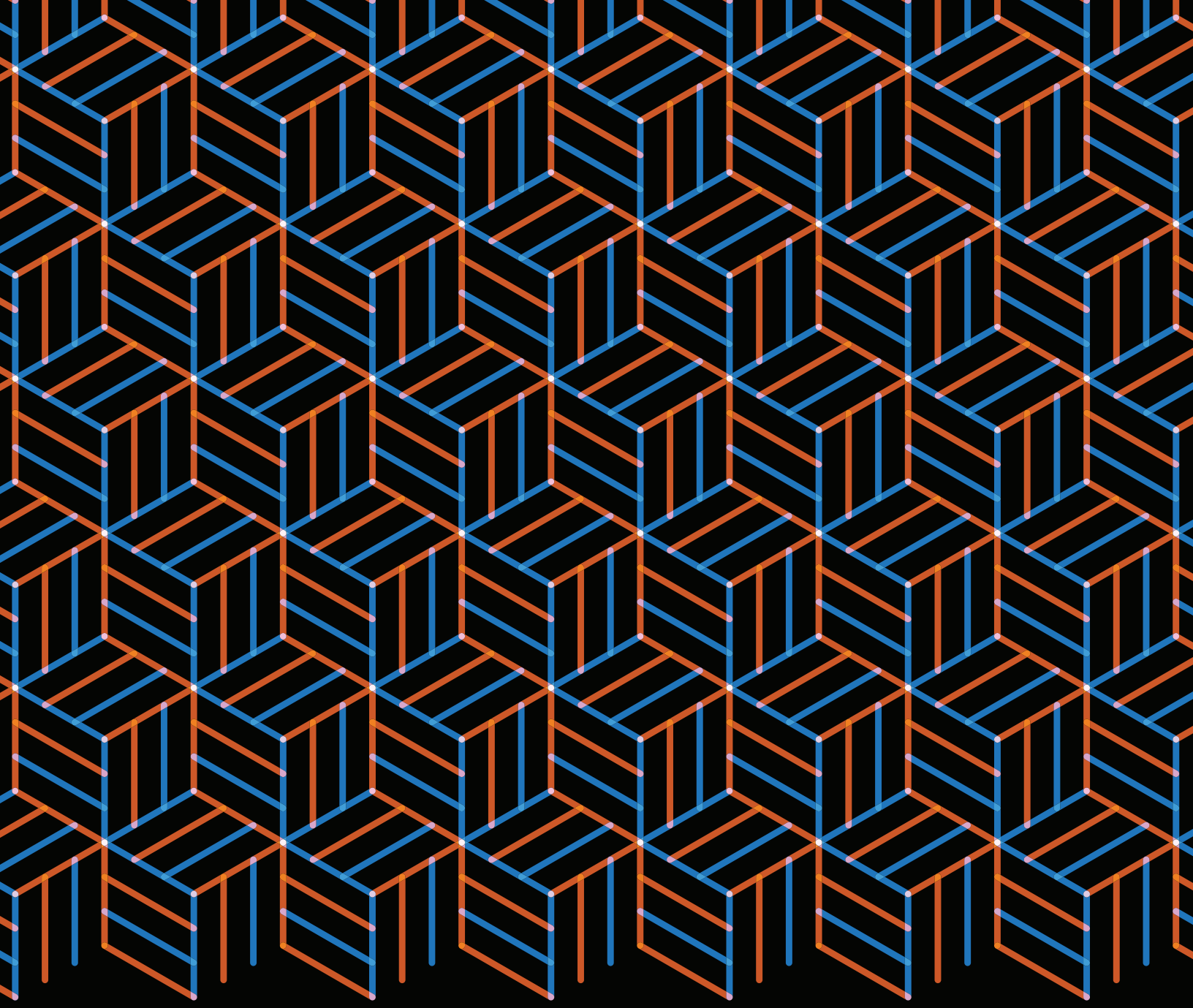


SOLUNA

Understanding the Blockchain

Version 1.1 – November 2021

Contents

Glossary


Description


Transition

Sealed Sheets

Validation


Hash Function Input


Hash Function Output

Blockchain Elements


Hash Value / Magic Machine

What is the Blockchain?

The Blockchain – A combination of technologies used to create a decentralized peer-to-peer network to manage ownership of digital assets.

Bitcoin is the first decentralized, censor-proof, portable, secure, durable, and scarce digital asset.”

CBInsights


LANDesk
FORTINET

The Origin

At about the same time the world was experiencing a global financial crisis, the beginnings of a new wave of innovation in the electronic age was underway.

On January 10, 2009, Hal Finney, a prominent cryptologist and cypherpunk, received an unusual email from an unfamiliar name – Satoshi Nakamoto.[1]

The email included a document that described a new form of digital money call Bitcoin. This "e-cash" was not going to be your typical payment gateway. It described a new form of currency and payment system based on a decentralized peer-to-peer network that required no trusted authority. In fact, it assumed no trust in the system and sought to eliminate the need for financial intermediaries altogether.[2]

Satoshi combined computer science, cryptography, and mathematics to produce a suite of technologies to realize this new network.

The market cap of this payment network, that Hal Finney ultimately helped build, has exceeded $125 Billion[3] and is used by millions of people and thousands of companies.[4]

The underlying technology powering Bitcoin is known as **the blockchain**.

The blockchain is a combination of technologies used to create a decentralized peer-to-peer network to manage ownership of digital assets.

To understand the blockchain, you must understand the problems Satoshi had to solve in order to create Bitcoin.

1. First, he had to eliminate the middleman by creating a completely peer-to-peer network where both the membership and the number of members is not known in advance.

2. Second, he had to create a distributed ledger that stores every transaction between all the peers in the payment network. The transactions had to form a clear understanding of ownership and every peer in the network needed to keep a copy. The ledger also had to be immutable and not rely on the trust of the peers.

3. Finally, he had to devise a way to maintain the integrity of the ledger, even in the event of malicious behavior by some peers in the network.

Solutions to these problems are the most important elements of the blockchain.

Peer-to-Peer Networks

On June 1, 1999, Shawn Fanning and Sean Parker founded Napster – the world's first peer-to-peer (P2P) network for sharing music.[5] Imagine iTunes without the cool devices and the central database controlled by Apple.

In Napster's model, all members of the computer network stored copies of music. Napster provided a central directory where each node listed those songs it had on its computer hard drive.

When each node (or peer) wanted to play, it simply asked Napster's central server which peer had the song. It then provided the internet address of the peer that had the song, and the requesting peer contacted their nearest neighbor to download a copy of the song to play.

The Napster network was similar to Satoshi's network with some exceptions. In the Bitcoin network there is no central server. In Satoshi's system, every peer has a copy of the full song directory. At its peak, Napster had over 80 million registered peers or users.[6] So, peers are known in Napster. In the Bitcoin network, peers do not register, and are unknown in advance.

Distributed Ledger Technology

Every time you make a deposit or a withdrawal from your bank account, your bank's computers update its central ledger.

It is a database containing all the account information and related transactions of their customers. It is the definitive record of the assets you own in the bank.

This works because you trust the bank to keep accurate records of all transactions. And, you also expect the bank to perform this in a secure and reliable fashion with no errors or fraud in the process.

But, what if you could not trust your bank? How would you perform financial transactions between you and another party? You could use cash, but what if the only option was a digital form of transfer (like a wire). How could you do it without the bank?

Satoshi invented a way.

He combined the concept of distributed ledger technology (DLT) and cryptography.

A distributed ledger is a database that is replicated over a P2P network. Essentially, every peer in the network has a complete copy of the database. Any change to the database is also shared with all the peers in the network.

Every transfer of ownership is recorded as a transaction in the database. It records to whom a digital asset was transferred and at what time. This transaction history becomes a complete audit trail that provides evidence of how every peer achieved his or her possession.[7]

Satoshi's implementation of DLT resembles a **folder full of sheets**. Each sheet of paper represents a series of transactions. Like a book, the pages are inserted into the folder in the correct, sequential order. Each page is a **block**.

This ever-growing folder becomes the **chain**. Every peer or node in the network has a copy of every sheet and the entire folder. This is the **blockchain**.

Ensuring all peers can reach consensus on changes to the folder or blockchain without the need for trust is a hard problem.

Enter The Magic Machine.

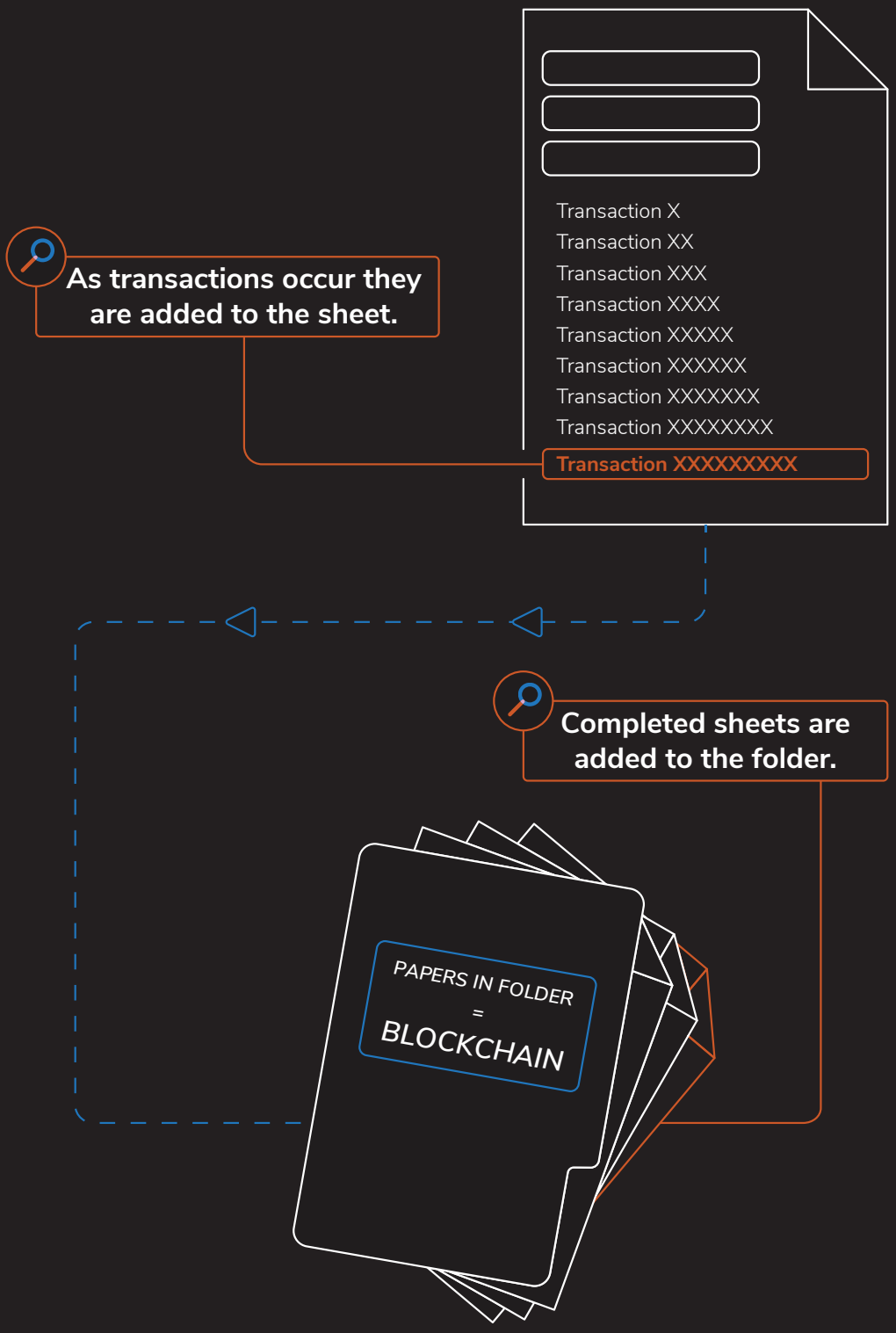


Figure 1: Sheets in Folder = Blockchain

Hash Functions: The Magic Machine

Suppose a magic machine existed that takes any length string and converts it into a fixed length number. Call it the fingerprint number. This is because this machine's output is much like a digital fingerprint.

Also, suppose this magic machine has the following properties:

- The machine works incredibly fast,
- It always produces the same number for the same string,
- The machine only works one-way; in other words, it is impossible to derive the original input data given the fingerprint number,
- There is no way to predict how the fingerprint number changes when the string is changed, even slightly, and
- No two heterogenous inputs produce the same fingerprint number. (Just like two people can't have the same fingerprint.)

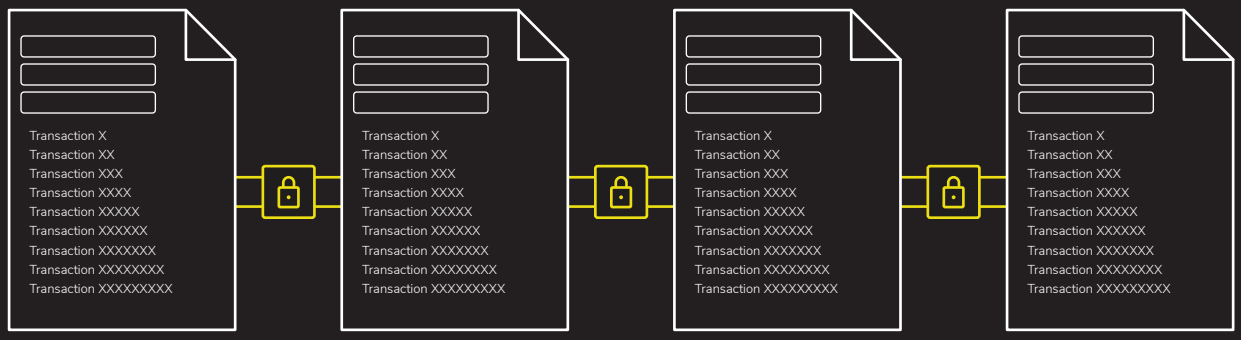


Figure 2: Chain of Hashed Sheets

In computer science, this magic machine is known as a cryptographic hash function. It is a set of mathematical operations that runs on digital data. The output of the function is known as the hash value. There are many different forms of these functions that makeup a family designed by the NSA.[8]

Satoshi chose Secure Hash Algorithm #256 (or SHA-256) for his digital money network.

Hash functions are very useful for determining if a set of data has maintained its integrity.

For instance, all a peer in Satoshi's network has to do is compare the computed hash value for a sheet from the folder with the known or expected hash value. If the values differ, the peer knows something is wrong. In essence, you can compare two sheets of transactions by simply comparing two numbers: their computed hash values.

One other useful thing about hash functions is they can be combined. The output of the hash from one set of data (like a page full of transactions) can be combined with a new set of data as input to the hash function. You can repeat this process forming a linked series of hash values. Hence, any change to the contents of a sheet breaks the entire link. You can do this at the page level or even at the transaction level to form a tree like structure.

The advantage of this tool is that data can be stored in a change-sensitive fashion. The sheets in Satoshi's folder can be linked into a cryptographically-sealed chain.

Later, if any of these hash values are found to be incorrect at any time, it is instantly evident that the data was changed at some point after the chain was created or while it was in transit to a peer in the network.

The Computer Puzzles and Proof-of-Work

Hash functions are useful for checking data integrity, comparing data, referencing data, and storing data in a secure and efficient fashion.[9]

They are also useful for creating elaborate puzzles that only computers can solve. The only way to solve these puzzles is by using lots of compute power and difficult computational work.

Recall earlier, the output of a hash function is a fixed length string. The length is set by the internals of the function. Hash values can also have leading zeros to achieve the required length.

Suppose I have a sheet of paper in Satoshi's network that contains a number of transactions. Remember, we call this a block. After we run the sheet through the magic machine we get a hash value.

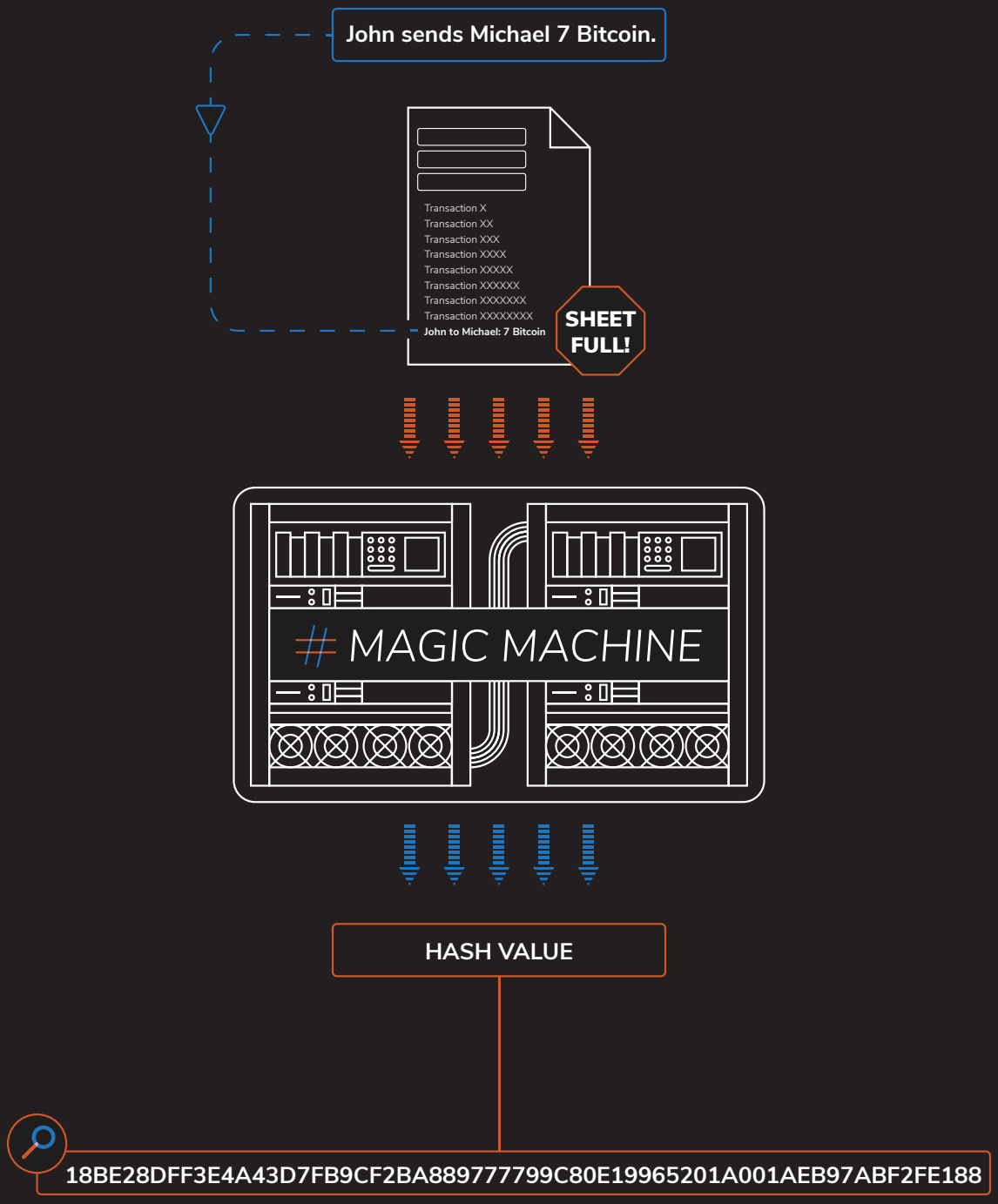


FIGURE 3: EXAMPLE OF A HASHED VALUE, BASED ON A SAMPLE TRANSACTION

Now, suppose I gave you the following puzzle to solve:

What number, that when combined with the sheet and put through the hash function produces a hash value with three leading zeros?

This puzzle has some important characteristics:

- You start with the original sheet of paper, and it remains unchanged.
- You must find a number, which you can change. This is called a nonce (number used once).
- The hash function is the same hash function used to produce the hash value for the sheet.
- The resulting hash value has a restriction, it must have three preceding zeros.

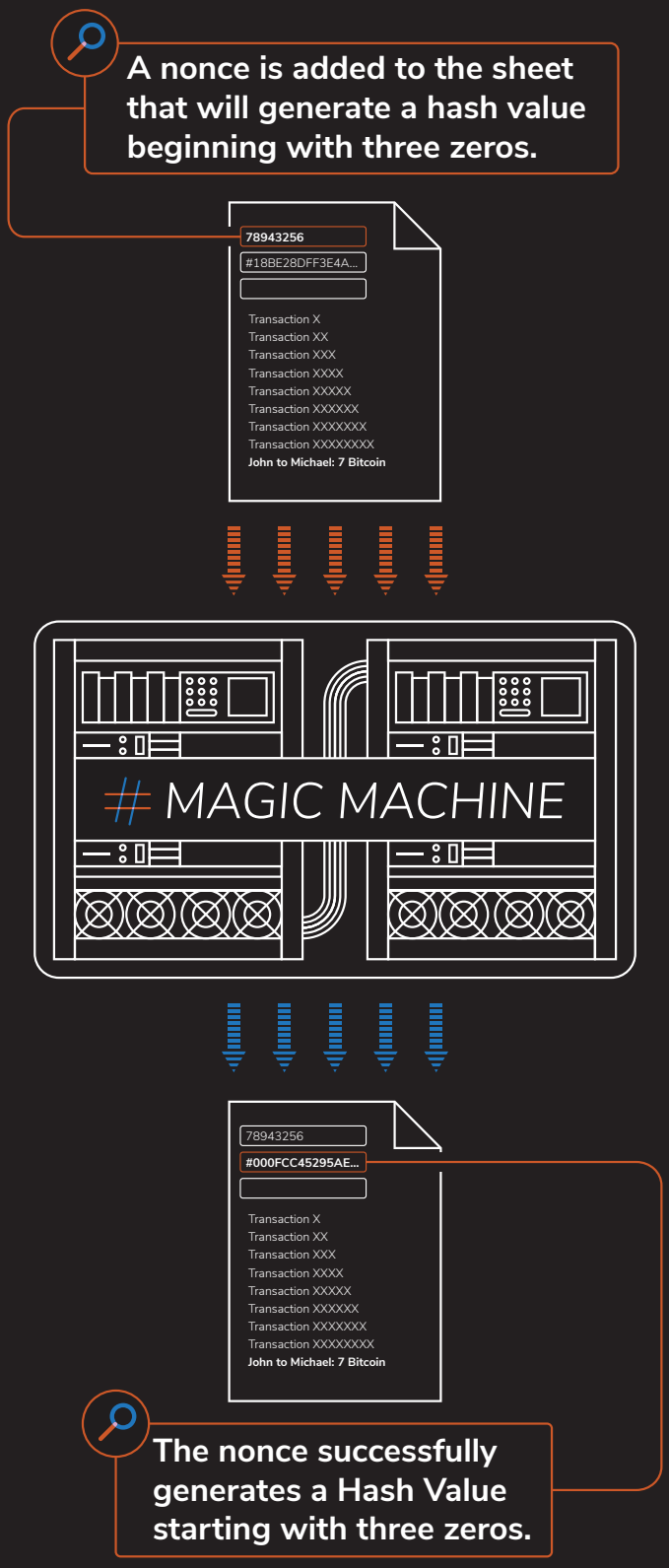


FIGURE 4: ADDING THE NONCE TO SOLVE THE PUZZLE

Because there is no way to get a hint from the original hash value and since hash functions only work one-way – we would have to use trial and error to solve this puzzle.

In fact, we'd literally have to **try every number from zero to infinity** until the resulting hash has three leading zeros.

This trial and error approach is equivalent to guessing the sequence of numbers to find the secret passcode for a combination lock. You would have to try every possible sequence until you find the one that opens the lock. This approach is guaranteed to work, but it is time consuming.

That is the idea.

The nonce that produces a hash value that meets the desired leading zeros is the solution to the puzzle.

It also turns out the number of leading zeros and the input values (sheet and nonce) are designed specifically to make the computational work harder every time.

The number of leading zeros (the restriction) is directly correlated to how challenging it will be for a computer to solve the puzzle.

So, in the world of hash puzzles, the number of leading zeros is often referred as the **difficulty level or difficulty**. The higher the difficulty, the more computational power, and average time it will take to guess the nonce.

Once a puzzle is solved, it is easy to verify. A validator will simply combine the original sheet with the nonce and put it through the magic machine. If the output has the right number of zeros, then we know the puzzle has been solved.

These puzzles are one of the most important tools for making Satoshi's Bitcoin network work. Any peer claiming to have solved the puzzle has to present the nonce. A nonce is therefore referred to as **proof-of-work** since its success in solving the puzzle proves that someone has done the work necessary to do so.

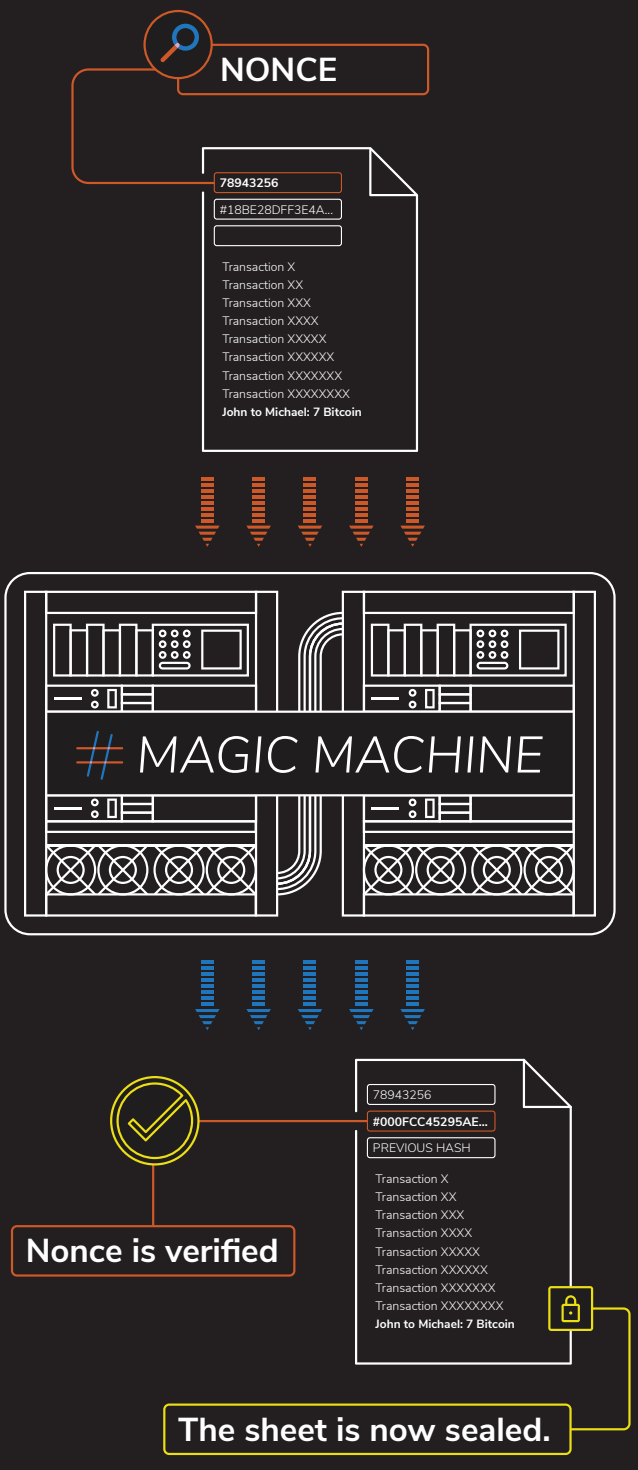


FIGURE 5: PROOF OF WORK (CHECKING THE NONCE)

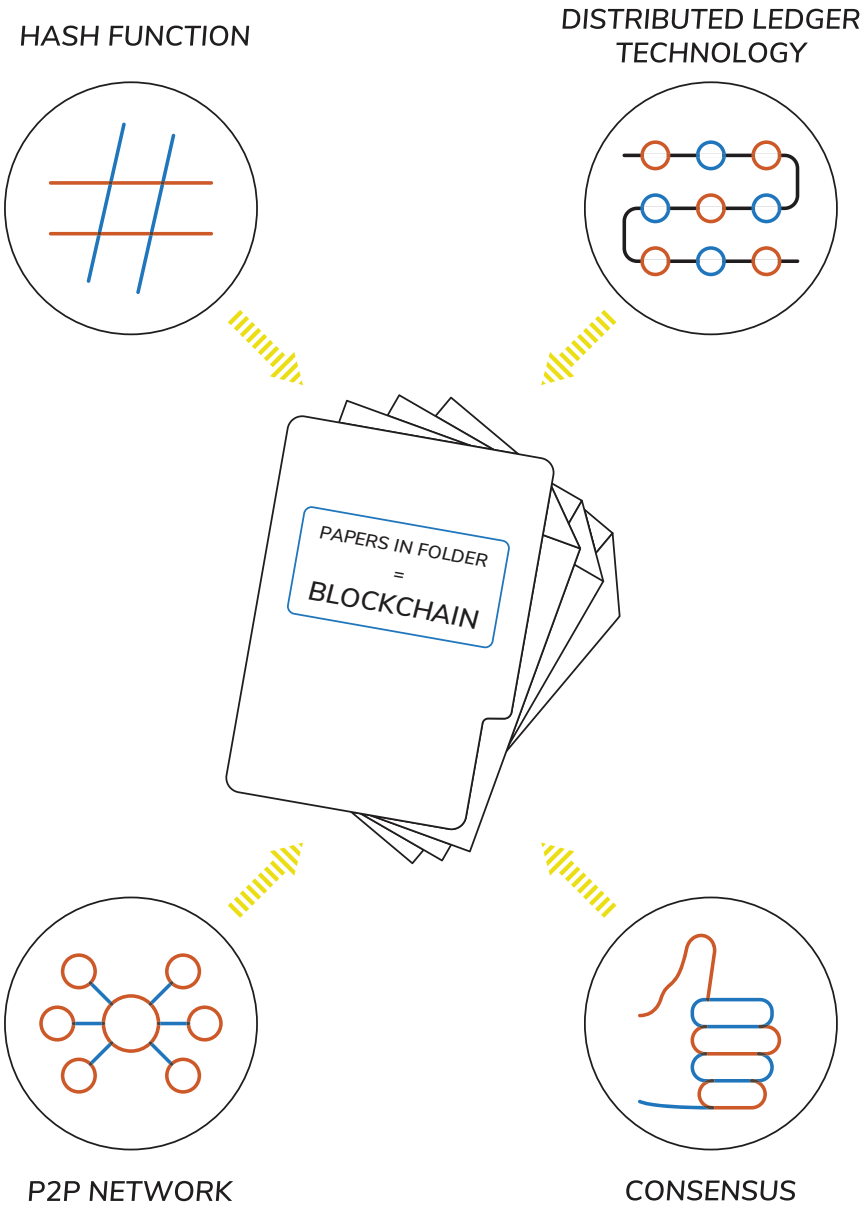
Satoshi uses hashing strategically in the architecture of Bitcoin (and its supporting blockchain) to preserve its integrity.

First, he uses it to store the pages in a change-sensitive way (using the combination properties discussed earlier).

Next, he uses it to produce a unique digital fingerprint of each sheet in the folder (full of transaction data).

Finally, he uses the puzzles to get peers in the network to expend computational effort for changing the sheets in the folder.

FIGURE 6: COMPONENTS OF THE BLOCKCHAIN



Mining: Putting It All Together

Now that we understand the problems Satoshi had to solve and their respective solutions, we now see how we combined them all to form a new digital currency – Bitcoin.

To do so, we'll use an example.

As we recall, in Satoshi's P2P network there is no middleman, and the asset that is owned and exchanged is a digital "token" called Bitcoin.

Let's imagine he implemented Bitcoin using the old centralized approach.

What if John gets a call from his friend Michael asking for money to help him in an emergency during his business trip overseas. Michael needs US$1800 to cover the cost of his return trip home.

John calls his account manager at his bank and makes a request to send $1800 dollars to Michael. John's account manager checks the bank's ledger to make sure John has the required funds before sending the money to Michael.

Now, imagine we can no longer trust John's bank or account manager. Perhaps he charges really high fees for overseas transactions or makes lots of errors in keeping the ledger up to date. Or perhaps, the bank was recently hacked, and the database was compromised. Whatever the reason, our middleman is no longer trustworthy.

John and Michael hear about Bitcoin and decide to use Satoshi's network.

Any number of peers (including John and Michael) are part of the network. Each member is responsible for maintaining a public copy of the distributed ledger. Recall, the ledger is a folder filled with sheets, themselves filled with transactions.

Let's say John wants to send 0.2 Bitcoin (the equivalent of $1800 as of 5/1/18)[10] to Michael. He broadcasts his intention to the network.

Each peer checks to make sure John has enough Bitcoin to perform the transaction. Then each peer writes the transaction in a free space on their transaction sheet. Other peers might perform similar transactions. For example, