سبحانہ وتعالی اعلم

احمد افغان

6 ربیع الثانی 1436ھ

مفتی محمد حسین باجوری صاحب کی رائے

اس کرنسی کی درج ذیل خصوصیات قابلِ غور ہیں۔

1) کوئی مجاز و معتبر اتھارٹی جو اس کی اجراء اور استخدام کو اپنی ذمہ داری پر جاری کر سکے۔ (یہ بات ثمن خلقی میں بھی تھی، لہذا مضر نہیں۔ افغان)

2) اس کے ضائع ہونے کے احتمالات کافی زیادہ ہیں۔ مثلاً ہارڈ ڈرائیو کی خرابی پاس مرڈ کا کم ہو جانا۔ (آئی ٹی کی اس ترقی کے بعد تعلیم یافتہ لوگوں کے لیے یہ احتمال بے حیثیت ہے۔ افغان)

3) اس کا آخر تک تعاقب ممکن نہیں ہوتا، لہذا اس کے ذریعے مضر اشیاء، مخدرات وغیرہ کی تجارت کو فروغ مل سکتی ہے۔ (درست)

4) کرنسی نوٹ ویسے استحصال کا ذریعہ ہے (اگرچہ عرف و تعامل اور متبادل نہ ہونے کی وجہ سے اس کے استعمال کی اجازت ہے) جبکہ کرنسی نوٹس میں بہت سارے حدود و قیود ہیں تو جبکہ پیپر کرنسی کی جگہ عالمی کرنسی بننے کی جیسا

کہ اس کے بنیادی مقاصد میں یہ بات شامل ہے کہ کرنسی کو ساری دنیا کے لئے ایک اور یکساں کیا جائے جیسا کہ نیٹ کے ذریعے اسالیب النشر یکساں ہو چکے ہیں۔

5) Block Chain کے ذریعے صفقات کی حفاظت کافی حد تک باعث اطمینان ہے لیکن یہ سارا حفاظتی نظام جن آلات کے ذریعے ہوتی ہیں وہ کسی بھی وقت کرپٹ ہو سکتے ہیں۔(اس وقت دنیا کا سارا فائنشل نظام ڈیجیٹلائزی چل رہا ہے، یہ امکان ہر جگہ ہے۔ افنان)

6) ڈیجیٹنگ کرنسیز کا یہ سلسلہ چلتا جارہا ہے چنانچہ 60 کے قریب کرنسیاں وجود میں آچکی ہیں جن میں سے چھ کو اساسی عملات قرار دیا جاتا ہے۔

7) جب ایک قوت حاکم اس کے پیچھے نہیں تو اس کے طلب ورسد کا صحیح اندازہ اور اس کے تحت اس کی حقیقی حالت کو کنٹرول کرنا یا معلوم کرنا ناممکن کے درجے میں ہے جس کی وجہ سے تعزیر و تبلیس بہت آسان ہے۔(مسائل تو پیدا ہی کنٹرول کی وجہ سے ہو رہے ہیں، اگر خالصتاً طلب ورسد پر ہو جیسے نقدین میں اصل نظام یہی تھا، تو بہتر ہے)

8) کرنسی ایسی چیز ہونی چاہئے ہر عام و خاص کی بروقت رسائی ممکن ہو اور اس میں یہ صفت نہیں۔(صغری مسلم نہیں)

9) کرنسی ایسی ہونے چاہئے جس کی ریزگاری اور وحدات باآسانی دستیاب ہوں، یہاں بہت پیچیدہ طریقے ہیں، نیز ایک Bitcom کے ہزاروں اکائیاں بن سکتی ہیں، جو ناقابل ضبط بھی ہیں۔

10) جرمنی کے علاوہ سرکاری سطح پر اس کی تمنیت کی حیثیت تسلیم نہیں۔(اکثر دنیا اسے سند جواز فراہم کر چکی ہے۔ دیکھیے)

(https://en.wikipedia.org/wiki/Legality_of_Bitcoin_by_country

11) اس طرح کرنسیوں کی ریٹ میں نامعلوم وجوہات کے غیر متوقع اور شدید اتار چڑھاؤ جاری رہتا ہے چنانچہ 6 جنوری 2014ء میں ایک Bitcom کی ریٹ 917 ڈالر جب کہ اس سال دسمبر میں 330 ڈالر تک آگیا تھا۔ اور 2014ء کا سب سے خراب اور باعث نقصان کرنسی ریٹ قرار پایا۔ اس وجہ سے بینک اس سے اعتراز کرتے ہیں۔ (خدشہ حقیقی ہے)

مذکورہ بالا وجوہ اس میں خرید بھی تحقیق کر جانے کی وجہ سے اس طرح کی کرنسی کی زبردست حوصلہ شکنی کرنی چاہئے، تاہم جہاں رائج ہو تو وہاں آپ کے ذکر کردہ وجوہات کی بناپر اس پر کئے جانے والے معاملات کو درست قرار دیا جانا چاہئے، ویسے بھی نوٹ میں اصلی مالیت مخصوص نمبر کی وجہ سے ہے باقی مشکل وصورت تو نمبر کے نقل وحمل کو آسان بنانے کے لئے ہے، لہٰذا کوئی جوہری فرق نہیں۔

مفتی حسین صاحب کی اس قسم کے معاملات میں یہ رائے ہے کہ ہمیں صرف حکم فقہی نہیں لکھنا چاہیے، بلکہ ان کے خارجی منافع و مضار کو مد نظر رکھتے ہوئے مشورہ بھی دینا چاہیے۔ یا سد ذریعہ کے طور پر کراہت کا حکم لگانا چاہیے۔ (ناقل)

رائے گرامی مفتی ارشاد اعجاز (شریعہ ایڈوائزر بینک اسلامی)

بٹ کوائن کی اساس تو کسی ملک کے نقود ہی ہوتے ہیں اور ممکنہ طور پر بٹ کوائن کسی اثاثے کے بدلے بھی جاری کیا جاسکتا ہے. یعنی ڈالر یا پاؤنڈ کو ایک آئی ٹی کے سسٹم (سافٹویئر) میں ڈپازٹ کرکے دینے والے کا اکاؤنٹ کریڈٹ کردیا جاتا ہے پھر مختلف تبادلوں کے نتیجے میں یہ کرنسی استقلال حاصل کرلیتی ہے. اس کا مطلب یہ ہوا کہ یہ کرنسی اصالتاً کسی اور کرنسی یا اثاثے کی بنیاد پر قائم ہونے کے بعد استقلال حاصل کرتی ہے۔

کرنسی کے نظام پر دو حیثیتوں سے گفتگو کی جانی چاہیے. ایک شرعی اور دوسری حیثیت انتظامی ہے۔

شرعاً تو کرنسی کے اجراء پر کوئی خاص قید و بند تو نہیں ہے۔ حکومت کے علاوہ افراد بھی فی نفسہ اس کو جاری کر سکتے ہیں جیسے بیع مقایضہ میں افراد کسی بھی مشروع چیز کو ثمن بنا سکتے ہیں۔

انتظامی رخ پر کرنسی کے اجراء اور نظم و نسق پر بہت سی شرائط کا لحاظ رکھا جانا ضروری ہو گا۔ کرنسی خداع پر مبنی نہ ہو، افراد کے کنٹرول کی وجہ سے اس میں تعامل کرنے والوں کے حقوق کا تحفظ، حکومتی قوانین کی پاسداری اور اس طرح کے دیگر انتظامی امور کا لحاظ ضروری ہو گا۔

لہذا میری رائے میں بٹ کوائن فی نفسہ جائز زر مبادلہ ہے کیونکہ اس کی اساس اگرچہ خود کرنسی یا اثاثے تھے مگر اب یہ خود مستقل بالذات زر کا درجہ کسی نہ کسی حد تک رکھتا ہے۔ اور زر کے لئے کسی اثاثے یا نقود کی اساس پر ہونا ضروری نہیں جیسا کہ فیاٹ منی کے جواز پر علماء کی آراء سے یہ واضح ہوتا ہے۔ البتہ اس کے جواز کے فتوی کے ساتھ قانونی اور انتظامی شرائط کا ذکر ضروری ہے تاکہ مستفتی کو اس کی صحیح حیثیت کا علم ہو سکے خصوصاً وہ ممالک جہاں یہ قوانین کے تحت ممنوعات میں شامل ہو وہاں اس میں تعامل ناجائز ہو گا۔

واللہ اعلم بالصواب والغیر۔

ارشاد احمد اعجاز

بسم اللہ الرحمن الرحیم

الجواب حامدًا ومصلیًا

بٹ کوئن (Biteoin) اور دیگر غیر حسی کرنسیوں (Digital Currencies) کے متعلق ماہرین اقتصاد کے فراہم کردہ مطالعتی مواد پر تفصیلی غور وفکر کرنے کے بعد، بٹ کوئن کی فقہی تکییف اور اس کے جواز یا عدم جواز کے متعلق جواب دینے سے پہلے، تین امور قابل غور ہیں:

۱۔ ایک یہ کہ غیر حسی کرنسی بالخصوص بٹ کوئن کی اصلیت کے متعلق ماہرین اقتصاد کی کیا تحقیق ہے۔

۲۔ بٹ کوئن اور اس کے ہم مثل دیگر غیر حسی کرنسیوں کی فقہی تکییف اور اسکا مروجہ آلہ تبادلہ یعنی کرنسی نوٹ پر فقہی انطباق۔

۳۔ انتظامی امور کے رخ سے بٹ کوئن کی حیثیت اور اس کے جواز پر مدار شرائط۔

بٹ کوئن کی حقیقت ماہرین اقتصاد کی نظر میں:

موجودہ دور میں غیر حسی کرنسیوں میں سے سب سے زیادہ رواج پکڑنے والی کرنسی بٹ کوئن ہے، جس کے حوالہ سے ماہرین اقتصاد کے تحقیقی مقالے نیز قانونی اور انتظامی جائزہ موجود ہیں۔ چنانچہ بٹ کوئن کا قانونی جائزہ لینے کے لئے امریکہ کے ایوان بالا میں قانون سازوں کی زیر صدارت دو مجلسیں منعقد ہوئی، جن میں ایک مشہور مرکزی ادارہ تحقیق (Congressional Research Service) کے پیش کردہ مقالہ میں بٹ کوئن کا پورا جائزہ لیا گیا ہے۔ بٹ کوئن کی اصلیت معلوم کرنے کے لئے مذکورہ مقالہ میں چند امور قابل غور ہیں جن کا ذکر درجہ ذیل ہے:

۱۔ بٹ کوئن ایک غیر حسی کرنسی ہے جس کا کوئی جسمانی وجود نہیں، اور اسکا پورا مدار انٹرنیٹ پر ہے۔

۲۔ بٹ کوئن ایک مکمل آزاد مصدر غیر حسی کرنسی ہے جس کے پیچھے کوئی طاقتور مرکزی یا حکومتی ادارہ نہیں۔ چنانچہ امریکہ کے وزارت خزانہ نے اس کو غیر مرکزی قرار دیا ہے۔

۳۔ مروجہ کرنسی نوٹ کی طرح بٹ کوئن کو بھی سونے کی پشت پناہی حاصل نہیں۔

۴۔ مارکیٹ میں بٹ کوئن کی طلب ورصد کا معیار کافی بلند ہے، عوام اور بالخصوص تاجروں کا رجحان بٹ کوئن کے لین دین کی طرف بڑھتا جارہا ہے۔

