UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF FLORIDA

IRA KLEIMAN, as the personal representative of the Estate of David Kleiman, and W&K Info Defense Research, LLC, *Plaintiffs,* v. CRAIG WRIGHT, *Defendant.*	CASE NO.: 9:18-cv-80176-BB

AMENDED EXPERT REPORT OF ANDREAS M. ANTONOPOULOS

I submit this Amended Report in the above-captioned action pursuant to Federal Rule of Civil Procedure 26(a)(2)(B) and the Scheduling Order in this case. This Report is submitted on behalf Ira Kleiman, as the personal representative of the Estate of David Kleiman, and W&K Info Defense Research, LLC (collectively, "Plaintiffs").

If called as a witness, I could and would testify to the truth of these facts and opinions under oath.

I. Background and Qualifications

1. I am an expert in Bitcoin and open blockchain technology. I have worked exclusively in the Bitcoin and Open Blockchain industry since 2012.

2. I earned my bachelors degree (1994) in computer science and my master's degree (1995) in data communications, networks and distributed systems, both from University College London while simultaneously working in IT.

3. Since 1990, I have worked in the Information Technology sector, with an emphasis on networks, distributed systems, security, and training. I've secured three patents for network technology inventions and have published more than 200 articles and reports on security, data centers, cloud computing and cryptographic currencies.

4. In 2014 O'Reilly Media published my first book, Mastering Bitcoin, a technical book for programmers. The book is widely viewed as the definitive guide on the subject and to date is the world's most cited book on Bitcoin.

5. Subsequently, I authored three additional books on the topics of bitcoin and open blockchains, with 2 more being published in December 2019 and in the 4th quarter of 2020 respectively. I have testified as an expert witness before regulators with respect to Bitcoin

technology, once in 2014 before the Canadian Senate Banking and Commerce Committee, and again in 2015 before the Economics References Committee of the Australian Senate.

6. I am a frequent keynote speaker at technology and security conferences worldwide. I have been interviewed by Bloomberg, CNN, CNBC, CBS, NBC, ABC, BBC, the Financial Times and many more media organizations for my industry expertise.

7. Additional facts about my background and qualifications, including a complete list of books that I have authored during the past several years, are set forth in my curriculum vitae, attached as Exhibit A.

8. I am being compensated for my services in this case at a rate of $500 per hour, plus expenses. My compensation is not dependent on the outcome of the litigation.

II. ASSIGNMENT

9. I have been asked to provide a description of the Bitcoin protocol, a high-level overview of the technology underpinning this protocol, and a brief history of its creation and existence.

10. In addition, I have been asked to describe the concept of a Bitcoin fork. As set forth below, it is my opinion that the same private keys associated with a particular Bitcoin address containing unspent bitcoin prior to August 2013 can be used to control digital assets associated with Bitcoin forks, including Bitcoin Cash (BCH), Bitcoin Satoshi's Vision (BSV) and others.

11. I have been asked to review the known public communications, communication platforms and forums and email addresses used by Satoshi Nakamoto

12. I have been asked to analyze data sets produced by Defendant purporting to be lists of bitcoin addresses (and corresponding blocks) that were mined by Defendant, comment on the security of transferring private keys as a means to sell bitcoin and comment on and verify signed messages.

III. MATERIALS REVIEWED AND INFORMATION CONSIDERED

13. In forming the opinions expressed in this report, I have relied on my education, knowledge, experience, and training in computer science and blockchain technology, as well as my specific education, knowledge, experience, and training in the fields of computer science, blockchain technology, bitcoin, data communications, networks and distributed systems. In addition to the documents cited and information provided in this report, I have also considered the documents listed in Exhibit B in forming my opinions.

14. I may review additional documents and information produced by the parties, as well as deposition testimony provided after the submission of my report, if any. I reserve all rights to comment on and respond to such information at trial or at deposition, as necessary.

15. I may expand or modify my opinions as my investigation and study continues and supplement my opinions in light of any relevant orders from the Court or in response to any additional information I review, any matters the Defendant raises, or any opinions Defendant's experts may provide.

16. In several of the following sections, the term "practically impossible" refers to the principle of an irreversible function, where the only known way to calculate a result of the inverse function is to attempt all possible input combinations (known as a "brute force" or "collision" attack). Since the number of "all possible input combinations" in these systems is a

number in the order of 77 decimal or 256 binary digits, it is impossible to try all possible combinations for all practical purposes. This concept underlies the security of all cryptographic systems.

IV. The Bitcoin Cryptocurrency

17. A cryptocurrency is a digital asset designed to work as a medium of exchange and/or a store of value. Cryptocurrencies leverage a variety of cryptographic principles to secure transactions, control the creation of additional currency units, and securely transfer the ownership and control of the digital assets.

18. Bitcoin is the world's first decentralized cryptocurrency, noted by the symbol BTC. At its core, Bitcoin is a distributed system comprised primarily of open source software, a peer-to-peer network, a standardized protocol, a system of rules called consensus rules, a security and control mechanism called proof-of-work, and a database in the form of a ledger called a blockchain. The ledger tracks the ownership and transfer of every fraction of bitcoin in existence.

19. Bitcoin exists only in intangible form on the bitcoin blockchain ledger. The bitcoin blockchain records amounts of bitcoin denominated in *satoshi*, the smallest unit (1 bitcoin is 100 million satoshi). The blockchain also records non-personally identifiable control of each bitcoin amount, allowing owners to assert control using numeric access codes called *keys.*

V. Bitcoin Ownership And Control

20. Unlike traditional banks, where each customer has a bank account and is identified as the owner, control of bitcoin is attested primarily through control of cryptographic *keys*. A specific amount, measured in *satoshi*, is recorded on the bitcoin blockchain as a *transaction output* (or simply "output") together with a *locking script* that defines the conditions

required to control that amount. The locking script is represented (encoded) as a bitcoin address. Locking scripts can be satisfied by presenting an equivalent *unlocking script* which satisfies the conditions of the locking script, thereby allowing everyone to verify that the funds can be spent.

21. When funds are said to be *"sent"* to a bitcoin address, the funds are locked with a locking script that sets the spending conditions required to spend them.

