UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF FLORIDA

UNITED AMERICAN CORP., a Florida company, Plaintiff v. BITMAIN, INC., SAINT BITTS LLC d/b/a BITCOIN.COM, ROGER VER, BITMAIN TECHNOLOGIES LTD., BITMAIN TECHNOLOGIES HOLDING COMPANY, JIHAN WU, PAYWARD VENTURES, INC. d/b/a KRAKEN, JESSE POWELL, AMAURY SECHET, SHAMMAH CHANCELLOR, and JASON COX, Defendants.	**COMPLAINT** Civil Action No. _____

Plaintiff United American Corp. ("Plaintiff" or "UAC"), by and through undersigned counsel, hereby sues Bitmain, Inc., Saint Bitts LLC d/b/a Bitcoin.com ("Bitcoin.com"), Roger Ver, Bitmain Technologies Ltd., Bitmain Technologies Holding Company (together with Bitmain, Inc. and Bitmain Technologies Ltd., "Bitmain"), Jihan Wu, Payward Ventures, Inc. d/b/a Kraken ("Kraken"), Jesse Powell, Amaury Sechet, Shammah Chancellor, Jason Cox (Sechet, Chancellor, and Cox are collectively referred to as "Bitcoin ABC") (collectively, "Defendants"), for damages and for injunctive relief. In support thereof, Plaintiff alleges as follows:

NATURE OF THE ACTION

1. This action involves a scheme by a tight knit network of individuals and organizations to manipulate the cryptocurrency market for Bitcoin Cash, effectively hijacking the

Bitcoin Cash network, centralizing the market, and violating all accepted standards, protocols and the course of conduct associated with Bitcoin since its inception.

2. This well-planned scheme caused a global capitalization meltdown of more than $4 billion and caused many U.S. Bitcoin holders – including Plaintiff – to suffer damages and irreparable harm.

3. In addition to the significant damages incurred by all stakeholders in Bitcoin Cash as a result of the Defendants' overt take over and manipulation of the market, there are significant long-term implications for world economies and particularly the U.S. economy.

4. The market manipulation is *centralizing* what is intended to be a *decentralized* transactional system enabling the corruption of the democratic and neutral principles of the Bitcoin Cash network.

5. As set forth in greater detail below, Defendants have engaged in unfair methods of competition, and through a series of unconscionable, deceptive and unfair acts and/or practices, manipulated the Bitcoin Cash cryptocurrency market for their benefit and to the detriment of the Plaintiff and the other stakeholders.

PARTIES

6. Plaintiff United American Corp. is a corporation organized and existing under the laws of Florida with its principal place of business at 5201 Blue Lagoon Dr., Suite 800, Miami, Florida 33126.

7. Defendant Bitmain, Inc. is a corporation organized and existing under the laws of Delaware with its principal place of business in San Jose, California.

8. Defendant Saint Bitts LLC d/b/a Bitcoin.com is a limited liability company organized and existing under the laws of Saint Kitts and Nevis with its principal place of business in Tokyo, Japan.

9. Defendant Roger Ver is an individual domiciled, upon information and belief, in Tokyo, Japan and is *sui juris*.

10. Defendant Bitmain Technologies Ltd. is a limited company organized and existing under the laws of Hong Kong with its principal place of business in Beijing, China.

11. Defendant Bitmain Technologies Holding Company is a corporation registered in the Cayman Islands.

12. Defendant Jihan Wu is the CEO of Bitmain Technologies Ltd. and, upon information and belief, is an individual domiciled in San Jose, California, and is *sui juris*.

13. Defendant Payward Ventures, Inc. is a corporation organized and existing under the laws of Delaware with its principal place of business in San Francisco, California. Payward Ventures, Inc. is registered in San Francisco County as the owner of the fictitious business name "Kraken" and operates the Bitcoin exchange Kraken.com.

14. Defendant Jesse Powell is the CEO of Kraken, is an individual domiciled in San Francisco, California, and is *sui juris*.

15. Defendant Amaury Sechet is an individual domiciled in Doue la Fontaine, France and is *sui juris*.

16. Defendant Shammah Chancellor is an individual domiciled in San Francisco, California and is *sui juris*.

17. Defendant Jason Cox is an individual domiciled in San Mateo, California and is *sui juris*.

JURISDICTION AND VENUE

18. This Court has federal question jurisdiction over this matter pursuant to 28 U.S.C. § 1331 because it involves a civil action arising under the Constitution, laws, or treaties of the

United States. Specifically, the allegations of Count I involve violations of Section 1 of the Sherman Act.

19. This Court also has subject matter jurisdiction pursuant to 28 U.S.C. § 1332 because Plaintiff is a citizen of Florida, and Defendants are citizens of different states other than Florida or citizens or subjects of a foreign state, and the amount in controversy exceeds $75,000, exclusive of interest and costs.

20. This Court has personal jurisdiction over Defendants because Defendants have engaged in business in the State of Florida and have purposefully availed themselves of the benefits and privileges of conducting business in this jurisdiction.

21. Venue is proper in this District pursuant to 28 U.S.C. § 1391 because a substantial part of the events and omissions at issue in this action occurred in this District.

FACTUAL BACKGROUND

Cryptocurrency

22. Cryptocurrency is a form of digital currency that uses cryptography to secure electronic transactions and to control the creation of new virtual currency units. Popular forms of cryptocurrency include Bitcoin, Bitcoin Cash, and Ethereum.

23. Though a form of "virtual currency," the value of a cryptocurrency is real and trades in currency markets.

24. New cryptocurrency is created through a process known as "mining." People compete to "mine" virtual currencies using computing power to solve complex math puzzles. The solutions to these puzzles are then used to encrypt and secure the cryptocurrency. The computers or pools of computers (nodes) which are the first to solve these puzzles are rewarded with new cryptocurrency.

25. Once earned, virtual currency is stored in a digital wallet associated with the computing device that solved the puzzle.

26. These math puzzles are solved by servers using computer power (or powered by computers). The puzzles do not require any calculations by the person mining the currency. As competition to create more virtual currency has increased, the mathematical puzzles have become more complex, making virtual currency more difficult to obtain. Computers that were once capable of efficiently mining Bitcoin could now take centuries to obtain the same results.

The Genesis of Bitcoin and Bitcoin Cash

27. The original vision of the document known as the "Satoshi Nakamoto whitepaper" published on October 31, 2008, was a simple one: to create a purely "peer-to-peer" version of electronic cash that would allow online payments from one party to another without going through a financial institution. The Whitepaper coined the term "Bitcoin" to represent this digital "cash," more generally referred to as "digital currency." A true and correct copy of the Whitepaper is attached hereto as **Exhibit A**.

28. At a high level, the integrity of the Bitcoin system relies on a network of decentralized public ledgers that confirm and maintain the records of digital transactions on a "blockchain" in a highly cryptographic environment. Whereas centralized ledgers are highly vulnerable to tampering and fraud, confidence and trust within a blockchain transactional network is established through decentralized ledgers that are identical and continuously updated and compared. These decentralized ledgers create an environment where one would have to tamper with the majority of ledgers simultaneously and in exactly the same manner within the same cryptographic environment to engage in any sort of tampering.

29. The strength of Bitcoin Cash as a digital currency lies in it being a "permissionless" system with a decentralized public ledger (the blockchain). To accomplish and maintain the system requires mechanisms for reaching a global, decentralized consensus on the valid blockchain. Two of those mechanisms are: (a) the Proof-of-Work[1] – which applies on a block-by-block basis; and (2) assuring that the "main chain" at any given time is whichever valid chain of blocks has the most cumulative Proofs-of-Work associated with it (normally, the longest chain).

30. A mining pool is the pooling of resources by virtual currency miners, who share their processing power over a network, to split the reward equally, according to the amount of work they contributed to the probability of solving the puzzles. Mining pools have been established because: (1) the difficulty of the math puzzles has increased; (2) a given miner cannot be working on more than one problem at a time; and (3) there is no way of knowing which miner will solve a given problem.

31. The reward per miner within a pool will be a direct function of the collective reward over a period of time divided by the number of miners. Because mining is very energy consuming and electricity represents the largest operating cost (both in powering the miner and the cost of air conditioning to cool miners as applicable), to be profitable, miners must generate higher rewards over a period of time than the cost of electricity needed to mine in the same period of time. As such, as difficulty increases, so does the cost of mining.

32. For a cryptocurrency network to remain secure and trusted, the entire process must remain distributed and decentralized so that no single individual, entity or pool can control

[1] The Proof-of-Work is designed to eliminate the insertion of fraudulent transactions in the blockchain.

more than 50% of computing power. If this 50% figure is exceeded, the network is no longer decentralized. Then, those using the network will be forced to utilize a centralized network in which they lack confidence and trust.

United American Corp.

33. In late 2017, Plaintiff announced publicly that it was moving heavily into blockchain and blockchain technologies. This was to be a multi-phased approach that encompassed blockchain solutions, both at the network level for the execution of blockchain transactions and at the mining level for the mining of cryptocurrencies.

34. At the network level for the execution of blockchain transactions, on December 22, 2017, Plaintiff announced the creation of BlockNum, a distributed and decentralized ledger technology and the first blockchain to be based on SIP-Protocol (Session Initiated Protocol), which is used by the vast majority of telecommunications companies around the world. BlockNum allows the execution of blockchain transactions between any two telephone numbers regardless of their location meaning that transactions can occur simply and without the need for "cryptocurrency wallets" backed by the Bitcoin Cash network. Plaintiff also filed a patent application for BlockNum with the U.S. Patent and Trademark Office.

35. Also in late December 2017, Plaintiff incorporated two subsidiaries to be used for exploitation of its developing business in blockchain: Blockchain Data Centers Inc. and United Blockchain Corp.

36. At the mining level, Plaintiff focused on the development of a low cost, rapid deployment solution for operation of cryptocurrency mining – the BlockchainDome. The BlockchainDome is a passive "cooling ground-coupled heat-exchanger" technology that uses Canadian well and chimney principals combined with a technique for utilizing negative air

pressure in its mining rigs. Plaintiff also filed a patent application for the BlockchainDome with the U.S. Patent and Trademark Office.

37. Plaintiff's development of these technologies was intended to mine the Bitcoin Cash network. The reason Plaintiff has focused on a "peer-to-peer" payment system is because it will eventually generate more in transaction fees than the mining generates.

38. Plaintiff's construction of the first BlockchainDome commenced in March 2018 and to date it has erected four domes and operated over 5,000 Bitcoin Cash-based miners. The Plaintiff's total investment in development and deployment of this infrastructure exceeds $4 million.

39. The economics of the domes depend on mining Bitcoin Cash within normal market conditions. Cryptocurrency mining, like any other mining, is predicated on the basic principle that the value of the mining output exceeds the cost to mine that output. Plaintiff has designed its BlockchainDomes to be highly efficient and among the lowest, if not the lowest, cost producers.

40. At the same time, the broader, macro-economics of Bitcoin Cash mining are based on market forces in a *decentralized* market whereby no one entity controls the market (allowing for an unbiased value of the currency). Without decentralization, normal market forces are less effective because mining power can be shifted to control markets. This shift can ultimately result in predatory pricing thereby reducing the economic value of the output so low as to eliminate competition and ultimately result in market control and centralization.

The Bitcoin Cash Upgrade

41. Prior to the network upgrade scheduled for November 15, 2018, the Bitcoin Cash network was mined by several different nodes applying various computer software

implementations (i.e. Bitcoin Unlimited, Bitcoin ABC, Bitcoin SV, Bitcoin XT, etc.). All of these software implementations were compatible with each other and were all responding to the same rules set.

42. On November 15, 2018, at 11:40 am EST, the Bitcoin Cash network was scheduled for automatic software upgrades for each of the different software implementations.

43. Because two of the software implementations (Bitcoin ABC 0.18.4 or Bitcoin SV 0.1.0)[2] decided to proceed with upgrades that would no longer respect the same rules set, a dispute arose over which of the two rules sets being applied by the two software implementations would be the rules set that the Bitcoin Cash blockchain was going to follow moving forward.

44. Consistent with Nakamoto's Whitepaper, the determination over *which* rules set would be applied by software implementations on the network going forward, would be based on the "vote"[3] of the various nodes mining the network – i.e., which node implementations exercised more computer hashing power through its attached mining rigs while working to continue the chain.

45. Whichever rules set received the most "votes" in the aforementioned "hash war" was going to continue the Bitcoin Cash blockchain going forward. The "losing" rules set would be forced to create a new and distinct chain.

46. Upon information and belief, the scheduled Bitcoin Cash network upgrade was manipulated by Defendants in an effort to artificially take control of the network blockchain moving forward.

---

[2] Bitcoin Unlimited, XT and others followed the ABC implementation.

[3] Nakamoto's Whitepaper states that nodes in the system "vote with their CPU power, expressing their acceptance of valid blocks by working on extending them…" *See* Exhibit A at ¶ 12.

The Scheme and the Players

47. It is clear that during the Bitcoin Cash software update there was a systematic and organized scheme by the Defendants to bring forward significant computing hashing power to the Bitcoin Cash network on a temporary basis for the sole purpose of dominating the Bitcoin Cash ABC 0.18.4 software chain implementation.

48. Understanding the Defendants' scheme requires understanding the players involved as they are not legally affiliated.

49. The China International Capital Corporation ("CICC") is one of China's leading investment banking firms that engages in investment banking, securities, investment management, and other financial services.

50. CICC has the exclusive mandate for the Initial Public Offering of Bitmain Technologies Ltd.

51. Bitmain Technologies Ltd. – founded in 2013 by Jihan Wu and Micree Zhan – is the largest designer of what is referred to as "ASIC" or Application Specific Integrated Circuit chips for mining operations. The Bitmain ASIC chip powers the Antminer series of mining servers that are the dominant servers operating on a number of cryptocurrency networks such as Bitcoin and Bitcoin derivatives.

52. Estimates of Bitmain's market share for ASIC servers ranges from 67 to 80% and it is estimated that Bitmain controls well in excess of 60% of the world's cryptocurrency mining computer (hashing) power.

53. Bitmain also operates Antpool and BTC.com, two of the largest Bitcoin and Bitcoin Cash mining pools in the world. As of December 2, 2018 (based on a 7 day average) these two pools collectively controlled 31% of Bitcoin mining and 40% of Bitcoin Cash ABC.

54. Bitcoin.com is a privately-owned company registered in the off shore islands of St Kitts and Nevis under the organization of Saint Bitts LLC (with headquarters in Tokyo). Bitcoin.com provides Bitcoin and Bitcoin Cash services, such as purchasing and selling these cryptocurrencies, and choosing a wallet for both. It has servers and programmers in the United States and operates the Bitcoin.com pool (currently 7.4% of Bitcoin Cash ABC) with hash power provided by Bitmain. It also offers other services such as news, an online store and online gaming.

55. Bitcoin.com was founded and remains owned by Roger Ver ("Ver"), a U.S. natural citizen who renounced his U.S. citizenship in 2014 after obtaining a Saint Kitts and Nevis passport. Upon information and belief, Ver is currently living in Tokyo.

56. Ver is a self-described "Bitcoin Angel Investor" and became interested in cryptocurrencies early in Bitcoin's history. He invested in a number of Bitcoin projects and startups including the Kraken trading platform, Ripple and BitInstant – founded by ex-convict Charlie Shrem.[4]

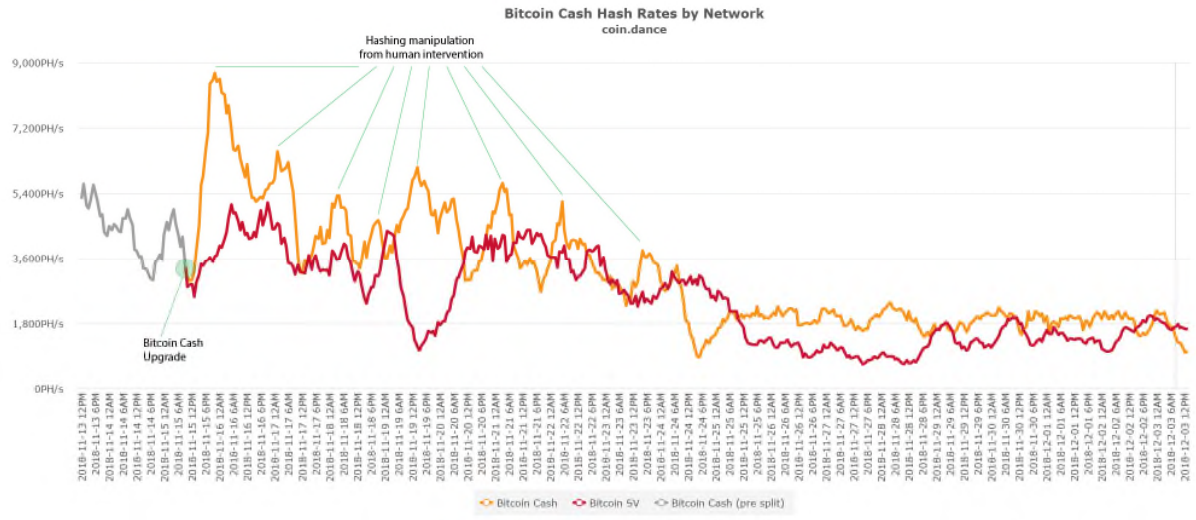
57. Ver is a strong advocate of Bitcoin Cash and the original forking of Bitcoin into Bitcoin and Bitcoin Cash in 2017. He has openly supported the development and implementation of the ABC version of Bitcoin Cash.

58. Sterlin Lujan is Bitcoin.com's Communications Ambassador and is responsible for representing the company in the United States. *See* https://sterlinlujan.com/about/.

[4] Shrem was sentenced to 2 years in prison for his involvement of transferring some $1 million in Bitcoin to the "Silk Road," a black market platform which was popular for money laundering and illegal drug transactions on the dark web (the site was shut down by the FBI in 2011). Ver was invested in Silk Road and has tweeted support for the site and the concept. *See* https://www.businessinsider.com.au/charlie-shrem-arrested-bitcoin-ceo-2014-1.

59. During the November 15, 2018 Bitcoin Cash network upgrade, Ver and Bitcoin.com colluded with Jihan Wu and Bitmain (whose electricity rates are subsidized by the Chinese government)[5] to reallocate pools of Bitmain servers from the Bitcoin Core network ("BTC") to Bitcoin.com's pools in the Bitcoin Cash network minutes before the implementation of the Bitcoin Cash network upgrade. The effect was to bring pools of servers to mine the upgrade from *another* network (i.e., "rent" hashing power), that were not previously mining the Bitcoin Cash blockchain, thereby increasing Bitcoin.com's hashing power by over 4,000%.

60. The impact of redirecting hashing power from another network can be seen clearly in the following graph:



[5] It is no secret that access to cheap electricity in China has been a major advantage to Bitmain. The company has taken advantage of cheap coal-fired power from coal-abundant regions in China such as Xinjiang and Inner Mongolia, which have in recent years taken to crypto mining to boost their less-developed economies. Local authorities in China have provided Bitmain with a highly subsidized electricity rate. The subsidized electricity provided to by China to Bitmain has enabled Bitmain to dump large amounts of hashing power into the Bitcoin network at a rate that is under cost relative to its competitors. The effect of this is that there is not a level playing field for those who are not subsidized by the Chinese government.

The lighter/orange line represents the hashing power of the Bitcoin ABC pool and the darker/red line the hashing power of the Bitcoin SV pool. Immediately after the software upgrade, the Bitcoin ABC pool hashing power rises to a level that had not previously been seen indicating the intermittent deployment of "rented" hashing. This type of hashing peak is ***not*** a normal occurrence. The peaks continued several times in the subsequent days until they leveled off to normal levels once Bitcoin ABC's dominance was established.

61. The above described actions were intentional and clearly planned in advance, with Bitmain organizing deployment (or actually redeployment) of up to 90,000 Bitmain Antminer S9 servers in early November.

62. Ver himself took to Twitter to pat himself on the back on the unprecedented level of hashing power he brought to bear on the network upgrade – more hashing power than the entire network had earlier that very same day, stating:

63. Bitcoin.com itself acknowledges that Bitcoin's creator Satoshi Nakamoto "outlined the design of the Bitcoin system and protocol" in his Whitepaper. *See* https://www.bitcoin.com/about-us. Yet, the above described actions by Bitcoin.com violated the central tenets and principles established by his Whitepaper and relied on by stakeholders and the market.

64. Nakamoto's Whitepaper makes express that nodes in the system "vote with their CPU power, expressing their acceptance of valid blocks by working on extending them…" While nodes "can leave and rejoin the network," it has always been understood that it is the nodes that are mining the blockchain that are able to "vote with their CPU power."

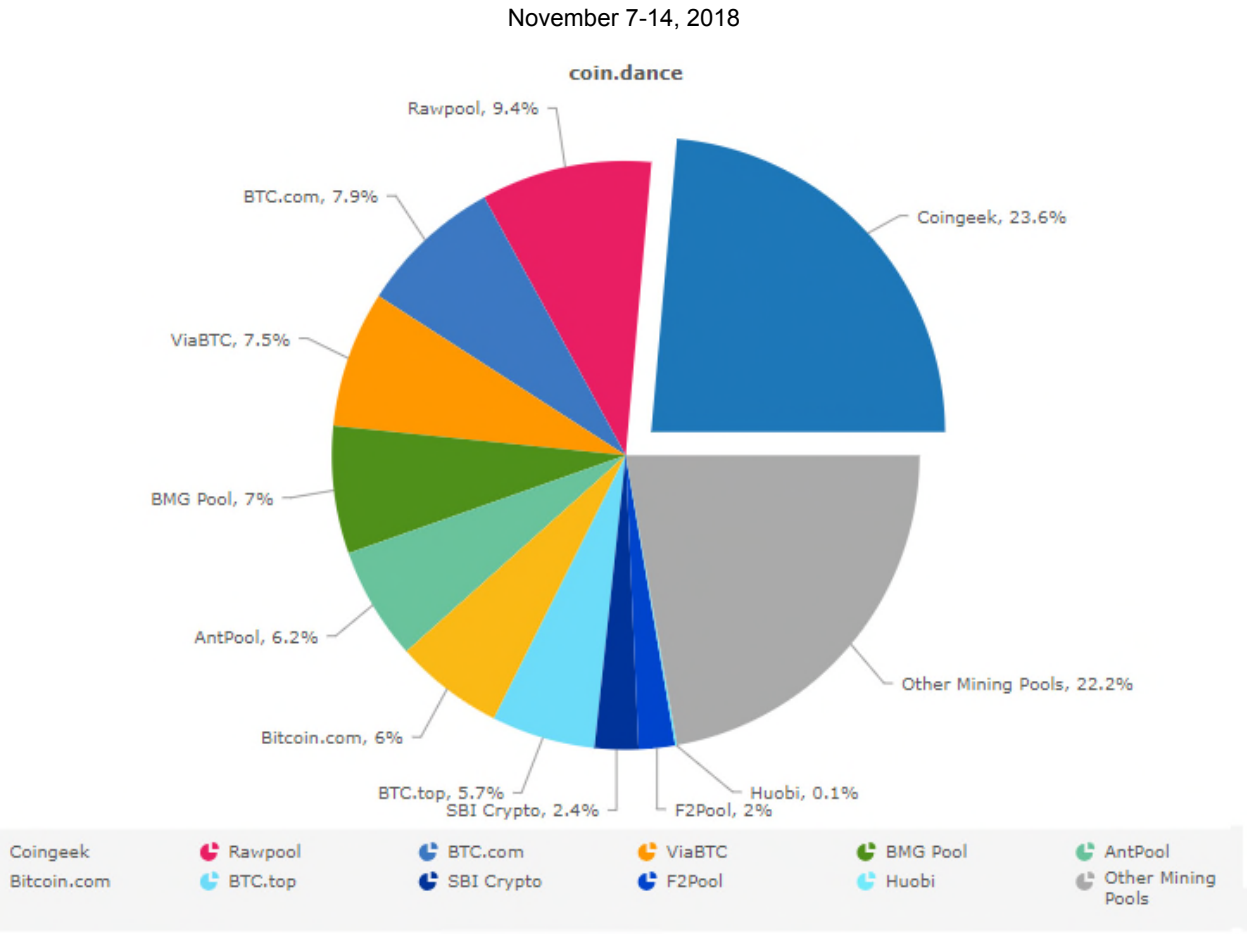
65. By essentially bringing in mercenaries from *another* network (the BTC network) to temporarily mine the Bitcoin Cash network during the software upgrade and then leave, Bitmain and Bitcoin.com effectively hijacked the blockchain. Their actions diluted the "vote" being exercised by the existing nodes[6] during the upgrade, violated the ground rules of the network that other users had relied on and respected for years, and artificially pumped up the chain implementation with computer hashes to dominate the temporary software upgrade.

66. To appreciate the effective hijacking of the blockchain, one need only look at the percentage of Bitcoin blocks being awarded – and the diversity of the miners to which they were being awarded – immediately *before and after* the network upgrade on November 15, 2018.

67. The following pie chart illustrates the distribution of Bitcoin Cash Blocks during the week immediately preceding the network upgrade (as reported by coin.dance). Bitcoin.com

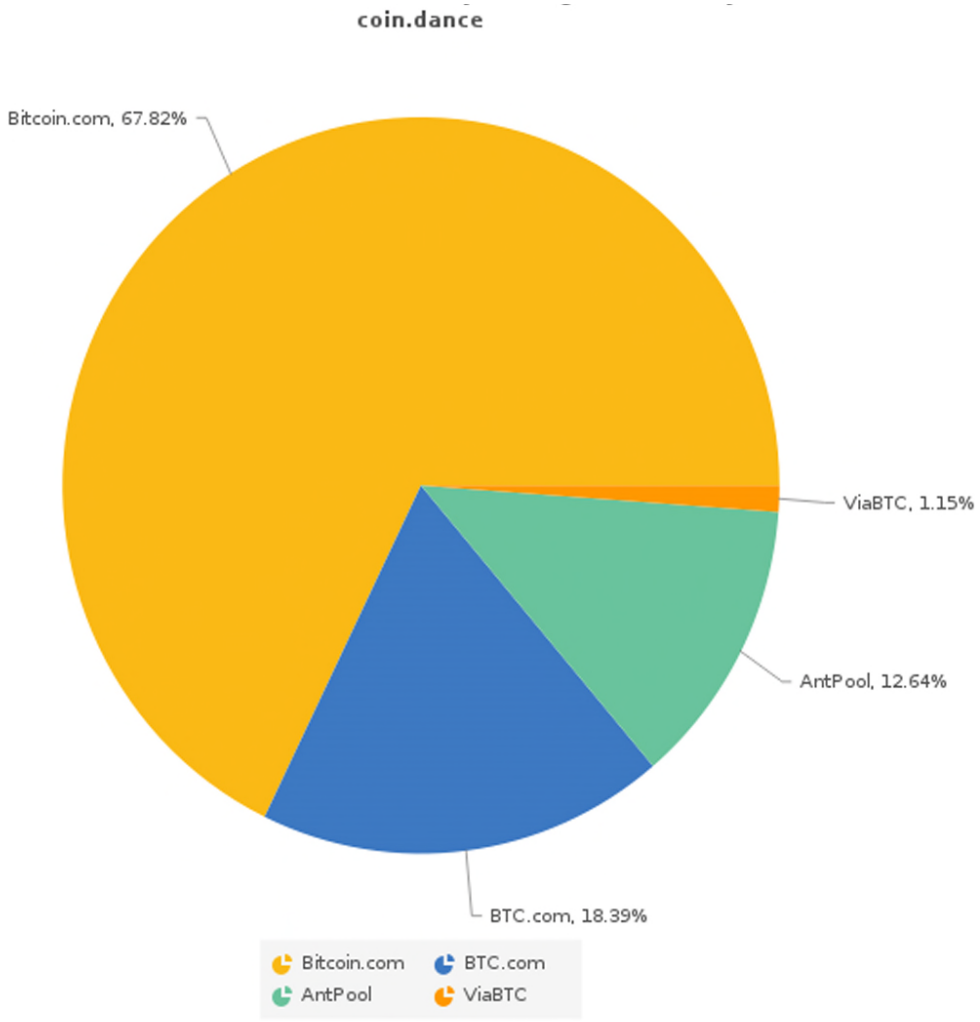
[6] Before Bitcoin.com brought its Bitmain mercenaries to bear on the blockchain, over 70% of the existing nodes had elected to mine the Bitcoin SV chain.

and the Bitmain pools (AntPool, BTC.com, and ViaBTC) were collectively awarded 27.6% of the blocks during the *preceding* week.



68. The next pie chart illustrates the distribution of Bitcoin ABC Blocks on November 16, 2018, the day *after* the upgrade. Bitcoin.com and the Bitmain pools (AntPool, BTC.com, and ViaBTC) were being awarded 100% of the blocks immediately after the network upgrade.[7]

[7] At one point, the Bitmain/Bitcoin.com pool controlled 90-95% of all hashing on the resulting Bitcoin Cash network (BCH).



69. But the scheme did not end there. The next day on November 16, 2018, Bitcoin ABC through defendants Amaury Sechet, Shammah Chancellor, and Jason Cox, implemented a "poison pill" in the chain referred to as a "checkpoint."

70. The implemented checkpoint is problematic because it also "centralized" what should be a *decentralized* market due to the way the checkpoint was added and its location close to the tip of the blockchain.

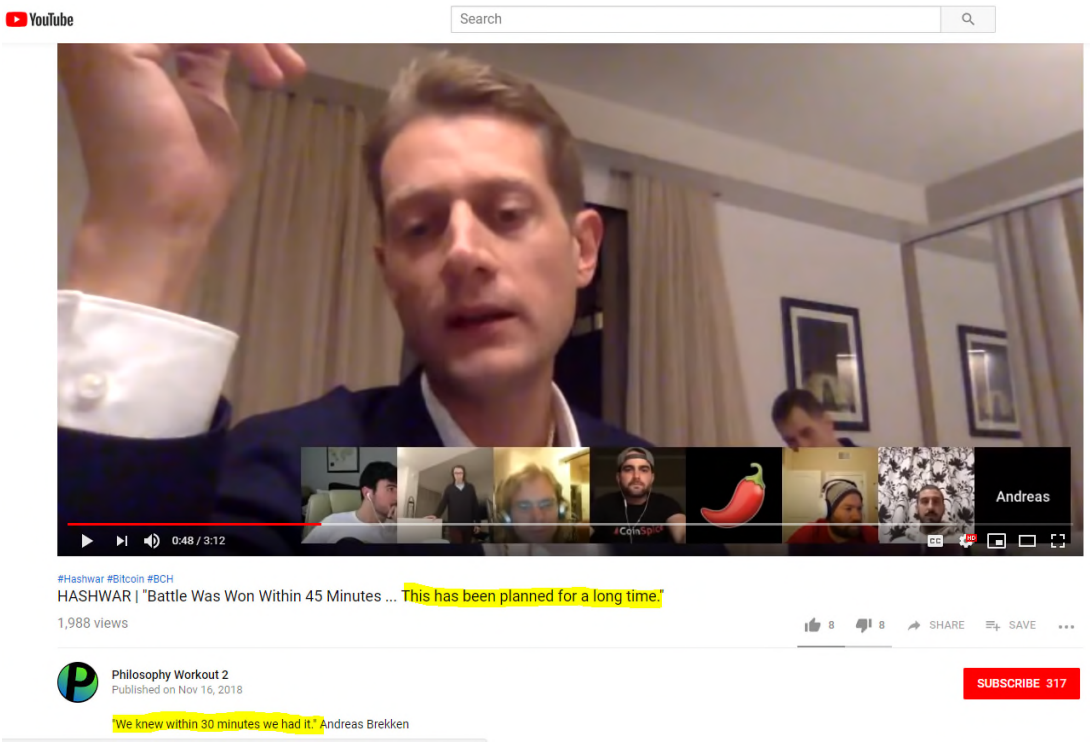
71. The integrity of a blockchain depends on a consensus being reached on the longest blockchain and that blockchain being accepted by all nodes on the network. While in

theory the blockchain ledger becomes more and more immutable as time passes, a fork can arise at any depth on the chain and become the main chain *if* that is the consensus.

72. The decision by Bitcoin ABC to "lock down" the block chain after an arbitrary number of blocks close to the tip of the blockchain – through a mechanism referred to as "checkpoints" and "Deep Reorg Prevention" – will allow anyone with 51% hashing power to quickly cement control of the blockchain ledger. They would also cement control over future changes to Bitcoin cash functionality as well as changes to the consensus rules. Combining this checkpoint power with the hashing power of Bitcoin ABC backers amounts to centralization. Anyone who combines hashing power and checkpoints in this fashion will be able to override *any* consensus reached by the rest of the network, forcing others to conform or create an unwanted hard fork.

73. Making a centralized checkpoint that destroys the core principle of decentralized consensus was a significant and fundamental change to the blockchain that was made without consulting other Bitcoin development groups and the community at large.

74. Indeed, as early as the next day after the update, individuals in the cryptocurrency industry such as Andreas Brekken (self-proclaimed "advisor to some of the most successful blockchain projects in the world" and software engineer at Kraken), held online forums acknowledging that Bitcoin ABC developers and crypto exchanges such as Kraken agreed to implement centralized checkpoints. *See* https://www.youtube.com/watch?v=UjAHJY0QZhs; *see also* https://brekken.com/about. Brekken goes on to admit in the video "this has been planned for a long time" and "we knew within 30 minutes we had it." The following is a screenshot of the referenced video:



75. Indeed, days after Bitcoin.com hijacked the network and introduced checkpoints, Lujan himself tweeted the following on behalf of and regarding Bitcoin.com taking control:

76. Shortly after Bitcoin.com and Ver's hostile takeover of Bitcoin Cash, Kraken – a well-known Bitcoin exchange[8] in which Ver himself is a principal investor – and Kraken's CEO Jesse Powell, decided that Kraken would maintain the BCH ticker for the ABC chain and indicated to users that the SV chain was a high-risk environment. By doing so, Kraken and Powell effectively recognized the ABC chain as the official blockchain of Bitcoin Cash and the "winner" of the network upgrade.

77. As a result of the aforementioned market manipulation, the value of the cryptocurrency that Plaintiff mines in its BlockchainDomes has fallen significantly. The combined value of the forked currency is lower than the pre-fork currency and the resulting confusion has been severely detrimental to the market overall. Some trading platforms have chosen to list only one of the two resulting currencies, thus reducing liquidity and the value of the currencies.

78. The Defendants' collective actions and manipulation of the market by among other things, violating the Nakamoto Whitepaper and consensus rules and hijacking the Bitcoin Cash network have created significant uncertainty and a lack of confidence in the network. Under normal *decentralized* market conditions, this type of uncertainty would not exist.

79. Plaintiff has suffered and continues suffering significant damages through the loss of value of the currency – a direct result of the centralization of what should be a decentralized network and the lack of democracy within the network as anticipated by the industry.

---

[8] Kraken is a US-based cryptocurrency exchange established in 2011 by Jesse Powell with the support of Ver (his friend from high school) which operates in the U.S., Canada, the E.U. and Japan. The exchange provides the mechanism to trade between Euros/US dollars/Canadian dollars/Japanese Yen and various cryptocurrencies such as Bitcoin, Bitcoin Cash and several other cryptocurrencies. It purports to be the largest Bitcoin exchange in Euro volume and liquidity.

COUNT I
(VIOLATION OF SECTION 1 OF THE SHERMAN ACT)

80. Paragraphs 1-79 of this Complaint are incorporated as if fully set forth here.

81. Defendants and their unaffiliated co-conspirators entered into and engaged in a conspiracy in unreasonable restraint of trade in violation of Section 1 of the Sherman Act and Section 4 of the Clayton Act.

82. During the applicable period, Defendants took control of the Bitcoin Cash cryptocurrency market by artificially pumping up the chain implementation with computer hashes to dominate the temporary software upgrade and implemented a new software version with checkpoints that controlled and manipulated the value of the Bitcoin Cash network going forward.

83. The conspiracy consisted of a continuing agreement, understanding or concerted action between and among Defendants and their co-conspirators in furtherance of which Defendants manipulated the cryptocurrency market for Bitcoin Cash, effectively hijacked the Bitcoin Cash network, centralized the market, and violated all accepted standards and protocols associated with Bitcoin since its inception, and fixed, maintained, suppressed, stabilized and/or otherwise made artificial the values associated with the Bitcoin Cash network. Defendants' conspiracy is a per se violation of the federal antitrust laws and is, in any event, an unreasonable and unlawful restraint of trade and commerce.

84. Defendants' conspiracy, and resulting impact on the market for Bitcoin Cash, occurred in or affected interstate and foreign commerce.

85. As a proximate result of Defendants' unlawful conduct, Plaintiff and others like it have suffered injury to their business or property. The Plaintiff is entitled to treble damages for the violations of the Sherman Act alleged herein.

COUNT II
(NEGLIGENT MISREPRESENTATION)

86. Paragraphs 1-79 of this Complaint are incorporated as if fully set forth here.

87. As participants in the Bitcoin Cash network, Defendants represented to Plaintiff and the market that they would abide by the Whitepaper and accepted standards and protocols.

88. Since its inception, the design of the Bitcoin system and protocol have been established by Nakamoto's Whitepaper. It has always been understood that it is the nodes that are mining a blockchain that are able to "vote with their CPU power."

89. By essentially bringing in mercenaries from *another* network (the BTC network) to temporarily mine the Bitcoin Cash network during the software upgrade and then leave the network, Bitmain and Bitcoin.com effectively hijacked the blockchain. They diluted the "vote" being exercised by the existing nodes[9] during the upgrade, violated the ground rules of the network that other users had relied on and respected for years, and artificially pumped up the chain implementation with computer hashes to dominate the temporary software upgrade. Then, for good measure, the Defendants implemented a checkpoint that "centralized" what should be a decentralized market due to the way the checkpoint was added and its location close to the tip of the blockchain.

90. Defendants knew or should have known that they did not intend to abide by the fundamental principles and protocols accepted by users of the Bitcoin Cash network.

91. Plaintiff justifiably relied on Defendants' misrepresentations by investing millions of dollars in development and deployment of infrastructure specifically for the mining of Bitcoin Cash.

---

[9] Before Bitcoin.com and Ver brought their Bitmain mercenaries to bear on the blockchain, 80% of the existing nodes had elected to mine the Bitcoin SV chain.

92. As a result of Defendants' misrepresentations, Plaintiff has been damaged and will continue to suffer damages.

COUNT III
(NEGLIGENCE)

93. Paragraphs 1-79 of this Complaint are incorporated as if fully set forth here.

94. As participants in the Bitcoin Cash network, Defendants owed a duty of care to the Plaintiff to abide by the Whitepaper and accepted standards and protocols.

95. Defendants breached their duty of care to the Plaintiffs by failing to conform to and abide by the Whitepaper and accepted standards and protocols and hijacking and assuming control of the Bitcoin Cash network and market.

96. The Plaintiff has suffered actual damages as a result of the Defendants' conduct.

97. The damages suffered by the Plaintiff as a result of the Defendants conduct were foreseeable.

COUNT IV
(EQUITABLE ESTOPPEL)

98. Paragraphs 1-79 of this Complaint are incorporated as if fully set forth here.

99. As participants in the Bitcoin Cash network, Defendants caused Plaintiff and the market to believe that they would abide by certain accepted standards and protocols.

100. Since its inception, the design of the Bitcoin system and protocol have been established by Nakamoto's Whitepaper certain accepted standards and protocols. It has always been understood that it is the nodes that are mining a blockchain that are able to "vote with their CPU power."

101. By essentially bringing in mercenaries from another network (the BTC network) to temporarily mine the Bitcoin Cash network during the software upgrade and then leave the

network, Bitmain and Bitcoin.com effectively hijacked the blockchain. They diluted the "vote" being exercised by the existing nodes during the upgrade, violated the ground rules of the network that other users had relied on and respected for years, and artificially pumped up the chain implementation with computer hashes to dominate the temporary software upgrade. Then, for good measure, the Defendants implemented a checkpoint that "centralized" what should be a decentralized market due to the way the checkpoint was added and its location close to the tip of the blockchain.

102. Defendants knew or should have known that they did not intend to abide by these fundamental principles and protocols accepted by users of the Bitcoin Cash network.

103. Plaintiff justifiably relied on the fact that Defendants would abide by the accepted standards and protocols of the network by investing millions of dollars in development and deployment of infrastructure specifically for the mining of Bitcoin Cash.

104. As a result of Defendants' failure to do so, Plaintiff has been damaged and will continue to suffer damages.

COUNT V
(UNJUST ENRICHMENT)

105. Paragraphs 1-79 of this Complaint are incorporated as if fully set forth here.

106. Bitmain, Bitcoin.com, and Ver have been unjustly enrichment by the conduct described above.

107. It would be inequitable for Defendants to be permitted to retain the benefit which Defendants obtained from their manipulative acts and at the expense of Plaintiff.

108. Unjust enrichment requires the receipt of a benefit and unjust retention of the benefit at the expense of another.

109. Bitmain, Bitcoin.com, and Ver received the benefit of mining significant sums of Bitcoin Cash through their aforementioned scheme while other users such as Plaintiff were cut out of the network and lost the value of their significant investments.

110. These parties should be required to disgorge all monies, profits and gains which they obtained and will unjustly obtain at the expense of Plaintiff and reimburse Plaintiff for the loss of investment resulting from their actions.

COUNT VI
(CONVERSION)

111. Paragraphs 1-79 of this Complaint are incorporated as if fully set forth here.

112. The Defendants are wrongfully exercising dominion and control over Bitcoin Cash and its blockchain network and market inconsistent with the use and possessory rights of the Plaintiff.

113. The Defendants' conduct has deprived the Plaintiff of the right to utilize and possess Bitcoin Cash and its blockchain network as intended pursuant to the Whitepaper and its accepted standards and protocols and the conduct is inconsistent with the Plaintiff's rights to use the network pursuant to said standards and protocols.

114. The Plaintiff has suffered damages as a result of the Defendant's unlawful conversion of the Bitcoin Cash network and market.

115. Demand for the Defendants to return the converted property is unnecessary as it would be futile.

COUNT VII
(INJUNCTIVE RELIEF)

116. Paragraphs 1-79 of this Complaint are incorporated as if fully set forth here.

117. As previously articulated, Defendants have engaged unfair methods of competition, and through a series of unconscionable, deceptive and unfair acts or practices, manipulated a cryptocurrency market for their benefit and to the detriment of Plaintiff and many others.

118. The Defendants' collective actions and manipulation of the market by violating the Nakamoto Whitepaper and consensus rules and hijacking the Bitcoin Cash network have created significant uncertainty and a lack of confidence in the network. Under normal decentralized market conditions, this type of uncertainty would not exist.

119. Consequently, Plaintiff's ability to conduct its operations has been virtually shut down.

120. Defendant's actions have caused and will continue to cause irreparable harm to Plaintiff and many others.

121. Plaintiff has no adequate remedy at law and the entry of an injunction will not disserve or affect the public interest, but will promote the public interest in maintaining a decentralized Bitcoin Cash network.

122. Specifically, Plaintiff seeks an injunction: (a) precluding Amaury Sechet, Shammah Chancellor, and Jason Cox via Bitcoin ABC from continuing to implement checkpoints on the Bitcoin Cash network and any other implementation of the software that would prevent the resulting chains from being able to be re-merged; and (b) requiring them to return the blockchain to its previously decentralized form with the previous consensus rules.

PRAYER FOR RELIEF

WHEREFORE, as a result of the foregoing, Plaintiff prays for relief and judgment, as follows:

A. For an order declaring that the Defendants conduct violates the statutes and common law claims referenced herein;

B. That the unlawful conduct alleged herein be adjudged and decreed to be an unlawful restraint of trade in violation of Section 1 of the Sherman Act and Section 4 of the Clayton Act;

C. Awarding restitution, compensatory damages and/or disgorgement in favor of Plaintiff against Defendants for all harm suffered as a result of Defendants' wrongdoing, in an amount to be proven at trial, including interest thereon;

D. Awarding injunctive relief against Defendants to: (1) prevent Bitcoin ABC from continuing to implement checkpoints on the Bitcoin Cash network and any other implementation of the software that would prevent the resulting chains from being able to be re-merged; and (b) requiring them to return the blockchain to its previously decentralized form with the previous consensus rules;

E. For an order of restitution and/or disgorgement and all other forms of equitable monetary relief;

F. Awarding Plaintiff reasonable costs and expenses incurred in this action, including counsel fees and expert fees; and

G. Awarding such other and further relief as the Court may deem just and proper.

JURY DEMAND

Plaintiff hereby demands a trial by jury on all claims so triable in this action.

Dated: December 6, 2018

Respectfully submitted,

By: /s/ *Brian P. Miller*

BRIAN P. MILLER
Florida Bar Number: 980633
Email: brian.miller@akerman.com
MICHAEL O. MENA
Florida Bar Number: 010664
Email: michael.mena@akerman.com
JOANNE GELFAND
Florida Bar Number: 515965
Email: joanne.gelfand@akerman.com

AKERMAN LLP
Three Brickell City Centre
98 Southeast Seventh Street, Suite 1100
Miami, FL 33131
Phone: (305) 374-5600
Fax: (305) 374-5095

Attorneys for Plaintiff United American Corp.

Exhibit “A”

Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

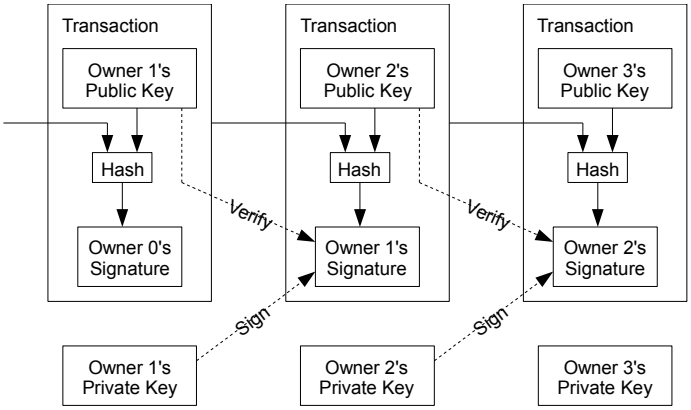
1. Introduction

Commerce on the Internet has come to rely almost exclusively on financial institutions serving as trusted third parties to process electronic payments. While the system works well enough for most transactions, it still suffers from the inherent weaknesses of the trust based model. Completely non-reversible transactions are not really possible, since financial institutions cannot avoid mediating disputes. The cost of mediation increases transaction costs, limiting the minimum practical transaction size and cutting off the possibility for small casual transactions, and there is a broader cost in the loss of ability to make non-reversible payments for non-reversible services. With the possibility of reversal, the need for trust spreads. Merchants must be wary of their customers, hassling them for more information than they would otherwise need. A certain percentage of fraud is accepted as unavoidable. These costs and payment uncertainties can be avoided in person by using physical currency, but no mechanism exists to make payments over a communications channel without a trusted party.

What is needed is an electronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a trusted third party. Transactions that are computationally impractical to reverse would protect sellers from fraud, and routine escrow mechanisms could easily be implemented to protect buyers. In this paper, we propose a solution to the double-spending problem using a peer-to-peer distributed timestamp server to generate computational proof of the chronological order of transactions. The system is secure as long as honest nodes collectively control more CPU power than any cooperating group of attacker nodes.

2. Transactions

We define an electronic coin as a chain of digital signatures. Each owner transfers the coin to the next by digitally signing a hash of the previous transaction and the public key of the next owner and adding these to the end of the coin. A payee can verify the signatures to verify the chain of ownership.

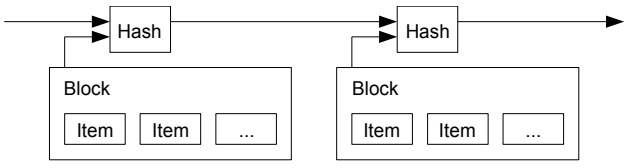


The problem of course is the payee can't verify that one of the owners did not double-spend the coin. A common solution is to introduce a trusted central authority, or mint, that checks every transaction for double spending. After each transaction, the coin must be returned to the mint to issue a new coin, and only coins issued directly from the mint are trusted not to be double-spent. The problem with this solution is that the fate of the entire money system depends on the company running the mint, with every transaction having to go through them, just like a bank.

We need a way for the payee to know that the previous owners did not sign any earlier transactions. For our purposes, the earliest transaction is the one that counts, so we don't care about later attempts to double-spend. The only way to confirm the absence of a transaction is to be aware of all transactions. In the mint based model, the mint was aware of all transactions and decided which arrived first. To accomplish this without a trusted party, transactions must be publicly announced [1], and we need a system for participants to agree on a single history of the order in which they were received. The payee needs proof that at the time of each transaction, the majority of nodes agreed it was the first received.

3. Timestamp Server

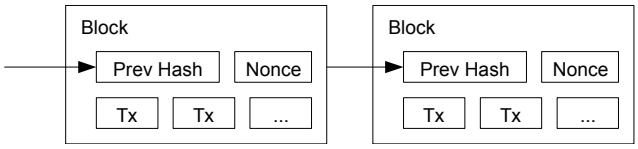
The solution we propose begins with a timestamp server. A timestamp server works by taking a hash of a block of items to be timestamped and widely publishing the hash, such as in a newspaper or Usenet post [2-5]. The timestamp proves that the data must have existed at the time, obviously, in order to get into the hash. Each timestamp includes the previous timestamp in its hash, forming a chain, with each additional timestamp reinforcing the ones before it.



4. Proof-of-Work

To implement a distributed timestamp server on a peer-to-peer basis, we will need to use a proof-of-work system similar to Adam Back's Hashcash [6], rather than newspaper or Usenet posts. The proof-of-work involves scanning for a value that when hashed, such as with SHA-256, the hash begins with a number of zero bits. The average work required is exponential in the number of zero bits required and can be verified by executing a single hash.

For our timestamp network, we implement the proof-of-work by incrementing a nonce in the block until a value is found that gives the block's hash the required zero bits. Once the CPU effort has been expended to make it satisfy the proof-of-work, the block cannot be changed without redoing the work. As later blocks are chained after it, the work to change the block would include redoing all the blocks after it.



The proof-of-work also solves the problem of determining representation in majority decision making. If the majority were based on one-IP-address-one-vote, it could be subverted by anyone able to allocate many IPs. Proof-of-work is essentially one-CPU-one-vote. The majority decision is represented by the longest chain, which has the greatest proof-of-work effort invested in it. If a majority of CPU power is controlled by honest nodes, the honest chain will grow the fastest and outpace any competing chains. To modify a past block, an attacker would have to redo the proof-of-work of the block and all blocks after it and then catch up with and surpass the work of the honest nodes. We will show later that the probability of a slower attacker catching up diminishes exponentially as subsequent blocks are added.

To compensate for increasing hardware speed and varying interest in running nodes over time, the proof-of-work difficulty is determined by a moving average targeting an average number of blocks per hour. If they're generated too fast, the difficulty increases.

5. Network

The steps to run the network are as follows:

1) New transactions are broadcast to all nodes.
2) Each node collects new transactions into a block.
3) Each node works on finding a difficult proof-of-work for its block.
4) When a node finds a proof-of-work, it broadcasts the block to all nodes.
5) Nodes accept the block only if all transactions in it are valid and not already spent.
6) Nodes express their acceptance of the block by working on creating the next block in the chain, using the hash of the accepted block as the previous hash.

Nodes always consider the longest chain to be the correct one and will keep working on extending it. If two nodes broadcast different versions of the next block simultaneously, some nodes may receive one or the other first. In that case, they work on the first one they received, but save the other branch in case it becomes longer. The tie will be broken when the next proof-of-work is found and one branch becomes longer; the nodes that were working on the other branch will then switch to the longer one.

New transaction broadcasts do not necessarily need to reach all nodes. As long as they reach many nodes, they will get into a block before long. Block broadcasts are also tolerant of dropped messages. If a node does not receive a block, it will request it when it receives the next block and realizes it missed one.

6. Incentive

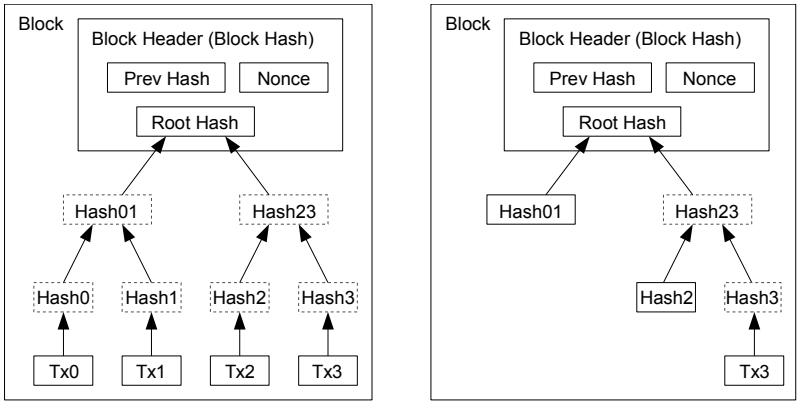
By convention, the first transaction in a block is a special transaction that starts a new coin owned by the creator of the block. This adds an incentive for nodes to support the network, and provides a way to initially distribute coins into circulation, since there is no central authority to issue them. The steady addition of a constant of amount of new coins is analogous to gold miners expending resources to add gold to circulation. In our case, it is CPU time and electricity that is expended.

The incentive can also be funded with transaction fees. If the output value of a transaction is less than its input value, the difference is a transaction fee that is added to the incentive value of the block containing the transaction. Once a predetermined number of coins have entered circulation, the incentive can transition entirely to transaction fees and be completely inflation free.

The incentive may help encourage nodes to stay honest. If a greedy attacker is able to assemble more CPU power than all the honest nodes, he would have to choose between using it to defraud people by stealing back his payments, or using it to generate new coins. He ought to find it more profitable to play by the rules, such rules that favour him with more new coins than everyone else combined, than to undermine the system and the validity of his own wealth.

7. Reclaiming Disk Space

Once the latest transaction in a coin is buried under enough blocks, the spent transactions before it can be discarded to save disk space. To facilitate this without breaking the block's hash, transactions are hashed in a Merkle Tree [7][2][5], with only the root included in the block's hash. Old blocks can then be compacted by stubbing off branches of the tree. The interior hashes do not need to be stored.



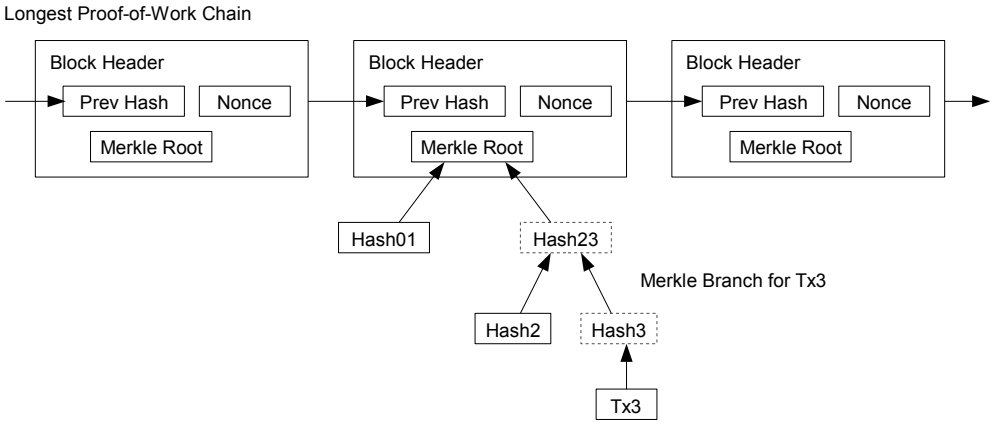
Transactions Hashed in a Merkle Tree

After Pruning Tx0-2 from the Block

A block header with no transactions would be about 80 bytes. If we suppose blocks are generated every 10 minutes, 80 bytes * 6 * 24 * 365 = 4.2MB per year. With computer systems typically selling with 2GB of RAM as of 2008, and Moore's Law predicting current growth of 1.2GB per year, storage should not be a problem even if the block headers must be kept in memory.

8. Simplified Payment Verification

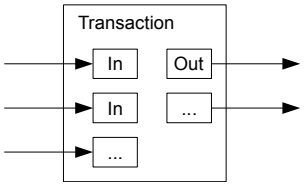
It is possible to verify payments without running a full network node. A user only needs to keep a copy of the block headers of the longest proof-of-work chain, which he can get by querying network nodes until he's convinced he has the longest chain, and obtain the Merkle branch linking the transaction to the block it's timestamped in. He can't check the transaction for himself, but by linking it to a place in the chain, he can see that a network node has accepted it, and blocks added after it further confirm the network has accepted it.



As such, the verification is reliable as long as honest nodes control the network, but is more vulnerable if the network is overpowered by an attacker. While network nodes can verify transactions for themselves, the simplified method can be fooled by an attacker's fabricated transactions for as long as the attacker can continue to overpower the network. One strategy to protect against this would be to accept alerts from network nodes when they detect an invalid block, prompting the user's software to download the full block and alerted transactions to confirm the inconsistency. Businesses that receive frequent payments will probably still want to run their own nodes for more independent security and quicker verification.

9. Combining and Splitting Value

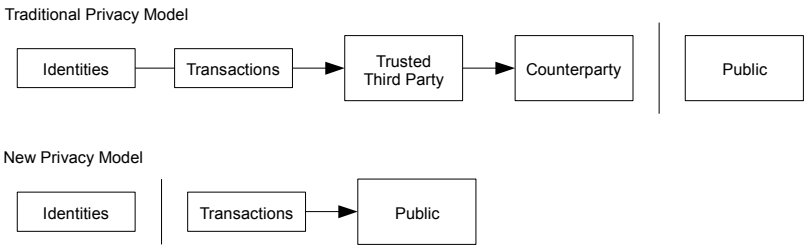
Although it would be possible to handle coins individually, it would be unwieldy to make a separate transaction for every cent in a transfer. To allow value to be split and combined, transactions contain multiple inputs and outputs. Normally there will be either a single input from a larger previous transaction or multiple inputs combining smaller amounts, and at most two outputs: one for the payment, and one returning the change, if any, back to the sender.



It should be noted that fan-out, where a transaction depends on several transactions, and those transactions depend on many more, is not a problem here. There is never the need to extract a complete standalone copy of a transaction's history.

10. Privacy

The traditional banking model achieves a level of privacy by limiting access to information to the parties involved and the trusted third party. The necessity to announce all transactions publicly precludes this method, but privacy can still be maintained by breaking the flow of information in another place: by keeping public keys anonymous. The public can see that someone is sending an amount to someone else, but without information linking the transaction to anyone. This is similar to the level of information released by stock exchanges, where the time and size of individual trades, the "tape", is made public, but without telling who the parties were.



As an additional firewall, a new key pair should be used for each transaction to keep them from being linked to a common owner. Some linking is still unavoidable with multi-input transactions, which necessarily reveal that their inputs were owned by the same owner. The risk is that if the owner of a key is revealed, linking could reveal other transactions that belonged to the same owner.

11. Calculations

We consider the scenario of an attacker trying to generate an alternate chain faster than the honest chain. Even if this is accomplished, it does not throw the system open to arbitrary changes, such as creating value out of thin air or taking money that never belonged to the attacker. Nodes are not going to accept an invalid transaction as payment, and honest nodes will never accept a block containing them. An attacker can only try to change one of his own transactions to take back money he recently spent.

The race between the honest chain and an attacker chain can be characterized as a Binomial Random Walk. The success event is the honest chain being extended by one block, increasing its lead by +1, and the failure event is the attacker's chain being extended by one block, reducing the gap by -1.

The probability of an attacker catching up from a given deficit is analogous to a Gambler's Ruin problem. Suppose a gambler with unlimited credit starts at a deficit and plays potentially an infinite number of trials to try to reach breakeven. We can calculate the probability he ever reaches breakeven, or that an attacker ever catches up with the honest chain, as follows [8]:

p = probability an honest node finds the next block
q = probability the attacker finds the next block
q_z = probability the attacker will ever catch up from z blocks behind

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

Given our assumption that $p > q$, the probability drops exponentially as the number of blocks the attacker has to catch up with increases. With the odds against him, if he doesn't make a lucky lunge forward early on, his chances become vanishingly small as he falls further behind.

We now consider how long the recipient of a new transaction needs to wait before being sufficiently certain the sender can't change the transaction. We assume the sender is an attacker who wants to make the recipient believe he paid him for a while, then switch it to pay back to himself after some time has passed. The receiver will be alerted when that happens, but the sender hopes it will be too late.

The receiver generates a new key pair and gives the public key to the sender shortly before signing. This prevents the sender from preparing a chain of blocks ahead of time by working on it continuously until he is lucky enough to get far enough ahead, then executing the transaction at that moment. Once the transaction is sent, the dishonest sender starts working in secret on a parallel chain containing an alternate version of his transaction.

The recipient waits until the transaction has been added to a block and z blocks have been linked after it. He doesn't know the exact amount of progress the attacker has made, but assuming the honest blocks took the average expected time per block, the attacker's potential progress will be a Poisson distribution with expected value:

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

To get the probability the attacker could still catch up now, we multiply the Poisson density for each amount of progress he could have made by the probability he could catch up from that point:

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

Rearranging to avoid summing the infinite tail of the distribution...

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

Converting to C code...

```
#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;
}
```

Running some results, we can see the probability drop off exponentially with z.

```
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
```

Solving for P less than 0.1%...

```
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. Conclusion

We have proposed a system for electronic transactions without relying on trust. We started with the usual framework of coins made from digital signatures, which provides strong control of ownership, but is incomplete without a way to prevent double-spending. To solve this, we proposed a peer-to-peer network using proof-of-work to record a public history of transactions that quickly becomes computationally impractical for an attacker to change if honest nodes control a majority of CPU power. The network is robust in its unstructured simplicity. Nodes work all at once with little coordination. They do not need to be identified, since messages are not routed to any particular place and only need to be delivered on a best effort basis. Nodes can leave and rejoin the network at will, accepting the proof-of-work chain as proof of what happened while they were gone. They vote with their CPU power, expressing their acceptance of valid blocks by working on extending them and rejecting invalid blocks by refusing to work on them. Any needed rules and incentives can be enforced with this consensus mechanism.

References

[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 minimal trust 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, no 2, 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 Conference on 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 and Privacy*, IEEE Computer Society, pages 122-133, April 1980.

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