۵۔ بٹ کوئن کا استعمال دیگر رائج کرنسی مثلاً: ڈالر اور یورو کی طرح ہو رہا ہے۔

(مذکورہ مقالہ: 'Bitcoin: Questions, Answers, and Analysis of Legal Issues' مشمولہ ہے)

بٹ کوئن کی فقہی تکییف:

بٹ کوئن اور دیگر غیر حسی کرنسیوں میں پائی جانے والی خصوصیات کو مد نظر رکھتے ہوئے یوں معلوم ہوتا ہے کہ ان میں اور مروجہ کرنسی نوٹ میں شرعی لحاظ سے کافی قدر مطابقت پائی جاتی ہے۔ چنانچہ بٹ کوئن میں دو بنیادی امور پائے جاتے ہیں جو اس بات پر دلالت کرتی ہے کہ بٹ کوئن میں، شرعی نقطہ نگاہ سے، مال ہونے کی اور ذریعہ تبادلہ یعنی ثمن ہونے کی صلاحیت موجود ہے:

ا۔ بٹ کوئن میں 'مال' ہونے کی صلاحیت:

بٹ کوئن کی خصوصیات اور فقہاء کرام کے 'مال' کے ذکر کردہ تعریفات میں ہم آہنگی پائی جاتی ہے۔ چنانچہ فقہاء متاخرین میں سے علامہ شامی رحمہ اللہ نے مال کی تعریف یوں کی ہے:

الدر المختار وحاشية ابن عابدين (رد المحتار) (4/ 501)

المراد بالمال ما يميل إليه الطبع ويمكن ادخاره لوقت الحاجة، والمالية تثبت بتمول الناس كافة أو بعضهم، والتقوم يثبت بها وبإباحة الانتفاع به شرعا.

اور شیخ مصطفی احمد الزرقاء نے 'المدخل الفقہی العام' میں مال کی جامع تعریف کرتے ہوئے فرماتے ہیں:

المدخل الفقهي العام (٣/ ١١٨)

المال:هو كل عين ذات قيمة مادية بين الناس.

مال کی مذکورہ تعریف دیجیٹل کرنسی اور بالخصوص بٹ کوئن پر مکمل منطبق ہوتی ہے۔ 'مال' کی تعریف میں تین بنیادی امور کا ذکر ہوا ہے۔ ایک یہ کہ مال اس کو کہا جاتا ہے جس کی طرف طبیعت سلیمہ مائل ہو، جس کو بعض فقہاء کرام نے 'شئ مرغوب' سے تعبیر کیا ہے۔ دوسرا یہ کہ اس شئ مرغوب کو بوقت حاجت محفوظ کرنا ممکن ہو۔ اور تیسرا یہ کہ اس شئ مرغوب کے لین دین کا عرف عام قائم ہو جائے۔ چنانچہ بٹ کوئن میں بھی مذکورہ تین اوصاف پائے جاتے ہیں، جس کی واضح دلیل یہ ہے کہ مختلف کرنسیوں کے ریٹ بتانے والے بیشتر، مشہور و معروف، ویب سائیٹ، بٹ کوئن کا بھی ریٹ بتاتے ہیں۔ جس سے یہ معلوم ہوتا ہے کہ اس کا استعمال عرف عام میں قائم ہو چکا ہے۔ اور جہاں تک بٹ کوئن کو محفوظ کرنے کی بات ہے سو اس کو بھی دیگر غیر حسی مال و متاع (Virtual Wealth) کی طرح برقی آلہ میں محفوظ کیا جا سکتا ہے۔

۲۔بٹ کوئن میں 'ثمن' ہونے کی صلاحیت:

عہد حاضر میں کسی چیز کے ثمن اصطلاحی بننے اور اس کے ثمنیت پر اتفاق رائے پیدا ہونے کی دو صورت ہو سکتی ہیں ۔ایک یہ کہ حکومت کسی چیز کو ثمن قرار دیدے اور یوں عوام اس کو قبول کرنے پر مجبور ہو جائیں، اس کو اصطلاحی زبان میں 'زر قانونی' اور Legal Tender، کہا جاتا ہے۔اور دوسری صورت یہ ہے کہ عوام میں خود کسی شئ مرغوب کا چلن ہو جائے اور اس کو ذریعہ تبادلہ تسلیم کر لی جائے۔

چنانچہ 'المدونۃ الکبری' میں تحریر فرماتے ہیں:

ولو أن الناس أجازوا بينهم الجلود حتى تكون لها سكة وعين لكرهتها أن تباع بالذهب والورق.

'ثمن' کے ارتقا کے متعلق 'انسائکلوپیڈیا برٹانکا' میں لکھا ہے کہ:

"Anything can serve as money that habit or social convention and successful experience endow with the quality of general acceptability, and a veriaty of Items have so served – from the wampum(beads made from shells) of American Indians, to cowries(Brightly coloured shells) in India, to whales theeth among the Fijans, to tobacco among early colonists in North America, to large stone disks on the Pacific island of Yap, to cigarettes in post-World War II Germany and in prisons the World over. The development of money has been marked by repeated innovations in the objects used as money". (Encyclopedia Britannica, Ed:15, Vol:24, Pg: 333)

ترجمہ:

'ہر وہ چیز ثمنیت کی صلاحیت رکھتی ہے جس کا چلن، اسکے کام گار اور نفع بخش تجربات کے مراحل سے گزرنے کے بعد، عرف عام میں بطور ثمن کے ہو جائے۔ اسکی واضح مثال

مختلف زمانوں میں مختلف اشیاء کے اندر پائی جاتی ہیں۔ چنانچہ امریکی انڈین کے عہد میں 'وامپم' (صدف سے بنی ہوئی لڑیاں)، انڈیا میں 'کوریز' (چھلکوں سے بنے ہوئے چمک دار گولے)، 'فجی' میں ویل (حوتان) کے دانت، شمالی امریکہ میں تمباکو، 'یاپ' کے جزیرہ میں قرص نما بڑے پتھر، اور جنگ عظیم دوم کے بعد 'جرمنی' اور دنیا بھر کے قید خانوں میں سگریٹ کو بطور ثمن اور زر تبادلہ کے استعمال کیا جاتا تھا۔ ثمن کے ارتقا میں امتیاز، ان اشیاء کے ایجاد و اختراع سے ہوئی جن کا استعمال بطور ثمن کے ہوتا تھا'۔

یہ بات بھی مسلم ہے کہ کسی شی میں ثمنیت ہونے کی صلاحیت پائے جانے کے لئے یہ ضروری نہیں کہ اس کو حکومت نے 'زر قانونی' (Legal Tender) قرار دیا ہو۔ چنانچہ کرنسی نوٹ کے ابتدائی مراحل میں جب اس کی کوئی خاص شکل وصورت نہیں تھی اس وقت لوگ سنار اور صراف سے سکوں کے عوض جاری کردہ وثیقہ اور سندیں حاصل کرتے تھے جس کو محض بھروسہ اور اعتماد کی بنیاد پر قبول کیا جاتا تھا۔ نہ اسکی کوئی قانونی حیثیت تھی اور نہ ہی اپنے حق کی وصولیابی میں اسکو قبول کرنے پر کوئی مجبور کیا جاتا تھا۔ اور دور حاضر میں اس کی ایک واضح مثال چیک اور انعامی بانڈز ہے۔

تاہم اس بات کی وضاحت ضروری ہے کہ بٹ کوئن درحقیقت وثیقہ کی حیثیت نہیں رکھتا بلکہ اس کا اساس کسی ملک کے نقود یا اثاث ہی ہے، جس کے تبادلہ سے اس کو استقلال حاصل ہوا ہے۔ اور اس کے استقلال حاصل ہونے کے بعد اس کو لوگ یا تو خرید و فروخت میں ذریعہ تبادلہ کے طور پر استعمال کرتے ہیں یا پھر اس کو استثمار کے لئے حاصل کرتے ہیں۔

بٹ کوئن کے مستقل بالذات ثمن اصطلاحی ہونے کے اور وثیقہ کی حیثیت نہ رکھنے کے چند وجوہات یہ ہیں:

۱۔ بٹ کوئن کے ضائع ہونے کی صورت میں حکومت اس کا کوئی بدل ادا نہیں کرے گی۔ جبکہ دیگر مالی دستاویزات اور قرض کے سندات کے ضائع ہونے کے وقت حکومت کی طرف سے ان سندات کا بدل کا انتظام کیا جاتا ہے۔

۲۔ دور حاضر میں بٹ کوئن کا لین دین مروجہ کرنسی نوٹ کی طرح انجام دے رہی ہے اور کسی کے خیال میں یہ نہیں ہوتا کہ وہ قرض کا لین دین کر رہا ہے، اور بدلہ میں بٹ کوئن بحیثیت وثیقہ کے حاصل کیا جارہا ہے۔

۳۔ جیسے آج کل کرنسی نوٹ کا استحکام سونے سے نہ رہا اسی طرح بٹ کوئن کو بھی کسی ثمن خلقی (سونا / چاندی) کی پشت پناہی حاصل نہیں۔ بٹ کوئن کی قدر و قیمت اس کے مادری موجود کرنسی نوٹ ہی کی وجہ سے ہے۔

بٹ کوئن اور دیگر ذریعہ تبادلہ کو اگر تقابلی نظر سے دیکھا جائے تو یوں معلوم ہوتا ہے کہ بٹ کوئن 'زر قانونی' (Legal Tender) نہ ہونے کی حیثیت سے چیک اور انعامی بانڈز کے مانند ہے کہ اس کو قبول کرنے میں کسی کو مجبور نہیں کیا جاسکتا اور اسکے مستقل بالذات 'ثمن اصطلاحی' ہونے کی حیثیت سے کرنسی نوٹ (فلوس نافقہ) کی طرح ہے۔ خلاصہ یہ کہ بٹ کوئن اپنے تمام شرعی قید و بند کیساتھ مروجہ کرنسی نوٹ کی طرح 'فلوس نافقہ' ہی کے زمرے میں آتا ہے۔ چنانچہ جو فقہی احکام کرنسی نوٹ پر متفرع ہوتے ہیں مثلاً وجوب زکاۃ، سلم، استصناع، مضاربہ و مشارکہ میں راس المال ہونے کی صلاحیت، صرف، اور ربا، اسی طرح بٹ کوئن پر بھی وہی فقہی احکام جاری ہوں گے۔

بٹ کوئن اور حکومتی قوانین کی پاسداری:

جہاں تک ملکی قانون کی پاسداری کا لحاظ رکھنے کی اور قانون شکنی سے اجتناب کی بات ہو تو یہ ان خارجی امور سے وابستہ ہیں جنکا تعلق نظم و نسق سے ہے، اور انتظامی معاملات میں، عمومی اور اجتماعی فلاح و بہبود کے ملحوظ خاطر، ملکی قوانین میں بیشتر اوقات ترمیمات کی اور بعض اوقات منسوخ ہونے کی گنجائش ہوتی ہے۔ لہذا جن ممالک میں بٹ کوئن کے استعمال کی ممانعت ہو ان ممالک میں اسکا استعمال شرعاً بھی جائز نہیں ہوگا اور جن ممالک میں اس کے استعمال سے کسی بھی صورت میں ملکی قوانین و ضوابط کی خلاف ورزی نہ ہو تو ان ممالک میں بٹ کوئن کو بطور مال و ثمن استعمال کرنا جائز ہوگا۔

