

1. On behalf of	Claimants
2. Witness	Craig Steven Wright
3. Statement No	1
4. Date:	28 July 2023

**IN THE HIGH COURT OF JUSTICE
BUSINESS AND PROPERTY COURTS OF ENGLAND AND WALES
INTELLECTUAL PROPERTY LIST (CHD)**

Claim No. IL-2021-000019
(the "COPA Claim")

BETWEEN:

CRYPTO OPEN PATENT ALLIANCE

Claimant

- and -

DR CRAIG STEVEN WRIGHT

Defendant

Claim Nos. IL-2022-000035
(the "Coinbase Claim")

BETWEEN:

**(1) DR CRAIG STEVEN WRIGHT
(2) WRIGHT INTERNATIONAL INVESTMENTS LIMITED**

Claimants

- and -

**(1) COINBASE GLOBAL, INC.
(2) CB PAYMENTS, LTD
(3) COINBASE EUROPE LIMITED
(4) COINBASE, INC.**

Defendants

Claim No. IL-2022-000036
(the "Kraken Claim")

BETWEEN:

**(1) DR CRAIG STEVEN WRIGHT
(2) WRIGHT INTERNATIONAL INVESTMENTS LIMITED**

Claimants

- and -

**(1) PAYWARD, INC.
(2) PAYWARD LTD.
(3) PAYWARD VENTURES, INC**

Defendants

Claim No. IL-2022-000069
(the "BTC Core Claim")

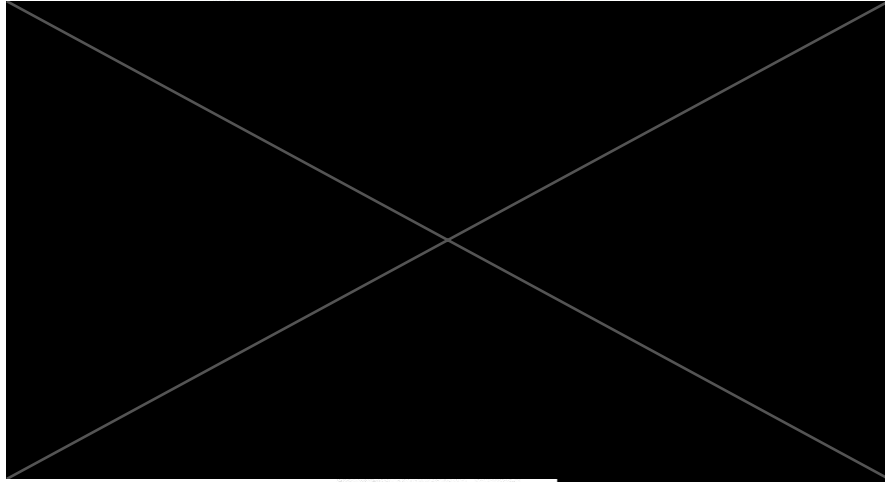
B E T W E E N:

- (1) DR CRAIG STEVEN WRIGHT**
- (2) WRIGHT INTERNATIONAL INVESTMENTS LIMITED**
- (3) WRIGHT INTERNATIONAL INVESTMENTS UK LIMITED**

Claimants

- and -

- (1) BTC CORE (A PARTNERSHIP OF ENTITIES AND INDIVIDUALS INCLUDING THE SECOND TO TWENTY-SIXTH DEFENDANTS)**



- (16) BLOCK, INC.**
- (17) SPIRAL BTC, INC.**
- (18) SQUAREUP EUROPE**
- (19) BLOCKSTREAM CORPORAT**
- (20) CHAINCODE LABS, I**
- (21) COINBASE GLOBAL I**
- (22) CB PAYMENTS, LTI**
- (23) COINBASE EUROPE LIM**
- (24) COINBASE INC.**
- (25) CRYPTO OPEN PATENT A**
- (26) SQUAREUP INTERNATIONA**

Defendants

FIRST WITNESS STATEMENT OF DR CRAIG

I, **CRAIG STEVEN WRIGHT** of [REDACTED] STATE AS FOLLOWS:

1. I am Craig Steven Wright, the defendant in the COPA Claim, as defined above, and one of the claimants in the Coinbase Claim, the Kraken Claim and the BTC Core Claim, each as defined above (together the "**Non-COPA Claims**"). I make this statement on my own behalf and am also duly authorised to make it on behalf of the other claimants in the Non-COPA Claims.
2. The facts and matters set out in this witness statement are within my own knowledge unless otherwise stated, and I believe them to be true. Where I refer to information supplied by others, the source of the information is identified. Facts and matters derived from other sources are true to the best of my knowledge and belief.
3. This witness statement has been drafted by me, pursuant to in-person meetings, video conferencing calls and written exchanges with my solicitors, Travers Smith LLP, and previously my former solicitors, Ontier LLP.

Introduction and qualifications

4. With an expansive career spanning more than two and a half decades, I have ingrained myself in numerous aspects of information technology, digital forensics, and cybersecurity. My professional endeavours have led me down various avenues, from launching startups to developing advanced technological solutions.
5. I hold citizenship in Australia, Antigua, and Barbuda. However, as of October 2015, I and my wife and children made a significant life change and moved to England (which I will return to below). The country welcomed us with open arms and quickly became our home. I was granted permanent residency here on 12 March 2021. To solidify our commitment to this nation and its people, I applied for British citizenship as soon as I became eligible. We eagerly await confirmation of this citizenship, looking forward to the future and the opportunities it holds for us here in the UK. My wife and I specifically selected England as our base to expand our investments and foster the burgeoning industry we were creating. Part of this decision was influenced by my studying law at Northumbria University in North England. It instilled a deep appreciation for how English law operates within me, specifically its fairness, predictability, and the sound principles it's built upon.
6. Indeed, my academic journey has been a long and diverse one. As of today, I hold more than 16 Master's degrees and two doctoral degrees. I hold a PhD in Computer Science and Economics from Charles Sturt University in Australia. My postgraduate degrees span multiple disciplines, including Law, History, Economics, Game Theory, Computer Science, Philosophy, and Statistics. This broad academic base gives me a unique perspective and allows me to approach problems from various angles. I take great pride in my academic qualifications. I strive to constantly expand my knowledge and stay at the forefront of my fields of interest.

7. As the Chief Scientist of nChain UK Limited, a role I've held since October 2015, I focus on the research and development of advanced blockchain technologies. nChain UK Limited serves as the research and development (R&D) arm of the nChain group of companies, a conglomerate I helped establish in 2015. The primary mission of nChain is to equip businesses with secure database solutions based on blockchain technology. From 2015 to 2017, the nChain group operated under the name nCrypt (but I will refer to it as "nChain" throughout this statement).
8. As a high-functioning individual with autism and a high IQ, my world experience is unique. This blend often generates ideas or approaches that could easily be missed from a neurotypical viewpoint. However, this doesn't shield me from the social challenges of autism or the mental health issues often associated with autism. Navigating social situations can still be challenging due to difficulties understanding social cues, maintaining eye contact, or engaging in small talk. My approach to interpersonal interactions focuses more on facts and information rather than remembering specific names or personal details about individuals. Consequently, unless I have ongoing interactions or a need to recall specific details about someone, I may not remember their name or other personal information even though I have met them. While everyone's experience of autism can be very different, the patterns I've mentioned are based on my personal journey.
9. Perhaps the most significant contribution I have made in my career is the creation of Bitcoin, the world's first distributed digital cash system that works transparently. I did this under the pseudonym 'Satoshi Nakamoto'. I'm proud to have played a pivotal role in ushering in a new era of financial technology and micropayments, laying the groundwork for countless innovations in the blockchain and "cryptocurrency" space.

The Essential Characteristics of Bitcoin

10. Given the high complexity of the Bitcoin system, the following summary is inevitably condensed. It represents a simplified overview of the features relevant to the rest of this statement.
11. Between 2007 and 2008, I dedicated a substantial amount of time to research into solving the foundational problems of Bitcoin and blockchain. During this period, I documented my findings by composing a paper titled "Bitcoin: A Peer-to-Peer Electronic Cash System," more commonly called the "Bitcoin White Paper." As I will expound below, I posted a public link to the White Paper online on the 31st of October 2008. The system delineated in the White Paper describes a peer-to-peer electronic payment system called the "Bitcoin System". The system enables online payments, especially micropayments (typically, this refers to amounts less than a dollar), to be sent directly from one entity to another, eliminating the necessity for an intermediary like a financial institution. I architected the Bitcoin System to operate without needing a trusted third party (internet payment intermediary) to oversee or authorise transactions. The design pivots around the principle of competitive peer-to-peer verification.
12. Bitcoin transactions are documented in a public ledger or database structured as a 'chain' of 'blocks' of data, referred to as a 'blockchain' (the "**Bitcoin Blockchain**"). Each block is

essentially a record in the Bitcoin Blockchain that encompasses details of validated transactions, a timestamp, and the hash of the preceding block. For clarity, a hash is a function that maps data of arbitrary size to a fixed size. Every transaction within the Bitcoin system is recorded in these blocks. As such, the Bitcoin Blockchain maintains a record of every transaction ever processed, enabling traceability of all Bitcoin movements. Competitive systems, referred to as nodes, validate transactions ensuring that these are 'honest' while monitoring other network nodes. Nodes in Bitcoin are defined in section 5 of the White Paper. There are very few nodes in operation, and the amount of data centres are limited.

13. Nodes, which are devices in the network participating in transaction processing in the Bitcoin System, are integral to its operation. These nodes engage in "mining" Bitcoin, which involves the formation of timestamped blocks. Simply put, Bitcoin operates as a distributed timestamp server geared towards preventing double-spending. Double spending is analogous to cheque fraud. Nodes are financially supported through a mix of block subsidies and transaction fees.
14. Nodes compete to solve a "hash puzzle" that satisfies a target difficulty predefined by the Bitcoin software. This competition serves two purposes: first, it distributes rewards proportionately to a node's investment (in solving puzzles) in the system, and second, it ensures nodes are de-anonymised if they acquire significant power over the network. When a specific node's solution to the current hash problem is recognised as valid by the other nodes, the block is deemed complete and added to the Bitcoin Blockchain. However, it's worth noting that a node will only receive payment once its solution is accepted and built upon to a depth of at least 100 other blocks by competing nodes. Thus, nodes (and their operators) collate transaction-related data and keep it in a time-ordered ledger.
15. I engineered the process of validation, verification, and announcement in the Bitcoin system to be nearly instantaneous. However, the system does account for instances in which two nodes might find a solution to the "hash puzzle" more or less simultaneously. It is crucial to understand that nodes don't control the network; instead, they adhere to the inherent rules of the Bitcoin system. These nodes act as commercial agents tasked with enforcing the network's regulations.
16. When nodes successfully mine Bitcoin, they receive a distribution consisting of a certain amount of Bitcoin in the form of a subsidy, along with the transaction fees documented in the new block. This distribution can be seen as a 'reward' or 'subsidy' for mining and the fees combined. As time passes, the Bitcoin quantity included in this distribution progressively diminishes. The system is designed with an in-built limit of just under 21 million Bitcoin. Each nominal unit of bitcoin represents 100 million indivisible electronic tokens. Once all initial Bitcoin is distributed, the nodes will continue to earn their remuneration via fees.
17. As the creator of Bitcoin, I designed it with a focus on several key characteristics. One of the crucial elements is traceability and identity, which is the system's ability to track

transactions and ultimately identify the parties behind them. This feature is vital in ensuring accountability and preventing fraudulent activities within the network.

18. Another significant feature of Bitcoin is its capacity to facilitate micropayments. The peer-to-peer nature of the Bitcoin system allows for these small-scale transactions without necessitating intermediary fees. This opens up new possibilities for digital commerce, particularly in scenarios where traditional payment systems may impose prohibitive fees.
19. Furthermore, Bitcoin has an inherent mechanism for preventing double-spending. This is the risk of a user spending the same digital coin more than once. The system accomplishes this without needing a trusted third party, thus further enhancing Bitcoin's distributed nature. The integration of these features results in a robust digital cash system that is both secure and efficient, empowering users in ways that traditional monetary systems have not.
20. The novelty of Bitcoin lay not in the creation of new, individual components but in the innovative combination and application of various existing technologies and concepts. These technologies and concepts, such as digital signature algorithms, hash functions, balanced binary trees (also known as Merkle trees), proof-of-work, time-stamping, distributed ledgers, and game theory, had existed independently prior to Bitcoin. However, it was their integration within a single framework that constituted an unprecedented leap in the development of digital cash systems.
21. The term "blockchain" did not exist in the public domain prior to Bitcoin and the publication of the Bitcoin White Paper. It was a concept that resided only in my mind and in conversations I held with a select few individuals. It was not until after the advent of Bitcoin that the term "blockchain" was used to describe the technology underpinning it and, eventually, a host of other digital assets and distributed ledger technologies.
22. There has been a concerted effort by certain individuals and groups, often associated with CypherPunk and anarchist ideologies, to distort the original intention of Bitcoin and present it as a tool for evasion of legal oversight. It is a common misconception that it is an anonymous, untraceable "cryptocurrency". "Cryptocurrencies", as commonly understood, can be exploited for illicit activities because users' identities can be effectively cloaked. However, Bitcoin was not designed to serve this purpose. Bitcoin transactions are pseudonymous rather than anonymous. While personal identities are not directly tied to transactions, each transaction is publicly recorded on the blockchain, making it traceable. Every transaction is visible on the network, offering transparency whilst retaining user pseudonymity. My vision was to create a digital cash system that respects the principles of transparency, accountability, and the rule of law.

"Signing" a message.

23. It is possible to prove possession of a private key by using a digital signature algorithm. This entails using a mathematical operation known as an elliptic curve digital signature algorithm (ECDSA), which uses both the underlying data and your private key. This operation yields a unique piece of data: a verifiable digest (the alleged digital "signature").

A corresponding mathematical operation involves the original data, the verifiable digest, and your public key to verify the digest. If the operation yields a specific expected result, the digest is verified.

24. There is a common misperception that references the digest as a 'digital signature' and to this process of using a digital signature algorithm as 'signing a message'. In some parts of the digital cash industry, this has been promoted misleadingly as signing even without the sender's identity being linked. This claim is entirely inaccurate. Before relying on a key for digital signatures or other cryptographic purposes, it's essential to establish identity through other means. In the absence of proof of identity, the process only verifies that the individual has physical or electronic possession of the private key associated with a specific public key.

Early coding experiences

25. My fascination with coding and computing began when I dabbled with C and C++ around the age of eight or nine. By age 11, I had already started writing code for games. I used C and C++ because they were the languages that games were written in. As I discuss below, while I have worked extensively with various coding languages, C++ has remained a cornerstone of my expertise.

My work that influenced the development of Bitcoin

26. Having been deeply invested in the evolution of digital cash systems since the late 1990s, I have spent decades shaping what eventually materialized as Bitcoin, which has defined my professional journey. In the initial stages of its development, Bitcoin was referred to as Timecoin, a term that I adopted until I transitioned to the now well-known moniker, Bitcoin, in mid-2008. Although, for some time after that, I used both terms (and a few other names) interchangeably.
27. My primary objective throughout the creation and evolution of Bitcoin was to create a system of electronic cash that could simultaneously deliver micropayments and effectively curtail fraudulent transactions.
28. While I will not delve into my entire employment history, a number of my work experiences and business ventures were instrumental in shaping Bitcoin. These experiences fuelled my understanding and expertise in this domain and underscored the depth of my commitment to creating a secure, efficient, and trustworthy digital cash system.

The 1990s and Project BlackNet

29. During the early to mid-1990s, I explored digital cash systems while working at OzEmail (a major internet service provider in the 1990s) as the Manager of Corporate Engineering. One of our projects involved the implementation of a payment protocol known as Millicent. Like Bitcoin, Millicent wasn't a cryptocurrency in the truest sense, as I have explained above not all digital cash is cryptocurrency. It was explicitly designed to enable efficient and transparent payments, and therefore it was not cryptographic or encrypted.

The concept of every transaction being transparent, which was quite avant-garde in the '90s, was central to Millicent. Despite its eventual failure due to inherent limitations, Millicent significantly shaped my perspectives on digital cash systems.

30. By the late 1990s, I found myself deeply engaged with the budding digital cash industry, despite being relatively young. During that period, I attended DecUS (the Digital Equipment Computer Users' Society).
31. In 1998, I embarked on an ambitious endeavour called 'Project BlackNet'. This project was named after a proposition by Tim May, a renowned cryptologist I had the privilege of meeting at an internet conference. Project BlackNet was an audacious attempt at creating a fully secure, encrypted internet intended explicitly for business-to-business transactions. One of the critical components of BlackNet was the introduction of micropayments using tokens dubbed 'crypto credits'.
32. The concept of 'crypto credits' was conceived within the framework of BlackNet in combination with the ideas I had taken from Millicent. This laid the foundational groundwork for what would later become Bitcoin.

DeMorgan

From 1997 to 2003 my work was primarily conducted through DeMorgan, a business that I founded. DeMorgan was a name used historically within my family. It changed a long time ago, but my sister Danielle has adopted it as her last name.

33. As I explain below, I had been working at the Australian Stock Exchange (the "ASX") but in 1997, driven by my innovative ideas and the growing potential of digital token systems, I decided to branch out independently. This was when I founded DeMorgan. I envisaged DeMorgan as a platform through which I could conduct extensive research and development in digital cash and continue my work in information security.
34. DeMorgan was more than just a vehicle for my pursuits; it also provided services to numerous companies. Over time, DeMorgan began to expand, eventually employing around 50 individuals. Each team member was crucial in driving the research and development efforts of the company forward. Our collective knowledge and skills laid the foundation for some leading-edge work in distributed systems and information security.
35. I set out further below the projects which were most instrumental in shaping the formative stages of Bitcoin and the principles upon which it was built.

Australian Stock Exchange

36. In 1996, I took on the role of Head of Information Security for the ASX. My responsibilities centred around the development of sturdy information security systems and protocols. An essential part of my job was architecting their communication network, known as NIPPA—an acronym for 'Network Infrastructure and Production Project ASX.' The NIPPA system was designed to facilitate the exchange of dematerialised information or tokens, an aspect of the project that would later play a significant role in my development of Bitcoin.

37. I built a strong reputation at the Australian Stock Exchange, which led to them becoming one of DeMorgan's earliest clients. After I left the ASX in 1997 they contracted my services (through DeMorgan) based on my previous work, and I continued with similar projects that I had begun in their employ.

Lasseter's online casino

38. In 1998, DeMorgan was engaged by Lasseter's Online Casino, the first legally sanctioned online casino globally. This association lasted for about seven years and was instrumental in paving the way for the secure online gaming experience that players enjoy today. Lasseter's was ahead of its time with a pioneering poker platform. However, they faced a considerable hurdle in establishing and maintaining robust security and logging systems. These were crucial to retain player trust and meet the stringent regulatory standards.
39. Drawing on my extensive background in information security, my team and I worked closely with colleagues such as Mark Archbold to help Lasseter's surmount this obstacle by conceptualising and implementing advanced security measures and logging systems. Due to the lower-grade Internet connections prevalent at the time, which had a high likelihood of restarting, I had to devise a solution to send the logs reliably. I implemented a system which integrated Command and Control (C&C) systems (typically associated with malware) with Peer-to-Peer (P2P) software. This allowed the distribution of logs over up to eight links. Since multicast was not a viable option, a gossip-based protocol and a binary tree system in timestamped rounds were employed instead. In this context, a 'round' is similar to what is referred to as a 'block' in today's blockchain terminology. This method of linking rounds represented an early precursor to the blockchain. These solutions not only met regulatory standards but also instilled a greater sense of trust among the players. This assignment underscored the potential and necessity of secure, traceable online transactions, a concept that later became integral to the design of Bitcoin.
40. During my tenure with Lasseter's, I tried to tackle the diverse set of challenges that the online casino was grappling with. One of the most substantial and pervasive issues was the lack of a dependable digital money system. At that time, Visa and Mastercard were Lasseter's main payment methods. However, this reliance on credit cards for online gaming came with complications, including security concerns, monitoring unauthorised access and exorbitant credit card fees.
41. I conceptualised various token systems to alleviate these issues to facilitate online poker play. These tokens were intended to function as digital cash, enabling secure, swift, and efficient transactions within the platform. Unfortunately, the online gaming industry was beset with difficulties, which led to Lassater's online operations closing before the solutions I had been working on could be deployed.
42. Nonetheless, my experience with Lassater's was crucial in shaping my understanding and appreciation of the need for a secure, efficient, and reliable digital payment system. It planted the seeds that would later germinate into the idea of Bitcoin, a digital cash system that eliminated the need for intermediaries, provided a secure transaction environment, and was accessible to anyone with an internet connection.

43. My early experiences developing systems for online poker games played a critical role in the creation of Bitcoin. In the initial code for Bitcoin, I included the rudiments for implementing a peer-to-peer poker game. The embedded code featured functions necessary for the basic operations of a poker game, including dealing and shuffling cards, conducting betting rounds, and ranking hands. This code was an extension of the software I had developed in collaboration with Global Gaming Services (GCS), which was incorporated into the Lassater's platform.
44. However, at the time of Bitcoin's launch, the poker game was not fully functional, and the relevant code was ultimately removed in the subsequent software versions. Nevertheless, the insights I gained from this experience, particularly the need for a robust, secure, and efficient system for digital transactions, proved instrumental in shaping the development of Bitcoin.

Vodafone

45. From 1998 to 2002, DeMorgan had a significant working relationship with Vodafone. One of the main projects that my team and I undertook for them involved designing and implementing a new infrastructure system. We aimed to create a robust and efficient system that would cater to the demands of a high-volume carrier like Vodafone. We needed to ensure that the system could manage massive volumes of traffic while maintaining high levels of performance and security, reflecting Vodafone's status as a global telecommunications giant. This experience further honed my skills in handling large-scale digital systems, contributing significantly to my capabilities as a digital architect, which would later find expression in the creation of Bitcoin.
46. While working with Vodafone, my team and I developed advanced logging servers, a task I frequently discussed with my colleague Rob Jenkins. This development required the creation of secure logging and payment channels, ensuring all system events and transactions were carefully tracked. Such an audit trail could then serve as a valuable tool for detecting security incidents, bolstering the system's overall security.
47. Our design employed a distributed cluster of servers divided among eight nodes. The logging was replicated in a peer-to-peer fashion across these systems. While the structure of this system bore some resemblances to Bitcoin, there was a crucial distinction - it was not distributed over the internet in the same manner Bitcoin was designed to be. Nonetheless, the experience of working on such a system was instrumental in shaping my understanding and approach to distributed systems. It was a significant steppingstone on the path to creating Bitcoin.

BDO

48. I left DeMorgan in 2003. In November 2004, I embarked on a journey as an Associate Director, Information Systems with BDO Kendalls, where I reported to Neville Sinclair, a partner at the time, and Allan Granger, then my managing partner. My role was multi-faceted, encompassing responsibilities within IT audits, digital forensics, and fraud prevention.

49. Beginning around 2005, while I was still employed at BDO, I began providing advisory services to CentreBet, a popular sports betting site in Australia. They had ambitious plans to go public, necessitating an impeccably secure database and accounting systems. This was a significant task, and they sought my expertise to ensure the resilience and security of their critical systems. During this engagement with CentreBet, I had the opportunity to work alongside Stefan Matthews, who headed their team. We've maintained a professional relationship ever since.
50. In 2006, Allan Granger introduced me to triple-entry accounting. This concept played a pivotal role in the development of Bitcoin. Traditional double-entry accounting records transactions as a debit in one account and a corresponding credit in another. However, this approach lacks an independent verification mechanism. On the other hand, triple-entry accounting introduces a third entry, a receipt secured cryptographically and recorded in a distributed ledger. This third entry independently verifies each transaction, significantly reducing the opportunity for fraud or manipulation of financial records.
51. The concept struck a chord with me and formed an integral part of Bitcoin's underlying technology. Each Bitcoin transaction leaves an indelible record on the Blockchain, enhancing transparency and security. This provides a means to verify transactions and ensures that the entire history of transactions is traceable. This is a significant advancement over traditional financial systems, where tracing funds can often be complicated and time-consuming.
52. In 2007, I introduced Allan to what would become Bitcoin, though (as I have explained above) I hadn't yet settled on that name. We exchanged ideas, and Allan's insights proved instrumental in refining and shaping the nascent concept. Around the same time, I conversed with Neville Sinclair about a timestamped database that would permanently record all transactions, significantly improving the reliability of client systems. Moreover, I discussed with Neville my vision for a token-based system that would form the foundation of this innovative digital cash system. Despite his inability to see the value in tokenised payments, these dialogues were instrumental to the progression of my thoughts and ultimately contributed to Bitcoin's development. I valued these discussions for providing alternative viewpoints, which led to a more comprehensive understanding and refinement of the concept.
53. From 2007 onwards, I also began collaborating with Ignatius Pang (a PhD student) on creating models for analysing graph-based connections using software developed by his university. These models became a foundational tool for understanding and developing complex, interconnected systems like Bitcoin. Ignatius' expertise proved invaluable throughout this process, particularly in designing small-world networks for peer-to-peer systems.
54. Small-world networks are a specialised type of mathematical graph where most nodes can be reached from any other node through a small number of steps. This concept is fundamental to Bitcoin's design, enabling its peer-to-peer network structure. Beyond his

specific technological contributions, Ignatius provided a broader perspective on the potential applications and implications of such systems.