22. The most common, but not the only, type of locking script is one that requires the owner to present a digital signature to prove ownership of the funds, known as a "pay to public key hash (P2PKH)" and is represented with a bitcoin address starting with "1". A bitcoin address that represents a P2PKH script requires the owner of the funds to demonstrate ownership by presenting an unlocking script that contains a *public key* and a *digital signature*. Such an unlocking script satisfies the conditions set by the locking script and every participant in the bitcoin system will be able to verify it as valid.

23. The private and public keys that are used in this type of bitcoin address are numbers that are generated by a user (the owner of the funds), and subsequently used to produce a bitcoin address to which funds can be "sent" (by locking them to that address).

24. The public key is used to produce the bitcoin address. The public key is revealed in an unlocking script, at the time of spending, thereby demonstrating that it is known by the owner.

25. The private key is essentially a randomly selected number, like a very long PIN number. For every valid private key, there exists a corresponding public key, which can only be generated through a mathematical function (elliptic curve multiplication) by someone who

knows the private key. It is practically impossible to reverse this mathematical function and acquire the private key from the public key.

26. For every valid public key there exists a corresponding bitcoin address, which can only be generated through a mathematical function (hashing) by someone who knows the public key. It is practically impossible to reverse this mathematical function and acquire the public key from the bitcoin address

27. However, a single set of private/public keys can be encoded to produce a number of different locking scripts, which in turn produce different bitcoin addresses. Yet, all these addresses can be spent with the same key. This method can be used to obscure the "balance" controlled by a private key.

28. Since private keys are never part of the blockchain, the method of their generation, storage, control or subdivision is not evident in the blockchain.

29. Furthermore, private keys are secrets that you can share with others. Sharing keys obscures who created a signature (repudiation risk) and reduces security (theft/leak risk). Once a person knows a private key, they can spend satoshis that require a signature from that key. Anyone who knows the private key (and can construct the unlocking script) can effectively unlock bitcoin.

30. A valid private key can be used to produce a digital signature on a specific bitcoin transaction, which can be verified by anyone in possession of the bitcoin transaction and public key. Producing a digital signature proves the person who created the signature has access to the private key. It is practically impossible to determine the private key from the digital signature, unless the signature was constructed incorrectly (for example with the choice of a

pseudo-random number that is not in fact random and can be guessed or is repeatedly used). The concept of an "account" and the concept of a "balance" do not actually exist in the bitcoin system. These concepts are user-interface metaphors presented to help users understand the system. Within the Bitcoin system, a bitcoin address is not an account, but an encoding of the locking script, which defines what conditions must be met to spend funds.

VI. Acquiring And Exchanging Bitcoin

31. There are several methods of acquiring bitcoin. The first is to "mine" it. The bitcoin system is secured by a system of decentralized security called "mining," which is a global computing competition. Participation in this competition allows winners to earn newly created bitcoin, and transaction fees if any, as a reward for their computing effort that provides security to bitcoin.

32. Another method to acquire bitcoin is by buying it, exchanging a national currency (such as US dollars) for some amount of bitcoin in an online market called an *exchange*.

33. Finally, bitcoin can be acquired by exchange for other assets, commodities or the value of labor, services and products. These value exchanges can take place in person or via various market mechanisms. In other words, you can earn bitcoin for your labor, or by selling items you own to someone who pays for them with bitcoin.

VII. Bitcoin Mining

34. The purpose of mining is to securely record transactions into the bitcoin blockchain. In order to securely record transactions in a decentralized way, the bitcoin system implements a global contest that requires miners to use a proof-of-work algorithm. Winners of the contest can earn newly minted bitcoin and transaction fees (if any) as a reward for their work.

35. In this competition, competitors called “miners” aggregate bitcoin transactions into a data structure called a bitcoin block. Each bitcoin block has a number of parts, including but not limited to the block header and transactions.

36. Each block contains a reference to a *parent block*, also known as the *previous block hash*. This reference effectively links blocks together, creating a chain of blocks from the current block back all the way to the genesis block. Thus, a chain of blocks becomes a blockchain.

37. Each miner constructs a *candidate block* and then they compete to validate that block by repeatedly attempting to guess a number that produces a valid solution to the *proof of work algorithm.*

38. Each miner runs a computer program to calculate possible solutions to the proof of work algorithm, using part of the block, the *block header*, as the input to the algorithm.

39. A valid solution to the proof of work algorithm is a block header hash (a number) that is numerically less than a network wide target called the *difficulty target*. In order for a miner to find such a solution, they must calculate many millions of hashes with different combinations of numbers in the block header.

40. Depending on the difficulty target, it may require many millions of guesses before a miner is able to find block header hash that satisfies the difficulty target and is therefore a valid solution to the proof of work algorithm.

41. New bitcoin awarded to miners are called the *block subsidy* and are paid to a bitcoin address selected by the miner and placed in the candidate block. If the miner produces a valid proof of work solution, the candidate block they constructed becomes part of the bitcoin

blockchain, and the reward that they included in the candidate block becomes realized on the bitcoin network, and spendable 100 blocks later.

42. The difficulty target is recalculated by all participants in the bitcoin system every 2016 blocks, or approximately every two weeks by a calculation called the *difficulty retargeting*. This calculation dynamically adjusts difficulty to keep the block issuance rate at an average of one block every 10 minutes over the 2016 blocks.

43. If more computation is devoted to mining by miners, the average time to find a block given a fixed difficulty is reduced. At the end of the 2016 block difficulty retargeting period, this will result in a global increase of the difficulty, so as to return the average block time to 10 minutes.

44. Conversely, if less computation is devoted to mining, the average time to find a block is increased and at the end of the retargeting period the difficulty is decreased.

45. As a result of the dynamic retargeting of difficulty, the long-term average time to find a block remains constant at 10 minutes.

46. Historically, as the value of bitcoin has increased, more computation has been dedicated to mining and the difficulty of mining has steadily increased. Practically, bitcoin mining used to be possible on an average desktop computer at inception (January 2009), whereas now bitcoin mining requires hundreds of thousands of specialized computing devices (the devices are also confusingly called "miners", as are the human participants in the activity of mining). What once could be done by a few people with a few computers now requires a global industrial-scale computing infrastructure.