حوالہ جات

الدر المختار وحاشية ابن عابدين (رد المحتار) (5/ 176)

[مطلب في أن النص أقوى من العرف]

(قوله كر وشعير إلخ) أي كهذه الأربعة والذهب والفضة فالكاف في الموضعين استقصائية كما في الدر المنتقى (قوله ولا يتغير أبدا) أي سواء وافقه العرف أو صار العرف بخلافه (قوله ولو مع التساوي) أي التساوي وزنا في الحنطة وكيلا في الذهب لاحتمال التفاضل بالعيار

المنصوص عليه أما لو علم تساويهما في الوزن والكيل معا جاز ويكون المنظور إليه هو المنصوص عليه....(قوله لأن النص إلخ) يعني لا يصح هذا البيع وإن تغير العرف فهذا في الحقيقة تعليل لوجوب اتباع المنصوص قال في الفتح: لأن النص أقوى من العرف لأن العرف جاز أن يكون على باطل كتعارف أهل زماننا في إخراج الشموع والسرج إلى المقابر ليالي العيد والنص بعد ثبوته لا يحتمل أن يكون على باطل، ولأن حجية العرف على الذين تعارفوه والتزموه فقط والنص حجة على الكل، فهو أقوى ولأن العرف إنما صار حجة بالنص وهو قوله - صلى الله عليه وسلم - «ما رآه المسلمون حسنا فهو عند الله حسن» اهـ (قوله وما لم ينص عليه) كغير الأشياء الستة (قوله حمل على العرف) أي على عادات الناس في الأسواق لأنها أي العادة دالة على الجواز فيما وقعت عليه للحديث فتح (قوله وعن الثاني) أي عن أبي يوسف، وأفاد أن هذه رواية خلاف المشهور عنه (قوله مطلقا) أي وإن كان خلاف النص، لأن النص على ذلك الكيل في الشيء أو الوزن فيه ما كان في ذلك الوقت إلا لأن العادة إذ ذاك كذلك وقد تبدلت فتبدل الحكم، وأجيب بأن تقريره - صلى الله عليه وسلم - إياهم على ما تعارفوا من ذلك بمنزلة النص منه عليه فلا يتغير بالعرف، لأن العرف لا يعارض النص كذا وجه اهـ فتح (قوله ورجحه الكمال) حيث قال عقب ما ذكرنا: ولا يخفى أن هذا لا يلزم أبا يوسف لأن قصاراه أنه كنصه على ذلك وهو يقول: يصار إلى العرف الطارئ بعد النص بناء على أن تغير العادة يستلزم تغير النص، حتى لو كان - صلى الله عليه وسلم - حيا نص عليه. اهـ وتمامه فيه.

وحاصله توجيه قول أبي يوسف أن المعتبر العرف الطارئ بأنه لا يخالف النص بل يوافقه، لأن النص على كيلية الأربعة، ووزنية الذهب والفضة مبني على ما كان في زمنه - صلى الله عليه وسلم - من كون العرف كذلك حتى لو كان العرف إذ ذاك بالعكس لورود النص

موافقا له ولو تغير العرف في حياته – صلى الله عليه وسلم – لنص على تغير الحكم،

وملخصه: أن النص معلول بالعرف فيكون المعتبر هو العرف في أي زمن كان ولا يخفى أن هذا فيه تقوية لقول أبي يوسف فافهم.

الموسوعة الفقهية الكويتية (15/ 27)

ذهب الحنفية إلى أنه يشترط في الثمن لانعقاد البيع: أن يكون مالا متقوما.لأن البيع هو مبادلة المال بالمال بالتراضي. (2)

والمال هو ما يميل إليه الطبع ويمكن ادخاره لوقت الحاجة، والمالية إنما تثبت بتمول الناس كافة أو بعضهم.

والتقوم يثبت بها وبإباحة الانتفاع به شرعا. فما يكون مباح الانتفاع بدون تمول الناس لا يكون مالا، كحبة حنطة. وما يكون مالا بين الناس، ولا يكون مباح الانتفاع لا يكون متقوما، كالخمر. وإذا عدم الأمران لم يثبت واحد منهما كالدم.

فالمال أعم من المتقوم؛ لأن المال ما يمكن ادخاره ولو غير مباح كالخمر، والمتقوم ما يمكن ادخاره مع الإباحة. فالخمر مال غير متقوم، فلذا فسد البيع بجعلها ثمنا، وإنما لم ينعقد أصلا بجعلها مبيعا؛ لأن الثمن غير مقصود بل وسيلة إلى المقصود، إذ الانتفاع بالأعيان لا بالأثمان، ولهذا اشترط وجود المبيع دون الثمن فبهذا الاعتبار صار الثمن من جملة الشروط بمنزلة آلات الصناع.

ومن هذا قال في البحر: البيع وإن كان مبناه على البدلين، لكن الأصل فيه المبيع دون الثمن، ولذا تشترط القدرة على المبيع دون الثمن، وينفسخ بهلاك المبيع دون الثمن.

الموسوعة الفقهية الكويتية (41/ 176)

النقود الورقية: وقد غلب استعمالها في العصر الحديث، حتى حلت مكان النقود الذهبية والفضية، وأخذت وظيفتهما في التعامل في عامة بلدان العالم، وقد أشار إلى إمكان اتخاذ النقود من الورق الإمام مالك، من باب افتراض وقوع ما لم يقع وبيان حكمه، فقال: لو أن الناس

أجازوا بينهم الجلود حتى تكون لها سكة وعين لكرهتها أن تباع بالذهب والورق نظرة، وقال في موضع: لو جرت الجلود بين الناس مجرى العين المسكوك لكرهنا بيعها بذهب أو ورق نظرة (2) .

وقد عرف التعامل بالأوراق النقدية قديما، فقد حكى المقريزي أنه لما رحل إلى بغداد أخرج له أحد التجار ورقة فيها خطوط بقلم الخطا - أي بالخط المغولي - وذكر أن هذه الأوراق مأخوذة من ورق التوت، فيها لين ونعومة، وأن هذه الورقة إذا احتاج الإنسان في (خان بالق) من بلاد الصين لخمسة دراهم دفعها فيها، وأن ملكها يختم لهم هذه الأوراق وينتفع بما يأخذ بدلا عنها.

الموسوعة الفقهية الكويتية (15/ 30)

أما الفلوس والدراهم التي غالبها الغش:

فإن كانت رائجة فلا تتعين بالتعيين، لكونها أثمانا بالاصطلاح، فما دام ذلك الاصطلاح موجودا لا تبطل الثمنية، لقيام المقتضي. وإن كانت غير رائجة فتتعين بالتعيين؛ لزوال المقتضي للثمنية وهو الاصطلاح، وهذا لأنها في الأصل سلعة، وإنما صارت أثمانا بالاصطلاح، فإذا تركوا المعاملة بها رجعت إلى أصلها.

بدائع الصنائع في ترتيب الشرائع (5/ 185)

قوله: إن الفلوس أثمان فلا يجوز بيعها بجنسها متفاضلا كالدراهم، والدنانير، ودلالة الوصف عبارة عما تقدر به مالية الأعيان، ومالية الأعيان كما تقدر بالدراهم، والدنانير تقدر بالفلوس فكانت أثمانا؛ ولهذا كانت أثمانا عند مقابلتها بخلاف جنسها، وعند مقابلتها بجنسها حالة المساواة، وإن كانت ثمنا فالثمن لا يتعين، وإن عين كالدراهم، والدنانير فالتحق التعين فيهما بالعدم فكان بيع الفلس بالفلسين بغير أعيانهما، وذا لا يجوز؛ ولأنها إذا كانت أثمانا فالواحد يقابل الواحد فبقي الآخر فضل مال لا يقابله عوض في عقد المعاوضة، وهذا تفسير الربا.... (وأما) الفلوس: فإن كانت كاسدة فلا تجوز الشركة، ولا المضاربة بها؛ لأنها عروض وإن كانت نافقة: فكذلك في الرواية

المشهورة عن أبي حنيفة، وأبي يوسف وعند محمد تجوز والكلام فيهـا مبني على أصل وهو أن الفلوس الرائجة ليست أثمانا على كل حـال عند أبي حنيفة، وأبي يوسف؛ لأنها تتعين بالتعيين في الجملة، وتصـير مبيعا بإصلاح العاقدين حتى جاز بيع الفلس بالفلسين بأعيانها عندهما، فأما إذا لم تكن أثمانا مطلقة؛ لاحتمالها التعيين بالتعيين في الجملـة في عقود المعاوضات، لم تصلح رأس مال الشركة كسائر العروض وعنـد محمد الثمنية لازمة للفلوس النافقة، فكانت من الأثمان المطلقة، وهـذا أي جواز بيع الواحد منها باثنين، فتصلح رأس مال الشركة كسـائر الأثمان المطلقة من الدراهم، والدنانير.

الدر المختار وحاشية ابن عابدين (رد المحتار) (2/ 300)

[فرع] في الشرنبلالية: الفلوس إن كانت أثمانا رائجة أو سلعا للتجارة تجب الزكاة في قيمتها وإلا فلا. اهـ

أبحاث هيئة كبار العلماء (1/ 56)

وقال شيخ الإسلام ابن تيمية: وأما الدرهم والدينار فما يعرف له حد طبعي ولا شرعي، بل مرجعه إلى العادة والاصطلاح؛ وذلك لأنـه في الأصل لا يتعلق المقصود به؛ بل الغرض أن يكون معيارا لما يتعـاملون به، والدراهم والدنانير لا تقصد بنفسها، بل هي وسيلة إلى التعامل بها ولهذا كانت أثمانا بخلاف سائر الأموال، فإن المقصود الانتفـاع بهـا نفسها فلهذا كانت مقدرة بالأموال الطبيعية أو الشرعية، والوسـيلة المحضة التي لا يتعلق بها غرض لا بمادتها ولا بصورتها يحصل بها المقصود كيف ما كانت. اهـ (1) وهذا يمكن القول بأن النقد شيء اعتباري، سواء كان ذلك الاعتبار ناتجا عن حكم سلطاني أو عـرف عـام.... لعلماء الاقتصاد ثلاث نظريات في سر قابلية النقد للتبادل العام، قـد تكون كل منها صحيحة في فترة ما:

(1)الأولى: النظرية المعدنية: إن النقد مادة لها قيمة في نفسـها قبـل اتخاذها وسيطا للتبادل فلذلك حصلت الثقة بها وكانت ذات قابلية – عامة للوساطة في التبادل، وهذه النظرية صحيحة حينما كـان النقـد

معدنيا، أما اليوم فإن النقد كل ما لقي من الناس قبولا عاما وثقة في اعتباره وسيطا للتبادل فيدخل في ذلك النقد الورقي سواء أكان له غطاء حسي أم كان من اعتبار الحاكم له وسيطا وضمانه له.

(2)الثانية: النظرية السلطانية: وهذه النظرية تقول بأن أمر السلطان هو الذي أكسب النقد قبولا عاما وثقة به ولاشك أن مجرد أمر السلطان لا يكفي في ذلك دون أن يستند إلى مبرر يضمن اطمئنان الأمة إلى هذا الوسيط؛ لتقف إلى جانب السلطان وتنفذ أمره طائعة مختارة.

