The Bitcoin whitepaper, Bitcoin: A Peer-to-Peer Electronic Cash System, was published in 2008 by Satoshi Nakamoto. Bitcoin is revolutionizing the global payments industry and people around the world are rethinking the meaning of their money. Moreover, the underlying technology and network that process Bitcoin transactions, known as **blockchain**, is transforming industries from banking to supply chain, farming to healthcare, just to name a few. All this is made possible by Satoshi Nakamoto's groundbreaking work published in 2008 which outlines what Bitcoin is and how it works, as presented in the original Bitcoin whitepaper.

Essentially thousands of computers are connected through the network of computers throughout the world are networked via internet and they allow for confirmations

**How To Use This Quick Reference Guide**

I have used this guide to help me process the depth of my understanding of Bitcoin and the underlying Decentralized Ledger Technology on which Bitcoin has been built. I hope it offers you a digestible simplified explanation of Nakamoto's work.

Below are notes for the 12 sections of the Bitcoin whitepaper.

*Text in italics will be used to provide commentary and annotations that distinguish my interpretation from those of Satoshi Nakamoto's.*

**1. Introduction**

Bitcoin creator, ***Satoshi Nakamoto*** discusses our current reliance on “trusted” third parties such as banks and credit card companies to process electronic payments. This traditional method may work for most transactions however not for all. Problems do occur when there is buying and selling of goods on the internet. Here are some of the weaknesses of the traditional electronic payments involving third parties:

- **Transactions** can be reversed since banks must mediate disputes that without a doubt will come up.

*Think of disputes that regularly take place between merchants, customers and third parties, such as credit card companies, e-commerce payment processors, PayPal or tax authorities.*

- Banks' intervention increases transaction costs and limits the average minimum transaction size.

*Consumers frequently buy low-cost items on the web. However, bank involvement costs a lot and these costs are passed on to customers through transaction fees and other charges. Consider expenses from returns and exchanges that pile up in a given year and you will see that transaction costs will increase significantly. Finally, in a service (i.e. yoga studio) economy, when a provider completes a service they should rightfully get paid however the current system allows transactions to be reversed, putting a service provider (yoga studio) at risk of not getting paid.*

- The possibility of a transaction's reversal hangs over everyone's head. It requires people to trust a third party such as central banks to resolve payment disputes.

*Many merchants and consumers don't trust financial institutions. They are expensive, poor customer service, may not be trustworthy; and often give too much information to the government without informing the clients. This also creates privacy concerns. In this section, Nakamoto outlines the limitations of the traditional payment system, and is sharing his proposed solutions.*

- The system accepts a certain percentage of fraud as unavoidable. Nonetheless, fraud increases everyone's cost of doing business. Nakamoto proposes an electronic payment system that is based on cryptographic proof instead of trust.

*Cryptography involves the use of code and protocols to establish secure communications.*

Such a system would let two parties transact directly with each other. The new method, namely **Bitcoin**, features the following:

1. Peer-to-peer payments over an online network.
2. The elimination of third parties and replacing trust with verification.
3. Transactions would be irreversible and Nakamoto's opinion is that this irreversibility would protect sellers from fraud.
4. Nakamoto shares that escrow mechanisms can be implemented to protect buyers.
5. A peer-to-peer distributed timestamp server would generate mathematical proof of the chronological order of transactions. The system is secure as long as the honest participants collectively control more computing power than attackers/hackers.

*Nakamoto believes that it's better to verify transactions rather than trust an external third party, especially when it comes to something as important as money. Secondly, irreversibility minimizes fraud. Decentralized computers would prove the exact order of these irreversible transactions, creating user confidence that the records in the electronic audit trail, the blockchain, are valid and accurate.*

**2. Transactions**

In this section, Nakamoto's description of the electronic transaction process, namely the blockchain, gets technical. In simple terms, he defines an electronic "coin" as a chain of digital signatures. Owners digitally sign a hash of the previous transaction and add a **public key** of the next owner to the end of the coin. A recipient of the coin, a payee, can verify the signatures in order to verify the chain of ownership.

*A Bitcoin doesn't exist anywhere per se, at least not in the traditional sense of physical cash. Rather, Nakamoto's concept of an electronic "coin" is a chronological series of verified digital signatures.*

*To illustrate, think of Nakamoto's virtual coin as a UPS or FedEx package that you sign at your doorstep before sending it to a forwarding address. But the difference is that a publicly-available ledger is placed right on the packing slip which shows the entire history of all prior deliveries of the same package.*

*The information includes all originating addresses as well as timestamps detailing where and when exactly each delivery took place. Such an extensive, transparent, and comprehensive audit trail, he argues, would provide assurance to both recipient and the entire network that the chain of deliveries/transactions is accurate and secure.*

However, Nakamoto points out a potential problem with duplicate payments. A recipient/payee can't verify that a coin's owner didn't send the same coin to other recipients/payees, which is referred to as the double-spend problem.

