1 The three "B's" of Bitcoin

When discussing Bitcoin, it is important to distinguish exactly which technology we are referring to. When broken down to its most primitive level, Bitcoin can be viewed as three separate innovations; The Big "B", the "Blockchain" and the Little "b" [1][2].

1.1 The Big "B"

The Big "B" Bitcoin, that is the singular capitalized term, is referring to the protocol, software, and community of the decentralized computer network [3]. This was originally outlined in a white paper [4] authored under the pseudonym Satoshi Nakamoto in November of 2008 and was quickly followed by an open source release of the Bitcoin proof-of-concept source code in January 2009 [5]. This proof-of-concept software client has been periodically updated (about 75% of the code has been rewritten in the six years) since it was initially released, remains open source and serves as the reference software for individuals seeking to develop Bitcoin-related software (now commonly known as "Bitcoin Core") [6]. This reference client incorporates all improvements or adjustments made to the underlying Bitcoin protocol so any developer creating software adaptations can know that if their software is compatible with systems running the reference client, it will be compatible with the Bitcoin Network as a whole [1].

Prior to bitcoin, there were a number of digital currencies with varying levels of traction (Liberty Reserve [7] and E-Gold [8] being the most prominent) which offered secure payments without revealing account numbers or identities. However, in reality these were centralized services with non-public transaction histories that relied on the central issuer to verify transactions. The Bitcoin protocol describes a decentralized system with no hierarchical structure which is progressively built [9] by a community of contributors. This network exerts a tremendous amount of computing power toward the singular purpose of validating and clearing transactions on the Bitcoin Network.

It is this decentralised, open, public ledger which is arguably the most powerful innovation to come out of the Bitcoin specification and it is the Bitcoin protocol which sets out the rules for maintaining it. The Bitcoin protocol is, therefore, a solution to the 'Byzantine General's problem [10] which outlines the difficulties in a system generating a consensus and prior to Bitcoin was thought to be unsolvable. We now have a technology which provides with an immutable record of transactions without the need for a central gatekeeper controlling how transactions are recorded [11].

This decentralization has tangible benefits besides immutability as the fact that the protocol is operated by a group of peers means there is no central point of failure which negates a number of potential problems. The first of these being internal abuse, that is, this decentralized system removes the need to trust any central authority to 'do the right thing'. This is best demonstrated when considering the cryptocurrency side of bitcoin. Many fiat currencies have experienced hyperinflation due to a government printing money, for example Zimbabwe in 2008 [12] where inflation reached over 3.5Million%. In contrast, the decentralized Bitcoin network forms a consensus on the difficulty of the mathematical challenge used to confirm the next set of transactions every 2,016 blocks [13]. This is akin to setting the rate at which new bitcoins are created and therefore reduces the risk of internal abuse causing hyper inflation as a majority consensus is needed to alter the rate.

Another problem reduced by decentralization is that of attack. As a majority consensus is needed for software updates to be propagated [12][14] it becomes prohibitively difficult for an attacker to compromise the underlying protocol. Nodes 'vote' on whether to accept protocol changes and an attacker would need a good percentage of computational power to have a chance of dictating what gets implemented.

A similar case can be made for censorship, A majority vote is required for changes to be applied, potential changes which are not in the interest of the many will likely be rejected. This results in a more open system and stops a single controlling entity dictating what can and cannot be done (such as PayPal restricting its use in gambling-related ventures due to government intervention [15]).

1.2 The Blockchain

The second "B", the Blockchain, represents the second greatest innovation from Nakamoto. This is the distributed ledger which underpins the entirety of the Bitcoin system. A distributed ledger is a consensus of replicated, shared, and synchronized digital data geographically spread across multiple

sites, countries, and/or institutions [16]. This ledger is stored locally on every node in the network running the full version of the bitcoin software [6] and records every transaction sent and confirmed on the Bitcoin network (the current size of the Blockchain is around 92GB, December 2016 [17]). This complete history, coupled with the fact that it is an open network means that anyone can see what is happening in the network, not just now but during all periods in the past. This is extremely powerful as it allows an individual to fully audit the entire Bitcoin Blockchain without relying on external parties. This process is, in fact, what happens when you first download the full version of Bitcoin Core [13].

While the Bitcoin Blockchain is not the only form of distributed ledger in existence, it is the most publicly proven method to achieve distributed consensus and does this via the 'proof-of-work mining' process [16]. This is how new information gets added to the blockchain, by nodes in the network running a special 'mining' variant of the Bitcoin software which uses considerable computing resources to win the right to add another block to the Blockchain which is accompanied by a reward for the winning user. The concept of 'proof-of-work' is a method of ensuring that the information being added to the Blockchain was difficult (in terms of cost and time) to be made, though is easy for others to validate that the requirements were met [18]. This means that the expenditure of computing power serves to secure the integrity of the Blockchain, while the miners themselves verify through public-private key cryptography the validity of each transaction they include in a block.

Blocks are chained together making it impossible to modify transactions included in any one block without modifying all following blocks; as a result, the cost to modify a particular block increases with every new block added to the block chain, magnifying the effect of the proof of work [13][19]. This is why, although a bitcoin transaction is deemed clear upon its inclusion in a block on the Blockchain, best practices dictate that a user considers a transaction confirmed after its inclusion in a block and the addition of five subsequent blocks to the Blockchain [20].

The difficulty of the proof-of-work mining needs to be controlled, so that an average mining time of 10 minutes per block is maintained. This time is somewhat arbitrary but is an attempt to find a balance between accepting transactions quickly and minimizing instability and waste in the network, as, while a new block is being distributed other miners will be working on an obsolete problem. As more miners join the network the block creation rate will increase due to the greater collective computational power. Therefore, every 2,016 blocks the difficulty of the mathematical challenge is recalculated so that the average mining time returns to normal [13][18].

Despite the media often suggesting that bitcoin is an anonymous payment system, the Blockchain is in fact a transparent record of all user transactions on the network. Bitcoin is in fact pseudonymous, and your transactions in the network are like writing under a pseudonym. If an author's identity is ever linked to their pseudonym then everything written under that pseudonym will be revealed [21]. This is particularly poignant when considering the Blockchain as every transaction is stored forever, therefore a compromised address could lead to all transactions being linked to a person. There are however ways to reduce the amount of statistical analysis which can be done on transactions that a person is a part of which help to achieve reasonable anonymity.

1.3 The little "b"

The third "b", bitcoin, refers to the Bitcoin Network's payment system where the lowercase version of bitcoin refers to the core unit of value on the Bitcoin network [1]. New bitcoins enter the network as a reward for miners spending resources to confirm transaction blocks. In total 21 million bitcoins will be created as mining rewards, over 70% of all bitcoins have been mined to date and approximately 90% will have been mined by 2026 [1]. A bitcoin can be subdivided to eight decimal places, with the smallest unit a satoshi having a value of 1/100,000,000th of a bitcoin.

The question of 'what is the value of a bitcoin' is somewhat a controversial topic. Bitcoin resembles a currency in many ways; there will only ever be 21 million bitcoins that will exist in the bitcoin network and every bitcoin can be divided to eight decimal places, so there are many partial bitcoins that can exist [22]. Historically, currencies have been backed by a tangible asset, for example gold, but it is the Bitcoin network that gives bitcoins value. Therefore bitcoin should not be considered a currency, but an open ledger within which there is value due to the networks ability to verify the authenticity and ownership of a bitcoin and the ability to transfer possession nearly instantaneously for little to no cost without the reliance on a trusted third party [1].

In general, you must spend some bitcoins to broadcast a transaction into the network and for it to be included in the Blockchain.

Transactions typically include a payment of nominal amount of bitcoins as a "miners fee", usually around 0.0001 bitcoins, but this is optional. However, inclusion of a miners fee will likely prioritize a transaction for inclusion in the next solved block as miners will want to maximise their reward [1]. As there are a finite number of bitcoins in the network, these fees will play a progressively larger incentive in ensuring there are miners available to continue confirming transactions on the network.