VIII. Block Subsidy and Bitcoin Issuance

47. Bitcoin operates a deflationary monetary policy that reduces the amount of bitcoin introduced into circulation based on a predetermined schedule of issuance that is encoded in the bitcoin validation (consensus) rules. The currency issuance schedule was set by Satoshi Nakamoto in the first release of the software and has been enforced by all participants in the system ever since.

48. When the Bitcoin protocol was first launched in January 2009, the system recorded a block subsidy of 50 new bitcoin payable to the winning miner, for each block of transactions added to the blockchain ledger.

49. Every 210,000 blocks the bitcoin rules specify a reduction to the block subsidy by dividing it in half.

50. Block 210,000 (mined Nov 28, 2012) was the first block to include a subsidy of 25 BTC, down from 50 BTC prior to that block.

51. Block 420,000 (mined June 9th 2016) was the first block to include a subsidy of 12.5 BTC, down from 25 BTC prior to that block.

52. Block 630,000 (expected in 2020) will include 6.25 BTC block subsidy. The reduction in issuance will continue until approximately the year 2140 when the last block containing a block subsidy (of 1 satoshi) is mined. Thereafter blocks will not include a block subsidy.

53. The actual amount of bitcoin that will ever be created is slightly less than 21 million, but for simplicity it is often rounded up to 21 million in conversations and presentations about bitcoin. To date, slightly more than 18 million of the total have been mined.

54. In addition to the block subsidy, miners who win the proof-of-work competition also earn fees from transactions. The sum of all fees paid in each transaction included in a block is paid to the winning miner in the same way as the block subsidy.

55. The block subsidy and transaction fees are included in a special transaction, the first transaction in each block, called the *coinbase transaction*. The coinbase transaction is "written" by the miner when they construct their candidate block and pays the sum of fees and block subsidy to a bitcoin address of the miner's choosing.

IX. History of Bitcoin

56. On October 31, 2008, a white paper authored under the pseudonymous name Satoshi Nakamoto ("Satoshi") titled "*Bitcoin: A Peer-to-Peer Electronic Cash System*" was posted to a mailing list of cryptography enthusiasts, from the email address satoshi@vistomail.com. This paper detailed novel methods of using a peer-to-peer network to generate what it described as "a system for electronic transactions without relying on trust."

57. According to public postings and statements presumably made by Satoshi, the software implementation of bitcoin had already been written before the white paper, to assure Satoshi that it would work.

58. Less than three months later, the system outlined became a reality, as the bitcoin network was launched with the first block, called the *genesis block*. On January 3, 2009, Satoshi mined the genesis block which contained the first 50 bitcoins. To place a timestamp on the occasion, Satoshi inserted a text message into the coinbase transaction that reads, "The Times 03/Jan/2009 Chancellor on brink of second bailout for banks" referring to that day's headline in

the British newspaper, The Times. This message served as proof that the genesis block could not have been created prior to January 3rd 2009.

59. Satoshi also created a website under the domain name bitcoin.org and continued to collaborate with other developers on the Bitcoin protocol until mid-2010. Around this time, they handed control of the Bitcoin source code repository to Gavin Andresen, another active member of the bitcoin development community, and disappeared.

60. During Bitcoin's early history, cryptocurrencies were a niche technology with a small development community. Consequently, there was little competition for maintaining the ledger or mining bitcoins. Early miners (2009-2012) could use consumer-level computers (such as desktop computers and laptops) perhaps with the addition of graphic cards (Graphical Processing Units or GPUs) to mine bitcoin. Since there was no specialized equipment required, mining was an activity that used consumer-level hardware such as laptop, desktop, and server computers.

61. The mining difficulty, which allowed a single computer to mine a block in 10 minutes in 2009, increased very slowly through the first year. It is estimated that it took approximately 4 million hashing operations per second in order to produce a valid proof-of-work for a block in 10 minutes (an average of 2.4 billion hashes before a correct solution was "guessed").

62. It wasn't until the beginning of 2010 that the difficulty started increasing more rapidly, as more miners started participating. As more miners participated and devoted computing resources to mining, the difficulty increased every 2016 blocks to compensate for the increased computation.

63. By the end of 2010 the difficulty had increased by a factor of 1000, still relatively easy to achieve with a few hundred consumer computers equipped with Graphics Processing Units (GPUs).

64. In January of 2013 the first specialized hardware (Application Specific Integrated Circuits or ASICs) for mining bitcoin was produced. From this point on, bitcoin mining became an industrial-scale activity requiring large capital investments. Mining with ASICs is several orders of magnitude more efficient than mining with generic computing devices, it is no longer profitable to mine without ASICs.

65. ASIC mining has pushed the mining difficulty up significantly. The total computing power (hashrate) dedicated to bitcoin mining in 2019 hovers between 75 and 100 exa-hashes (EH) per second (10^{18} hashes per second) as compared to tens of mega-hashes (MH) per second (10^{6} hashes per second) in early 2009.

X. Bitcoin Forks

66. Since its inception in 2009, Bitcoin has inspired the creation of over one thousand other projects. Many of these projects are cryptocurrencies that emulate the Bitcoin software, but others have made significant changes in an attempt to create an entirely new cryptocurrency with distinct functions or ones better suited to a specific market niche.

67. Some changes to the Bitcoin software create completely new blockchains, with new characteristics and names. These are usually referred to as *alt-coins* (short for alternative coins). Some alt-coins are not based on the Bitcoin software at all, but use similar technology to build completely different systems.

68. Changes to the Bitcoin software (source code) are called a source-code *fork*, not to be confused with a blockchain fork, which is a change in the *consensus rules* of the bitcoin blockchain. Not all source-code forks result in blockchain forks or are ever made public. There exist competing implementations of the Bitcoin software that operate under identical consensus rules, are fully interoperable, and are used on the Bitcoin network.

69. Some consensus rule changes to the Bitcoin software are backwards-compatible in such a way that existing installations of the Bitcoin software can continue to follow the rules and any blocks or transactions produced by the new software are still valid under the old rules. These are called *soft-forks* of the blockchain.

