Bitcoin

A Peer-to-Peer Electronic Cash System

We the Participants of the Network,

in Order to form a more perfect Medium of Exchange, to establish Trust where no Trustee is required, to insure the Integrity of every Transaction, to maintain a common and public Ledger, and to secure the Liberty of Value to ourselves and our Posterity, do ordain and establish this System of Peer-to-Peer Electronic Cash.

A purely Peer-to-Peer Version of Electronic Cash shall permit Payments to pass directly from one Party to another, and no Financial Institution shall stand between them.

ART. I. *Of Introduction.* Commerce upon the Internet has come to rest wholly upon Financial Institutions serving as trusted third Parties. In this lies the inherent Weakness of the trust-based Model: Transactions remain ever reversible; Mediation swells the Cost of small Dealings; and the Merchant must demand of his Customer more than the Transaction itself requires. What is wanted is an electronic Payment founded upon cryptographic Proof in the Place of Trust, whereby any two willing Parties may transact directly, the one with the other, without Need of any Intermediary.

ART. II. *Of Transactions.* An electronic Coin we declare to be a Chain of digital Signatures. Each Owner shall convey the Coin to the next by setting his Signature upon a Hash of the prior Transaction, together with the public Key of him who receives it, and by appending the same unto the Coin's End. The Payee may verify the Signatures, and establish thereby the whole Chain of Custody. Yet herein lies a Peril: the Payee cannot know whether some former Owner has spent the Coin twice. This we resolve without Recourse to any Mint, by public and singular Agreement upon the Order in which the Transactions were received.

ART. III. *Of the Timestamp Server.* Our Remedy commences with a Server of Timestamps, which shall take the Hash of a Block of Items to be stamped, and publish that Hash abroad for all the World to witness. Each Timestamp shall include within its Hash the one that came before it, forming thereby a Chain, wherein every Timestamp fortifies all that preceded it; and no Record, once so fixed, may be altered alone.

ART. IV. *Of Proof-of-Work.* To raise this Server of Timestamps upon a distributed Footing, we employ a Proof-of-Work: the Scanning for a Value whose Hash begins with a requisite Number of Zero Bits. The Labor once spent, the Block cannot be changed but by the spending of it anew; and as further Blocks are chained thereafter, to alter one is to redo all that follow it. Thus shall Representation be measured, not by the counting of Addresses, which any Man might multiply at his Pleasure, but by Proof-of-Work alone: one Processor, one Vote.

ART. V. *Of the Network.* The Network shall be run in this wise: new Transactions shall be broadcast to all Nodes; each Node shall gather them into a Block; each shall labor to find its Block's Proof-of-Work; the Proof being found, the Block shall be broadcast abroad; the Nodes shall accept the Block only if its Transactions be valid and not already spent; and they shall signify their Acceptance by laboring to raise the next Block upon it. The longest Chain the Nodes shall hold to be the true one, and upon it alone shall they build.

ART. VI. *Of Incentive.* By Convention, the first Transaction of every Block shall be a special one, creating a new Coin owned by the Maker of that Block. This rewards the Nodes for their Support and, there being no central Authority, disburses the Coins into Circulation, as Gold is drawn from the Earth by the Expense of Labor. The Reward may be funded also by Fees upon Transactions; and once a predetermined Number of Coins have entered Circulation, the Incentive may pass wholly to such Fees, and be entirely free of Inflation. Such Incentive may keep the Nodes honest: for should some greedy Assailant command more Power than all the honest Nodes together, he must choose between defrauding Men of their Payments and the honest Generation of new Coin; and he shall find the Rules the more profitable.

ART. VII. *Of Reclaiming Disk Space.* When the latest Transaction of a Coin lies buried beneath Blocks sufficient in Number, the spent Transactions preceding it may be discarded, that Storage be spared. And that the Block's Hash be not thereby broken, the Transactions shall be hashed within a Merkle Tree, whereof only the Root is entered into the Block. Old Blocks may then be compacted, their interior Branches stubbed away; for of these no further Keeping is required.

ART. VIII. *Of Simplified Payment Verification.* A Man may verify his Payments though he keep no full Node. He need hold only the Block Headers of the longest Chain, obtained by inquiring of the Nodes until he be persuaded he holds the longest; and he may fetch the Merkle Branch that binds his Transaction to the Block wherein it was stamped. The Transaction itself he cannot inspect; but seeing it bound to its Place in the Chain, he beholds that a Node has accepted it, and the Blocks added thereafter confirm the Assent of the whole Network.

ART. IX. *Of Combining and Splitting Value.* That Value be managed apart from the handling of each Coin severally, Transactions shall admit of many Inputs and many Outputs. Commonly there shall be a single Input of some larger Sum, or several Inputs joining smaller Sums together; and no more than two Outputs: the one for the Payment, and the other, if any be needed, returning the Change unto the Sender.

ART. X. *Of Privacy.* The elder Model of Banking preserved Privacy by admitting none to the Knowledge of a Dealing, save the Parties themselves and the trusted third Party. Here Privacy may yet be kept, though the Transactions be public, by holding the public Keys anonymous. The World may see that some Sum passes from one to another, yet nothing therein binds that Sum to any Name. And for each Transaction let a fresh Pair of Keys be employed, that they be not traced unto a common Owner.

ART. XI. *Of Calculations.* Consider an Assailant who would fashion a Chain swifter than the honest one. He cannot conjure Value from nothing, nor seize Coin that was never his; for the Nodes will suffer no invalid Transaction to pass. His Hope is only to take back some Payment he himself has lately made; and the Probability that he ever overtake the honest Chain falls away exponentially with every Block that is laid upon it.

ART. XII. *Of Conclusion.* We have set forth herein a System of electronic Transaction that leans not upon Trust. Beginning with Coins fashioned of digital Signatures, we have raised a Peer-to-Peer Network recording the public History of Transactions in Proof-of-Work, soon rendered beyond the Power of any Assailant to alter, so long as honest Nodes command the greater Strength. The Network is robust in its unstructured Simplicity: the Nodes work all at once with little Coordination; they need no Identity, being free to depart and to rejoin at Will, accepting the Proof-of-Work Chain as Witness of all that passed in their Absence. They vote with their Power of Computation; and whatsoever Rules and Rewards be needful may be enforced by this Consensus.

Done upon the Network by the Consent of the Participants, the Thirty-first Day of October, in the Year of our Lord Two Thousand and Eight.

Satoshi Nakamoto

31 OCTOBER 2008

WETHEPARTICIPANTSOFTHENETWORK.COM