55. Ignatius contributed significantly to the early stages of my conceptualisation process that eventually led to the development of Bitcoin. His input and expertise not only helped shape the technical underpinnings of Bitcoin but also offered valuable insights into its potential applications and implications. I do not know whether I used the term 'Bitcoin' with him before its launch.

My LLM thesis at the University of Northumbria

56. Between 2005 to 2007, in addition to my work at BDO, I was also pursuing an LLM at the University of Northumbria. My study focused on the legal status and implications of internet intermediaries in online transactions.
57. Over several months, I painstakingly drafted and edited my LLM thesis, ensuring several people thoroughly reviewed it. Among them were members of the academic staff at Northumbria, my ex-wife Lynn, Denis Mayaka (a lawyer based in the Seychelles and Kenya) whom I had collaborated with since 2008, and David Bridges. David, who was Chief Information Officer (CIO) at an Australian bank, provided invaluable insights, given his depth of understanding of the technology and financial sectors. The feedback I received from Northumbria primarily revolved around referencing, formatting, and my use of computer science terminology. As a result, I eliminated some of the computer science jargon and ensured that I used legal terminology consistently. Despite the range of inputs, all substantive changes to the thesis were made by me.
58. My Master of Laws (LLM) thesis centred on internet payment intermediaries, specifically within financial law. It provided a comprehensive analysis of the roles and responsibilities of trusted third parties within online transactions. The fundamental purpose of this investigation was to illustrate the necessity for these intermediaries to adhere to various legal and regulatory provisions while simultaneously managing to reduce operational costs. The crux of my thesis revealed the cost issues plaguing online intermediaries, which significantly contributed to the high costs associated with digital transactions. My exploration of these issues subsequently informed my vision for Bitcoin, which sought to minimise transaction fees and reduce reliance on intermediaries by utilizing a peer-to-peer network for transaction validation and a cryptographic protocol for security.
59. While the academic discourse and professional language varied between law and computer science, the underlying concepts bore striking similarities. In legal terminology, I used the phrase "internet intermediary" to refer to entities facilitating online transactions. In computer science, the exact role was called a "trusted third party." Despite the differences in nomenclature, the principle at the core of both concepts was identical: they both referred to a central entity that enabled and ensured the security of online transactions.
60. Though the words were different, the essence was the same: a central authority was involved in facilitating and ensuring the integrity of transactions. This principle carried a

significant influence on my conceptualisation of Bitcoin. However, a critical distinction that sets Bitcoin apart is its innovative approach to eliminating the need for a central authority while ensuring the security and reliability of transactions.

The decision to create Bitcoin pseudonymously and the choice of Satoshi Nakamoto

61. In November or December of 2008, I accepted redundancy from BDO. While my official duties ended in December, I remained on-call for the first two weeks in January 2009. However, this arrangement didn't require me to be physically present in the office, granting me the time and flexibility I needed to launch Bitcoin. I consciously decided not to seek another job immediately, choosing to dedicate myself fully to Bitcoin. As detailed below, I created the Genesis Block, shortly after.
62. This decision, however, was not met with enthusiasm at home. My wife at the time, Lynn, was unhappy that I hadn't consulted her beforehand, and she raised valid concerns about whether this new project would be financially sustainable. The uncertainties surrounding Bitcoin at its inception were significant, but I was determined to see my vision for a secure, efficient, and reliable digital payment system come to fruition.

Satoshi Nakamoto

63. I chose to develop Bitcoin under a pseudonym primarily due to the potential legal and regulatory ramifications associated with digital money systems. I was particularly wary of the U.S. government, which had previously posed challenges for clients like Lasseters. Around 2007, while I was in the throes of developing Bitcoin, I closely followed the case of Douglas Jackson, the founder of E-Gold, who was indicted for money laundering due to the misuse of his platform. The arrest of the CEO of Sporting Bet around the same period further underscored my concerns. All these experiences instilled in me the necessity of maintaining privacy during the initial stages of Bitcoin's development.
64. Despite adopting the pseudonym Satoshi Nakamoto, my intention was not to shroud this identity in secrecy. The goal was not total anonymity but a certain level of privacy. This allowed me to focus on my work and ensured that the spotlight remained on the innovation and potential of Bitcoin rather than the individual behind it. In my real life, I first shared my identity with a small circle of people including my mother, my uncle Don Lynam, some close friends such as David Bridges, and my then wife, Lynn.
65. I've always held a deep admiration for Japanese culture. This fascination traces back to my childhood spent at my grandfather's house. He had served in the Philippines during the Second World War, a time when it was under Japanese control. Upon his return, he developed a profound interest in Japanese culture and collected various Japanese artefacts. These relics captivated me; they inspired me to take up martial arts when I was about ten. Throughout my life, I have adopted various Japanese pseudonyms. In the 1990s, when I was in my twenties, I often referred to myself as 'Dosai Gatai' or 'Doshai' or 'Dosai' translating roughly to 'vengeance'. I also borrowed the name of one of my martial arts instructors, Masutasu Sheogai. I used other names when I was younger, but I do not remember them all. I made no secret of these pseudonyms, even sharing them with my

family and a few of my friends. Some of my early acquaintances in the technology field during the 1990s were aware of these aliases, as well as my sister Danielle, who would often tease me about them.

66. For the Bitcoin project, I opted to adopt the alias 'Satoshi Nakamoto.' Before this project, I had sporadically used this name in online forums, particularly on IRC (internet relay chat) starting around 2005. The name 'Nakamoto' holds significance for me due to my admiration for the philosopher Tominaga Nakamoto, whom I consider to be the Japanese counterpart of Adam Smith. Tominaga Nakamoto's writings encompassed diverse subjects, including the value of truth and integrity, the importance of equitable transactions, and the study of trade economics. Moreover, his impact extended to the politics and grain distribution in Japan.
67. The selection of 'Satoshi' was influenced by two factors. Firstly, I came across the name through a character called David Satoshi Morgan, featured in the book "The House of Morgan," which delves into the history of the JP Morgan family and their banking endeavours. On a lighter note, I found humour in that "Satoshi" also referred to the Pokémon trainer in Japanese, equivalent to "Ash" in English. This choice was particularly relevant as the Pokémon phenomenon had gained immense popularity during that period.
68. When I initially chose the pseudonym 'Satoshi,' I was drawn to its connection with the Pokémon trainer and the symbolic significance it held in other contexts. One such reference that resonated with me was its association with the mythical Phoenix. The Phoenix, known for its ability to rise from its ashes, symbolised renewal, rebirth, and resilience. This powerful imagery captivated me, reflecting the core principles underlying the digital cash system I envisioned.
69. Interestingly, during the 1980s, the Phoenix motif had caught the world's attention unexpectedly. It adorned the cover of The Economist while discussing the concept of a global digital currency. The idea of a currency transcending borders and operating globally aligned with the transformative potential of Phoenix's rebirth. I was aware of this when I was working on digital currency projects in the 1990s.

Work on the Bitcoin source code

70. In 2007, I created what would eventually become the Bitcoin source code. To develop this digital cash system, I chose to work with C++ and utilised Microsoft Visual Studio on the Windows Operating System, incorporating the Boost Library (a tool used to accelerate the running of code). While it may have been an unconventional choice at the time, as many developers favoured the Linux/GNU operating system, I have always been accustomed to Microsoft Windows. Thus, the Bitcoin software was tailored to function seamlessly on this platform. The combination of Microsoft Visual Studio, C++, and the Boost Library catalysed my vision of a distributed digital cash system that has since revolutionised the world of finance and technology. Overall, my journey as a developer and my experiences with C++ has been instrumental in laying the foundation for the creation of Bitcoin and shaping my expertise in cryptographic code development and security reviews.

71. As I have explained above, throughout my career, C++ has played a prominent role in various capacities. Although my current work primarily involves Python, because of its efficacy in higher-level tasks, C++ continues to be an integral part of my coding knowledge and skills, underscoring its enduring relevance in my professional career. To give some examples:
 - 71.1 During my tenure with Integyrs, a company specialising in cryptographic code development (which I founded and ran between early 2009 to early 2011), I employed C++ extensively.
 - 71.2 My role as a BDO auditor involved conducting security reviews of code for prominent organizations, including banks, necessitating in-depth exploration of diverse programming languages, including C++.
 - 71.3 I have acquired multiple SANS/GIAC certifications that pertain to both C++ and C#. These certifications have enhanced my proficiency in these languages and equipped me with valuable insights into secure coding practices and advanced programming techniques. For example, I obtained the GIAC Secure Software Programmer .NET (GSSP-.NET) in 2008, which required expertise in developing secure software applications using .NET technologies and the use of Visual Studio programming. I also had a number of other GIAC certifications, including several prestigious GIAC Security Expert (GSE) designations, which are reserved for the most accomplished security practitioners who have demonstrated exceptional skills and knowledge in their field.
 - 71.4 I have coded competitively, entering in a C++ coding competition with the SANS Institute and coming first, third, fourth and seventh; there was no limit to the number of times I could enter.
72. In the period leading up to August 2007, my work on developing the Bitcoin source code was relatively limited. Instead, I primarily engaged in web testing components and experimenting with various test structures. However, as the timeline progressed beyond that point, my focus shifted towards foundational coding and creating a minimum viable product (MVP) prototype. During this stage, I delved into understanding and implementing the fundamental building blocks that would form the foundation of the Bitcoin system.
73. As 2008 unfolded, my attention was directed to determining the specific parameters that would govern the functioning and stability of the Bitcoin network. This crucial phase involved defining essential elements shaping the system's operation. One pivotal aspect was establishing the Genesis block, a momentous step that laid the foundation of the entire blockchain network (which I describe further below).
74. I relied on a user-friendly tool called TortoiseSVN to integrate SVN (a system of version control) with Microsoft Visual Studio. TortoiseSVN seamlessly integrates with Windows Explorer, allowing easy version control operations directly from the file system. At the time I regularly travelled between multiple locations including Lisarow, Bagnoo, and Sydney. SVN allowed me to have my work stored in a single place when I travelled. Additionally, I

found the collaborative features of SVN to be invaluable. It facilitated effortless collaboration with other contributors to the Bitcoin project (such as Gavin Andresen, discussed below), enabling us to work on separate features simultaneously and merge our changes efficiently.

75. To set up the integration, I created a repository on SourceForge (an online collaboration platform for developers), providing a centralised location for the Bitcoin source code. Then, using TortoiseSVN, I checked out the repository on my local machine, creating a working copy of the codebase. This working copy served as the foundation for my development efforts.
76. During the crucial period of 2007 to 2008, while maintaining a full-time position at BDO, I worked on developing the Bitcoin code in parallel. Balancing these commitments required careful time management and unwavering determination. In an average week, I dedicated approximately three hours each day to addressing various issues and challenges related to Bitcoin. However, weekends presented an opportunity for more focused and extended efforts, allowing me to devote around eight to ten hours daily to this ambitious endeavour. These extra hours enabled me to delve deep into the intricacies of Bitcoin, conducting experiments and refining the overall concept behind this revolutionary digital cash system.
77. By early 2008, I had a preliminary version of the code that could be described as a "toy version," allowing me to experiment with running different nodes and testing basic functionalities. At that point, certain crucial features, such as digital signature templates, were not yet integrated. By the end of the first quarter of 2008, I had managed to create a basic version that functioned as a foundation for the future development of Bitcoin.
78. Throughout this journey, I designed the code alone but actively sought input from others to enrich the project. I engaged with individuals under my real identity and Satoshi Nakamoto during the development process to gather valuable perspectives.
79. In early 2008, I discussed the Bitcoin code with Mark Turner, a friend and fellow developer. I communicated with Mark using my real identity, as he was someone I knew personally and trusted. Mark provided candid feedback on the user interface, expressing his honest opinion that he found it "ugly" in its current state. As a result of Mark's input and other similar discussions, I tried to improve the front-end software, considering his expertise in user interface design. Unfortunately, my skills as a front-end designer are limited, and I did not manage to make the front-end as user-friendly as I would have preferred.

Communicating as Satoshi

80. I communicated as Satoshi through two email accounts – satoshin@gmx.com and Anonymous/Vistomail (Satoshi@anonymouspeech.com and Satoshi@vistomail.com, both of which were operated through one account on anonymousspeech.com).
81. The first account I set up was the GMX email account around December 2007. At this stage I did not need web hosting servers, and GMX was a secure email provider. Once the registration was complete, I gained access to the GMX email service, and my assigned GMX

email address allowed me to send and receive emails under the account linked to the pseudonym.

82. I had been using anonymousspeech.com through the handle "Sakura" since 2002 because they offered VPN software and provided online services such as cloud servers (this was before large companies were involved in cloud services). I used it to host gaming sites and other things that I wanted to keep private, and for business activities that I conducted overseas. Vistomail is an email domain used by anonymousspeech.com. In March 2008, I created satoshi@anonymousspeech.com and associated the email address with my anonymousspeech account. I did the same with satoshi@vistomail.com in June 2008. This configuration enabled me to use multiple email aliases while managing all the incoming messages through the primary Vistomail account.
83. In August 2008, I acquired the domain name bitcoin.org through anonymousspeech.com. This purchase marked a milestone in the development and promotion of Bitcoin as the domain name would serve as the primary online platform for disseminating information about the digital token system. Although I posted on the Bitcoin.org forum as Satoshi I did not manage the website. From February 2009 when Martti Malmi approached me volunteering to run the site I allowed others to act as web and forum administrators. I trusted these individuals and anyone that Martti appointed to conduct that role professionally.
84. In addition to the Bitcoin.org forum, I actively engaged in discussions and shared my thoughts on various platforms under the pseudonym Satoshi Nakamoto. This included communication mediums such as IRC (Internet Relay Chat), a popular platform for real-time text-based communication, and SourceForge. Furthermore, I contributed to the cryptography mailing list, a platform for discussing cryptographic protocols and innovations and the P2P Foundation's forum, where I shared insights and updates about the Bitcoin project.
85. Between late 2008 and 2010, I primarily authored content under the Satoshi pseudonym. The demands of Bitcoin's early development, both in intensity and time, left little room for personal writing pursuits. Hence, during this period, my writings were predominantly focused on disseminating and engaging in the discourse around Bitcoin, always through the enigmatic persona of its creator. While posting as Satoshi, I refrained from sharing personal details or expressing political views.

Writing and sharing the White Paper

86. Between March 2007 and May 2008, I began crafting the White Paper by hand, using a pen and paper. The process was iterative as I continuously expanded upon the concepts and ideas related to Bitcoin. I employed a voice recognition program called Dragon. This software allowed me to dictate my thoughts and ideas, so that I could further refine and edit them over time. Voice recognition technology proved valuable, streamlining the process of producing a cohesive and organised version of the White Paper.

87. However, the initial version was more extensive than necessary. In 2007, I shared a preliminary draft with a select group of family members and trusted contacts to garner their feedback. One of the individuals I contacted was my uncle, Don Lynam. At the time, I was studying at Charles Sturt University, I most probably would have sent these communications using my university email account. Don's critique was that the draft was too lengthy and recommended that I make it more concise to enhance its accessibility. I also discussed the paper with my cousin, Max Lynam.
88. The subsequent draft took shape from March to May 2008, setting the foundation for the White Paper as we know it today.
89. In March and May 2008, I also shared a draft of the Bitcoin White Paper with Dave Kleiman, at the time he was my closest friend. Our communication took place via email, Skype and online forums. I had first engaged with Dave on online forums nearly two decades prior, and our relationship had evolved significantly over the years. Dave possessed considerable digital forensics expertise, making him an ideal collaborator for Bitcoin. He diligently reviewed and provided edits to a draft of the White Paper, contributing to its final version. However, Dave was not a programmer and did not interact with code development. I wanted to collaborate with Dave to leverage Bitcoin to develop information security systems superior to the prevalent Supervisory Control and Data Acquisition (SCADA) computer systems. I was, and continue to be, convinced that Bitcoin could be effectively used to bolster IT infrastructure security because of its timestamping and immutable log trail; any alteration would be immediately recorded and known. This usage of Bitcoin was designed to help significantly enhance the security of IT infrastructures. However, I couldn't pursue this project with Dave as he was frequently ill and hospitalised during that time.
90. In around July 2008 I tried to communicate with Tuomas Aura, a computer science professor from Finland. Aura had penned ideas about proof-of-work concepts that later (when updated) shaped the aspects of the consensus system I wanted to implement in Bitcoin. I respected his work and deemed that he could provide valuable input. However, my outreach efforts to him, unfortunately, remained unanswered.
91. In August 2008 I reached out to a small number of individuals, including Wei Dai and Adam Back, by sharing the link to the White Paper via email as Satoshi Nakamoto, most likely using my satoshi@anonymousspeech.com address. I sent them a link to upload.ae where I had uploaded a single draft of the White Paper. It is important to note that while upload.ae is a file-sharing site; it is not technically public, as individuals need a specific link to access the uploaded files. Only a few individuals, including Wei Dai and Adam Back, knew that link.
92. Wei Dai was a distinguished academic who had previously proposed a digital currency concept called B-Money, which profoundly impacted my thinking. His work was highly influential and laid the groundwork for some ideas incorporated into the Bitcoin project. Notably, Wei Dai's contributions were the first that I acknowledged in the White Paper. After I provided him with a copy of the White Paper, he played a significant role in the

development process, guiding me to various signature algorithm libraries, including his secure hash algorithm (SHA-256), which I successfully incorporated into the Bitcoin codebase.

93. Adam Back was known for his work on Hashcash (a proof-of-work algorithm different to that in bitcoin which he had proposed to combat email spam). He showed little interest in Bitcoin. His attitude was quite dismissive; he stated that digital cash had been attempted before and was bound to fail. At the time, I did not understand he was pointing at issues associated with creating a cryptocurrency and not digital cash.
94. Contrary to popular belief, Bitcoin's proof-of-work system does not utilise Adam Back's Hashcash system. Instead, it more closely aligns with the methodologies described in Aura's paper. Due to Aura's lack of response, I felt it necessary to reference Adam Back in the Bitcoin White Paper due to the thematic parallels in our work and Back's notable presence in the field.
95. While developing the concepts for Bitcoin, I was pursuing a Master's degree in Statistics (MStat) at Newcastle University in Australia, which I had begun in 2005. I proposed to focus my postgraduate dissertation on the statistical and graph theoretic aspects of Bitcoin, hoping to explore its underlying structure and mechanics in more depth. Ultimately, I had to divert my focus and write my dissertation on Levine's theory instead.
96. I presented the concepts I was working on to Microsoft and CentreBet. This was done under my name (for this, I was not using the Satoshi pseudonym). However, my proposals were met with a general lack of interest. I implemented the core of the system within Hoyts in Australia, a digital cinema chain and attempted to promote the ideas with other organisations including QSCU, now original bank.
97. Around October 2008, I handed over a draft of the White Paper to Stefan Matthews, who was serving as the Chief Information Officer at CentreBet at that time. If memory serves me right, I left a printed copy of the draft on his desk. Given his role at a betting platform, I hoped Stefan would recognise the potential of Bitcoin and its underlying blockchain technology, particularly how a tokenised payment system could enhance and diversify the customer payment options at CentreBet.
98. In the autumn of 2008, I attended a series of business meetings at the Microsoft campus in Seattle. The specific names from those events have become hazy with time. These meetings took place before the launch of Bitcoin. My interest then revolved around Microsoft developing a commercialised internet platform, with integrated micropayments; a vision starkly different from the advertisement-based model that Microsoft Bing eventually adopted. I envisioned Microsoft operating Bitcoin at scale, pushing it into the mainstream. Microsoft demonstrated interest in this proposition; we deliberated over a role where I would receive stock options, and they would gain access to my intellectual property.

99. However, the unfolding financial crisis derailed these discussions, ending them abruptly. Realising that collaboration with Microsoft wasn't in the cards, I decided to take matters into my own hands and launch Bitcoin independently.

Publication of the White Paper

100. On the 31st of October 2008, operating under the pseudonym Satoshi, I made a post on the cryptography mailing list hosted on metzdowd.com. The post announced that I had been working on a novel peer-to-peer electronic cash system without needing a trusted third party. Included in this announcement was a link to the White Paper, which had been uploaded to Bitcoin.org, the domain name I had registered two months prior. This was the first instance of the White Paper being shared on a public forum. By the time I uploaded the White Paper, the essential elements of the code were already in place, with subsequent modifications being largely tweaks to the existing structure. I decided to share the White Paper on the cryptography mailing list because I knew it was a community of individuals who would likely engage with and appreciate the concept. I had been a subscriber of this mailing list for over two decades and actively contributed to it under my name and various pseudonyms. This platform had previously been the venue for discussions on similar ideas, such as public key identification systems, digital token systems, and digital signing and security principles. It seemed the appropriate forum to introduce the concepts I had developed in the White Paper.
101. During the 90s and early 2000s, I was also actively engaged in the CypherPunk mailing list. This community was a collection of individuals who shared an interest in privacy, cryptography, and using these tools to effect social and political change.¹ In this post, I adopted a Japanese pseudonym, a common practice for me then.
102. In addition to the CypherPunk mailing list, I used these pseudonyms on other platforms, including USENET and IRC networks such as Freenode and EfNet. These platforms, like the mailing lists, were vital spaces for discussions on various topics related to cryptography, digital security, and privacy.
103. The initial reaction to the White Paper was primarily marked by indifference. The majority seemed to dismiss or overlook the idea, a fact that I was largely unperturbed by. However, some individuals were concerned that governmental authorities would inevitably co-opt Bitcoin. This sentiment was a source of frustration for me, as the fundamental premise of Bitcoin was to reduce reliance on central authorities, not to eliminate their presence or relevance. Moreover, the anti-government sentiment was not part of my design for releasing Bitcoin.
104. I envisaged Bitcoin evolving into a commercial system with the underlying infrastructure ultimately hosted in data centres and administered by corporations. It was not about every individual running a node but about a more efficient and decentralised model of financial

¹ One of my posts from 1996 can be found at: <http://cypherpunks.venona.com/date/1996/09/msg01445.html>.

transactions. The misinterpretation and distortion of the concept of 'decentralisation' became a recurrent source of frustration for me.

105. Among those who did engage with the concept, Hal Finney was notably supportive. He had been an influential figure in developing cryptography and security. It's worth noting that our communications occurred exclusively under the Satoshi Nakamoto pseudonym; he only knew me as Satoshi. While our exchanges were not extensive, his contributions were quite beneficial. He expressed his interest through an email and later assisted with certain aspects of the code, as I will elaborate on later. A software developer, Mike Hearn, also shared his thoughts and feedback on the project. These early adopters played a crucial role in the nascent stages of Bitcoin, providing invaluable insights and contributions.
106. Following the initial announcement, I uploaded the Bitcoin White Paper on SourceForge, an online platform I frequently used for open-source projects. I made minor adjustments to the White Paper over time, between October 2008 to March 2009 updating and uploading new versions as needed. However, these modifications were not particularly substantive and didn't alter the underlying principles or core design of Bitcoin.