(3)الثالثة: النظرية النفسانية: بأن النقد هو الذي تطمئن النفس إلى اعتباره قوة شرائية مطلقة ثقة به واطمئنانا إليه سواء أكان له غطاء أم لا، وسواء أكانت له قيمة ذاتية أم لا، وسواء أمر السلطان باعتباره أم حصل التراضي والتعارف على استعماله وقبوله.

أصول الإفتاء وآدابه:(240)

من المسلم لدى الفقهاء ان الحكم يدور علي اللعلة وجودا وعدما, فان وجدت العلة ثبت الحكم وان انعدمت انتفي الحكم. ثم قد تكون علة الحكم دائمة لا تنقطع ابدا, وحينئذ لا يتغير الحكم في زمن من الازمان, كحرمة الزنا, والسرقة, وشرب الخمر, وأكل الخنزير في غير حالات الإضطرار. فإن علل هذه الأحكام دائمة لاتنقطع ابدا. وقد تكون علة الحكم قابلة للتغير والإنقطاع, فحينئذ يتغير الحكم بتغيرها.

أصول الإفتاء وآدابه:(250)

كلمة "العرف" في اللغة ماخوذ من المعرفة, ويستعمل بمعني العادة المعرفة. قال الامام السقي رحمه الله تعالى في المستصفى:

"العرف والعb vادة:ما استقر في النفوس من جهة قضايا العقول, وتلقته الطباع السليمة بالقبول"()

وإن العرف ان كان مقتصرا علي طائفة من الناس أو علي اهل بلد مخصوص, فإنه يسمى عرفا خاصا. وإن عم سائر الناس والبلاد, فإنه يسمى عرفا عاما.

فقه البيوع–على المذاهب الاربعة(1/27)

إن الكهرباء والغاز اصبحا اليوم من اغز الأموال التي يجري فيها التنافس, ويصعب ادخالهما في الأعيان القائمة بنفسها, ومع ذلك يجوز بيعهما و شرائهما. وقد تعامل الناس بذلك من غير نكير, فما ذكرنا عن ابن عابدين من تعريف المال, هو الراجح بدون تقييده بالأعيان القائمة بنفسها. وما ليس بعين لايحكم بعدم جواز بيعه لمجرد انه ليس بعين ما لم يلزم منه محظور آخر. والمراد منقولهم "ما يميل إليه الطبع" في تعريف المال, أن يكون منتفعا به,فما لا ينتفع به ليس مالا, ولا يجوز كونه محلا للبيع والشراء.

واللہ تعالیٰ اعلم بالصواب

عبداللہ اعوان

دارالافتاء جامعہ دارالعلوم کراچی

بسم اللہ الرحمن الرحیم

موطیہ ۱۲ ۲ ۱۳ / ۲۹ / ۲۱ ۲۳ ۲ ۱۴۲۳

السلام علیکم ورحمۃ اللہ وبرکاتہ

علماء کرام سے ایک اہم مسئلے کے بارے میں راہنمائی مطلوب ہے

آج کل انٹرنیٹ پر ڈیجیٹل کرنسی کی کئی کمپنیاں قائم کر رہی ہیں بعض لگتے ہیں کہ اب دنیا میں کاغذ کے نوٹ ختم ہو جائیں گے اور انکی جگہ ڈیجیٹل کرنسی لے لیگی. اور واقعی دنیا کے بڑے بڑے بینکوں نے اس کرنسی کو قبول بھی کر لیا ہے ۔ اور وہ رجسٹرڈ ہو چکی ہے ان کمپنیوں میں ایک کمپنی ون کوائن (Onecoin) کے نام سے قائم کر رہی ہے جو اپنی ایک ڈیجیٹل کرنسی متعارف کروا رہی ہے اور بہت سارے لوگ نفع کمانے کی غرض سے ڈھڑا ڈھر اس کمپنی کے ممبر بنتے جا رہے ہیں

اس کمپنی کا ماننا ہے کہ ڈیجیٹل کرنسی تبھی عام ہو گی جب لوگ اسکو استعمال کرنا شروع کر دیں گے . اسلئے اس کمپنی نے لوگوں کی توجہ حاصل کرنے کیلئے اس میں سرمایہ کاری کرنے پر کئی منافع بخش طریقے فراہم کئے ہیں

پہلا طریقہ :-

منافع حاصل کرنے کا پہلا طریقہ یہ ہے کہ جو اس کمپنی کی رکنیت حاصل کرنا چاہتا ہے تو اسے ۱۰۰ یورو سے لیکر 28000 یورو تک میں کوئی ایک پیکیج حاصل کرنا ہوتا ہے کمپنی ان پیکجز کو (ایجوکیشن یا تعلیمی پیکیجز کا نام دیتا ہے) اس کے ساتھ ساتھ ان پیکجز کے بدلے کمپنی اس ممبر کو ٹوکن بھی دیتی ہے ان ٹوکنوں کی تعداد ہر پیکج کے حساب سے الگ الگ ہے ہر ایک ٹوکن عرصہ تقریباً ۹۰ دن گزرنے کے بعد ان ٹوکنوں کو دگنا کر دیتی ہے۔

ٹوکن دگنا ہونے کے بعد ممبران کو اختیار حاصل ہوتا ہے کہ وہ ان ٹوکنوں کو ڈیجیٹل کوائنز (سکوں) میں تبدیل کروالیں جو کمپنی فسٹی میں کر کے دیتی ہیں ڈیجیٹل کوائنز حاصل کرنے کے بعد ہر صارف کو اختیار حاصل ہوتا ہے کہ وہ ان کوائنز کو بیچ سکے۔

اس طرح صارف کو تقریباً دگنا فائدہ حاصل ہوتا ہے کیونکہ کوائنز اچھی قیمت میں بک جاتے ہیں۔

دوسرا طریقہ ، منافع حاصل کرنے کا دوسرا طریقہ Compensation Plan کا ہے جو اختیاری ہے لازمی نہیں یعنی اگر کسی کو فائدہ حاصل کرنا ہو تو وہ اس طریقے کو اختیار کرے ورنہ نہیں پھر اسکی بھی تین صورتیں ہیں

پہلی صورت Direct Sale کی ہے

یعنی جو ممبر کمپنی کی رکنیت حاصل کرلے اور اس کے بعد کسی کو بھی کمپنی کے بارے میں بتائے اور وہ بندہ اس کے اکاؤنٹ کے تحت کمپنی کا ممبر بن جائے تو وہ نیا آنے والا ممبر جتنے بزنس کی سرمایہ کاری کرتا ہے اس کا دس فیصد (10%) کمپنی پہلے والے ممبر کو دیتی ہے جو اس نئے آنے کا سبب بنا اور یہ آمدنی ایک دفعہ ہوتی ہے۔

دوسری صورت Network Bonus کی ہے (نیٹ ورک بونس)

اس صورت میں کسی بھی ممبر کے تحت دائیں اور بائیں جانب جتنے بھی لوگ بالواسطہ یا بلاواسطہ ممبر بنتے ہیں ان کی پیکیج وار مجموعی سرمایہ کاری کا دس فیصد حصہ کمپنی اس پہلے والے ممبر کو ادا کرتی ہے جس کے نیچے ان کی رکنیت واقع ہوئی اور یہ ادائیگی کمپنی ہفتہ میں ایک دفعہ کرتی ہے۔

(3) تیسری صورت matching Bonus کی ہے

اس کی تفصیل یہ ہے کہ کوئی ممبر رکنیت حاصل کرنے کے بعد جن لوگوں کو ڈائریکٹ سپانسر کرکے کمپنی کا ممبر بناتا ہے تو کمپنی کی اصطلاح میں First generation (پہلی نسل) کہتے ہیں اور پہلی نسل یا درجے کے لوگوں کو ڈائریکٹ سپانسر کرکے کمپنی میں لانے والے جو پہلے والے ممبر تھے وہ دوسری نسل کہلاتے ہیں اسی طرح تیسری اور چوتھی نسل تک سلسلہ ہوتا ہے

تو پہلی نسل یا درجے کے ممبر پیکیج وار Bonus سے جتنا کماتے ہیں اس کا دس فیصد پہلے والے ممبر کو ملتا ہے اسی طرح دوسری تیسری اور چوتھی نسل والوں کی پیکیج وار کمائی کے حساب سے پہلے والے ممبر کو ملتا ہے اور یہ Maching Bonus جتنے میں ایک دفعہ اور چار نسلوں یا درجوں تک دس فیصد کے حساب سے ملتا ہے چوتھے زیادہ نہیں

اس کے علاوہ کمپنی کبھی کبھار ڈیجیٹل کرنسی (Coins) کے حامل ممبران کے لیے ایک اور اضافی بونس بھی کرتی ہے کہ کمپنی میں ان کے جتنے بھی کوائنز موجود ہیں مقررہ تاریخ کو وہ تعداد کتنی ہو جائیگی ہے

اس کے ساتھ ساتھ کمپنی ایک قسم کے بونس اور ایوارڈ مختلف ممبران کو دیتا رہتا ہے ان کے کاروبار کی کے حساب سے دیتی ہیں

آئیے مہربانی اس ساری تفصیل کی روشنی میں چند سوالات کے جوابات مرحمت فرمائیں

سوال نمبر (۱)

اس کمپنی میں منافع حاصل کرنے کا جو پہلا طریقہ مذکور ہے اس کی شرعی حیثیت کیا ہے؟

سوال نمبر (۲)

منافع حاصل کرنے کے دوسرے طریقے کی تین صورتیں ہیں ہر ہر صورت کا شرعی حکم کیا ہے؟

سوال نمبر (۳)

تمام ممبران کے کوائفز کو کسی مقررہ تاریخ پر دگنا کرنے کی شرعی حیثیت کیا ہے؟

سوال نمبر (۴)

اہم سوال یہ ہے کہ اگر کوئی اس کمپنی میں صرف کوائفز حاصل کرنے کیلئے رکنیت حاصل کرلے اور Networking کے ذریعے مزید لوگوں کو رکن نہ بنائے تو کیا شرعاً ایسا کرنا صحیح ہوگا؟

سوال نمبر (۵)

عمومی طور پر اس کمپنی میں سرمایہ کاری کرنا شریعت اسلامیہ کی نظر میں کیسا ہے؟

نوٹ:

برطانیہ میں مقیم کئی علماء اور مفتیان کرام اس کمپنی کی رکنیت حاصل کرکے اس فرض کو اختیار کرچکے ہیں اور ان کے پاس برطانیہ کے کسی مفتی صاحب کا فتویٰ بھی ہے جس کے تحت وہ اس بزنس کو بلاشبہ جائز کہہ رہے ہیں [redacted] کے ذیل لنک پر دستیاب ہے

Http://amjad.muhammad.com/documents/Fatwa/Is%20the%20Earning%20Compensation%20Plan%20Permissible%20Halal%20according%20to%20the%20Shariah%20%28Islamic%20Law%29-update1.pdf

(شکریہ)

نام = غلام حیدر خان

0324-2626496

ایڈریس کراچی

واضح رہے کہ کسی کرنسی کا قائمقام اور اصطلاحی ثمن ہونے کیلئے ضروری ہے کہ اس علاقہ کی حکومت اور اسٹیٹ کی جانب سے اس کرنسی کو سکہ اور ثمن تسلیم کرکے اس کو تمام معاملات (لین دین) کا درجہ دے اور لوگوں کا اس میں رغبت اور میلان ہونا ضروری ہے

مذکورہ ڈیجیٹل کرنسی نہ تو کسی حکومت کی طرف سے تسلیم شدہ کرنسی ثمن ہے اور نہ ہی تمام لوگوں میں اس کا رواج ہے لہٰذا اسکی ثمنیت قابل اعتبار نہیں ہے اور بعض چند ٹوکن جن کی کوئی مالیت حقیقت فی الواقع نہیں ہے اس کی قیمت ۱۵۵ یورو سے 28000 تک ہے مقرر کرنا درست نہیں ہے، نیز اگر ان کرنسیوں کو ثمن بھی مان لیں تو ثمن کا آپس میں تبادلہ کرتے وقت ایک ہی مجلس میں قبضہ ضروری ہے جبکہ مذکورہ کمپنی ٹوکن دینے کے ۹۰ دن بعد ان ٹوکنوں کو دگنا کرکے ڈیجیٹل کو عشر (سکوں) میں تبدیل کرکے دیتی ہے تو یہ بھی بیع صرف میں ادھار کی ایک صورت ہونے کی وجہ سے ناجائز ہے۔ لہٰذا سوال میں مذکور منافع کا یہ طریقہ بھی ناجائز ہے۔

فتاوی شامی میں ہے

والمالية تثبت بتمول الناس كافة

او بعضهم والنقود تثبت بهما

وباباحة الانتفاع به شرعا

(ج ۴/ ۵۰۱ ط ایچ سعید)

وفيه ايضا:

هو مبادلة شيء مرغوب فيه بمثله

على الوجه المخصوص

(ج ۴/ ۵۰۶ ط ایچ سعید)

بدائع الصنائع میں ہے

وأما الشرائط فمنها قبض البدلين
قبل الإفتراق. لقوله عليه الصلاة
والسلام في الحديث المشهور
والذهب بالذهب مثلاً بمثل
يداً بيد والفضة بالفضة مثلاً بمثل
يداً بيد الحديث)

(بدائع الصنائع في شرائط الصرف ج ۵/۲۱۵)

۲۔ مذکورہ کمپنی کے منافع حاصل کرنے کا دوسرا طریقہ جس کی تین صورتیں ہیں یہ تینوں صورتیں دراصل کمیشن کے تحت آتی ہیں اور کمیشن کی بیع اسلامی معیشت میں مستقل تجارتی حیثیت نہیں ہے اس لیے کہ محنتی محنت (جو کہ تجارت کا ایک اہم جزو ہے) کے غالب عنصر سے خالی ہونے کی بنا پر فقہاء کرام نے اصولاً اس کو ناجائز قرار دیا ہے، لیکن لوگوں کی ضرورت اور تعامل کی وجہ سے اس کی محدود اور شروط اجازت دی ہے، بنا بر ایں مذکورہ کمپنی کا مقصد زیادہ سے زیادہ لوگوں کا سرمایہ اپنے کاروبار میں لگا کر اور ممبر سازی کر کے زیادہ سے زیادہ رقم حاصل کرنا اور اس حاصل ہونے والی رقم سے لوگوں کو کمیشن فراہم کرنا ہے، لہٰذا اس کمپنی سے معاملہ کرنا اور اس میں سرمایہ کاری کر کے منافع حاصل کرنا جائز نہیں ہے، چونکہ اس کمپنی کے کوائنز اور ٹوکن خریدنا جائز نہیں ہے اسی طرح اس کمپنی کے ممبرین کو مذکورہ تینوں صورتوں (Network Bonus, Direct Sale Bonus, Matching Bonus) کے ذریعے کمیشن حاصل کرنا بھی درست نہیں ہے۔

(واللہ)

فتاویٰ شامی میں ہے

والربح إنما يستحق بالمال أو بالعمل
أو بالضمان.

(کتاب المضاربۃ ۵/۶۴۶ سعید)

وفيه أيضاً

سئل عن محمد بن سلمة عن أجرة
السمسار، فقال أرجو أنه لا بأس
به وإن كان في الأصل فاسداً
لكثرة التعامل وكثير من
هذا غير جائز

(مطلب فی اجرۃ الدلال ۶/۶۳ سعید)

الأشباه والنظائر میں ہے)

ما أبيح للضرورة يقدر بقدرها

(القاعدة الخامسة الضرر يزال ص۸۵ قدیمی)

وفيه ايضاً

وصرح به في منار الختار
الهداية ثم قال والعقد إذا
فسد في بعضه فسد في
جميعه۔

(القاعدة الثانية ص۱۱۷ قدیمی)

(جاری ہے)

(۳) ۔۔۔۔۔۔۔ مذکورہ کمپنی کے کوائنز (سکوں) کا حصول اور ان کی خرید و فروخت چونکہ ناجائز ہے اسی طرح ان کوائنز کو دگنا کر کے بیچنا بھی ناجائز ہے۔

البنایۃ شرح الہدایۃ میں ہے

إن فساد العقد في البعض إنما
يوقف السباق إذا كان للتضامن

(ج: ۸/ ۱۷۷)

نیز ان کوائنز (سکوں) کی زیادتی بلا عوض ایک عقد میں لازم ہونے کی وجہ سے بھی جائز نہیں ہے

فتاویٰ شامی میں ہے:

(فصل) ولو حكما فدخل ربا النسيئة
والبيوع الفاسدة فكلما من الربا
فيجب رد عين الربا ولو قائما لا رد ضمانه
لأنه يملك بالقبض فيه وبعد
(خال عن عوض) ..... مشروط ذلك"
الفضل لأحد العاقدين) - الخ

(ج: ۲/ ۱۶۸، ۱۹۹، سعید)

(۴) ۔۔۔۔۔۔۔ مذکورہ کمپنی کا ٹوکن اور کوائنز کا لین دین کرنا چونکہ ناجائز ہے اس لیے اگر کوئی اس کمپنی میں صرف کوائنز حاصل کرنے کیلئے رکنیت حاصل کرے اور نیٹ ورکنگ (Networking) کے ذریعے اگرچہ ممبر سازی نہ کرے تب بھی ان کوائنز کو خرید نا جائز نہیں ہے۔

نیز اس طرح کے مشکوک کمپنی کے کاروبار میں سرمایہ کاری کرنا بھی

(جاری ہے)

درست نہیں ہے اس لئے کہ شریعت اسلامیہ میں کاروبار اور کمپنی دین
کا مدار معاملات کی صفائی اور دیانت و امانت پر ہے اور فرضی چیزوں
کے بجائے اصلی اور حقیقی چیزوں کے خرید و فروخت اور حقیقی محنت پر
زور دیتی ہے اور مفتی امجد صاحب کے فتوے سے یہ بھی بات واضح
ہوتی ہے کہ (ون کوئن) (one coin) کمپنی کے معاملات صاف اور واضح نہیں
ہیں لہٰذا ان سے اجتناب کرنا ضروری ہے
تفسیر کبیر میں ہے:

قال بعض اللہ تعالیٰ إنما
حرم الربا حيث أنه يمنع الناس
عن الاشتغال بالكاسب.....
فلا يكاد يتحمل المشقة والكد
والتجارة والصناعات الشاقة

(التفسیر الکبیر للرازی، سورۃ البقرۃ ۲، ۹۱، ایران)

احکام القرآن میں ہے

يعني لكل أحد من أكل مال نفسه
ومال غيره بالباطل وأكل مال
نفسه بالباطل انفاقه في
معاصي الله وأكل مال الغير بالباطل
قد قيل فيه وجهان أحدهما
قال السدي وهو أن يأكل بالربا
والقمار والبخس والظلم

(حمار ۲۲)

وقال ابن عباس رضي الله تعالى عنه
والحسن رحمه الله تعالى أن يأكله
بتغيير عرف
(ج: ٢، ٢١٦، دار الكتب العلمية بيروت)
(فقط والله أعلم)

كتبه
محمد طيب حيدري
المتخصص في الفقه الإسلامي
بجامعة العلوم الإسلامية علامه
محمد يوسف بنوري ٹاؤن كراچی
١٥/ ٣/ ١٤٣٨
١٥/ ١٢/ ٢٠١٦

