کرپٹو کرنسی کی ماہیت وحقیقت

ڈاکٹر مبشر حسین رحمانی
لیکچرر کمپیوٹر سائنس ڈیپارٹمنٹ، (سی آئی ٹی) آئرلینڈ

یہ سائنسی طور پر ثابت ہے کہ بٹ کوائن نہ تو حسّی طور پر موجود ہوتے ہیں اور نہ ہی ڈیجیٹل طور پر ان کا کوئی وجود ہے۔ یہ بات غیر ماہرین کے لیے تو حیران کُن ہو سکتی ہے، مگر سائنسدانوں اور محققین کے سامنے بٹ کوائن کی باریکیاں بالکل واضح ہیں۔ ذیل میں ہم بٹ کوائن کے مُوجِد ساتوشی ناکاموٹو سمیت معروف محققین اور سائنسدانوں کے بٹ کوائن کی تکنیکی ماہیت وحقیقت سے متعلق ٹھوس سائنسی اقتباسات پیش کرتے ہیں۔ یہ سائنسی شواہد اتنے واضح ہیں کہ مزید وضاحت کی ضرورت نہیں ہے۔

''درحقیقت کوائن موجود نہیں ہوتے، صرف ٹرانزیکشن ہوتی ہیں جو کہ ملکیت کے حقوق تفویض کرتی ہیں، لہٰذا ایک کوائن کا حقیقی مساوی جو ہم سوچ سکتے ہیں وہ دراصل ٹرانزیکشن کی ایک چین ہے۔''[۱]

''بٹ کوائن یونٹ آف اکاؤنٹ ہیں جو کہ انفرادی نمبرز اور لیٹرز سے کرنسی کی اِکائی بناتا ہے، اس کی قیمت صرف اس لیے ہے، کیونکہ صارفین اس کے لیے ادائیگی کرنے کے لیے تیار ہوتے ہیں۔''[۲]

''سچائی یہ ہے کہ بٹ کوائن یا والٹ جیسی کوئی چیز نہیں ہے، بس ایک کوائن کی ملکیت کے بارے میں نیٹ ورک کے درمیان معاہدہ ہے۔ لین دین کرتے وقت نیٹ ورک پر فنڈز کی ملکیت ثابت کرنے کے لیے ایک ''پرائیویٹ کی'' کا استعمال کیا جاتا ہے۔''[۳]

''بٹ کوائن ہر کوائن کو محفوظ نہیں کرتا اور نہ یہ محفوظ کرتا ہے کہ کون اس کوائن کا مالک ہے۔ اس کے بجائے یہ ایک ڈسٹری بیوٹڈ لیجر بک سسٹم کا استعمال کرتا ہے (جسے ''بلاک چین'' کہا جاتا ہے) اس منطق کی بنیاد پر کہ اگر آپ کو ہر ٹرانزیکشن کے بارے میں معلوم ہے جو کہ کسی ایڈریس نے کی ہے، تو آپ کو معلوم ہوگا کہ کیا اس کے پاس خرچ کرنے کے لیے رقم ہے کہ نہیں۔''[۴]

''ہم الیکٹرانک کوائن کی تعریف اس طرح کرتے ہیں کہ یہ ڈیجیٹل دستخطوں کی زنجیر ہے۔ ہر مالک پچھلے لین دین کے ہیش اور اگلے مالک کی ''پبلک کی'' پر ڈیجیٹل طور پر دستخط کرکے اور کوائن کے

آخر میں ان کو شامل کر کے کوائن کو اگلے کو منتقل کرتا ہے۔ ایک وصول کنندہ ملکیت کی چین کی تصدیق کے لیے دستخطوں کی تصدیق کر سکتا ہے۔‘‘[۵]

’’بٹ کوائن ایک الیکٹرانک، ورچوئل کرنسی ہے جس کی سِکّوں یا بینک نوٹوں کی طرح کوئی حِسّی نمائندگی نہیں ہوتی ہے۔‘‘[۶]

’’ایک سِکّہ، یا اس کا حصہ، بٹ کوائن لیجر میں صرف ایک ٹرانزیکشن ہے۔ بٹ کوائن کی ملکیت ایک ’’پبلک کی‘‘ (pk) کے ذریعے ثابت کی جاتی ہے، جس کی خفیہ ’’پرائیویٹ کی‘‘ صرف درست مالک کے پاس ہوتی ہے۔‘‘[۷]

’’بٹ کوائن کے معاملے میں، ہر ٹرانزیکشن ایک کمپیوٹر سے دوسرے کمپیوٹر میں کرنسی کی منتقلی کی نمائندگی کرتا ہے۔ تمام کمپیوٹر ہر ایڈریس پر موجودہ بیلنس سے آگاہ ہوتے ہیں اور موجودہ بلاک چین کی ایک کاپی کو برقرار رکھتے ہیں، جو کہ پچھلے لین دین کی تاریخ پر مشتمل ریکارڈ ہے۔ ہر ٹرانزیکشن کے بعد بلاک چین کی حالت بدل جاتی ہے۔‘‘[۸]

’’حقیقت میں، بٹ کوائن ڈیجیٹل دستخطوں کا ایک سلسلہ ہے۔‘‘[۹]

’’اپنے نام کے باوجود، بٹ کوائن میں کوئی سکے نہیں ہیں سوائے نمبروں اور حروف کے جو کرنسی کی اکائیوں کو تشکیل دیتے ہیں۔‘‘[۱۰]

’’تکنیکی نقطۂ نظر سے بٹ کوائن جیسی کرپٹو کرنسی کے لیجر کو ’حالت کی منتقلی‘ کے نظام کے طور پر سوچا جا سکتا ہے، جہاں پر ایک ’’حالت‘‘ ہوتی ہے جو کہ تمام موجودہ بٹ کوائنز کی ملکیت کو ظاہر کرتی ہے اور ایک ’’حالت کی منتقلی کا فنکشن‘‘ ہوتا ہے جو ایک حالت اور ایک ٹرانزیکشن لیتا ہے اور نتیجہ کے طور پر ایک نئی حالت پیدا کرتا ہے۔‘‘[۱۱]