70. As part of the normal process of consensus, two miners both following the same rules may, by coincidence, solve the proof-of-work algorithm and produce two competing valid blocks almost simultaneously. This is called a *consensus fork* and is a transient phenomenon that is an expected behavior in the system. Consensus forks are usually resolved within a few blocks as the two competing chains reconverge when more blocks are mined.

71. Consensus forks are not to be confused with hard forks (below) where the rules diverge and there is no possibility of automatic reconvergence.

72. If a change in the Bitcoin software leads to the creation of bitcoin transactions or bitcoin blocks that are not compatible with the existing consensus rules, existing installations of the software cannot follow the new rules, as they consider them invalid.

73. If miners decide to mine according to both the new and the old rules, the blockchain will split into two blockchains. Blocks mined according to the new rules will only be accepted by miners operating software under the new rules. Blocks mined according to the old

rules may or may not be accepted by both old and new miners, depending on the nature of the change in the rules.

74. A split in the blockchain caused by the introduction of non-backwards-compatible consensus rules is called a *hard-fork.*

75. Notably, a hard-fork occurred on August 1st, 2017 on the Bitcoin blockchain, at block height [redacted] at approximately 12:37 p.m. UTC. Given the two different sets of rules, effectively, two different blocks were created by different miners as block [redacted] when a block larger than 1MB was presented to the bitcoin network for validation.

76. The two competing blocks, each valid according to a different set of rules, share and reference the same parent block, in this example block [redacted] This shared parent, with two different children is the split that gives this phenomenon the name "fork".

77. At that point, all participants in the system who followed the old rules, rejected the larger block as a violation of consensus rules, while those following the new rules accepted it as valid. One chain (and one set of miners, one set of software implementations) followed the existing rules of Bitcoin, whereas another chain (and set of participants) used a different set of rules, leading to a split. The fork of Bitcoin operating under the new 2MB block-size rules is called Bitcoin Cash.

78. Around the same time, a backwards-compatible change was also introduced to Bitcoin in the form of a soft-fork. This change is called *Segregated Witness or Segwit.* Segwit is a set of changes to the interpretation of transactions that moves digital signatures to a different data structure (the Witness Merkle Tree), reducing the opportunity for a specific type of attack

(third-party transaction malleability) and increasing capacity of each block through changes in the capacity accounting rules.

79. Segwit was one of the likely points of contentions that motivated the Bitcoin Cash fork. The Segregated Witness soft-fork change was not included in the rules of Bitcoin Cash.

80. When a hard-fork occurs on a blockchain, the two sides of the fork (called simply forks) share a common history up to the block just before the change of the rules. In the example of Bitcoin Cash above, Bitcoin Cash and Bitcoin share a common history up to, and including, block [redacted] (the common parent). From block [redacted] two divergent blockchains emerge, sharing a common history back to a common genesis block.

81. As a result of a hard-fork, such as the above mentioned Bitcoin/Bitcoin Cash fork of August 2017, any owners of any funds recorded on the ledger on a block prior to the fork thereafter own coins on *both* forks. The reason for this effect is that the locking scripts recorded in the common history are the same, and therefore the funds can be unlocked in the same way in both chains going forward.

82. The coins on the two forks share a common past but have an independent future. Any transactions that occur on one chain, do not necessarily occur on the other chain. There is an exception to this, where transactions occurring on one chain are *replayed* on the other chain. This can only happen if the transactions on the two chains are interoperable and can occur without the consent of the creator of the transaction (a situation known as *third-party-replay*).

83. Any owner of coins on a chain that undergoes a hard-fork into two chains will effectively control coins on both chains from that moment onwards. The two coins are usually

identified by different names and they may be traded on exchanges for each other and/or for national currencies. Therefore, each coin has a different price in the markets.

84. Hard forks have happened numerous times in the history of Bitcoin. To date, however, the original Bitcoin system (BTC) remains the most valuable in terms of its correlation to the US dollar, with a market capitalization of between $100 and $150 billion in December 2019. However, other noteworthy Bitcoin forks include Bitcoin Cash, Bitcoin Satoshi Vision, Bitcoin Gold, etc. Some 40 forks of Bitcoin have been identified.

85. There is no limit on the number of forks that can occur. Anyone can create a fork with minimal programming knowledge. The fork does not have to be announced or known to anyone else, making it impossible to know how many forks exist. Only the most notable and publicly known forks are listed on websites that track such activity.

86. Any persons who owned unspent bitcoin before August 1st 2017, and retained ownership of the keys or other mechanisms (scripts) for asserting ownership over that bitcoin, will also own and have the ability to make transactions on most coins forked from Bitcoin subsequently, as long as the locking scripts are redeemable in the forks and they retain control of the keys and/or scripts.

87. While the vast majority of Bitcoin forks currently have negligible value and illiquid markets, at least 3 forks have significant market value and liquidity. The chart below shows some of these forks. On December 3rd 2019 the following top 4 bitcoin forks are shown on the coincap.io site that tracks market activity from many different exchanges, in declining market capitalization:

Name	Symbol	Estimated Market Capitalization (million	USD Value per 1 coin (approx)

		$USD)	
Bitcoin	BTC	$133,720	$7400
Bitcoin Cash	BCH	$3,900	$215
Bitcoin Satoshi Vision	BSV	$1,770	$98
Bitcoin Gold	BTG	$105	$6

I will be prepared to update these values as needed, including but not limited, at the time of my testimony at trial.

XI. Analysis of Satoshi Public Communications

88. I was asked by Plantiff’s attorneys to examine the publicly posted communications of Satoshi and the email addresses and accounts used by Satoshi in these communications.

89. The first message from Satoshi Nakamoto appears in the Cryptography Mailing List on October 31st, 2008, originating from email address “satoshi@[redacted]. In this posting Satoshi announces Bitcoin and provides a link to the Bitcoin Whitepaper.

90. Satoshi engages in conversations with several other users on the mailing list in response to questions, using “satoshi@[redacted]” as his email address.

91. On January 8th 2009, Satoshi posted another message on the Cryptography Mailing List from email address “satoshi@[redacted] announcing the release of the Bitcoin software, version 0.1 with a link to download the software.

92. Satshi continued to post messages in the Cryptography Mailing List from the email address "satoshi@[redacted] until December 2010.

93. The Bitcoin Whitepaper linked in the Cryptography Mailing List announcement attributes the work to "Satoshi Nakamoto satoshin[redacted]www.bitcoin.org".

94. In addition to the known email addresses used by Satoshi Nakamoto to announce Bitcoin, Satoshi also communicated regularly via pseudonymous forum posts on several platforms.

95. Satoshi announced the Bitcoin v0.1 software on the P2P Foundation Forum with an account with the user name "Satoshi Nakamoto".

96. Satoshi Nakamoto is also presumed to be the person who co-founded and communicated frequently on the BitcoinTalk.org forum, under the username "satoshi", starting in November 22 2009 and ending in December 12 2010.

XII. Analysis of Address Lists

97. Plaintiff's attorneys provided me with four separate files containing lists of bitcoin blocks and transaction IDs, which Defendant provided to Plaintiff's as part discovery. I was asked to analyze and compare them. Each block and transaction ID can also be used to uniquely reference a specific bitcoin address or public key that received the mined bitcoin. Some of the files provided contained these bitcoin addresses, whereas some only contained the block height and transaction ID.

98. Specifically the four lists I received for analysis and comparison are:

a. output-step2.csv - The original list produced by Shadders, referred to as "Shadders List" below.

b. CW.txt and DK.txt - Lists provided during settlement discussions, referred to as "CW" and "DK" below

c. DEF_01586024.CSV - List provided to the court by Defendant in Feb 2020, referred to as "CSW Filed" below.

99. Upon receipt of the four files, and prior to any analysis or processing, a SHA256 fingerprint of each file had the following results:

a. output-step2.csv:

ee6223acfdcf098c73b34180647c017a0f629616ef0ed9661adb4907f58eacb0

b. CW.txt:

510fc44edce8d508498851d76bb2591960666ef6c17437224acdd6189691d13b

c. DK.txt:

83ebe3d19659b5666dc8e95f61d41e256273b25378347c0ccc3a9ae40e6f6f70

d. DEF_01586024.CSV:

dc29d38e1276c22c4857824e4c5177b0872b32698c3d2f9232d9a1866ec40d91

100. Additionally, I was provided with a copy of Steve "Shadders" Coughlan's deposition testimony and asked to consider it as part of my analysis.

101. According to the testimony, Shaders is an employee of the Defendant and he produced the "Shadders List" list by writing software to filter the bitcoin blockchain database according to a set of criteria provided by Defendant. Shadders testified the list identifies a complete list of bitcoin addresses that were mined by Defendant, based upon the provided criteria. (*Shadders testimony p. 27 line 10*)

102. The program written by Shadders in Java, to create the Shadders List, contained a bug that incorrectly applied one of Defendant's filtering criteria, resulting in additional entries that should have been excluded, as per Steve Shadders' testimony, starting on page 27, line 8. The bug that misapplied Defendant's criteria and resulted in the additional entries in the Shadders List will hereafter be referred to as the "Shadders Bug".

103. I was informed that the CW and DK lists had been independently produced by the trust and delivered by Defendant to Plaintiff during settlement negotiations, with the CW list representing all bitcoin addresses owned by Craig Wright and the DK list representing all bitcoin addresses owned by David Kleiman.

104. I was informed that the CSW Filed list was produced to the Court by Defendant as the list of addresses extracted from an encrypted communication delivered by "bonded courier" from a trust, and is claimed by Defendant to be the set of actual bitcoin addresses whose private keys are controlled by the trust.

105. Additionally, I used publicly available data such as the bitcoin blockchain, as well as email and mailing list messages, to complete my analysis.

106. To facilitate the comparison of these data sets, I made minor changes to files as follows:

a. Shadders List: Renamed the 2nd column name in the header from "cb_txid" to "txid" to match the naming of columns in the other data files

b. DK: Added a column header to DK, to match the column header in CW

c. CSW Filed: Removed 3 lines containing invalid/junk data from the end of the file, as follows:

Line 16406: ,,,,

Line 16407: ,,,,

Line 16408: ,820250,,,

107. I concatenated the data from CW and DK lists, to produce a new list named "Combined", to represent the totality of the addresses owned by the trust, at the time they were provided to the Plaintiff's attorneys.

108. I began my analysis by comparing the list data to transactions that are credibly attributed to Satoshi Nakamoto and publicly documented by numerous recipients of these transactions. It is widely known that Satoshi spent some of the bitcoin they mined. Therefore, I expected to see those bitcoin addresses included in some or all of the lists.

109. The first known Satoshi transaction occurred in block #170 as a payment from Satoshi to Hal Finney in transaction f4184fc596403b9d638783cf57adfe4c75c605f6356fbc91338530e9831e9e16 and is famously known as the first user-to-user transaction to be included in a block other than mined bitcoin. The coins spent in that transaction were mined in block [redacted] spent in block [redacted] and are not included in any of the lists produced by Defendant.

110. Another known Satoshi transaction is a payment from Satoshi to Dustin Trammell, in transaction d71fd2f64c0b34465b7518d240c00e83f6a5b10138a7079d1252858fe7e6b577 and documented by emails exchanged between Dustin Trammell and Satoshi (satoshi@[redacted]. The coins

spent in that transaction were mined in block [redacted] and are not included in any of the lists produced by Defendant.

111. Another known Satoshi transaction is a payment from Satoshi to Mike Hearn in transaction ea84d39ef6f7b3b23fbf899e11a9bb18478a19413579a69f3005359da7a62c49 and documented in a series of emails published by Mike Hearn, between Hearn and Satoshi (satoshi[redacted]. The coins spent in that transaction were mined in block [redacted] and are not included in any of the lists produced by Defendant.

112. Surprisingly, none of the four lists included the bitcoin addresses referenced in the transactions above that are publicly known to have been mined and then spent by Satoshi.

113. As part of my analysis of the data lists provided to me (Shadders List, CW, DK, CSW Filed), I compared the data sets to identify commonalities and differences between them. All lists included at least the “block_height” and “txid” columns, which formed the basis of comparison.