الجواب صحیح
محمد شفیق عارف
١٥/ ٣/ ١٤٣٨ھ

صحیح
محمد عادل

مصنف کے قلم سے دیگر شاہکار

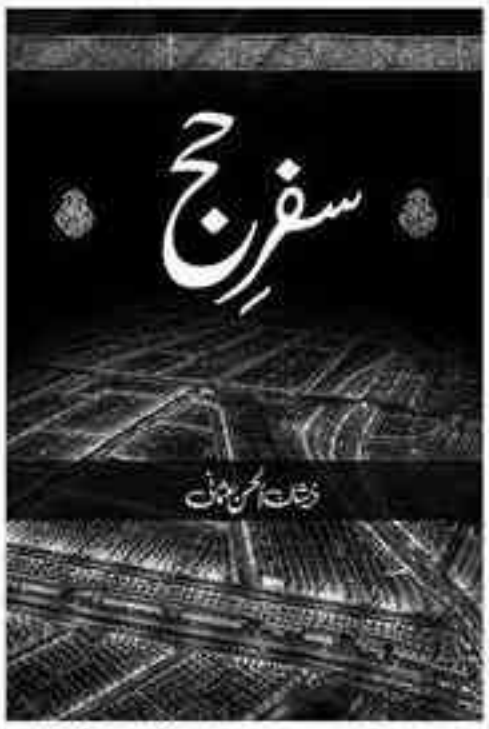
جستجو کا سفر

شعور۔علم سے آگہی کا سفر

سفرِ حج

سی++

Kaggle for Beginners

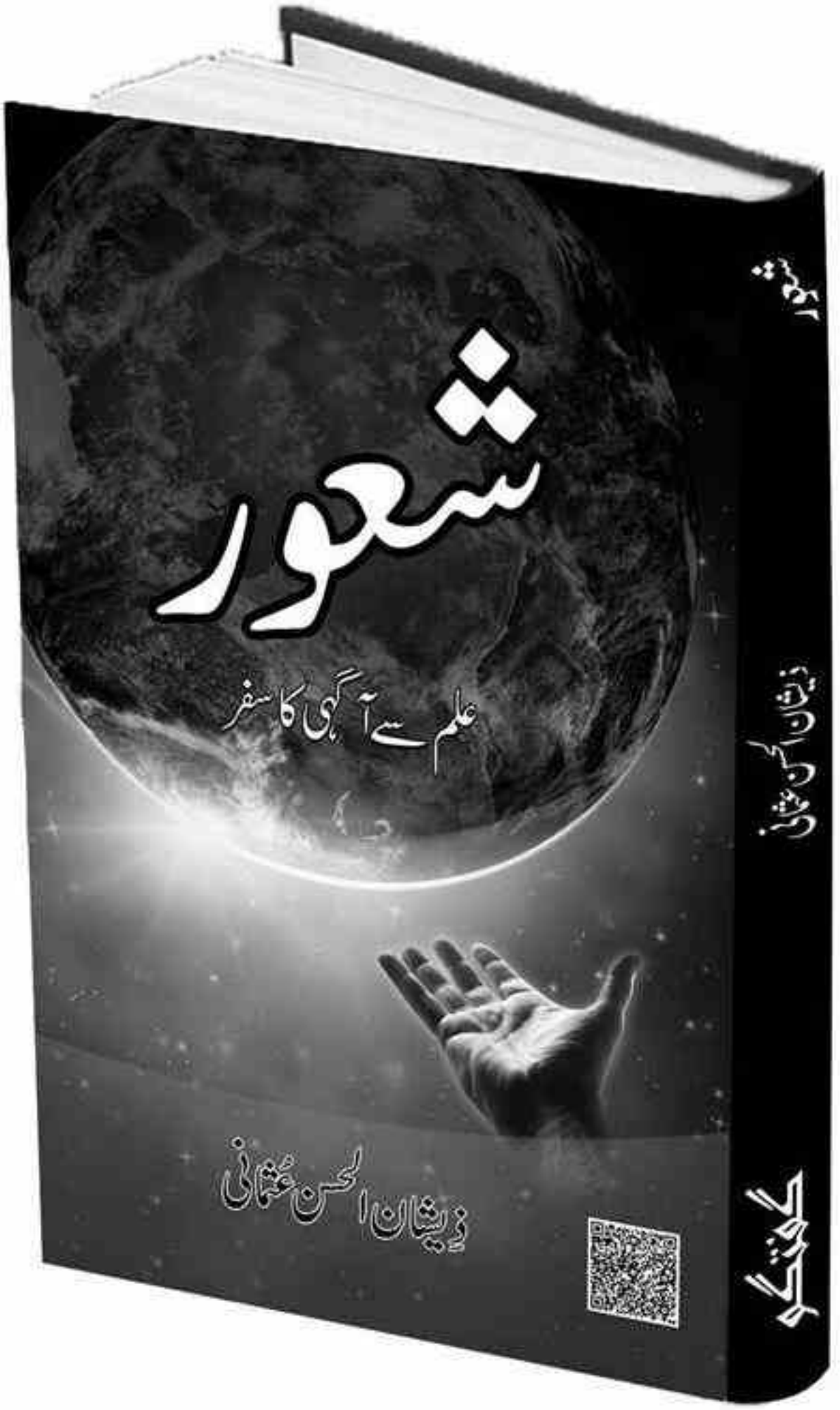


اپنے گھر کتاب حاصل کرنے کیلئے ابھی آرڈر کیجئے:

+92 340 4455990 | info@gufhtugu.com

معاشرے کے سسکتے موضوعات کا احاطہ کرتی تحریریں

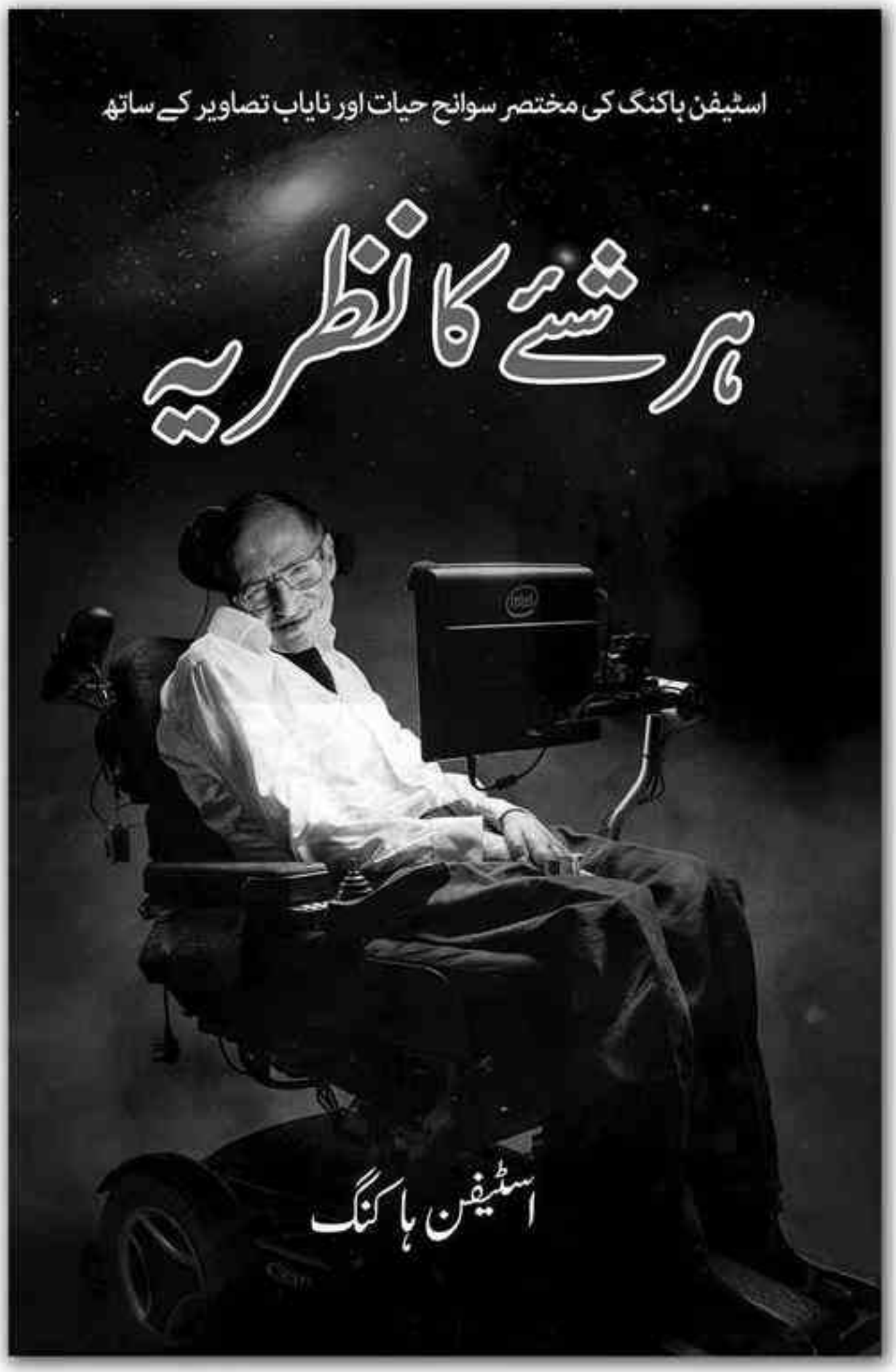
ایک صاحب دل کے قلم سے



اپنے گھر کتاب حاصل کرنے کیلئے ابھی آرڈر کیجئے:

+92 340 4455990 | info@gufhtugu.com

آنجہانی سائنسدان اسٹیفن ہاکنگ کی مشہور زمانہ کتاب
Theory of Everything کا اردو ترجمہ
مختصر سوانح اور نایاب تصاویر کے ساتھ

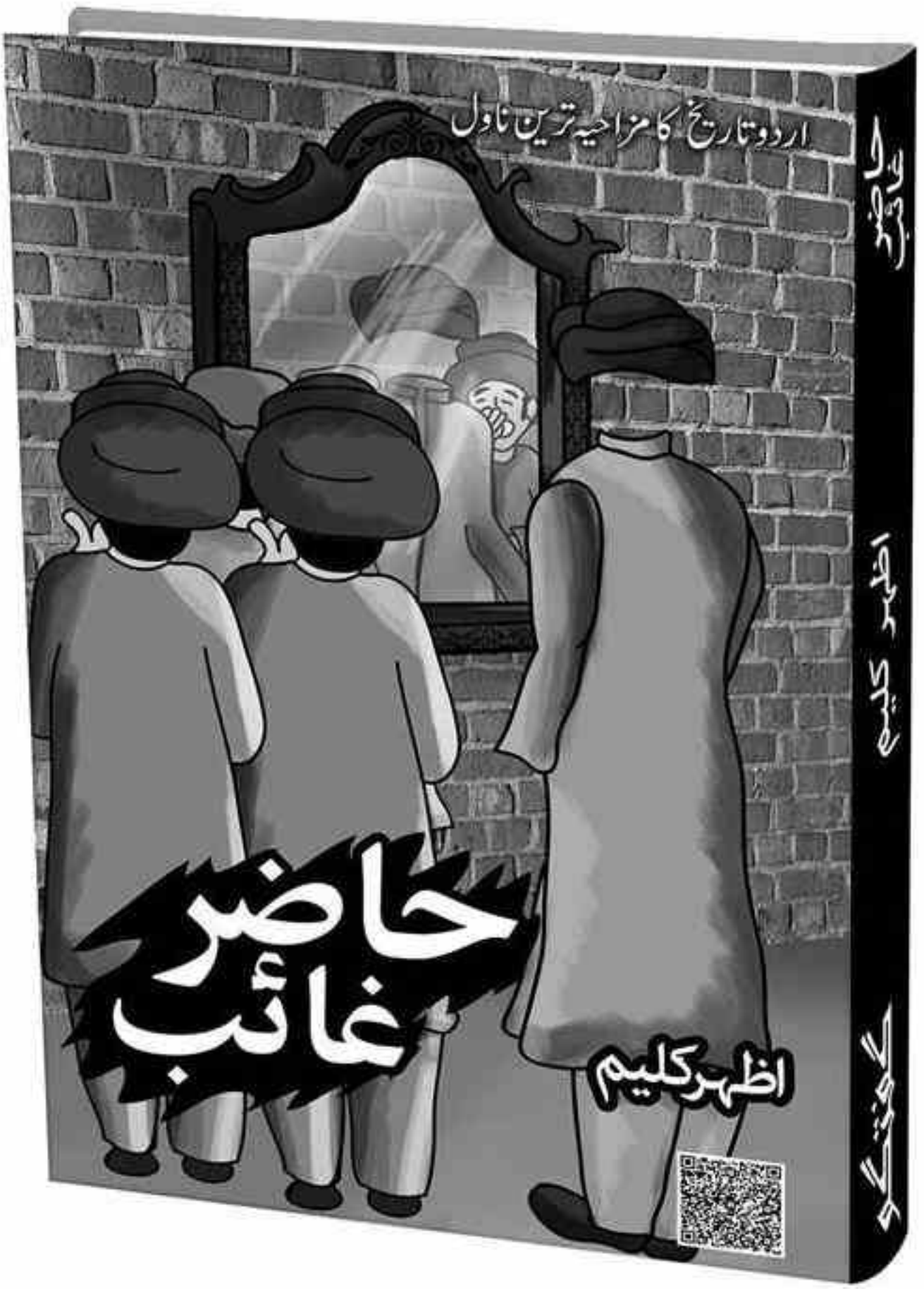


اپنے گھر کتاب حاصل کرنے کیلئے ابھی آرڈر کیجئے:

+92 340 4455990 | info@gufhtugu.com

"قہقہہ وہ ہوتا ہے کہ جسے نچوڑیں تو آنسو نکلیں"
(انور مسعود)