’’بٹ کوائن ایک ڈیجیٹل کرنسی کا نظام ہے جس کی بنیاد پیئر ٹو پیئر ورچوئل ڈیٹا پر ہے۔ بٹ کوائنز کو استعمال کرنے کے لیے لوگوں کو کمپیوٹر پر بٹ کوائن ’’والٹ‘‘ انسٹال کرنا ضروری ہے۔ اس والٹ میں ایک باقاعدہ اپ ڈیٹ فائل کے علاوہ کچھ نہیں ہے، جس میں اب تک کی گئی تمام بٹ کوائن ٹرانزیکشن کی فہرست ہے۔ بٹ کوائن کو ’’پبلک اور پرائیویٹ کی کرپٹولوجی‘‘ کے امتزاج کا استعمال کرتے ہوئے دوسرے صارف کے والٹ میں منتقل کیا جا سکتا ہے۔ ٹرانزیکشن میں بٹ کوائنز کی تعداد شامل ہے، بشمول فریکشنز، اور ایک ٹرانزیکشن۔ منفرد ڈیجیٹل دستخط، جو ’’پرائیویٹ کی‘‘ کے ذریعے محفوظ ہے۔‘‘[۱۲]

’’مختصراً، ایک بٹ کوائن کو ایک مالک سے دوسرے مالک کے درمیان ٹرانزیکشن کے ایک سلسلے (چین) کے طور پر سمجھا جاسکتا ہے، جہاں مالکان کی شناخت ’’پبلک کی‘‘ کے ذریعے سے ہوتی ہے، جو تخلص کے طور پر کام کرتی ہے۔‘‘[۱۳]

مندرجہ بالاٹھوس سائنسی حوالہ جات کے اقتباسات سے یہ اُمور واضح ہوتے ہیں کہ:

- بٹ کوائن حسّی طور موجود نہیں ہوتے۔
- بٹ کوائن کی سکّوں یا بینک نوٹوں کی طرح کوئی حسّی نمائندگی نہیں ہوتی ہے۔
- بٹ کوائن ڈیجیٹل طور پر موجود نہیں ہوتے۔
- بٹ کوائن میں ڈیجیٹل کوائن موجود نہیں ہوتے۔
- بٹ کوائن ہر کوائن کو محفوظ نہیں کرتا اور نہ یہ محفوظ کرتا ہے کہ کون اس کوائن کا مالک ہے۔
- بٹ کوائن ڈیجیٹل دستخطوں (سگنیچرز) کی زنجیر ہے۔[۱۴]
- بٹ کوائن میں صرف ٹرانزیکشن ہوتی ہیں جو کہ ملکیت کے حقوق تفویض کرتی ہیں۔
- بٹ کوائن کو قبضے میں نہیں لیا جاسکتا۔
- بٹ کوائنز کو استعمال کرنے کے لیے لوگوں کو کمپیوٹر پر بٹ کوائن ’’والٹ‘‘ انسٹال کرنا ضروری ہے۔ اس والٹ میں ایک باقاعدہ اپ ڈیٹ فائل کے علاوہ کچھ نہیں ہے، جس میں اب تک کی گئی تمام بٹ کوائن ٹرانزیکشن کی فہرست ہے۔
- صارفین کے درمیان صرف ٹرانزیکشن کا تبادلہ ہوتا ہے، نہ کہ بٹ کوائن کا۔
- یہ لیجر کی حالت ہوتی ہے جو کہ اَپ ڈیٹ ہوتی ہے، جس کی بنیاد پر بٹ کوائن کا بیلنس معلوم کیا جاتا ہے۔
- بٹ کوائن کا بیلنس معلوم کرنے کی منطق یہ ہے کہ اگر آپ کو ہر ٹرانزیکشن کے بارے میں معلوم ہے جو کہ کسی ایڈریس نے کی ہے، تو آپ کو معلوم ہوگا کہ کیا اس کے پاس خرچ کرنے کے لیے رقم ہے کہ نہیں۔
- بٹ کوائن کو ’’پبلک اور پرائیویٹ کی کرپٹولوجی‘‘ کے امتزاج کا استعمال کرتے ہوئے دوسرے صارف کے والٹ میں منتقل کیا جاسکتا ہے۔ ’’پبلک‘‘ اور ’’پرائیویٹ کی‘‘ روایتی بینک کے اکاؤنٹ میں یوزر نیم اور پاس ورڈ کے مساوی ہیں۔

سوال یہ ہے کہ کیوں بٹ کوائن کی ماہیت کے بارے میں لوگ غلط فہمی کا شکار ہوجاتے ہیں؟ کچھ

لوگ دلیل دیتے ہیں کہ چونکہ انہوں نے ایک کرپٹوکرنسی والٹ انسٹال کیا ہے، جو ان کے بٹ کوائن کا بیلنس دکھاتا ہے، اور وہ بٹ کوائن کو ایک ایڈریس سے دوسرے ایڈریس پر کامیابی سے منتقل کر سکتے ہیں، لہٰذا اس لیے وہ یہ یقین کرنا شروع کر دیتے ہیں کہ بٹ کوائن ڈیجیٹل طور پر موجود ہوتے ہیں۔ یہ بٹ کوائن کے ڈیجیٹل وجود کے بارے میں ایک بہت بڑی غلط فہمی ہے۔ یہ یقین کرنا کہ بٹ کوائن ڈیجیٹل طور پر موجود ہوتے ہیں، تکنیکی اور سائنسی طور پر غلط ہے۔ اس غلط فہمی کی تردید کے لیے اور بٹ کوائن کے ڈیجیٹل وجود سے متعلق اس افسانے کی حقیقت کو ہم حتمی طور پر آشکار کرتے ہیں۔

کرپٹوکرنسی کی ماہیت سمجھنے کے لیے کچھ مثالیں

مثال نمبر: ۱

ٹرانزیکشن کی ایک تعریف یہ ہے کہ:

’’ٹرانزیکشن فریقین کے درمیان اَثاثوں کی منتقلی کی ریگارڈنگ ہے۔‘‘[۱۵]

ٹرانزیکشن کی اس سادہ سی تعریف میں تین اہم پہلو ہیں: اول: ’’فریقین‘‘، دوم: ’’اثاثے‘‘ اور سوم: ’’منتقلی‘‘۔ ٹرانزیکشن (لین دین) کی ریکارڈنگ کسی بھی روایتی طریقے جیسے کہ فزیکل رجسٹر اور کاپیاں، یا ڈیجیٹل طور پر کمپیوٹر کا استعمال کرتے ہوئے کی جاسکتی ہے۔ اب ہم چند سوالات پوچھتے ہیں۔

۱-اگر کوئی منتقلی نہیں ہوئی تو کیا ٹرانزیکشن (لین دین) ہوگئی؟

۲-اگر کوئی اثاثہ (مبیع یا فروخت کی چیز) موجود نہیں ہے تو کیا ٹرانزیکشن (لین دین) ہوگئی؟

۳-اگر کوئی فریق شامل نہیں ہے تو کیا ٹرانزیکشن (لین دین) ہوگئی؟

اسلامی قوانین کو سامنے رکھتے ہوئے حضرات علمائے کرام نے خرید و فروخت کی کچھ بنیادی شرائط بتائی ہیں۔ ذیل میں ہم ایسی ہی کچھ شرائط کا کتاب ’’An Introduction to Islamic Finance‘‘ سے ذکر کرتے ہیں۔

’’پہلی شرط: مبیع یعنی بیچی جانے والی چیز بیع کے وقت وجود میں آچکی ہو۔

دوسری شرط: مبیع یعنی بیچی جانے والی چیز بیع کے وقت فروخت کرنے والے کی ملکیت میں ہو۔

تیسری شرط: مبیع یعنی بیچی جانے والی چیز بیع کے وقت فروخت کرنے والے کے ... قبضے میں ہو۔

چوتھی شرط: بیع غیر مشروط اور فوری طور پر نافذ العمل ہو۔

پانچویں شرط: بیچی جانے والی چیز ایسی ہو جس کی کوئی قیمت ہو۔

چھٹی شرط: بیچی جانے والی چیز ایسی نہ ہو جس کا حرام مقصد کے علاوہ کوئی اور استعمال ہی نہ ہو، جیسے خنزیر یا شراب وغیرہ۔

ساتویں شرط: جس چیز کی بیع ہو رہی ہو وہ واضح طور پر معلوم ہونی چاہیے اور خریدار کو اس کی شناخت کرائی جانی چاہیے۔

آٹھویں شرط: بیچی جانے والی چیز پر خریدار کا قبضہ کرایا جانا یقینی ہو، یہ قبضہ محض اتفاق پر مبنی یا کسی شرط کے پائے جانے پر موقوف نہیں ہونا چاہیے۔

نویں شرط: قیمت کا تعین بھی بیع کے صحیح ہونے کے لیے ضروری شرط ہے، اگر قیمت متعین نہیں ہے تو بیع صحیح نہیں ہوگی۔

دسویں شرط: بیع میں کوئی شرط نہیں ہونی چاہیے۔'' [۱۶]

اب مندرجہ بالا تین سوالات اور شریعت میں خرید وفروخت کے مندرجہ بالا بنیادی شرائط کو ذہن میں رکھتے ہوئے آیئے! بٹ کوائن کا تجزیہ کرتے ہیں۔ ۳/جنوری سن ۲۰۰۹ء کو ساتوشی ناکاموٹو نے ایک نئے کھاتے (بٹ کوائن لیجر) کی شروعات کی جس میں ایک ایڈریس کے سامنے پچاس بٹ کوائن کا محض اندراج کیا۔ یہ پہلی ٹرانزیکشن تھی جو کبھی ہوئی تھی اور بٹ کوائن لیجر میں درج کی گئی تھی۔ اس پہلی ٹرانزیکشن کے بارے میں ہم ٹرانزیکشن آئی ڈی کے بارے میں جانتے ہیں، ہم تاریخ اور وقت کے بارے میں جانتے ہیں، اور بٹ کوائن کی کتنی تعداد اس ٹرانزیکشن میں لکھی گئی اس بارے میں بھی جانتے ہیں۔ یہ بالکل واضح ہے کہ پچاس بٹ کوائن کا اندراج (مائننگ کے عمل کے نتیجے میں) ایک ایڈریس پر ہوا جو کہ ساتوشی ناکاموٹو کا تھا۔ اُس وقت ان پچاس بٹ کوائن کی کوئی ذاتی یا خارجی قدر نہیں تھی۔ یہ صرف ایک سادہ سی ٹرانزیکشن تھی جسے کھاتے (لیجر) میں اندراج کیا گیا تھا جس میں کوئی اَثاثہ موجود نہیں تھا، کوئی اَثاثہ منتقل نہیں کیا گیا تھا، اور کوئی فریق شامل نہیں تھا۔

مفتیانِ کرام کے مطابق بٹ کوائن کی یہ سادہ سی ٹرانزیکشن شریعت میں خرید وفروخت کی کئی بنیادی شرائط (شرط نمبر ۱، ۲، ۳ اور ۵) کی بیک وَقت خلاف ورزی کر رہی ہے، لہٰذا بٹ کوائن کی خرید وفروخت محض ''مبیع کے بغیر ٹرانزیکشن کی خرید وفروخت'' ہے۔ ہمیں یہ سمجھنے کی بھی ضرورت ہے کہ محض ''کھاتے (لیجر) میں پیسے کا اندراج پیسہ نہیں ہے''۔ بٹ کوائن کسی بھی اَثاثے کی نمائندگی نہیں کرتا ہے، لہٰذا بٹ کوائن کے تناظر میں مبیع کا کوئی وجود ہی نہیں ہوتا، جس پر ملکیت اور قبضہ ہو سکے اور نتیجتاً بٹ کوائن کی ملکیت اور قبضے کا تعین ٹرانزیکشن کرنے یا محض کھاتے میں اندراج کرنے سے ثابت نہیں کیا جاسکتا۔

مثال نمبر: ۲

بٹ کوائن کی صحیح نوعیت کو سمجھنے کے لیے ایک اور مثال لیتے ہیں۔ ایک شخص ''الف'' ایک نئی کرپٹو کرنسی کے بارے میں سوچتا ہے اور اس کا نام ''کراچی کوائن'' KHC رکھتا ہے، کیونکہ یہ ایک تصوراتی کرنسی ہے، لہٰذا اس کی کوئی ذاتی قدر نہیں ہے۔ نیز شروع میں لوگ اس کرپٹو کرنسی کی قدر تسلیم نہیں کرتے۔ ''الف'' اس فرضی کرپٹو کرنسی کا مُوجِد ہے، لہٰذا وہ اس کرپٹو کرنسی کے کھاتے کی شروعات کھاتے میں اندراج کے ذریعے کرتا ہے۔