114. The Shadders List contains the most transactions, at 27,973. All the other data sets contain fewer and, importantly, are subsets of the Shadders List. There is no entry in any data set that does not also appear in the Shadders List.

115. There were no common entries between the CW List containing 16,430 entries and DK list containing 6,416 entries. The Combined List (CW + DK) contains 22,846 entries, or 5,127 entries fewer than the Shadders List, with no additional entries appearing.

116. I compared the CW List and Combined List to the Shadders List to identify entries that were not in the CW List, or the DK List but were present in the Shadders List.

117. In the bitcoin system, transaction IDs are produced by a double hashing (the application of the SHA256 hashing algorithm twice) of the transaction contents. A key property of any cryptographic hash algorithm is that it's output is uniformly distributed across the range of possible values, which in the case of SHA256 is the range of numbers from 0 to 2^256 - 1.

118. I know of no reason why a transaction ID would not be randomly distributed across that range, nor why any ID would be preferred, included or excluded from any list of transactions based on its value. It plays no role in the functioning of the bitcoin system other than as a unique ID.

119. Transaction IDs were not among the criteria testified by Shadders as used to produce the Shadders List and indeed the distribution of transaction IDs in the Shadders List appears random.

120. I would similarly expect the distribution of transaction IDs of any transaction list, to be uniformly and randomly distributed across the possible range of transaction IDs.

121. However when examining the CW List sorted by the (randomly produced) transaction ID, instead of a random distribution of transaction IDs we find two large empty ranges where no transactions exist. These ranges of transaction IDs are:

a. 49c585… through to 51fa91…, and

b. 5a8660… through to 64361d…

122. This anomaly is not present in the DK or Shadders List, but is present in both the CW List and the CSW Filed list.

123. In further analysis, the CSW Filed list contains 16404 entries, a subset of the CW List, with 26 fewer entries.

124. The 26 entries included in the CW List but that are missing from the CSW Filed List correspond to 26 coinbase transactions of mined bitcoin that were spent between August 6, 2017 and June 27, 2019.

125. To spend those coins, someone had to create a digital signature with the private key corresponding to each address and therefore must have had access to the private keys to create those transactions.

126. An additional three (3) entries of bitcoin mined, which are present in the CSW Filed List, have had those bitcoin spent since June 27, 2019:

a. Block [redacted] was spent Sun Jul 07 23:44:00 EDT 2019

b. Block [redacted] was spent Sun Jul 07 23:44:00 EDT 2019

c. Block [redacted] was spent Mon Sep 02 15:03:00 EDT 2019

127. After completing the analysis of the CSW Filed list against the CW List, I compared CSW Filed to the Shadders List and I observed the following:

a. The CSW Filed List contains 16404 entries

b. All of the entries in the CSW Filed List are also found in the Shadders List, without exception.

128. Every block in the Bitcoin blockchain contains a numeric value called the "Nonce" which is used by miners to randomize the block header.

129. Independent analysis conducted as early as 2013 (https://bitslog.com/2013/09/03/new-mystery-about-satoshi/) had identified a pattern in many of the blocks assumed to be mined by Satoshi Nakamoto. The pattern is that the

least-significant-byte of the Nonce in those early blocks does not fall on a random distribution, but instead is in a narrow range of 0-58 (out of 0-255 possible values).

130. Shadders testified that one of the six criteria used to produce the Shadders List was the publicly known mining fingerprint found in the Nonce least-significant-byte.

131. Shadders testified that he used this criterion to produce the Shadders List and also that due to the Shadders Bug, additional entries violating that criterion were erroneously included in the Shadders List.

132. I conducted an analysis of the Nonce least-significant-byte value for all 16404 blocks referenced in the CSW Filed List entries with the following results:

a. 14655 entries (of the total 16404 entries in CSW Filed) were in blocks whose Nonce value was within the 0-58 range specified by Defendant as indicative of his mining activities “fingerprint”.

b. 1749 entries (of the total 16404 entries in CSW Filed) were in blocks whose Nonce value is greater than 127 (i.e. in the range 128-255), that do not match the well known Satoshi mining fingerprint but exactly match the results of the Shadders Bug.

c. Significantly, there are no blocks in the CSW Filed List whose Nonce does not match either the criteria specified by Defendant as indicative of his mining activities (Nonce in range 0-58) or the Shadders Bug (Nonce in range 128-255).

133. The presence of 1749 entries that correspond to blocks with a Nonce least-significant-byte value greater than 127 in CSW Filed, exactly replicating the result of the Shadders Bug, and absent any other deviation from the expected Nonce value (0-58), strongly

suggests that the CSW Filed List was derived from a subset of the Shadders' List or produced by the same software containing the Shadders Bug.

134. The same 1749 entries that contain Nonces with values consistent with the Shadders Bug are also found in the CW List. This strongly suggests that the CW List was also derived from a subset of the Shadders' List or produced by the same software containing the Shadders Bug.

135. I conclude that the Shadders List, CW List, and CSW Filed Lists produced by Defendant are derived from the Shadders List or produced by the same software containing the Shadders Bug and could not have plausibly been produced independently of the Shadders List or software containing the Shadders Bug.

136. Furthermore, none of the lists are complete lists of all bitcoin mined by Satoshi, since they do not include bitcoin known to be mined by Satoshi.

137. Finally, bitcoin mined in blocks included in one or more of these lists has been spent at various times subsequent to their mining, and as recently as September 2nd 2019 (EDT).

XIII. Analysis of Security of the Sale of A Private Key

138. Plaintiff has asked that I comment on the relative security of transferring ownership of bitcoin by selling the private keys rather than conducting a transaction to transfer the bitcoin to the address of the seller.

139. The designer of bitcoin used digital signatures as a way to transfer ownership without transferring the private key, guaranteeing that the transfer of ownership was final, irreversible and verifiable by the recipient. The designer of bitcoin used this security best

practice because they likely understood cryptography, the security properties of digital signatures, and therefore the risks of transferring key material.