اردو تاریخ کا مزاحیہ ترین ناول

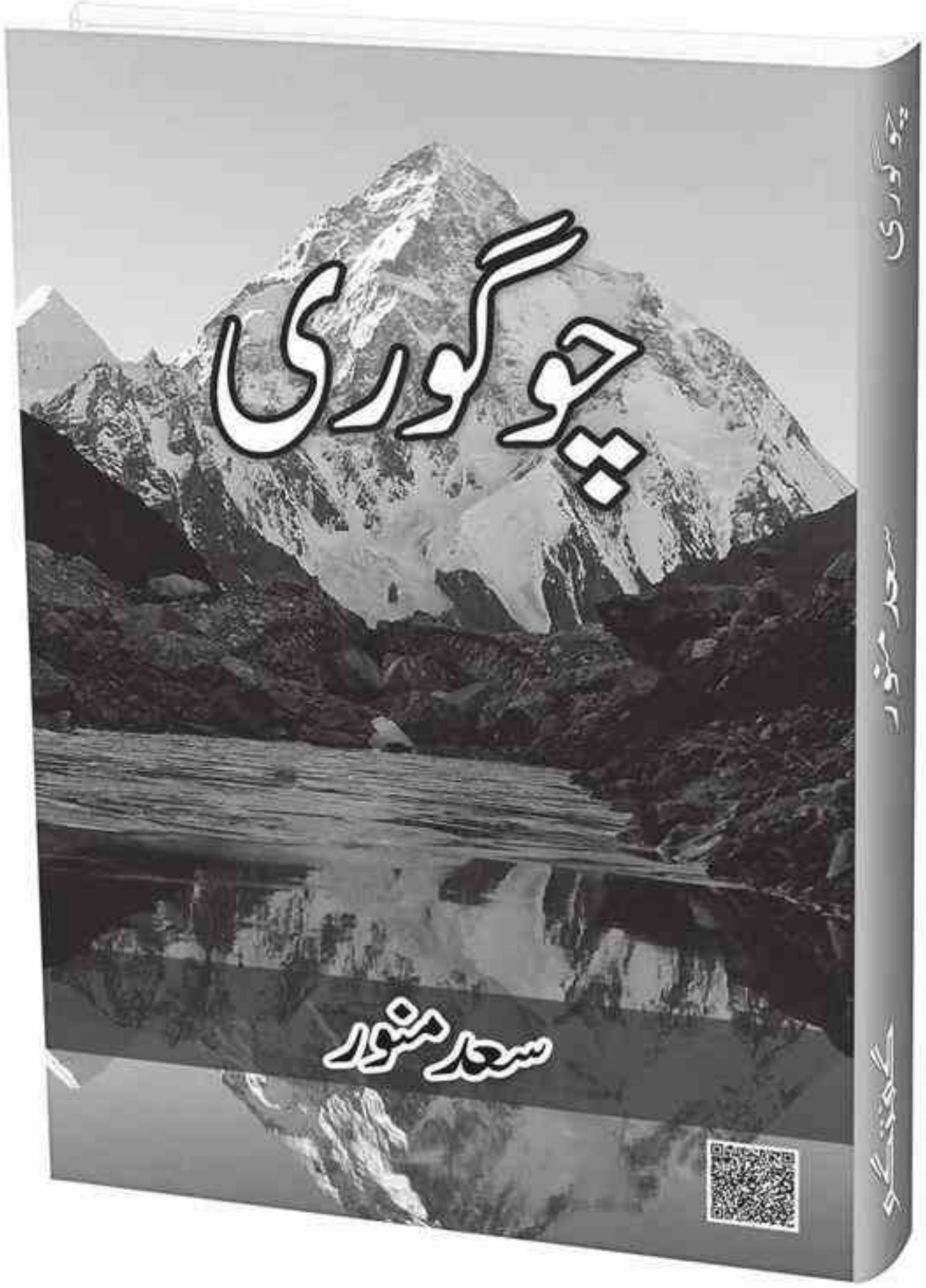


اپنے گھر کتاب حاصل کرنے کیلئے ابھی آرڈر کیجئے:

+92 340 4455990 | info@gufhtugu.com

اردو زبان میں اپنی نوعیت کا منفرد سفر نامہ

K-2 ٹریکنگ کرنے والوں کیلئے ایک رہنما کتاب

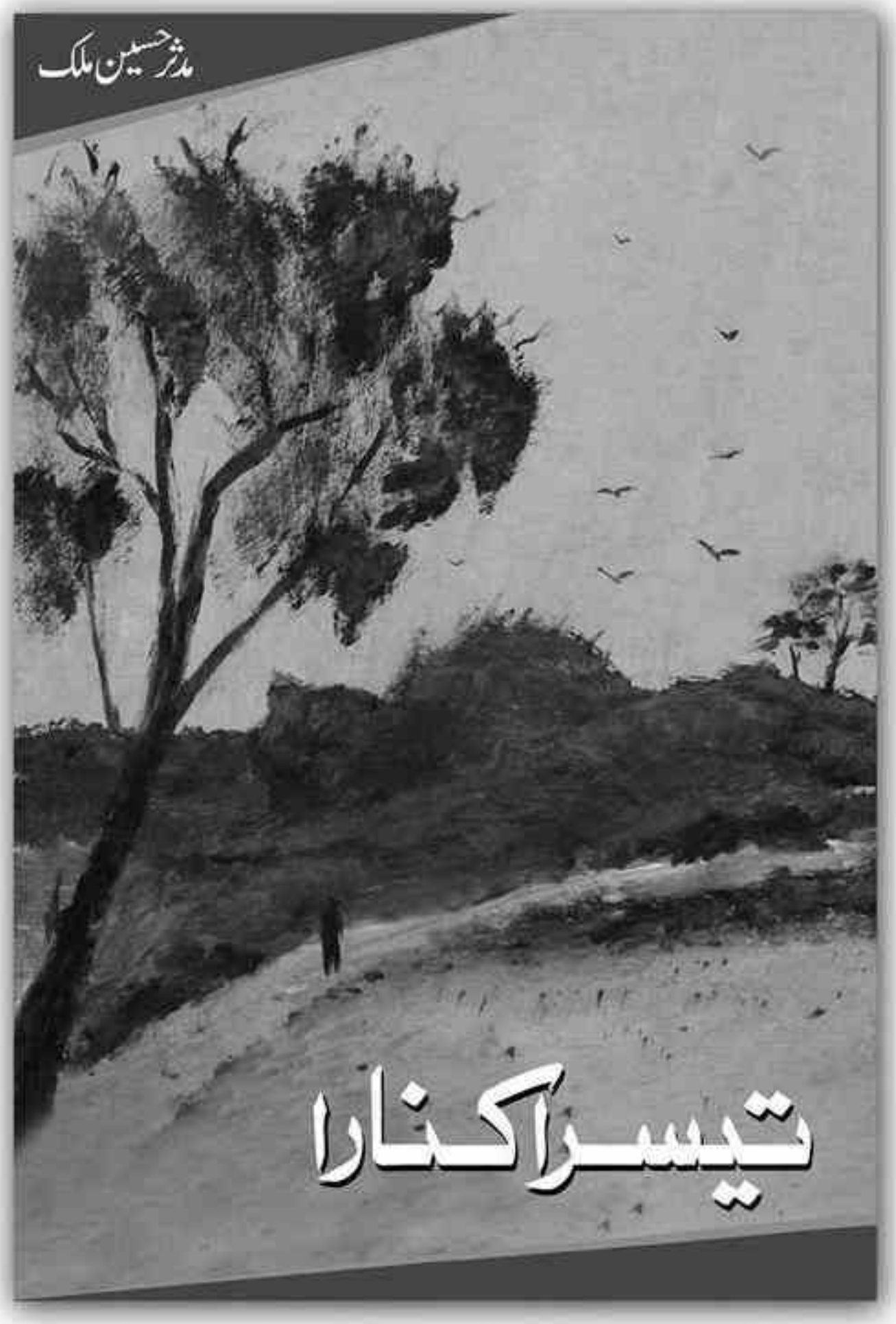


اپنے گھر کتاب حاصل کرنے کیلئے ابھی آرڈر کیجئے:

+92 340 4455990 | info@gufhtugu.com

معروف افسانہ نگار جناب **مدثر حسین ملک** کے قلم سے بنیادی موضوعات میں تصوف۔ عشق حقیقی۔ انسانی نفسیات اور انسانی فطرت پر خواہشات کا اثر شامل ہیں۔

اردو کلاسیکی افسانوں کا مجموعہ



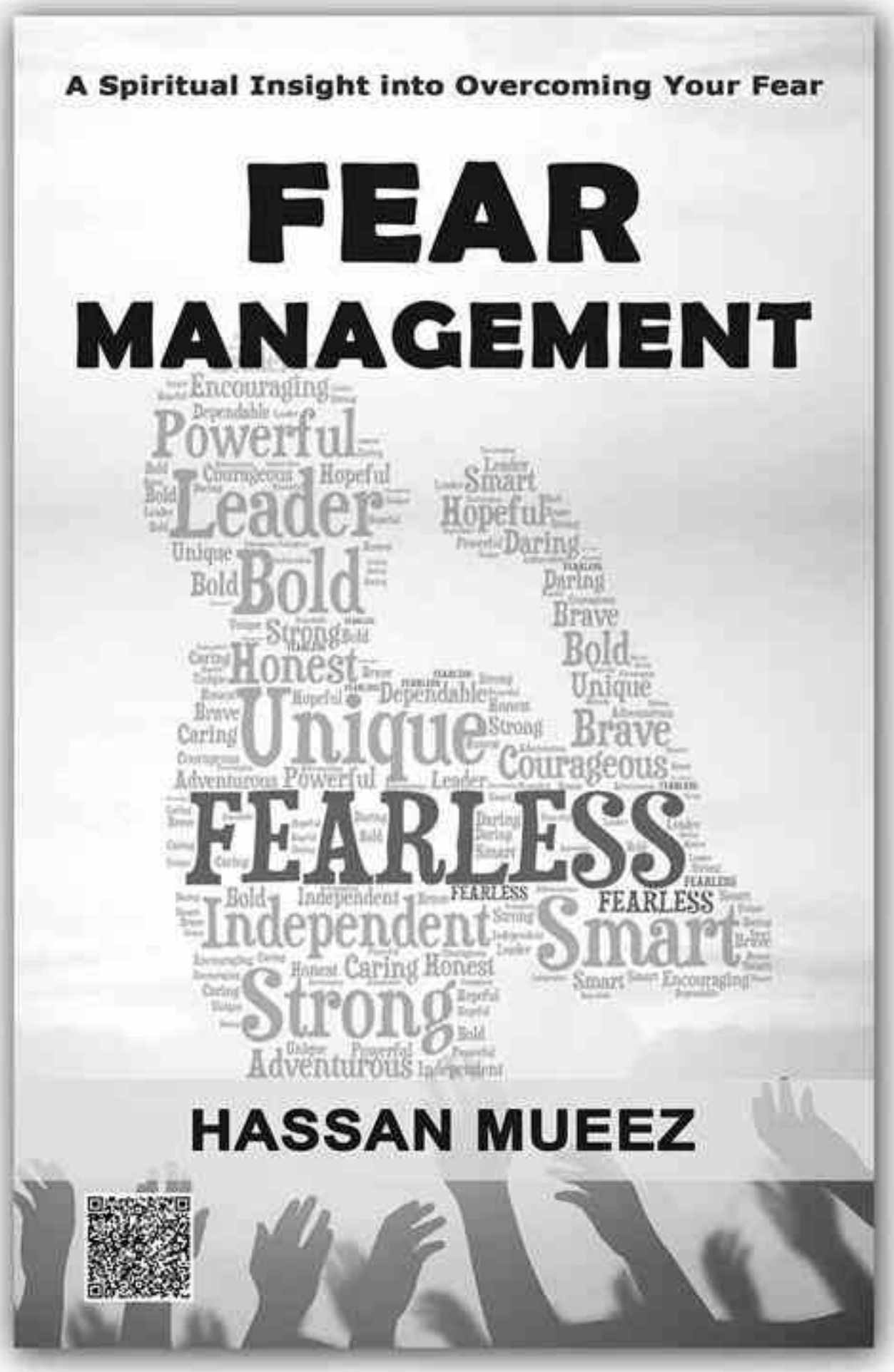
اپنے گھر کتاب حاصل کرنے کیلئے ابھی آرڈر کیجئے:

+92 340 4455990 | info@gufhtugu.com

Do you want to overcome Your *Fears*?