Tx ID	Details	KHC Amount	Value in US$	Date
001	الف – 25 KHC	25 KHC	0 $	10th Jan 2024
002	ب – 50 KHC	50 KHC	0 $	12th Jan 2024
003	ج – 10 KHC	0 KHC	0 $	15th Jan 2024

ٹیبل نمبر ا: کھاتے میں درج کچھ ٹرانزیکشن جو کہ مختلف اشخاص کے پاس کراچی کوائن کی ملکیت کو دکھا رہی ہیں۔

جیسا کہ قارئین ٹیبل نمبر ا میں دیکھ سکتے ہیں کہ ''الف'' نے کھاتے میں صرف کچھ ٹرانزیکشن کا اندراج کیا ہے، جس میں مختلف اشخاص کے پاس کراچی کوائن کی ملکیت کو دکھایا ہے۔ اب ''ب'' تیس کراچی کوائن ''ج'' کو منتقل کرتا ہے۔ کھاتے کی نئی حالت ٹیبل نمبر ۲ میں دیکھی جا سکتی ہے۔

Tx ID	Details	KHC Amount	Value in US$	Date
001	الف – 25 KHC	25 KHC	0 $	10th Jan 2024
002	ب – 50 KHC	50 KHC	0 $	12th Jan 2024
003	ج – 0 KHC	0 KHC	0 $	15th Jan 2024
004	"ب" نے ۳۰ کراچی کوائن "ج" کو منتقل کیے			17th Jan 2024
	ب کے پاس اب	20 KHC	0 $	
	ج کے پاس اب	30 KHC	0 $	

ٹیبل نمبر ۲: کھاتے میں درج کچھ ٹرانزیکشن جو کہ مختلف اشخاص کے پاس کراچی کوائن کی ملکیت کو دکھا رہی ہیں۔

اب ''ج'' یہ کہتا ہے کہ میں ۳۰ کراچی کوائن کا مالک ہوں۔ یہ ۳۰ کراچی کوائن مجھے ڈیجیٹل طور پر منتقل کیے گئے تھے، کیا کوئی اس کو تسلیم کرے گا؟ نہیں، عقلِ سلیم یہ کہتی ہے کہ اس طرح کی ملکیت قابلِ قبول نہیں ہوگی، کیونکہ یہ صرف کھاتے میں ٹرانزیکشن کا اندراج ہے اور ''مبیع'' سرے سے موجود ہی نہیں ہے۔ اصل میں یہ ۳۰ کراچی کوائن جو کہ ''ج'' کی ملکیت ہیں یہ صرف کھاتے میں فرضی نمبروں کا اندراج ہے۔ ان ۳۰ کراچی کوائن کا سافٹ ویئر کی طرح کوئی ڈیجیٹل وجود بھی نہیں ہے۔ اب اگر کچھ وقت گزرنے کے بعد لوگ ان کراچی

کوائن کی خرید وفروخت کرنا شروع کر دیں اور یہ یقین کرنا شروع کر دیں کہ ان کراچی کوائن کی کوئی ''قدر'' ہے، یہ سمجھنا بالکل بے بنیاد ہوگا اور اسی طریقے سے تخیلاتی معیشت کو بنایا جاتا ہے۔

جب لوگ دیکھتے ہیں کہ کراچی کوائن KHC کی خرید وفروخت مارکیٹ میں ہو رہی ہے اور لوگ ان کراچی کوائن KHC کو ٹریڈ کرنے کے بعد بہت زیادہ رقم کما رہے ہیں تو وہ سوچنے لگتے ہیں کہ یہ کراچی کوائن KHC ڈیجیٹل طور پر موجود ہیں، اور یہ ''ڈیجیٹل اثاثے'' ہیں۔ نیز وہ یہ بھی یقین کرنے لگتے ہیں کہ کراچی کوائن کسی کی ملکیت میں بھی آسکتے ہیں اور انہیں منتقل بھی کیا جا سکتا ہے۔ بس یہیں ان سے غلطی ہوئی ہے۔ درحقیقت کراچی کوائن KHC کی تجارت مبیع کے بغیر لین دین کی تجارت کی طرح ہے اور بٹ کوائن کے معاملے میں بالکل ایسا ہی ہو رہا ہے۔

ٹیبل نمبر ۲ میں ہم ٹرانزیکشن (Tx) ID 004 سے ٹرانزیکشن (Tx) ID 001 تک پیچھے جا سکتے ہیں اور حساب لگا سکتے ہیں کہ ''ج'' کو یہ ۳۰ کراچی کوائن کب اور کہاں سے موصول ہوئے۔ منی ٹریل واضح ہے، یہ شخص ''ب'' تھا جس نے شخص ''ج'' کو ۳۰ کراچی کوائن منتقل کیے اور شخص ''ب'' کے پاس اصل پچاس کراچی کوائن تھے اور جو ان پچاس کراچی کوائن کا مالک بنا کھاتے میں ان فرضی نمبروں کے اندراج سے اور ان پچاس کراچی کوائن کے پیچھے کوئی اثاثہ نہیں تھا۔ اب یہ ایک ستم ظریفی ہوگی کہ اگر ہم اس ''ٹرانزیکشن کی زنجیر'' کو کراچی کوائن کہنا شروع کر دیں اور یہ یقین کرنا شروع کر دیں کہ یہ کراچی کوائن ڈیجیٹل طور پر موجود ہیں اور بٹ کوائن کے اندر بھی بالکل ایسا ہی معاملہ ہوا تھا۔

مثال نمبر: ۳

''الف'' ہزار روپے قرض لیتا ہے ''ب'' سے۔ پھر ''الف'' ایک تحریر ''ب'' کو لکھتا ہے کہ میں آپ کو ایک ماہ میں یہ ہزار روپے واپس کر دوں گا، پھر اس پر اپنے دستخط کرتا ہے، یہ قرض کی رسید بن جاتی ہے۔ اب اگر لوگ اس قرض کی رسید بیچنا شروع کر دیں؟ یاد رکھیں کہ یہ صرف قرض کی ''رسید'' ہے۔ ہم سب جانتے ہیں کہ شریعتِ اسلامی میں قرض کی فروخت ممنوع ہے۔ [۱۷]