140. A transfer of a private key does not relinquish control of the bitcoin funds, but rather shares control to both buyer and seller, such that either party may spend the funds independently of the other party. Both parties are presumed to know the private key.

141. Furthermore, if bitcoin is spent from addresses whose private key is known to more than one party, there is no way to determine conclusively or prove who spent the bitcoin.

142. Therefore, the transfer of bitcoin private keys is not a transfer of bitcoin ownership but rather it is sharing of bitcoin ownership.

143. By contrast, a transaction that transfers bitcoin to a new address whose private key is known only to the owner of that address is an irrevocable transfer of ownership that terminates any control by the prior owner, conclusively.

XIV. Analysis of Signed Messages

144. Bitcoin private keys can be used to sign any arbitrary message, producing a digital signature that can be verified by anyone. Verification requires three elements: the message, the bitcoin address and the signature.

145. The digital signature is calculated on the hash (fingerprint) of the specific message being signed. This ensures that the message cannot be altered, nor repudiated, after signing.

146. Verification consists of recreating the hash (fingerprint) of the message and calculating whether the signature was produced on that exact message hash with the private key corresponding to that specific bitcoin address.

147. On 2019-05-04 a BCH transaction that was included in the Bitcoin Cash blockchain contained the following message:

“Address [redacted] does not belong to Satoshi or to Craig Wright.
Craig is a liar and a fraud.

G39S6i4XsfQnixN5ePMjVPboWvGXdnW8xFFAXiwEriZFCclflbD7umP58u3Sl+dvvXC5BxBrRNkTMNf92O1UIXw=”

https://explorer.bitcoin.com/bch/tx/9d41091fd659287c496c239b3b43000f8b7949dc98bcdc54cca5a501a3062dd6

148. The transaction containing this message was mined into block [redacted] of the Bitcoin Cash blockchain, establishing the fact that this message was created on or before May 4th 2019, approximately 2:19pm EST.

149. This posting contains what appears to be a signed message and a digital signature.

150. To verify this signed message, we need the three elements: a message, a bitcoin address and a signature.

151. The posting contains the message and signature, and we infer from context that the bitcoin address mentioned in the message was also used to sign the message.

152. Using the Electrum Bitcoin Wallet versions [redacted] and [redacted] and Bitcoin Core [redacted] I verified that the message “Address [redacted] does not belong to Satoshi or to Craig Wright. Craig is a liar and a fraud.” was signed by the private key corresponding to bitcoin address [redacted] and the signature posted is a valid signature for that message and bitcoin address. All three software packages verified the authenticity of the posted signature on this specific message by the private key corresponding to this specific bitcoin address.

153. By verifying the signature, I was able to infer the following:

154. The person who produced the signature posted on 2019-05-04 was in possession of the private key corresponding to the bitcoin address [redacted] at the time they produced the signature.

155. The posted message "Address [...] Craig is a liar and a fraud." was signed by the person possessing the private key for address [redacted]

156. Only someone with possession of the private key for address [redacted] could have signed that message and produced that signature.

157. The message has not been altered in any way since the digital signature was applied, because any modification of the message would change the message hash rendering the digital signature unverifiable.

158. Neither the message nor the transaction which contained the message have any information that we can use to infer when the signed message was produced or when the digital signature was calculated, except that it was on or before May 4th 2019.

XV. Reservation of Rights

159. I reserve all rights to modify or supplement this Report if I become aware of any errors or misstatements, or if I become aware of other data or other evidence relevant to my position. I also reserve all rights to respond to any statements made by the Defendant, witnesses or expert witnesses to which a response is appropriate.

160. I understand that several depositions remain to be taken in this matter. I may also modify or supplement my opinions in view of opinions or arguments made by any person, including Defendant's counsel and anyone engaged by Defendant to provide opinions. I may also

modify or supplement my opinions if the Court provides litigants with any pertinent additional rulings.

161. I may expand or modify my opinions as my investigation and study continues and supplement my opinions in light of any relevant orders from the Court or in response to any additional information I review, and matters the Defendant raises, or any opinions Defendant's experts may provide.

162. If called to testify at trial or a hearing in this case, I may use documents and/or materials to help me explain my opinions. I may also prepare and use graphics, images, photographs, video recordings, animations, and other presentation aids to help me explain my opinions. I may also use images, photographs, graphics, animations, and other presentation aids prepared by other witnesses to help me explain my opinions.

I declare under penalty of perjury that the foregoing Report is true and accurate.

Dated: April 10, 2020

ANDREAS M. ANTONOPOULOS

EXHIBIT A

CURRICULUM VITAE
Andreas M. Antonopoulos
[redacted]

ABSTRACT
Andreas M. Antonopoulos is a highly sought after world-class expert in Bitcoin and open blockchain technology. Andreas has been working exclusively in the Bitcoin and Open Blockchain industry since 2012.

In 2014 O'Reilly Media published Andreas' first book, Mastering Bitcoin, a technical book for programmers. The book is widely viewed as the definitive guide on the subject and to date is the world's most cited book on Bitcoin.[1] Subsequently, Mr. Antonopoulos has authored 3 additional books on the topics of bitcoin and open blockchains, with 2 more being published December 2019 and 4th Quarter 2020 respectively. He has testified before regulators as an expert witness with respect to Bitcoin technology, once in 2014 before the Canadian Senate Banking and Commerce Committee and again in 2015 before the Economics References Committee of the Australian Senate.

In addition to his own projects within the industry, which demand the majority of his time, since 2014 he has served as a teaching fellow at the University of Nicosia, assisting with curriculum content and design, as well as co-teaching the Introduction to Digital Currencies course. Additionally, in 2014 he served as Chief Security Officer for blockchain.info, a well-known bitcoin wallet and block explorer.

During college, Mr. Antonopoulos earned both his bachelors and masters degrees in Computer Science from University College London. During college, he studied networks and distributed systems while simultaneously working in IT. In fact, since 1990 Andreas has worked exclusively in the Information Technology sector, with an emphasis on networks, distributed systems, security, and training. He secured three patents for network technology inventions and has been published in peer reviewed journals as well as mainstream media sources.

Andreas has authored hundreds of syndicated articles on security, cloud computing, and data centers; and is a frequent keynote speaker at technology and security conferences worldwide. He has been interviewed by Bloomberg, CNN, CNBC, CBS, NBC, ABC, BBC, the Financial

[1] According to a December 2nd, 2019 Google Scholar search

Times and many more media organizations for his industry expertise. He has been featured in numerous documentary films and is a permanent host on the Let’s Talk Bitcoin podcast with more than 400 episodes recorded to date.

UNIVERSITY TEACHING AND RESEARCH

2014-to date	University of Nicosia - Teaching Fellow “M.Sc. Digital Currencies”
1995-1997	University College London - Research Fellow “Distributed Systems Lab”
1994-1995	University College London - Teaching Assistant “Internet and E-Commerce”
1992-1994	University College London - Computer Lab Assistant

EDUCATION

1994-1995	M.Sc. Data Communications Networks & Distributed Systems (DCNDS). University College London, London, UK. M.Sc. Project in cross-platform distributed data exchange framework as part of the EU (HANSA ESPRIT) funded project.
1991-1994	B.Sc. (Hons.) Computer Science. University College London, London,UK. B.Sc. Project in distributed collaborative computing, X-Windows screen-sharing protocol.
1989	Lycee Leonin, High School Diploma, Athens Greece

EXPERT WITNESS TESTIMONY

Canadian Senate Banking and Commerce Committee, presenting on Bitcoin and digital currencies, October 8, 2014.

Economics References Committee of the Australian Senate, presenting on Bitcoin and digital currencies, March 4, 2015

PUBLISHED BOOKS

2014	*Mastering Bitcoin*, O’Reilly Media[2] 1088 scholarly citations[3]
2016	*The Internet of Money Volume 1*, Merkle Bloom 58 scholarly citations
2016	*Mastering Bitcoin 2nd Edition*, O’Reilly Media 227 scholarly citations
2017	*The Internet of Money Volume 2*, Merkle Bloom
2018	*Mastering Ethereum*, O’Reilly Media 65 scholarly citations

[2] World’s most cited book on bitcoin, according to Google Scholar

[3] Citation counts by Google Scholar - updated November 2019

2019[4] *The Internet of Money Volume 3*, Merkle Bloom

2020[5] *Mastering the Lightning Network*, O'Reilly Media

PUBLISHED ARTICLES

1998 - date More than 200 published articles and reports on Security, Data Centers, Cloud Computing and Cryptographic Currencies. (comprehensive listing available upon request)

INTERVIEWS

2012 - date More than 100 interviews on the topics of bitcoin and open blockchains including Bloomberg, CNN, CNBC, CBS, NBC, ABC, BBC, and Financial Times. (comprehensive listing available upon request)

PATENTS

System and Method for Securing Virtualized Networks USPTO 61/720,343
System and Method of Subnetting a Virtual Network Identifier, USPTO 14/210,069
System and Method for Dynamic Management of Network Device Data USPTO 9479P001

JOURNAL PUBLICATIONS

Peer-Reviewed Framework for Distributed Application Generation, SPEEDUP
Volume 11, Number 1, pp.15-17, Scientific Journal, (Jun. 1, 1997)

[4] Published December 2019

[5] Due for publication Q4'2020

PROFESSIONAL HISTORY

2012 – to date **Founder, CEO -** aantonop Companies
Own and operate several companies focused on producing educational content about bitcoin and other open blockchains to people around the world. Manage a team of 11 people, producing videos, articles, interviews and books, public speaking, seminars, educational courses, and event management.

2014 - to date **Teaching Fellow** - University of Nicosia M.Sc Digital Currencies
Co-teach the open "MOOC" course for UNIC's MSc programme in digital currencies., the world's first university course in digital currencies. Curriculum development, teaching.

2014 Jan - Sep **Chief Security Officer** - Blockchain.info (bitcoin wallet and block explorer)
Served as the Chief Security Officer (CSO), coordinating strategy for security, secure software engineering practices, and security operations.

2003 – 2011 **Founding Partner, CIO, Lead Security Research Analyst** - Nemertes Research
Developed and managed research projects, conducted strategic seminars and advised key clients as the lead analyst in Information Security, Data Center and Cloud Computing. CIO for the firm, managed a diverse cloud infrastructure supporting distributed team. Responsible for HR and legal management. Founding partner and managing director.

2002-2003 **Director Security Practice** - ThruPoint Inc, NY
Directed a team of 70-80 network security, information security and penetration testing engineers, ensuring consistent delivery of consulting and professional services across a global delivery team. Supported sales efforts as team lead and promoted standardization of deliverables. Worked on accurately predicting and accounting for work effort, profit margin and project management in sales proposals.

2001 - 2002 **Security Practice Lead** - Greenwich Technology Partners, NY
Led the North East security practice, covering NY, NJ and CT, supporting sales operations (SME), delivering security advice and services and leading projects, including architecting global secure financial transaction network for SWIFT.

2000 - 2001 **Founder** - Managed Business Network, London, UK
Consulting and integration services. This company was a successor to Phaia Limited.

1997-2000 **Managing Director** / Co-Founder - Phaia Limited, London, UK
IT services and system administration.

1997-2000 **Instructor - Security, Networking** - Learning Tree International, London, UK
Taught IT professionals 4-day intensive seminars on data communications, IT security, operating system security and network security. Highest rated instructor in Information Security for 2 years running.

1995-1997 **Research Fellow** - University College of London, Computer Science Department, London, UK
ESPRIT-funded interactive media project. External Lecturer. Lead Research Fellow, ``Distributed Application Generation',” EPSRC-funded project.

1995-1997 **Founder** - Athena Systems Design Limited, London, UK
IT consulting, systems administration, network installation

1993-1995 **IT Manager** - Odey Asset Management, London, UK
Responsible for all IT at this legendary and pioneering british hedge fund. Systems administration, telecommunication, Internet security, email services, fax/telex servers, desktop support, trading systems (Reuters/Bloomberg), training.

1991-1993 **Freelance IT Consulting** - London, UK
IT support, systems administration, training

1990-1991 **Network Support Engineer, Trainer** - IBM Greece
Network installation, technical support, training.

Earlier work history available upon request