*For example, Alex owns only one Bitcoin but sends one coin each to two different merchants -- amounting to two Bitcoins paid with only one originating coin.* To solve the double-spend problem without relying on a third party, *Nakamoto* says that all transactions must be publicly revealed. Secondly, all participants of the payment system must adhere to the same timeline so that everyone agrees to a single history of the order in which transactions are received.

*A timeline and public history of all transactions prevent double-spending because later transactions would be considered an invalid, or perhaps fraudulent, payment from the same coin. Each coin has a unique timestamp and the earlier transaction would be accepted as the legitimate payment. One coin, one payment. Sending the same coin to a second merchant, per the above example, would show a different timestamp that occurred later in the timeline. And that would invalidate the second payment/transaction.*

**3. Timestamp Server**

A timestamp server takes a hash of a block of items and publicly announces the hash. The timestamp proves the existence of the data at the time. Each timestamp includes the previous timestamp in its hash. And each additional timestamp reinforces the ones before it. This sequence forms a chain.

*Here we see the emerging decentralized structure of blockchain technology. A* ***timestamp server*** *provides an essential function in protecting data records for the long-term. It provides proof that the data existed at a particular moment in* ***time*** *and that it has not changed, even by a single binary bit, since it notarized and* ***time-stamped****. They are key to preventing double-spending and fraud. It'd be virtually impossible to send duplicate coins because each coin contains different, chronologically-ordered timestamps. Using the analogy of a UPS/FedEx package, each delivery contains a unique timestamp on the packing slip, and that would mark the exact time of each and every delivery on the public ledger.*

*Bitcoin's file size in bytes increases as the transaction history gets larger. And larger files lead to longer processing times. Transaction processing -- or mining -- continually requires more CPU power to verify the transactions because the digital records themselves grow in size. Furthemore the power usage is not as high as being commented on in the mainstream news AND energy companies are in process of addressing this problem.*

**4. Proof-of-Work**

Nakamoto says that proof-of-work is used to implement a peer-to-peer distributed timestamp network (mentioned above). The process scans for a value that when hashed, results in a certain numerical expression. The timestamp network must reconcile this value with a block's hash. CPU power is needed to satisfy the proof-of-work, and the block cannot be changed without redoing the work. Later blocks are chained after it, and to change the block would require redoing all the blocks after it.

*The language may be technical and appear complex however the concept is simple. Proof-of-work is what safeguards the blockchain. Inherent in this unique number is a math puzzle that a computer must solve before a transaction can happen. Once a correct answer is given, it serves as proof that*

*the specified work has been done. When someone sends an electronic coin, they must take a hash's unique number and solve an inherent math puzzle. The answer is then passed to the recipient to check if the solution is correct -- an important validation step. If the answer is correct, the payment/transaction takes place and adds to the length of the blockchain. If not, the proposed transaction is rejected.*

Proof-of-work provides one vote per CPU, not by IP address. Otherwise an attacker may allocate several IPs in an attempt to hack the network. Secondly, the longest chain of blocks serves as proof that the CPUs invested the greater amount of work in that longer chain. This process secures the blockchain by requiring would-be-attackers to redo the work of the block and all blocks after it (i.e., solve all those math puzzles) and then try to surpass the work of all the honest computers in the network. Nakamoto says that it'd be an extremely difficult task for an attacker to do just that, and that the probability of success diminishes exponentially the more blocks are added to a chain.

*So how does proof-of-work protect the blockchain? In layman's terms, honest CPUs in the network solve each hash's math problem. As these computational puzzles are solved, these blocks are bundled into a chronologically-ordered chain. Thus the term blockchain. This validates to the entire system that all the required "math homework" has been completed. An attacker would have to redo all the completed puzzles and then surpass the work of honest CPUs in order to create a longer chain -- a feat that would be extremely unlikely if not impossible. This sequence makes Bitcoin transactions irreversible. Nakamoto points out that honest nodes in the network need to collectively possess more CPU power than an attacker.*

**5. Network**

Nakamoto outlines the steps for running the peer-to-peer network:

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

As mentioned in earlier sections, nodes always consider the longest chain to be the correct one and will work on extending it.

*This section shows why it's important to announce transactions to all nodes. It forms the basis for verifying the validity of each transaction as well as each block in the blockchain. As mentioned earlier, each node solves a proof-of-work puzzle and thus always recognizes the longest chain to be the correct version. As time progresses, the blockchain's record grows and provides assurance to the entire network of its validity.*

**6. Incentive**

The first transaction in a block is a special transaction that starts a new coin owned by the creator of the block. This achieves two things. First, the creation of a new coin rewards nodes/computers to support the network. Second, it's a way to initially distribute new coins into circulation since there is no central authority to issue them. The new coin rewards nodes -- aka Bitcoin miners -- for expending their time, CPU and electricity to make the network possible. They can also be rewarded

with transaction fees. Nakamoto envisions a limited number of coins to ever enter circulation, at which point miners can be incentivized solely by transaction fees that are inflation-free. New coins also incentivize nodes to play by the rules and remain honest. An attacker would have to expend a ton of resources to threaten the system, and getting rewarded by coins and transaction fees serve as a deterrent to such fraud.

*Mining gold requires labor, water and equipment and it's an activity similar to Bitcoin mining. The miners of electronic coins process transactions, for which they are rewarded with new Bitcoins and/or transaction fees. Since a maximum of 21 million Bitcoins will ever be mined, the system can be free of inflation. Therefore, Bitcoin can serve as a sustainable store of value, similar to gold. Compare that to fiat currency, such as the U.S. dollar. Due to inflation, the dollar has devalued nearly 97 percent since 1913. Bitcoin's incentive program is a mechanism that protects the peer-to-peer electronic payment system. The issuance of new Bitcoin as well as transaction fees keep nodes honest. Because it wouldn't be worth it to attack the very system that forms the foundation of their wealth. As the saying goes, you don't bite the hand that feeds you.*

**7. Reclaiming Disk Space**

To save disk space, Nakamoto says that nodes can discard data from old transactions, with only the root of the discarded transaction kept in the block's hash. *This enables the blockchain to remain intact, albeit with less data from old transactions.* He briefly describes a process for compacting data. But with Moore's Law, Nakamoto says that the future capacity of computer hardware should be sufficient to operate the network without miners having to worry about storage space.

**8. Simplified Payment Verification**

In this section, Nakamoto provides a technical explanation of how to verify payments without running a full network node. That requires getting the longest proof-of-work chain and checking if the network has accepted it. The verification is reliable as long as honest nodes control the network. But an attacker can create fraudulent transactions for as long as an attacker can overpower the network. One defense against an attack is for network nodes to broadcast alerts when they detect an invalid block. Such an alert could prompt a user's software to download the full block as well as alerted transactions in order to confirm the inconsistency. Nakamoto adds that businesses that receive frequent payments may want to consider operating their own nodes to achieve more independent security and quicker verification.

*There are non-Bitcoin blockchain protocols that large companies are applying outside finance. For example, a company can create an invite-only protocol that selects certain parties to participate in a private network of nodes. The point is, there are many ways to set up a blockchain network that follows a different set of rules for verification. Nakamoto describes one way to do so for a peer-to-peer payment system, but he says that businesses may want to adapt their processes based on their own unique circumstances.*

**9. Combining and Splitting Value**

Combining transaction amounts will result in more efficient transfers as opposed to creating a separate transaction for every cent involved.

*In other words, it'd be simpler and more efficient to send three Bitcoins in a single transaction rather than create three transactions of one Bitcoin each, assuming the coins are sent to the same recipient.*

To allow transaction values (amounts) to be split or combined, transactions can contain multiple inputs and outputs. There can be single or multiple inputs. But there can only be a maximum of two outputs: one for the payment, and one returning the change, if any, back to the sender.

*This process enables payments with specific amounts. A sender can send Bitcoin payment to another party and get back his/her change, if needed.*

**10. Privacy**

With traditional payments, users attain privacy when banks limit information available to the parties involved as well as the third party. With the peer-to-peer network, privacy can still be achieved even though transactions are announced. This is accomplished by keeping public keys anonymous. The network may be able to see payment amounts being sent and received, but transactions are not linked to identities. Additionally, Nakamoto proposes that a new private key should be used for each transaction to avoid payments being linked to a common owner.

*To maintain privacy, Nakamoto says it's important for public keys to keep a user's identity anonymous. While everyone may be able to see transactions, no identifiable information is distributed.*

**11. Calculations**

It's highly unlikely for an attacker to create an alternate chain faster than an honest chain. Nodes won't accept an invalid transaction or blocks containing them. Moreover, an attacker is limited in what he can attempt to do: They can only try to change one of his own transactions to retrieve coins he recently spent. The probability that an attacker succeeds drops exponentially the more valid blocks are added to the chain. Nakamoto says that an attacker would have to get lucky early on to have a remote chance. Moreover, a receiver creates a new public key and gives it to a sender shortly before signing. This makes it difficult for an attacker to execute a fraudulent transaction through a parallel chain.

*There's a higher probability that an honest node will find a block faster than an attacker. It'd be extremely difficult for an attacker to solve several proof-of-work puzzles in a row faster than the rest of the honest nodes. Every 10 minutes, there are new puzzles being solved by nodes in the network.*

**12. Conclusion**

The peer-to-peer system for electronic payments relies on a distributed network of honest nodes to validate transactions. Validation replaces the need to trust expensive third parties such as banks. The electronic coins are made from digital signatures, and proof-of-work that form the blockchain prevent double-spending. The system stays secure so long as honest nodes control more CPU power than an attacker. Moreover, the nodes accept longer blocks as valid and work on extending them. This protocol rejects invalid blocks, and potential fraud, in the process. Rules and incentives can be enforced using a voting system.

*In the final section, Nakamoto says that "The network is robust in its unstructured simplicity." Yes indeed!*

Thanks for reading my notes on the Bitcoin Whitepaper". Feel to sign up for a discovery call on how to use the benefits of blockchain tech in your business. hello@thecryptocoach.co.