اب تصور کریں کہ گر کوئی شخص ایک خالی کاغذ لے اور اس پر اپنے دستخط کرے، جب کہ کسی طرح کا بھی مبیع موجود نہ ہو، بغیر کسی مبیع کے اس خالی دستخط کی کیا اہمیت ہے؟

امریکہ کے نیشنل انسٹیٹیوٹ آف اسٹینڈرڈ اینڈ ٹیکنالوجی، ڈیپارٹمنٹ آف کامرس کے ڈیجیٹل دستخط کے معیار کے مطابق ڈیجیٹل دستخط کی تعریف یوں ہوگی:

''ڈیجیٹل دستخط تحریری دستخط کا ایک الیکٹرانک مساوی ہے؛ ڈیجیٹل دستخط کا استعمال اس بات کی

یقین دہانی کے لیے کیا جاسکتا ہے کہ دعویٰ کرنے والے نے معلومات پر دستخط کیے ہیں۔‘‘[۱۸]

بٹ کوائن کے تناظر میں بالکل ایسا ہی ہو رہا ہے، یعنی کوئی مال، کوئی قرض، کوئی خدمت، کوئی حق، اور کوئی اثاثہ نہیں ہے جو بیچا جارہا ہے۔ نتیجتاً ایسی کوئی چیز نہیں ہے جسے بٹ کوائن میں ’’مبیع‘‘ سمجھا جاسکے۔ بٹ کوائن کے تناظر میں یہ صرف ’’ڈیجیٹل دستخطوں کی زنجیر‘‘ ہے جس کو فروخت کیا جارہا ہے اور یہ وہی بات ہے جو کہ بٹ کوائن کے مُوجِد ساتوشی ناکاموٹو میں بٹ کوائن کے وائٹ پیپر میں درج کی ہے۔

’’ہم الیکٹرانک کوائن کی تعریف اس طرح کرتے ہیں کہ یہ ڈیجیٹل دستخطوں کی زنجیر ہے۔ ہر مالک پچھلے لین دین کے ہیش اور اگلے مالک کی ’’پبلک کی‘‘ پر ڈیجیٹل طور پر دستخط کرکے اور کوائن کے آخر میں ان کو شامل کرکے کوائن کو اگلے کو منتقل کرتا ہے۔ ایک وصول کنندہ ملکیت کی چین کی تصدیق کے لیے دستخطوں کی تصدیق کرسکتا ہے۔‘‘[۱۹]

مندرجہ بالا تین مثالیں بٹ کوائن کی صحیح تکنیکی نوعیت کو واضح طور پر بیان کرتی ہیں۔ ان مثالوں سے یہ بھی صاف ظاہر ہوتا ہے کہ کیوں عام لوگ بٹ کوائن کی نوعیت سے اُلجھ جاتے ہیں اور یہ ماننا شروع کردیتے ہیں کہ بٹ کوائن ڈیجیٹل طور پر موجود ہے۔ ہم نے تکنیکی اور سائنسی طور پر ثابت کیا ہے کہ بٹ کوائن ڈیجیٹل طور پر بھی موجود نہیں ہے۔

نئی کرپٹوکرنسی بننے کا عمل (کرپٹوکرنسی مائننگ)

نئی کرپٹوکرنسی (بٹ کوائن) مائننگ کے عمل سے وجود میں آتی ہے۔ مائننگ کے عمل میں مائنرز کے درمیان مسابقت ہوتی ہے، کوئی اسے دریافت کرنے میں کامیاب ہوتا ہے اور بیشتر ناکام۔ مائننگ کے عمل میں بہت غیر یقینی صورتِ حال ہوتی ہے، یعنی اس بات کی گارنٹی نہیں ہوتی کہ کوئی مائنر اپنے وسائل لگا کر مائننگ کے عمل میں کامیاب بھی ہوجائے گا۔ یعنی مائنر اپنے وسائل (کمپیوٹر اور بجلی) کو خرچ کرتا ہے، لیکن اسے اس کا صلہ ملنا یقینی نہیں ہوتا۔ عام کرپٹوکرنسی صارف کے لیے مائننگ کے عمل میں کامیاب ہونے کا کھربوں احتمالات میں سے ایک احتمال ہوتا ہے۔ نیز کرپٹوکرنسی مائننگ کے ذیل میں یہ بات بھی سمجھنی چاہیے کہ ’’کرپٹوکرنسی کے اندر ٹرانزیکشن (عقود) کا نفاذ دوسروں پر موقوف ہے اور اس کے بغیر ٹرانزیکشن مکمل نہیں ہوتی۔‘‘

’’جب کوئی صارف لیجر میں ٹرانزیکشن شامل کرنا چاہتا ہے، تو ٹرانزیکشن ڈیٹا کو انکرپٹڈ (خفیہ) کیا جاتا ہے اور نیٹ ورک پر دوسرے کمپیوٹرز کے ذریعے کرپٹوگرافک الگورتھم کا استعمال کرتے ہوئے تصدیق کی جاتی ہے۔ اگر کمپیوٹرز کی اکثریت کے درمیان اتفاقِ رائے ہے کہ ٹرانزیکشن درست ہے، تو ڈیٹا کا ایک نیا بلاک چین میں شامل کیا جاتا ہے اور نیٹ ورک پر موجود سبھی لوگوں کے ذریعے شیئر کیا جاتا ہے۔‘‘[۲۰]

ایک اور اہم مسئلہ میم پول Mempool سے ٹرانزیکشن کے انتخاب سے متعلق ہے۔ مائنرز

درحقیقت میم پول سے ٹرانزیکشن کا انتخاب کرتے ہیں اور انہیں بلاک کی شکل میں جمع کرتے ہیں۔ اس کا مطلب یہ ہے کہ ٹرانزیکشن کا انتخاب مائنرز کی مرضی پر منحصر ہے۔ چونکہ ٹرانزیکشنز کو منتخب کرنے کے پیچھے انعام ہوتا ہے، اس لیے عام طور پر وہ ٹرانزیکشنز منتخب کی جاتی ہیں جن کی ٹرانزیکشن فیس زیادہ ہوتی ہے۔ اس کے نتیجے میں کچھ ٹرانزیکشن کو دوسروں پر ترجیح دی جاتی ہے اور کم فیس والی ٹرانزیکشن زیادہ وقت تک انتظار کرتی ہیں۔ [۲۱] مائنرز بلاکس میں ان ٹرانزیکشن کو ترجیح دینے کی کوشش کرتے ہیں جن کی فیس بہت زیادہ ہوتی ہے اور انہیں ''وہیل ٹرانزیکشنز'' کہتے ہیں۔ کیا آپ ایک ایسے مالیاتی نظام کا تصور کرسکتے ہیں جس میں ٹرانزیکشن کے ساتھ یکساں سلوک نہیں کیا جاتا ہو؟ جی ہاں، یہ بٹ کوائن کے بنیادی ڈیزائن میں ہے۔