Fear of failure, fear of family, people, surroundings, fear of not delivering and fear of everything else?

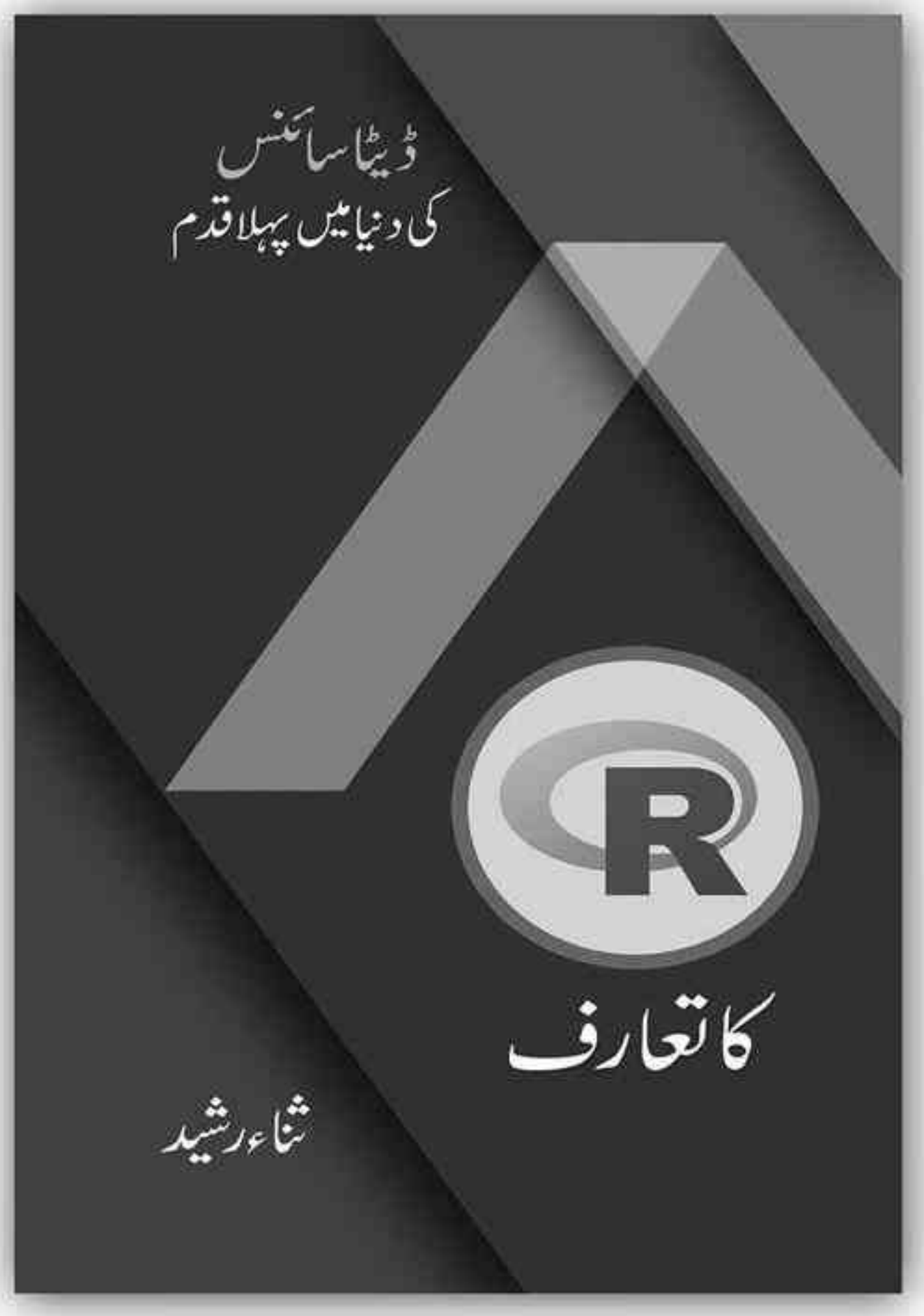
Read this book...



Contact Now to Deliver at your Home

+92 340 4455990 | info@gufhtugu.com

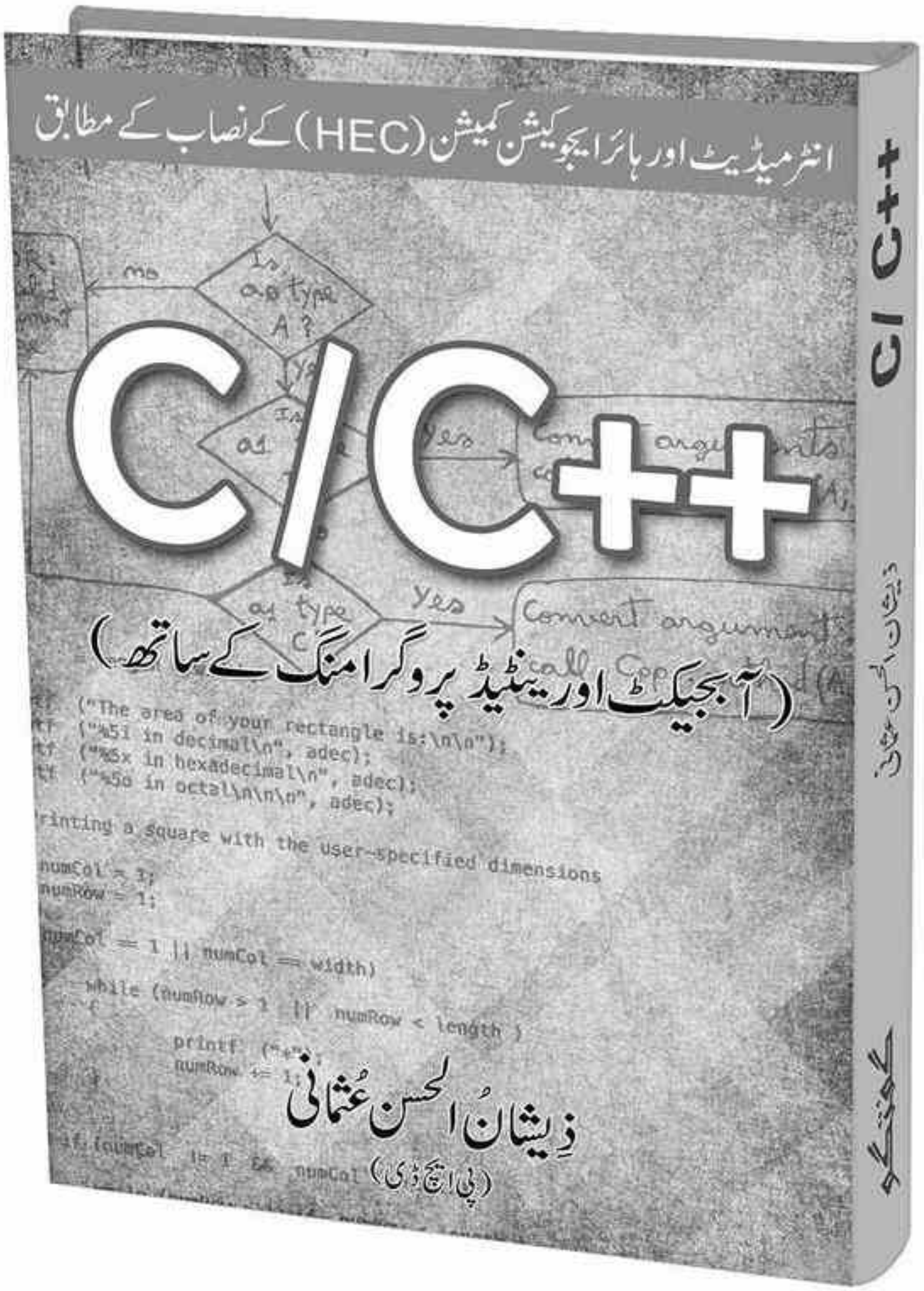
ڈیٹا سائنس سیکھنے والے طلبہ کیلئے
اپنے موضوع پر اردو میں پہلی اور واحد کتاب



اپنے گھر کتاب حاصل کرنے کیلئے ابھی آرڈر کیجئے:

+92 340 4455990 | info@gufhtugu.com

کمپیوٹر پروگرامنگ سیکھنے والے طلبہ و طالبات
کیلئے ایک بہترین رہنما کتاب



اپنے گھر کتاب حاصل کرنے کیلئے ابھی آرڈر کیجئے:

+92 340 4455990 | info@gufhtugu.com

پاکستان میں POD پبلشنگ متعارف کروانے والا منفرد ادارہ

اپنے الفاظ کو دوام بخشئے، اپنے احساسات کو قلم کی زبان دیجئے اور روشنائی سے روشنی پھیلایئے۔

اپنی کتاب شائع کروانے کیلئے ابھی رابطہ کیجئے

+92 340 4455990

ای میل کیجئے: info@gufhtugu.com

فیس بک پیج ملاحظہ فرمایئے: facebook.com/Gufhtugu

ویب سائٹ پر جایئے: www.gufhtugu.com

کتاب کے مصنف، ایتھیریم کے معاون موجد جوزف لیوبن کے ساتھ

کرپٹو کرنسی کیا ہے؟ بٹ کوائن کسے کہتے ہیں؟ بلاک چین کا تعارف، ہم اس ٹیکنالوجی کو کیسے سیکھ سکتے ہیں، کیسے اس کا فائدہ اٹھا سکتے ہیں۔ شرعی لحاظ سے اس کی کیا حیثیت ہے؟ ستوشی ناکاموتو کون تھا؟ مائننگ کیسے کرتے ہیں؟ آئی سی او کس شے کا نام ہے؟ اور اس جیسے سینکڑوں سوالوں کے جوابات کے لئے اس کتاب سے بہتر ذریعہ آپ کو شاید ہی کوئی ملے۔

آیئے ہمارے ساتھ کرپٹو معاشیات Crypto Economics کی دنیا میں قدم رکھیں۔

آپ کی دعاؤں اور تعاون کا شکریہ!

<ISBN 9789697758050>

9 789697 758050

گفتگو پبلی کیشنز

اسلام آباد

فون: +92-51-2231670 ای میل: info@gufhtugu.com

آن لائن خریداری کریں www.gufhtugu.com

فیس بک: facebook.com/Gufhtugu