Creation of the Genesis Block

107. On 4 January 2009 (UTC), I created the Genesis Block. Understanding that the Genesis Block holds a distinct position compared to the other blocks in the Bitcoin Blockchain is crucial. It's not a conventional block; instead, it serves as an anchor, a definitive starting point for the Bitcoin Blockchain. Contrary to popular misconception, no public or private key is associated with the Genesis Block. Furthermore, the Genesis Block was not the result of mining, nor was it part of any transaction involving Bitcoin being spent, and it was not designed to be spendable.
108. The Bitcoin code inherently requires the Genesis Block for its operation. Without the Genesis Block, there would be no Bitcoin. I manually crafted the Genesis Block and directly integrated the data into the Bitcoin code, essentially hardcoding it into the system (as opposed to mining it).
109. Ensuring that the Genesis Block was timestamped was a matter of great significance. The primary objective was establishing a definitive and undeniable timestamp indicating the moment the Bitcoin Blockchain was created. This concept is underscored in the Bitcoin White Paper.
110. I timestamped the Genesis Block using the headline of an article published in The Times on 3 January 2009. The headline read: "Chancellor on the brink of second bailout for banks." At that time, I was studying for an LLM at Northumbria University, which granted me complimentary access to The Times through the university's portal. I was a frequent reader of The Times then and continue to be so.
111. The headline was particularly interesting because it reflected a policy by Alistair Darling, the UK Chancellor at the time, that I vehemently disagreed with. He advocated for the partial nationalisation of certain struggling banks, a policy that starkly contradicted my

political beliefs, which I continue to uphold. While there was no direct correlation between the concepts underlying Bitcoin and the article, the headline's incorporation into the Genesis Block was my way of expressing objection to the political philosophy it embodied.

Uploading of the Bitcoin software and source code

112. On 9 January 2009, I uploaded an executable file and the corresponding source code to SourceForge. This version, v.0.1 Alpha, was the first iteration of Bitcoin I released to the public. Concurrently, I disseminated a link to the SourceForge Bitcoin Project's relevant section on the Cryptography Mailing List.
113. On SourceForge, I maintained two accounts under the Satoshi Nakamoto pseudonym: a user account and an administrator account (I cannot remember which was which). The separation of privileges between the two accounts was delineated. SourceForge was a reliable platform for distributing code, providing the capabilities to monitor and track different versions, ensuring proper management and version control.
114. Hal Finney (who, as I have explained above), had seen a draft of the White Paper in August 2008) was one of the key individuals who offered valuable early feedback. He approached me via email to provide his insights. For instance, due to the software, I was running for my work, I incorporated certain dynamic link libraries (DLLs) into the code. Hal alerted me that the Bitcoin software would crash for users lacking these DLLs. I hadn't initially considered this, and I appreciated his input.

The mining of Block 1 and the first Bitcoin transaction

115. Mining Bitcoin is an intensive process that demands substantial electricity consumption and incurs significant costs. In the early days, the only individuals engaged in mining were myself and my family, specifically my uncle, Don Lynam, and my cousin, Max Lynam. Starting from January 2009, they began operating a node from Don's farm.
116. I was concurrently conducting my mining operations, using numerous computer systems I had arranged in 69 racks at my residence in Australia, all networked within a Windows domain environment. I also utilised a computer that I charitably donated to a local church I was also operating from 3 laptops and 4 desktop systems in Tumby Umbi. The overall setup was extensive, allowing me to carry out robust operations which linked to the client systems I was experimenting on (e.g., CentreBet). These aided in furthering my Bitcoin node management pursuits.
117. The considerable electricity consumption associated with Bitcoin mining represented a significant expense for me, amounting to thousands of Australian dollars. It's important to note that my motivation for mining Bitcoin was not for financial gain; indeed, during its early stages, Bitcoin had no market value, and the cost of mining far outweighed any return. Instead, my primary incentive was to bring the Bitcoin system to life and set the Bitcoin Blockchain in motion. This endeavour was more about creating and establishing the digital cash system than reaping immediate financial benefits.

118. At the outset, I never envisaged that Bitcoin would gain the enormous value it holds today. Instead, my primary assumption was that the companies I would construct using the Bitcoin framework would garner significant worth. My plan was never merely to launch Bitcoin and accumulate wealth from its success. Instead, my vision was to create a platform that could be monetized through the development of businesses around it, particularly those that would benefit from the application of micropayments. By being an early adopter of my system, I hoped to gain a competitive edge over other enterprises.
119. In alignment with this vision, the company I collaborate with today, nChain, doesn't derive its value directly from Bitcoin. Instead, it's worth is tied to a comprehensive portfolio of blockchain technologies, showcasing the initial concept's versatility and expansive potential beyond just Bitcoin itself.
120. In the early days of Bitcoin my focus was on the technical and conceptual foundations of Bitcoin, the potential not on marketing or promotion. I am a technologist and a scientist, not a marketing professional. My goal was to advance the functionality and potential applications of Bitcoin rather than to promote Bitcoin as a trading system and foster its use as a transformative technology. My focus was predominantly on the technical aspects and the of Bitcoin as a technology, rather than its potential as an asset or a speculative investment. I saw Bitcoin as a tool that could be woven into the fabric of digital systems to enhance their security, efficiency, and potential for innovation. I urged individuals to run nodes, which inherently involves mining, but my intent was not to promote Bitcoin as a financial asset. Rather, my interest was in the underlying technology, its potential to revolutionize various industries, and its capabilities to provide secure solutions in a world increasingly reliant on digital technologies. The conversations I had revolved around the system itself, its potential applications, and what it could achieve in terms of security and efficiencies, not on its potential monetary gains.
121. In the early days of Bitcoin (around 2009 to 2010), my actions were primarily driven by the desire to initiate use and adoption of the technology, not by a pursuit of financial gain. For example, on 12 January 2009, the inaugural Bitcoin transaction occurred when I transferred Bitcoin from Block 9 to Hal Finney. This was not meant as an economic exchange because Bitcoin held no tangible value at the time; it was a practical demonstration of the system in action. Hal and I had been in continuous dialogue since around October 2008, predominantly through email, and he was actively exploring the system. Moreover, my transfers of Bitcoin to other key figures in the early Bitcoin community like Mike Hearn, and Gavin Andresen were freely done, without any associated cost. My transactions with the Russian "WebMoney" exchange in 2011 were also undertaken with the goal of encouraging utilization of Bitcoin rather than personal monetary benefit. These actions were taken to foster the usage and understanding of Bitcoin.

After the release of the White Paper (2009-2011)

Discussions with third parties

122. After the Bitcoin code was uploaded in early 2009, I continued discussions with third parties on potential commercial applications of Bitcoin.
123. As I have mentioned above, I provided Stefan Matthews (Chief Information Officer of CentreBet) with a draft of the White Paper in 2008. After that point, I engaged in multiple discussions with him and Shane Patterson, who was his deputy at the time. Our conversations were centred around the potential use cases of Bitcoin within the framework of CentreBet. We delved into possibilities ranging from fortifying their logging system to enabling customers to make tokenised small-scale gaming payments. In early 2009 I proposed a unique system that embodied the principles of a peer-to-peer (P2P) overlay and a blockchain. I worked on this over several months, culminating in a proposal that I authored dated 13 April 2009 [ID_004537]. The system was built upon intellectual property I had initially created for Vodafone (as explained above) and later updated for Lassater's (as explained above). The technology represented an advancement in distributed consensus mechanisms and P2P networks, extending the fundamental structure and operation of the Bitcoin system. However, despite my best efforts, I couldn't quite convince CentreBet of the potential of Bitcoin.
124. Around August 2009, to demonstrate that Bitcoin had monetary value, I offered Stefan Matthews 50,000 Bitcoin for A\$100. I did try to get less when he said no. However, Stefan chose not to proceed with the transaction.
125. Around the same time, I also contacted a few individuals associated with the IT department of Pornhub, the adult entertainment website. I acquainted with these individuals through the SANS Institute, a prominent global organization dedicated to information security.
126. My conversation with PornHub revolved around pitching the concept of Bitcoin. I was convinced that a subscription-based service model, underpinned by micropayments, could significantly benefit their operations. I also hypothesised that Bitcoin could bolster its information security, ensuring its customers weren't vulnerable to malware attacks. However, my proposal did not pique their interest. Despite my attempts at persuasion, they remained committed to their existing free, advertisement-driven business model and showed no inclination towards adopting a system for digital payments. My communications were facilitated through my email address affiliated with Integry's, one of my companies at that time (I remember this because I used that company for projects relating to code, as opposed to work using servers).

Moving away from communicating as Satoshi Nakamoto and administering Bitcoin

127. Around April 2011, I began to phase out my communications under the pseudonym Satoshi Nakamoto. By this time, the Bitcoin system had been successfully established and was functioning autonomously. With the framework in place, I felt it was time to divert my attention to other pursuits. Specifically, I founded a company named Panoptcrypt Pty Ltd, a term translating to "everything hidden in the open". My focus shifted towards this venture, dedicating myself to creating and developing innovative technological solutions.

128. Other personal reasons influenced my decision to withdraw as Satoshi Nakamoto, chief among them being an ongoing investigation by the Australian Tax Office (ATO). While the ATO had scrutinised me for some time, the particular investigation that troubled me in 2011 had begun around August 2009 (and extended into a full review in August 2010), when the tax office started issuing payment demands. While the initial review of my GST filing had occurred in July 2009, it was not until the following year, in 2010, that the ATO started aggressively pursuing an audit.
129. The escalating pressure from the ATO was not without its toll. By September 2010, my first marriage was teetering on the edge due to the mounting strain these issues placed on us. Come October 2010; although we were technically still married, we had unofficially separated and cohabited in the same house. By December 2010, the ATO audit had progressed into the initial stages of litigation.
130. Between August 2010 and August 2011, I worked closely with John Chesher, an accountant, and Andrew Sommer, a tax lawyer, to navigate and resolve these complex issues. However, the new year also brought about changes on the home front. In January 2011, my wife and I had officially and publicly separated, and I had moved out of the house by February 2011. These circumstances consumed much of my time and focus, thus catalysing my decision to move away from my Satoshi Nakamoto persona.
131. During my time as Satoshi, I made it clear to the Bitcoin community that the protocol, as defined in the White Paper, was designed to be unchanging, solidifying its principles and functionality. I publicly stated that the Bitcoin protocol is to be 'set in stone'. There is a distinction between protocols (such as TCP/IP) which do not change, and the code, which can be amended over time. The task ahead for Bitcoin was not to alter or modify the protocol but to ensure its careful stewardship and enable its scaling. I decided to delegate this responsibility to Gavin Andresen, a respected Bitcoin community member at that time. My choice of Gavin was based on my perception of his dedication and genuine interest in the project. It's important to note that my communications with Gavin during this time were carried out under the Satoshi pseudonym, and he was unaware of my true identity.
132. In October 2010, I sent Gavin Andresen a file containing the network alert key. Gavin understood he was in charge of this by April 2011. This key serves as a means to set all nodes on the network into 'debug' mode. The owner of the network alert key can leverage it to halt transactions or broadcast an alert to every user on the network. For instance, an alert could mandate an update or prevent the transmission of a specific block. The network alert key existed as an electronic file; I made a copy of it and forwarded it to Gavin via email.
133. Around the same time, I also granted Gavin access to the Bitcoin code on SourceForge. However, I assigned him a lower-level admin key to retain control over the project. This decision was intended to allow me to maintain ultimate control and oversight of the development process while delegating responsibilities and collaborating with Gavin to advance the Bitcoin project. This arrangement balanced shared involvement and maintained the final say in critical decisions, ensuring the project's continuity and long-

term vision. While I had many problems to address first, I had initially maintained access to the site so that I could return later when everything was sorted.

134. During the summer of 2011, I found myself disappointed by subsequent events. Martti Malmi, who was operating as an unofficial web server administrator for me, oversaw the day to day running and updates to the Bitcoin.org website and the associated forum, bitcoin.org/forum. In around June or July of 2011, Martti took down the bitcoin.org server and initiated a new server with the URL bitcointalk.org, over which I had no administrative rights.
135. My forum posts, made as Satoshi, were transferred to this new server, although some were left out, and Martti guided everyone to this new location. On inspecting this new server, I found that certain posts I had made were missing. I only discovered this towards the end of 2013, as I had not been monitoring closely.
136. Around the same period, the reins of the Bitcoin project began to shift further away from me. Wladimir van der Laan (one of the defendants in the BTC Core Claim) and Gavin Andresen transferred the Bitcoin code from SourceForge, where I had initially hosted it, to GitHub. This move wasn't merely a change in hosting platforms; it bore significant implications for the governance and trajectory of the project. Unlike SourceForge, GitHub utilises a different version control system named Git, which emphasises distributed control by granting multiple users comprehensive control over the code. This transition meant that when the core developers migrated the Bitcoin codebase to GitHub, they effectively assumed control of the project.
137. The period after I left day to day oversight of the project, assigning Gavin to steward this for me marked a new chapter in Bitcoin's history where my direct influence started to diminish, and other developers stepped into leadership roles, steering the system's future development and protocol amendments.

The encryption of the hard drive and the splitting of the AES key

138. As noted previously, in August 2010, the ATO launched an investigation against me, which continued until March 2013, when I won my case in the Administrative Appeals Tribunal. By August 2011, the investigation had proceeded into a full audit and litigation. Although I had been subject to investigations by the ATO in the past, this time, I had serious concerns that they would attempt to seize all my assets, including my intellectual property.
139. In response to these concerns, and after I began dating my current wife, Ramona, in 2011, I decided to safeguard my assets by placing them into a trust. These assets included the rights to the Bitcoin that my companies had mined since 2009. I took this measure to ensure that under no circumstances could the ATO seize that Bitcoin if my dispute with them led to bankruptcy proceedings against me.
140. Alongside this, I placed a significant volume of data beyond my direct control. This included many terabytes of my research data and notes on all of my intellectual property, and also the means of accessing the Bitcoin that I had mined.

141. I stored all this information on a hard drive many terabytes of my research data, was encrypted using the Advanced Encryption Standard (AES) with a 256-bit key. In an additional layer of security, I divided the AES key into 15 separate 'slices' which could be used to recreate the key using a process called a Shamir secret sharing scheme.
142. Some of the slices I kept in my possession, although I cannot remember exactly how many. I entrusted the remaining slices to individuals whom I considered reliable, such as Dave Kleiman, Denis Mayaka (my legal representative at that period and a trustee of my trust), Uyen Nguyen (a former intern), and several corporate agents who were associated with the trust in various roles, but whom I did not know personally.
143. A minimum of eight slices were required to recreate the AES key, decrypt the hard drive, and gain access to the deterministic algorithm (which would then enable the decryption and retrieval of the algorithms necessary to regenerate the private keys). This number was more than the quantity I had kept for myself.

Other events in 2011 – 2014

144. From 2011 to 2014, my primary focus shifted towards conducting the research I had envisioned all of which related to Bitcoin. My role as the CEO of a group of companies and as the chief researcher allowed me to invest my time towards various projects associated with scaling Bitcoin and creating identity systems. I closed operations under Information Defense and established additional companies to cater to distinct research undertakings, such as Panopticypt and Hotwire PE.
145. One of my key projects during this time was the creation of a supercomputer in a Panamanian data centre. I established this at the end of 2012, followed by a second one in 2014. This computational behemoth handled complex calculations and simulations associated with my research interests in testing the scaling of Bitcoin. Another pivotal project involved designing scalable node systems connected to Distributed Hash Table (DHT)-based storage and identity solutions. This was intended to investigate the capabilities of decentralised systems at large scales.
146. iDaemon (now renamed Terranode) was another critical project I developed during this period. This experimental scaling solution was designed to test the scalability of Bitcoin, probing its ability to handle millions of transactions per second. This was fundamental in understanding the true potential of Bitcoin and its adaptability to growing transaction volumes.
147. By 2013/14, I was responsible for around 50 staff members across my companies. The fluctuating nature of my income and the responsibility of payroll for a sizeable team presented some logistical issues regarding payments. Nonetheless, I continued my vision, working tirelessly to progress in my research and business ventures.
148. Starting in 2011, I also redirected a significant portion of my time back towards personal writing. I authored numerous articles under my actual name, Craig Wright, and published them on various platforms, elucidating my insights and perspectives. These compositions

delved into a broad spectrum of subjects, including Bitcoin's potential as a micropayment system and time-stamped ledger, its capacity to underpin digital currency systems, including financial derivatives and central bank digital currencies, and many other topics.

2014 – 2015: Rob MacGregor

149. As mentioned earlier, Stefan Matthews has been privy to my work on Bitcoin since 2008. In 2014, I contacted Stefan via email and phone, informing him about my various business ventures. Given his significant expertise, I intended to contact Stefan to explore potential investment avenues. We engaged in multiple discussions throughout 2014 and the early part of 2015, focusing on the business models and research undertakings of my companies. In parallel I engaged in discussions with Macquarie Bank.
150. My portfolio of companies was founded on the premise of leveraging blockchain technology and the global scalability of Bitcoin. These firms were deeply involved in several research projects registered with the Australian Tax Office and AusIndustry.
151. In 2014, Stefan introduced me to Rob MacGregor, who was operating a company named nTrust and brought extensive experience within the gambling industry and considerable expertise in navigating governmental channels. Our initial discussions centred around his potential investment in my business. While our initial negotiations did not materialize into an investment, Stefan reconnected us in 2015. At this time, Rob MacGregor had already been actively involved in Bitcoin, blockchain, and digital currency projects, primarily focusing on remittance solutions. Despite these initiatives, his company was struggling to successfully implement scalable solutions that were effective and functional.
152. Rob initially lacked enthusiasm for our work at my companies, but our dialogue was rekindled in 2015 as he began showing a more profound interest and engagement in our projects. In June 2015, he decided to visit us in Australia for a face-to-face meeting. During his visit, he invested considerable time in our office, conducting thorough due diligence and familiarizing himself with the various facets of our operations.
153. On 29 June 2015, I (on behalf on DeMorgan) entered into an agreement with Stefan Matthews' company, Sterling. From my perspective, this agreement aimed for DeMorgan to receive funding for its research projects and tax obligations, along with access to legal counsel and assistance in dealing with the ATO. In return, Rob MacGregor would gain access to my extensive collection of intellectual property.
154. I thought we would leverage this intellectual property to foster a platform for ongoing innovation and progress in the blockchain domain. This platform would be constructed on the solid foundation of existing intellectual property, which I or my enterprises had developed. In the period 2008-2014, my companies had generated many white papers, which detailed and documented a broad array of ideas I had been exploring and experimenting with. This intellectual treasure trove encompassed everything from bank settlement systems and central bank digital currency systems to identity systems and intellectual property around the scaling of Bitcoin.

155. Although the term sheet mentioned the rights to my life story, I understood two things about this. First, from my perspective, the deal wasn't solely focused on the narrative of Satoshi. Instead, we would delve into my entire life journey, including my academic research and the story behind the establishment of the nChain Group, which was to become a prominent intellectual property powerhouse with thousands of patents. The idea of the story would be to showcase the breadth of accomplishments and the enduring legacy of nChain as a driving force behind pioneering technological advancements through its extensive patent portfolio.
156. Second, I understood that any revelation of my background as Satoshi would be kept confidential until after nChain's patents had been filed and the company had become stable, which would take several years. I had understood that the focus would be on launching and building the company, allowing nChain to grow and establish itself as a significant intellectual property centre. The decision to keep my identity private was driven by the desire to avoid unnecessary distractions and ensure the success of nChain as a transformative technology company.
157. My understanding was that Stefan, whom I had shared my life story with, was the one who revealed my identity to Rob. I do not know exactly when Rob found out, but it must have been in the period between June and October 2015. While I knew that Stefan had informed Rob about my background, I did not understand or see the outcome where that would result in my immediate revelation as Satoshi.
158. In July 2015, my family and I decided in principle to move out of Australia so that I could work to set up nChain. We began considering different locations and, by September 2015, we had settled on moving to London. I frequently travelled back and forth between England and Australia, assisting with the necessary arrangements for the corporate transition.
159. In October 2015, we had started moving to London and I had completed the process to obtain residency. Rob's company, The Workshop, played a crucial role in handling the logistical aspects of the relocation and facilitating the smooth transition. They organised the packing and shipping of our furniture, ensuring that our belongings safely made their way from one continent to another. Additionally, they expertly managed all the necessary procedures related to visas and immigration, enabling our entry into the United Kingdom. The assistance provided by The Workshop during this transitional period was invaluable and alleviated much of the stress associated with such a significant life change.
160. The relocation to London began a complex dynamic between Rob and me. Looking back, I realise that our arrangements inadvertently granted Rob significant influence over our lives. His company's involvement in handling the logistics of our move created a sense of dependence on his decisions and actions.

The Wired/Gizmodo articles

161. Between November and early December 2015, I faced inquiries from reporters at Wired and Gizmodo concerning my identity as Satoshi Nakamoto, which I tried not to engage with at all. To my concern, it became apparent that my identity had been leaked to them.
162. The unexpected disclosure of my identity as Satoshi Nakamoto had unintended consequences, drawing public attention and speculation. This turn of events was not part of the initial agreement or my vision for the company's launch. My primary intention was to remain in the background and contribute to the growth and success of nChain without the burden of public attention.
163. In the face of the media inquiries and the leak of my identity, Rob MacGregor, whose judgment I trusted, advised me to maintain silence and refrain from responding to the reporters. He instructed me that this approach could potentially dissuade them from publishing the information. Recognising Rob's experience and insight, I followed his counsel and remained silent during that critical period.
164. By heeding Rob's advice, I sought to mitigate any further escalation of the situation and avoid inadvertently fuelling the media's interest. Keeping a low profile during this time allowed me to focus on the development of nChain and continue my contributions to the technological landscape. I now regret doing this.
165. As rumours began circulating that Wired intended to reveal my identity as Satoshi Nakamoto using material from my blog. I took immediate action to safeguard my privacy. I did not personally manage blogs, websites, or other media, but I asked members of my team (including Uyen Nguyen, Ray Hoang and Viveca Magnusson) to remove all content from the blog and ensure that it was no longer available to the public. This step was taken to prevent any potential misinterpretation or manipulation of the blog's contents and to shield myself from unwanted press attention., I also directed my team to delete all my personal information from other public websites such as Blogger and DeMorgan corporate site. I aimed to preserve my privacy and protect the overall integrity of my work.
166. On 9 December 2015, Wired and Gizmodo published their stories about my identity as Satoshi Nakamoto. The timing was particularly challenging as the news broke amid our ongoing efforts to establish nChain. The publication of these stories shattered my privacy, and the information spread rapidly across the globe, attracting widespread attention and speculation.
167. The intrusion into my private life and the subsequent public revelation of my identity as Satoshi Nakamoto left me feeling violated and deeply pained. It was a stark reminder of the vulnerability of our privacy and how easily it can be stripped away, subjecting our personal lives to global scrutiny. The experience had a lasting impact on me.
168. I never intended to reveal myself as Satoshi in such a manner, and I do not recall that I engaged with the enquiries from the journalists involved in the stories published by Wired and Gizmodo other than to briefly and tersely respond to Wired's phone call before promptly ending the conversation. As a result, significant portions of their articles were untrue, particularly concerning my tax affairs and the portrayal of Dave Kleiman's role.

169. The inaccurate portrayal of my tax affairs and the involvement of Dave Kleiman in the media's narrative only added to the distress caused by the disclosure of false information. These misrepresentations further underscored the challenges of managing public perception and the potential consequences of misinformation in the digital age.
170. Initially, my instinct was to pursue legal action against the misrepresentations and false narratives propagated by the media. However, Rob MacGregor, whom I trusted and sought advice from, advised me against legal action. Believing in his judgment, I followed his counsel, hoping it would be a path to preserve my privacy and protect my reputation. Again, I now regret this.
171. Shortly after the Wired article was published, Greg Maxwell (one of the defendants in the BTC Core Claim) issued a swift and vigorous rebuttal, alleging various inaccuracies and accusing me of being a fraud.

The events of early 2016

172. I first made acquaintance with writer Andrew O'Hagan either in December 2015 or January 2016 – I cannot recall the exact date. Our meeting occurred after I had relocated to the UK. At that point in time, my understanding was that Andrew's primary task would be to chronicle the evolution of nChain, the unfolding of our ambitious scaling project, and the process of accumulating our extensive collection of patents. To date, we have amassed a substantial portfolio, encompassing nearly 4,000 patent filings, which are the fruit of my prior research.
173. In O'Hagan, I saw a partner who could capture the intricate nature of our work over an extended time frame. I anticipated we would collaborate for the long haul, spanning five to ten years. I had already conceptualised over a thousand systems earmarked for development, each delineated in dedicated white papers. These systems spanned an array of areas, including solutions for the Internet of Things (IoT), Supervisory Control and Data Acquisition (SCADA), identity management, and the scalability of Bitcoin, the last of which is substantiated by the research behind iDaemon (which I have mentioned above).
174. Between December 2015 and March 2016, I found myself in a state of profound discontent. Despite the controversy and public scrutiny, I remained silent and refrained from making public statements responding to the articles. Concurrently, Rob altered his strategy. After the journalists revealed my identity and, in a scenario, where my vulnerability could be exploited, Rob overtly attempted to profit from my story. Numerous disputes between us marked this period. I harboured no intention of being commoditized and sold to tech giants like Google or Facebook, and I felt that my life's narrative didn't conform to the story Rob aimed to portray.
175. Success, in my perspective, was not solely a measure of monetary gains. I perceived that to be the prevailing mentality in Silicon Valley. This mindset seemed prevalent within the kind of corporations Rob desired to engage with, which trivialised the importance of human privacy and regarded individuals as mere commodities. This was a philosophy that I had always sought to dismantle. My principled commitment to privacy, personal agency,

and dignity served as crucial motivations behind the development of Bitcoin. I held faith in Bitcoin's potential to democratize and liberate individuals and opposed the idea of it being monopolized by a select few for their personal advantage.

176. My suspicions about Rob engaging in covert dealings intensified, as Rob made promises and did not keep them and pressured me into signing sessions. As time went on, it became evident that Rob's control extended far beyond our business relationship and the practical aspects of our relocation to London (which I have described above). My family's reliance on his company for various essential tasks gave him significant sway over our affairs. I began to feel beholden to his decisions, and this sense of dependence raised concerns about potential imbalances in our working relationship. The power dynamics that emerged after our move to London were complex, with Rob holding sway over me and my family.
177. Taking these events together with the increasing public attention on me, the first half of 2016 marked a period of immense stress and uncertainty in my life.

Private demonstration sessions

178. Ramona and I were asked to sign a range of legal agreements in relation to nChain at Rob's instigation. I did not carefully review each of these agreements. In hindsight, we should have insisted on more time to review the documents and sought independent legal counsel. Yet, given the power dynamics between my family and Rob, the daunting extent of the paperwork, and the lack of alternative courses of action, I felt obliged to accede to Rob's demands.
179. I was told that the primary objective of the legal agreements in this period was to guarantee the protection of the valuable assets associated with the Bitcoin project, safeguarding them from potential exploitation or misappropriation. I understood that these measures would enable us to establish nChain, facilitate relocating my businesses from Australia, and restructure them. This restructuring would allow me to continue working on and filing my patents.
180. I didn't perceive myself as committing to a formal 'reveal' process. I had already been 'unveiled' in the Wired and Gizmodo articles from December 2015. My main focus was rectifying the misrepresentations, given that the 'unveiling' hadn't been executed correctly. From their publication, I was acutely aware of the inaccuracies in the Wired and Gizmodo articles.
181. As I have explained above, I understood that relying on 'CypherPunk' methods, such as using cryptographic keys, was insufficient to prove my identity. Simply possessing a private key does not equate to verifying one's identity. Instead, I intended to employ various traditional means to demonstrate my qualifications and involvement in Bitcoin's creation. The use of verifiable data and evidence was the best way to counter the misrepresentations made by Wired and Gizmodo and to preserve the integrity of my contributions.

182. During this period, I engaged in several discussions with Stefan Matthews, Rob MacGregor, and Andrew O'Hagan, during which I permitted them to examine material related to my identity as Satoshi. While I provided some information via email, I presented most of these materials in person.
183. By March 2016, Rob MacGregor urged me to participate in private demonstration sessions with several individuals, insisting it was necessary. As I have explained at above a digital signature operation yields a unique piece of data using an elliptic curve digital signature algorithm (ECDSA). However, in the absence of proof of identity, the process only verifies that the individual has physical possession of the private key associated with a specific public key. Rooted in my beliefs about digital currency and its relationship with the rule of law is the notion that a private key should not be used as proof of ownership or identity.
184. Nevertheless, I finally agreed to perform a signature process in several private sessions due to the immense pressure I was under, and the promises Rob MacGregor had made to me. These promises included comprehensively resolving my tax situation with the ATO, arising from their most recent audit of my companies operationalising nChain, and publicly rectifying the false narratives about me propagated by Wired, and Gizmodo. Crucially, alongside the private demonstrations, Rob promised I could verify my identity through conventional methods, such as linking the company accounting systems, information associated with individuals that knew me at the time, my history with the project and related information such as citing my academic qualifications and providing a biographical account. This was far more important to me than any technical demonstration.
185. Around half a dozen private demonstrations took place between March and April 2016. The attendees varied in each session but commonly included individuals like Stefan Matthews, Rob MacGregor, and Andrew O'Hagan. During each demonstration, I used private keys associated with the earliest blocks my companies mined back in 2009. I consistently used the key from Block 9 across all sessions, coupled with varying keys associated with Blocks 1 through 11.

Re-assembling the AES key.

186. As I explained above I had encrypted the hard drive containing the keys for all of the blocks mined by me including Blocks 1 through 11. Before conducting this process, at least eight of the fifteen key slices needed to be reassembled.
187. I therefore reassembled the slices of the AES key from some of the individuals who had held slices. I then decrypted my hard drive, so that I was able to reconstitute the private keys to Blocks 1-11. I also obtained authorisation from the trust to carry out the digital signature process.

Andrew O'Hagan

188. Around early March 2016, I performed two private demonstrations for Andrew O'Hagan, during which I used the private key from one of the original blocks. The intention behind

this demonstration was to replicate what I had planned for later sessions with Jon Matonis and Gavin Andresen.

189. The first took place in an apartment near Soho where Ramona and I were staying. I am not certain whether O'Hagan fully comprehended the process during this initial demonstration. The second took place at my home in Wimbledon.
190. During these demonstrations, I requested O'Hagan to choose a number between 1 and 11. I don't recall the specific numbers he selected; however, I remember he chose different ones each time. I showed O'Hagan a message from the first address created after the hard-coded Genesis Block during the demonstration.

Jon Matonis

191. I had previously encountered Jon Matonis, who had been the head of the Bitcoin Foundation until December 2014, at a conference in Australia in 2014 where we had a coffee. I had not told him that I was Satoshi, but we talked about Bitcoin and how it worked.
192. Around April 2016 we convened in London in a hotel in Covent Garden. Rob had arranged this. We reminisced about the early days of Bitcoin, discussed my contribution to Bitcoin's development, and delved into the operations of the Bitcoin Foundation. The meeting was quite cordial, and Jon was pleased to see me. He mentioned that, after our meeting in 2014, he had confided to his wife that he had just met Satoshi Nakamoto.
193. Following our discussion, I used a digital signature algorithm to show Jon that I possessed the private keys linked to two early blocks, which are possibly Blocks 9 and 11, though I did not choose the keys.

Gavin Andresen

194. The arrangement for the meeting with Gavin Andresen was primarily handled by Stefan Matthews, who facilitated our email exchanges. While I was aware of some discussions surrounding this meeting, I wasn't privy to all the details. As I explain above, I had corresponded with Gavin Andresen as Satoshi in the period 2009-2011.
195. Before our meeting, Gavin reached out via email, expressing his desire to discuss "technical stuff." He suggested conducting this conversation over email, which he felt would give him a sense of whether our interaction mirrored his communications with Satoshi back in 2010. I respected Gavin's approach, as it aligned with my understanding of the multifaceted nature of digital identity and security.
196. To satisfy Gavin's request, I demonstrated various writing styles I had used as Satoshi, addressing topics I remembered discussing as these would help him recognise me as Satoshi. I articulated my desire for people not to see me as an unquestionable authority figure but to appreciate me for my scientific contributions. Following our email exchange, Gavin wanted to travel to London.

197. Gavin arrived in London in early April 2016, and we met in a private room at a central London hotel – I think it was the same hotel as I had met Jon. Both Rob and Stefan were present during this meeting. It was a significant personal moment for me, because he had helped to manage Bitcoin, and because it required unveiling parts of my life and work that I had kept hidden for an extended period. The in-person meeting with Gavin enabled me to share insights into the creation of Bitcoin that went beyond its mere technical components.
198. Our discussions began in the afternoon and turned out to be a captivating exchange that made us lose track of time. We delved into various topics around Bitcoin's past, present, and future. We discussed the early stages of Bitcoin, its fundamental underpinnings, the challenges it faced, and its evolution over time.
199. We took stock of Bitcoin's current state, analysing its growth trajectory, impact, and current challenges it faced. Additionally, we explored the potential future of Bitcoin, discussing solutions for scaling, enhancing transaction speeds, and various strategies to address its ongoing issues.
200. Our conversation also ventured into deeply personal territories. I discussed the turbulent period in my life during 2010, culminating in my decision to step away from Bitcoin's development forefront (for the reasons that I describe above) . I shared how stepping away from the Bitcoin project allowed me to dedicate more time to research and teaching, free from the constant stress of Bitcoin-related deadlines and tasks.
201. These discussions profoundly affected both of us. Although I'm familiar with rigorous academic discourse, this meeting held a distinct personal significance. I found it unexpectedly therapeutic to share these experiences with Gavin. For his part, Gavin expressed that my knowledge was consistent with his understanding of Satoshi's philosophy and perspective, leading him to recognise that I was indeed Satoshi Nakamoto. I do not recall him expressing any doubts about this during our interactions.
202. Once I felt that Gavin had accepted my identity, I was willing to use the digital signature process to confirm possession of the early keys. Despite his appreciation for the digital signature algorithm, my understanding is that he had already concluded that I was Satoshi.
203. Gavin had previously expressed concerns about potential malware or tampering with the signature process. As a former forensics professional, I was cautious not to provide him with any files, thus preventing him from saving copies for later use. This ensured that the demonstration remained secure and uncompromised.
204. After sorting out a few details, Rob MacGregor organised the purchase of a brand-new IBM ThinkPad laptop from a retail store. I had offered several solutions that Gavin didn't accept including paying him to keep his existing computer. Rob suggested purchasing the computer and Gavin thought this was a good idea. While waiting for the laptop to arrive, we took a break to eat and continue our discussions. Once the laptop arrived, Gavin took the lead in setting it up from scratch. He downloaded Electrum, a Bitcoin wallet software, which could be utilised to verify a digital signature.

205. We adopted this method to ensure the process was transparent and could be held accountable. It was Gavin who selected the machine, and it was Gavin who set it up. This ensured he was in control of the process.
206. I gave Gavin the choice to select any of the first 11 blocks for me to use for the demonstration. As I recall, he chose Blocks 1 and 9. I then generated signed messages using the keys associated with these blocks on my laptop.
207. Gavin used his USB drive to transfer the signatures from my laptop to the new one. I manually entered the underlying messages into the verification box and clicked 'verify'. The result came back as negative, which caused a brief moment of panic in the room until I realised, I had made a typing error. I corrected the typo and reran the verification, which this time was successful. The mood in the room instantly lightened; there was a palpable sense of relief and joy. Gavin and I shook hands, continued our discussions, and celebrated with a round of drinks. Following the session, I gave the laptop and USB drive to Ramona's son, who reformatted and rebuilt the laptop.

Journalists

208. A few weeks later, towards the end of April 2016, I had successive meetings with BBC, The Economist, and GQ journalists. I wasn't fully informed about the negotiations leading to these meetings and was unsure of their objectives.
209. I wasn't particularly taken by the journalists. Going through the digital signature process with them felt uncomfortable because, unlike Jon Matonis and Gavin Andresen, they hadn't established through conversation that I was Satoshi. After more arguments and conflicts with Rob MacGregor, I felt cornered into doing this. I trusted Rob to ensure the journalists would focus on my academic qualifications, accounting records and other means of validating my identity.
210. I first met with Rory Cellan-Jones from the BBC. Per my understanding, we had agreed beforehand that there would be no cameras and the meeting would be low-key, but he reneged on this agreement.
211. During my interview with Rory Cellan-Jones, I demonstrated possession of keys from blocks among the first eleven. This included Block 9, the block I had used for the first Bitcoin transaction with Hal Finney in January 2009. The BBC published a video snippet from this session but omitted our entire exchange.
212. I also met Ludwig Siegele from The Economist and demonstrated using the early keys on messages with keys from blocks, including Blocks 1 and 9. While I possessed all these early keys and had them on my computer, I did not demonstrate using all the keys.
213. By the time of the final interview with GQ, my frustration had mounted. Contrary to what I had been promised, they also brought cameras. GQ had sent a fashion reporter who dressed me up in a turtleneck in the style of Steve Jobs and wanted to take photographs. I found it profoundly distasteful as I wanted to be taken seriously as a scientist, not painted as a CypherPunk or a Silicon Valley celebrity.

214. The reporter was accompanied by an academic, Dr Nicolas Courtois. My impression of him was that he was more of a provoker than an impartial observer. He never asked me to demonstrate anything throughout our conversation. Instead, he seemed to be more preoccupied with flaunting his achievements. We argued when he stated that he and his students had breached Bitcoin security by cracking hundreds of ECDSA keys and breaking into dozens of wallets and access keys. This claim was blatantly false.
215. In my experience, cracking an ECDSA key to steal Bitcoin is practically impossible due to the computational complexity involved. The security of the ECDSA is based on the difficulty of solving a complex mathematical problem that even the most powerful computers cannot solve in a reasonable timeframe. I thought Dr Courtois was acting incredibly disrespectfully, was provocative and argumentative and I saw him as attempting to undermine me to portray himself as superior to Satoshi. His conduct disrupted the meaningful discussions that were supposed to take place.

2 May 2016

216. My memory of the events between 2 to 5 May 2016 is vague even after having been shown emails relating to this period (which I understand have been included in the list appended to this statement). This was a difficult period for me to discuss. As I will elaborate below, I was in a crisis, under tremendous pressure, frequently arguing, and barely sleeping, culminating in a suicide attempt. I have tried my best to recollect the conversations that transpired with the help of the documents shown to me. While I don't have a detailed memory of the sequence of events, I vividly remember the prevailing emotions of anger, betrayal, and fear.
217. On the morning of 2 May 2016, the articles were made public. Concurrently, a blog post titled 'Jean-Paul Sartre, signing and significance' was released. This blog post was not an attempt by me to prove my identity as Satoshi Nakamoto.
218. When the embargo ended, I was in Paris, concluding a holiday during the week with my wife and her children. We had plans to return to London by approximately 2.30 pm (British Summer Time) on 2 May.
219. I used the example of Jean-Paul Sartre, who was offered and declined a Nobel Prize. He argued that signing as "Jean-Paul Sartre" would carry a different weight than signing as "Jean-Paul Sartre, Nobel Prize Winner". This reflected my belief that titles change perceptions of a person. The process must be carried out for the right reasons and in an appropriate manner and should never be forced upon someone.
220. The released version of the 'Sartre' post differed from what I had originally intended. Rob MacGregor had altered it during my time in Paris. My intention behind the post was to express how I felt compelled into actions that I disagreed with. I aimed to establish my identity traditionally by examining my life, qualifications, and official records. I never intended to be the centre of a media spectacle. I preferred to work quietly in the background, generating new inventions.

221. It wasn't until I was on the Eurostar journey back to London that I became aware of the final content of the 'Sartre' post. During that journey, I had a telephone conversation with Rob. Due to frequent tunnel transitions, the call quality was poor. Rob mentioned the possibility of signing a public message. I told him that we could resolve the situation and I would publicly sign using a key associated with the early blocks if he fulfilled his commitments to me.
222. Following that call, I also began checking my online presence from the train. I discovered that Rob had been accessing and managing my email addresses, craig@tyche.co.uk and craig@ncrypt.com, and even making blog posts on my behalf. His team had handled a significant amount of external communication without my involvement.
223. After returning to London on 2 May 2016, we went straight to our house in Wimbledon. Stefan and Rob came to visit us for a long meeting that afternoon. Ramona was also present. Rob was angry and told me he needed me to transfer some of the Bitcoin associated with Satoshi. He yelled at me that I would be deported and try to ruin my life if I did not carry out a public signature process or move Bitcoin from one of the early blocks. He threatened that he would dump us all, and we would have nothing, with no way to pay rent or school fees. I told him I was unprepared to do this until I did all the work proving my identity.
224. Performing a public signature process, in the absence of other proof, would destroy my life's work because I would be selling out Bitcoin to the 'crypto', 'CypherPunk' philosophy for money.
225. I was up all night that night, trying to decide what I do. I was thinking through Rob's threats, and whether I should destroy my life's work. I wavered over whether or not to write a blog post, but I was tired and under stress, and I do not remember whether I wrote anything. I was facing a tough choice.

3 May 2016

226. The following morning, on 3 May 2016, I attended a brunch meeting in a Central London restaurant with Rob, Stefan, and my wife, Ramona. Rob's approach had significantly shifted, and instead of yelling, he tried to adopt a facade of concern for my well-being. He warned me of potential negative consequences if I did not comply with his demands, citing the public commitments I had already made. During this meeting, I didn't agree to write a blog post or move the Bitcoin; I was still unsure about my next move.
227. I was mentally and physically exhausted, having gone without sleep the previous night, so my recollection of that day's events was somewhat blurred. I remember Rob drafting another blog post under my name and discussing it with Ramona. However, I did not review the draft myself. Rob created an artificial sense of urgency, pressing us for time. My desire for credible, external verification of my identity remained steadfast, and I was still grappling with what course of action I should take. The situation also profoundly affected Ramona, feeling like Rob had threatened her and her children.

228. I understand that the "Extraordinary Proof" blog post was published by mid-afternoon on May 3, 2016. I was not immediately informed of its publication. However, Rob and Stefan clarified that they expected me to commit to publicly proving my identity.
229. We engaged in numerous discussions and disputes in the 24 hours following the publication of the "Extraordinary Proof" blog post. Rob insisted that it was universally perceived that I had authored the blog post and that no one would consider it was posted on my behalf. He argued that I was cornered into validating my identity 'his way'. I reiterated my refusal to move any Bitcoin.

4 May 2016

230. On 4 May 2016, I had another contentious meeting with Rob at my home in Wimbledon. Having not slept for two consecutive nights after days of incessant arguments, I was utterly drained. Stefan and Ramona, were also present. I don't recall if anyone else was present or if I had any other interactions that day.
231. In that meeting, Rob persistently tried to pressure me into moving Bitcoin from Block 9. While Stefan attempted to diffuse the situation, Rob resorted to yelling and threats. His behaviour was highly aggressive, and he accused me of attempting to ruin his life. The tension peaked when he gave me a final ultimatum; he threatened 'to destroy me' if I did not move the Bitcoin that day. He vowed to ensure Ramona, her children, and I would be deported, cut off from our banking, rendered homeless, and left desolate.
232. I was shattered. Rob's demands had pushed me to the brink, coercing me into a course of action that contradicted my deeply-held beliefs and threatened to annihilate everything I had built. Confronted with this unbearable choice between my life's work and my family, I felt overwhelmed. Leaving the room under the pretence of having a break as my wife was getting a cup of tea, I ascended the stairs, picked up a 12-inch SAS knife, and moved to the shower. There, in desperation, I inflicted a wound on my own throat. Bleeding and in pain, I wished for the end, eventually losing consciousness.
233. I regained consciousness later in a hospital. Ramona was present, but I was completely detached from the outside world, without even my phone for connection. While in the hospital, I learned Rob had published another blog post I had no part in nor approved of. I was unconscious at the time he drafted it. After returning home, my ordeal was evident; my throat was swathed in bandages making it difficult to conceal what had transpired.
234. After these events, my agreement with Rob MacGregor from 2015 disintegrated due to irreconcilable differences. Rob eventually sold his shares in nChain to a private equity company. I do not have the details of that deal.
235. I now know that Rob MacGregor's motivations between mid-2015 and May 2016 had not aligned with my best interests or my core values. Based on how events turned out, I have come to accept that he had an ulterior motive of capitalising on my identity as Satoshi Nakamoto for potential financial gain. In hindsight, the decision to trust Rob's counsel without fully understanding his motivations was the biggest mistake of my life.

Annex – List of Documents Shown to Dr Craig Wright During Witness Interviews

Documents shown to Dr Wright in the course of witness statement proofing sessions with Travers Smith LLP and Ontier LLP	
1.	ID_000553
2.	C00000971
3.	C00001292
4.	ID 002252
5.	ID 002274
6.	ID 002285
7.	ID_002087
8.	ID_002134
9.	ID_002233
10.	ID_002240
11.	ID_002250
12.	ID_002284
13.	ID_002303
14.	ID_002304
15.	ID_002315
16.	ID_002323
17.	ID_002325
18.	ID_002330
19.	ID_002343
20.	ID_002355
21.	ID_002356
22.	ID_002360
23.	ID_002369

24.	ID_002373
25.	ID_002377
26.	ID_002426
27.	ID_002656
28.	ID_002758
29.	ID_002950
30.	ID_003184
31.	ID_003272
32.	ID_003315
33.	ID_003992
34.	ID_004096
35.	ID_004311
36.	ID_004534
37.	ID_004542
38.	ID_000050
39.	ID_000051
40.	ID_000071
41.	ID_000128
42.	ID_000195
43.	ID_000227
44.	ID_000258
45.	ID_000260
46.	ID_000367
47.	ID_000371
48.	ID_000386
49.	ID_000388

50.	ID_000395
51.	ID_000396
52.	ID_000462
53.	ID_000504
54.	ID_000529
55.	ID_000530
56.	ID_000531
57.	ID_000549
58.	ID_000550
59.	ID_000568
60.	ID_000569
61.	ID_002973
62.	ID_002974
63.	ID_002975
64.	ID_002976
65.	ID_002977
66.	ID_002978
67.	ID_002979
68.	ID_003052
69.	ID_003840
70.	ID_003860
71.	ID_003879
72.	ID_003904
73.	ID_003993
74.	ID_003994
75.	ID_003995

76.	ID_003996
77.	ID_004000
78.	ID_000551
79.	ID_000525
80.	ID_004532
81.	ID_000739
82.	ID_000375
83.	ID_000554
84.	ID_000620
85.	ID_004533
86.	C00001010
87.	ID_004535
88.	ID_003348
89.	ID_001676
90.	ID_003964
91.	ID_003963
92.	ID_004536
93.	ID_003965
94.	ID_003418
95.	ID_000848
96.	ID_000619
97.	Privileged emails exchanged between Dr Wright and his current and former legal advisers


Confirmation of Compliance with PD 57AC and Statement of Truth

I understand that the purpose of this witness statement is to set out matters of fact of which I have personal knowledge. I understand that it is not my function to argue the case, either generally or on particular points, or to take the court through the documents in the case.

This witness statement sets out only my personal knowledge and recollection, in my own words. On points that I understand to be important in the case, I have stated honestly (a) how well I recall matters and (b) whether my memory has been refreshed by considering documents, if so how and when.

I have not been asked or encouraged by anyone to include in this statement anything that is not my own account, to the best of my ability and recollection, of events I witnessed or matters of which I have personal knowledge.

I believe that the facts stated in this witness statement are true. I understand that proceedings for contempt of court may be brought against anyone who makes, or causes to be made, a false statement in a document verified by a statement of truth without an honest belief in its truth.

DocuSigned by:

.....EFC03017AD2842B.....

SIGNED

28 July 2023
.....

DATED

Legal Representative's Certificate of Compliance

I hereby certify that:

1. I am the relevant legal representative within the meaning of Practice Direction 57AC.
2. I am satisfied that the purpose and proper content of trial witness statements, and proper practice in relation to their preparation, including the witness confirmation required by paragraph 4.1 of Practice Direction 57AC, have been discussed with and explained to Shoaib Yousuf.
3. I believe this trial witness statement complies with Practice Direction 57AC and paragraphs 18.1 and 18.2 of Practice Direction 32, and that it has been prepared in accordance with the Statement of Best Practice contained in the Appendix to Practice Direction 57AC.

Name: H. J. El

Position: PARTNER

Date: 28/7/2023