مندرجہ بالا اقتباسات سے یہ بات واضح ہوتی ہے کہ ٹرانزیکشن کی توثیق کا انحصار دوسرے شرکاء پر ہوتا ہے۔ کیا آپ نے کبھی کسی تجارتی ٹرانزیکشن (لین دین) کے بارے میں سوچا ہے جس میں آپ کو لازمی دنیا بھر کے ہزاروں لوگوں سے اس کی توثیق کرنی ہوگی؟ کیا یہ حیران کن اور غیر معقول نہیں ہے؟ مگر اس کے باوجود یہ بٹ کوائن کی اصل ماہیت ہے، لہٰذا علمائے کرام کے مطابق بٹ کوائن کے مائننگ کے عمل میں شرعی طور پر دو بنیادی نقائص پائے جاتے ہیں:

- بٹ کوائن میں ٹرانزیکشن کی توثیق کا انحصار دوسرے شرکاء پر ہوتا ہے اور اس کے بغیر ٹرانزیکشن مکمل نہیں سمجھی جاتی۔ آسان الفاظ میں اگر کوئی شخص کسی دوسرے شخص کو ٹرانزیکشن (بٹ کوائن) بھیجتا ہے، تو یہ سادہ ٹرانزیکشن اس وقت تک مکمل نہیں ہوتی جب تک کہ بٹ کوائن نیٹ ورک میں شرکت کرنے والوں کی اکثریت اس ٹرانزیکشن کی توثیق نہیں کرلیتی۔ ٹرانزیکشن کی توثیق کا یہ عمل شرعی طور پر درست نہیں۔
- کرپٹوکرنسی مائننگ کے عمل میں کافی غیر یقینی صورت حال ہے، یعنی اس بات کی کوئی گارنٹی نہیں ہے کہ مائنر اپنے وسائل کی سرمایہ کاری کرکے مائننگ کے عمل میں کامیاب ہوگا۔ یہ واضح طور پر ظاہر کرتا ہے کہ مائننگ کے عمل میں غیر یقینی یعنی ''غرر'' ہے جو کہ شرعی اصولوں کے خلاف ہے۔

عالمی معاشی ماہرین کی کرپٹوکرنسی سے متعلق آراء

کرپٹوکرنسی پر مالیاتی ماہرین اور ماہرینِ اقتصادیات کی طرف سے لکھے گئے سائنسی مضامین کی بہتات ہے جنہوں نے کرپٹوکرنسی پر اپنا نقطۂ نظر پیش کیا ہے۔ ہم یہاں چند نمائندہ حوالہ جات پیش کرتے ہیں، تاکہ ہمارے قارئین سمجھ سکیں کہ سنجیدہ مالیاتی ماہرین اور ماہرین اقتصادیات بھی بٹ کوائن کو زَر، ڈیجیٹل کرنسی، یا ڈیجیٹل اثاثہ نہیں سمجھتے۔

یورپی یونین کی اقتصادی اور مالیاتی امور کی کمیٹی یہ کہتی ہے: [۲۲]

’’ڈیجیٹل کرنسیوں کو بطور آلۂ مبادلہ Medium of Exchange استعمال نہیں کیا جارہا اور نہ ہی کیا جاسکتا ہے۔ کرپٹو کرنسیوں کو بطور قدر شمار کرنے کے Unit of Account استعمال نہیں کیا جاسکتا ہے۔ کرپٹو کرنسیاں، کرنسی کے بنیادی اوصاف پر پورا نہیں اُترتیں۔‘‘

’’یورپی سپروائزری اتھارٹیز صارفین کو خبردار کرتی ہیں کہ بہت سے کرپٹو اثاثے انتہائی رسکی اور سٹے بازی یعنی قیاس آرائی پر مبنی ہیں۔ یہ زیادہ تر ریٹیل صارفین کے لیے بطور سرمایہ کاری یا ادائیگی یا تبادلے کے لیے موزوں نہیں ہیں۔‘‘[۲۳]

کیون ڈیوس، جو یونیورسٹی آف میلبورن، آسٹریلیا میں فنانس کے پروفیسر ہیں، سمجھتے ہیں کہ کرپٹو جُوا ہے، جس کا کوئی سماجی فائدہ نہیں ہے، اور یہاں تک کہ کرپٹو کرنسی کے لیے ’’سرمایہ کاری‘‘ یا ’’کرپٹو اثاثے‘‘ کی اصطلاحات استعمال کرنے سے ہچکچاتے ہیں۔ انہوں نے اپنے حالیہ مضمون میں لکھا:

’’دوسرا، اصطلاح ’’اثاثہ‘‘ کا مطلب یہ ہے کہ وہ شے یا تو جاری کنندہ کی ذمہ داری ہے، یا مادّی یا غیر مادّی اثاثہ کی ملکیت کی نمائندگی کرتی ہے، جس میں یہ صلاحیت ہو کہ وہ مستقبل کی آمدنی یا سروسز آف ویلیو پیدا کرنے کے لیے استعمال ہونے کی صلاحیت رکھتی ہے۔ کرپٹو آئٹم کی واحد ممکنہ قیمت یہ ہے کہ کوئی دوسرا جُواری انہیں زیادہ قیمت پر خریدنے کے لیے تیار ہوسکتا ہے۔‘‘[۲۴]

ایک سائنسی تحقیق اس بات کو ثابت کرتی ہے کہ:

’’بٹ کوائن کسی دوسرے بڑے اثاثہ کی کلاس کے برعکس ہے۔ بٹ کوائن اپنے متعارف ہونے کے بعد سے بہت غیر مستحکم رہا ہے۔ خاص طور پر اس کا اتار چڑھاؤ فیصلہ کن طور پر سونے، امریکی ڈالر، یا اسٹاک مارکیٹوں کے اُتار چڑھاؤ سے زیادہ ہے (جس کی نمائندگی MSCI ورلڈ انڈیکس کرتا ہے)۔

بٹ کوائن سونا Gold اور امریکی ڈالر US Dollar اور دیگر اثاثوں سے کسی طرح بھی مماثلت نہیں رکھتا۔ بٹ کوائن کا بہت زیادہ نفع دینا اور اُتار چڑھاؤ سونے یا امریکی ڈالر کے مقابلے میں ایک انتہائی قیاس آرائی (سٹے بازی) پر مبنی اثاثہ سے مشابہت رکھتا ہے۔‘‘[۲۵]

ایک حالیہ سائنسی تحقیق میں ثابت کیا گیا ہے کہ اُن تمام بٹ کوائن میں سے جو کہ آج کل سرکولیشن میں ہیں ایک فیصد سے بھی کم یعنی 0.01 فیصد ایڈریس 58.2 (اٹھاون اعشاریہ دو فیصد) بٹ کوائن رکھتے ہیں۔[۲۶] لہٰذا بٹ کوائن بھی Pareto Distribution کی پیروی کرتا ہے، جس کے معنی یہ ہوئے کہ کسی بھی ملک کے معاشی

نظام میں ۲۰ فیصد لوگ ۸۰ فیصد دولت کو کنٹرول کرتے ہیں اور حیرت انگیز بات یہ ہے کہ مجموعی طور پر کرپٹو کرنسی اعداد وشمار کے مطابق اس سے بھی بری ہے۔ انہی محققین نے آٹھ مختلف کرپٹو کرنسیوں میں دولت کی تقسیم کا بھی تجزیہ کیا، یعنی ایک فیصد لوگوں (ایڈریس) کے پاس کُل کتنے مقدار کی کرپٹو کرنسی ملکیت میں ہیں۔

محققین نے ''بٹ کوائن بیلنس کے حساب سے سب سے بڑا والٹ''، ''صارف کی ٹرانزیکشن کی سرگرمیاں''، اور ''مختلف اقسام کے بٹ کوائن استعمال کرنے والوں (مائنرز، ایکسچینج، ریٹیلر، وغیرہ) میں دولت کی تقسیم'' پر ایک بہترین تکنیکی تحقیق کی ہے۔[۲۷] ایک اور تحقیق میں محققین نے ثابت کیا ہے کہ: ''بٹ کوائن کے ایک فیصد سے بھی کم صارفین ۹۵ فیصد سے زیادہ مارکیٹ والیم (حجم) میں حصہ ڈالتے ہیں۔''[۲۸]

ایک سائنسی تحقیق بٹ کوائن کے استعمال اور اس کا دیگر اثاثوں سے مقابلے کے تناظر میں لکھی گئی ہے۔ محققین کی تحقیق کا خلاصہ ہے کہ:

''بٹ کوائن کا دور دور تک کوئی تعلق نہیں ہے روایتی اثاثہ جات کے ساتھ جیسے اسٹاک، بانڈز اور کموڈٹیز، چاہے وہ عام اوقات ہوں یا مالیاتی بحران کے دن ہوں۔ بٹ کوائن ٹرانزیکشن کے اعداد وشمار کا تجزیہ ظاہر کرتا ہے کہ بٹ کوائن بنیادی طور پر ایک قیاس آرائی (سٹے بازی) پر مبنی سرمایہ کاری کے طور پر استعمال ہوتے ہیں نہ کہ متبادل کرنسی اور بطور آلۂ مبادلہ۔''[۲۹]

مجموعی طور پر ان محققین نے بٹ کوائن کا موازنہ پانچ اثاثوں کی کلاسوں یعنی ایکویٹی S&P500 اورS&P600 ، قیمتی دھات (گولڈ اور سلور سپاٹ)، چھ مختلف کرنسی جوڑے (EUR/USD، AUD/USD، JPY/USD، GBP/USD، CNY/ USD، HUF/USD) توانائی (WTI کروڈ آئل انڈیکس، HH نیچرل گیس انڈیکس)، اور بانڈ (بلومبرگ یو ایس کارپوریٹ بانڈ انڈیکس، بلومبرگ یو ایس ٹریژری بانڈ انڈیکس، بلومبرگ USD ہائی ییلڈ کارپوریٹ بانڈ انڈیکس) سے کیا ہے اور یہ نتیجہ اخذ کیا کہ بٹ کوائن تمام روایتی اثاثوں کی کلاسوں سے مختلف ہے۔

انہی محققین نے تحریر کیا ہے کہ تقریباً دو سے پانچ فیصد لوگوں نے بٹ کوائن کو چیزوں اور اشیاء کی خریداری کے لیے استعمال کیا، جبکہ پچانوے فیصد لوگوں نے اس کو بطور سرمایہ کاری کے استعمال کیا۔ اُن کی تحقیق کا خلاصہ یہ تھا:

''ہم یہ نتیجہ اخذ کرتے ہیں کہ بہت کم ایسے صارفین ہیں جو بٹ کوائن کو خالصتاً بطور آلۂ مبادلہ استعمال کرتے ہیں اور صارفین کی بہت بڑی تعداد بٹ کوائن کو سرمایہ کاری کے لیے استعمال کرتے ہیں۔''

خلاصہ کلام

سائنسدان اور محققین کرپٹو کرنسی کی ماہیت کے بارے میں واضح سمجھ رکھتے ہیں۔ اسی طریقے سے علمائے کرام کی اکثریت اور مستند دار الافتاء کا بہت ہی واضح موقف ہے کہ کرپٹو کرنسی کی اپنی ذاتی خرید وفروخت یا اس کے ذریعے سے دیگر اثاثہ جات کی خرید وفروخت جائز نہیں ہے۔ علمائے کرام کے مطابق یہ فرضی وتخیلاتی نمبر شرعی طور پر ''مال'' بننے کی صلاحیت ہی نہیں رکھتے۔ اس مضمون میں ہم نے علمائے کرام کے موقف کو مزید تقویت دینے کے لیے سائنسی حوالہ جات فراہم کیے ہیں۔ وہ دن گئے جب کرپٹو کرنسی کے بارے میں تکنیکی تفصیلات چھپائی جا سکتی تھیں۔ اب کوئی بھی کرپٹو کرنسی کی اصل ماہیت کو سمجھنے کے لیے اصل سائنسی ماخذ کو پڑھ سکتا ہے اور ہمیں یقین ہے کہ وہ اسی نتیجے پر پہنچیں گے، جیسا کہ ہمارے معزز علمائے کرام پہنچے ہیں، یعنی کرپٹو کرنسی محض **''کھاتے (لیجر) میں فرضی نمبروں کے اندراج کی تجارت ہے''** یا مزید واضح طور پر **''مبیع کے بغیر ٹرانزیکشن کی خرید وفروخت''** ہے۔

حواشی وحوالہ جات

[1] F. Tschorsch and B. Scheuermann, "Bitcoin and Beyond: A Technical Survey on Decentralized Digital Currencies," in IEEE Communications Surveys & Tutorials, vol. 18, no. 3, pp. 2084-2123, thirdquarter 2016.

[2] FATF REPORT, Virtual Currencies Key Definitions and Potential AML/CFT Risks , June 2014.

[3] https://www.newscientist.com/definition/bitcoin/

[4] Dominic Hobson, What is bitcoin? XRDS crossroads. ACM Magazine for Students, vol. 20, Issue 1, 2013.

[5] Satoshi Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System. Accessed: Apr 2023. [Online]. Available: https://bitcoin.org/bitcoin.pdf

[6] Harald Vranken, Sustainability of bitcoin and blockchains, Current Opinion in Environmental Sustainability, Volume 28, 2017.

[7] D. Drusinsky, "On the High-Energy Consumption of Bitcoin Mining," in Computer, vol. 55, no. 1, pp. 88-93, Jan. 2022.

[8] D. Puthal, N. Malik, S. P. Mohanty, E. Kougianos and G. Das, "Everything You Wanted to Know About the Blockchain: Its Promise, Components, Processes, and Problems," in IEEE Consumer Electronics Magazine, vol. 7, no. 4, pp. 6-14, July 2018.

[9] M. C. Kus Khalilov and A. Levi, "A Survey on Anonymity and Privacy in Bitcoin-Like Digital Cash Systems," in IEEE Communications Surveys & Tutorials, vol. 20, no. 3, pp. 2543-2585, thirdquarter 2018.

[10] Madise, Sunduzwayo, Back to the Future? Evolving Forms of Money (June 9, 2015). Available at SSRN: https://ssrn.com/abstract=2622080 or http://dx.doi.org/10.2139/ssrn.2622080

[11] V. Buterin, "A next generation smart contract and decentralized application platform", 2014. [Online]. Available: https://github.com/ethereum/wiki/wiki/White-Paper

[12] G. F. Hurlburt and I. Bojanova, "Bitcoin: Benefit or Curse?," in IT Professional, vol. 16, no. 3, pp. 10-15, May-June 2014.

[13] S. Meiklejohn et al., "A Fistful of Bitcoins: Characterizing Payments among Men with No Names" and was published in the Proceedings of the Internet Measurement Conference, 2013, ACM.

[14] "A digital signature is an electronic analogue of a written signature; the digital signature can be used to provide assurance that the claimed signatory signed the information". NIST Digital Signature Standard, U.S. Department of Commerce, 03rd February 2023. Link: https://csrc.nist.gov/projects/digital-signatures

[15] D. Yaga, P. Mell, N. Roby, and K. Scarfone, "Blockchain Technology Overview", NIST Interagency/Internal Report (NISTIR), National Institute of Standards and Technology, Gaithersburg, MD, 2018.

https://csrc.nist.gov/csrc/media/publications/nistir/8202/draft/documents/nistir8202-draft.pdf

[16] Mufti Muhammad Taqi Usmani, "An Introduction to Islamic Finance". Accessed: 31st Jan 2024.

[17] Justice Mufti Muhammad Taqi Usmani, "Causes and Remedies of the Recent Financial Crisis – From An Islamic Perspective", Turath Publishing, 2014.

[18] NIST Digital Signature Standard, U.S. Department of Commerce, 03rd February 2023. Link: https://csrc.nist.gov/projects/digital-signatures

[19] Satoshi Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System". Accessed: Apr 2023. [Online]. Available: https://bitcoin.org/bitcoin.pdf

[20] Sarah Underwood, "Blockchain beyond bitcoin", Communications of the ACM, Volume 59, Issue 11, pp 15–17, 2016.

[21] I. Malakhov, A. Marin, S. Rossi and D. S. Menasché, "Confirmed or Dropped? Reliability Analysis of Transactions in PoW Blockchains," in IEEE Transactions on Network Science and Engineering, in Print, 2024.

[22] GERBA, E. and RUBIO, M., "Virtual Money: How Much do Cryptocurrencies Alter the Fundamental Functions of Money?", Study for the Committee on Economic and Monetary Affairs, Policy Department for Economic, Scientific and Quality of Life Policies, European Parliament, Luxembourg, 2019.

[23] https://www.eba.europa.eu/eu-financial-regulators-warn-consumers-risks-crypto-assets

[24] Kevin Davis, "Why crypto is gambling and not investing", Financial Review, Jan 2022.

[25] Dirk G. Baur, Tohmas Dimpfl, and Konstantin Kuck, "Bitcoin, gold and the US dollar – A replication and extension", Finance Research Letters Volume 25, June 2018, Pages 103-110.

[26] Ashish Rajendra Sai, Jim Buckley, Andrew Le Gear, "Characterizing Wealth Inequality in Cryptocurrencies", Frontiers in Blockchian, Volume 4 - 2021.

[27] Hossein Jahanshahloo, Felix Irresberger, Andrew Urquhart, "Bitcoin under the microscope", The British Accounting Review, 2023.

[28] Anqi Liu, Hossein Jahanshahloo, Jing Chen & Arman Eshraghi, "Trading patterns in the bitcoin market", The European Journal of Finance, 2023.

[29] Dirk G. Baur, KiHoon Hong, Adrian D. Lee, "Bitcoin: Medium of exchange or speculative assets" Journal of International Financial Markets, Institutions and Money, Volume 54, 2018