Transactions will propagate across the Bitcoin network and be visible (in an unconfirmed state) in a matter of seconds. However, transactions may not be included in the next available block in a number of situations. The transaction may not have been received by the miner that solves the block, the block may have already been filled with other, higher priority unconfirmed transactions or the miner may have elected not to include the unconfirmed transaction [1].

References

[1] KAYE SCHOLER. *An Introduction to Bitcoin and Blockchain Technology*. 2016. URL: http://www.kayescholer.com/docs/IntrotoBitcoinandBlockchainTechnology.pdf (visited on 02/12/2016).

[2] itBit. *Five-Minute Bitcoin Primer: What is Bitcoin and How Does it Work?* 2015. URL: https://cdn2.hubspot.net/hub/424565/file-2382046756-pdf/itBit_Five-Minute_Bitcoin_Primer_-_What_is_Bitcoin_and_How_Does_it_Work.pdf?t=1446765105287 (visited on 02/12/2016).

[3] 2016. URL: https://en.bitcoin.it/wiki/Help:Introduction#Capitalization_.2F_Nomenclature (visited on 02/12/2016).

[4] Satoshi Nakamoto. *Bitcoin: A Peer-to-Peer Electronic Cash System*. 2008. URL: https://bitcoin.org/bitcoin.pdf (visited on 02/12/2016).

[5] Satoshi Nakamoto. *Bitcoin v0.1 released*. 2009. URL: http://www.metzdowd.com/pipermail/cryptography/2009-January/014994.html (visited on 02/12/2016).

[6] 2009. URL: https://github.com/bitcoin/bitcoin (visited on 02/12/2016).

[7] 2014. URL: http://www.investopedia.com/terms/l/liberty-reserve.asp (visited on 03/12/2016).

[8] Douglas Jackson. *e-gold is...* 2007. URL: http://blog.e-gold.com/2007/08/e-gold-is.html (visited on 03/12/2016).

[9] Simon Thorpe. *All you want to know about Blockchain but were afraid to ask*. 2016. URL: https://www.linkedin.com/pulse/all-you-want-know-blockchain-were-afraid-ask-simon-thorpe (visited on 03/12/2016).

[10] Leslie Lamport, Robert Shostak and Marshall Pease. *The Byzantine Generals Problem*. 1982. URL: http://research.microsoft.com/en-us/um/people/lamport/pubs/byz.pdf (visited on 03/12/2016).

[11] Dug Campbell. *The Byzantine Generals' Problem - dugcampbell.com*. 2015. URL: http://www.dugcampbell.com/byzantine-generals-problem/ (visited on 03/12/2016).

[12] 2015. URL: https://www.rt.com/business/267244-zimbabwe-currency-compensation-hyperinflation/ (visited on 03/12/2016).

[13] 2016. URL: https://bitcoin.org/en/developer-guide#proof-of-work (visited on 03/12/2016).

[14] Brave New Coin. *A gentle introduction to blockchain*. 2016. URL: http://www.the-blockchain.com/docs/A-gentle-introduction-to-blockchain-technology-web.pdf (visited on 03/12/2016).

[15] 2016. URL: https://www.paypal.com/selfhelp/article/FAQ915 (visited on 03/12/2016).

[16] 2016. URL: http://www.blockchaintechnologies.com/blockchain-definition (visited on 03/12/2016).

[17] 2016. URL: https://blockchain.info/charts/blocks-size?timespan=all (visited on 03/12/2016).

[18] 2016. URL: http://www.blockchaintechnologies.com/blockchain-mining (visited on 03/12/2016).

[19] 2016. URL: http://redpinata-development.com/bitcoin-academy/index.php/reader/items/proof-of-work.html (visited on 07/12/2016).

[20] 2016. URL: https://en.bitcoin.it/wiki/Confirmation (visited on 03/12/2016).

[21] 2016. URL: http://bitcoinsimplified.org/learn-more/anonymity/ (visited on 04/12/2016).

[22] itBit. *Bitcoin, Blockchain, and the Future of Financial Transactions*. 2015. URL: http://www.the-blockchain.com/docs/Bitcoin,%20Blockchain,%20and%20the%20Future%20of%20Financial%20Transactions.pdf (visited on 02/12/2016).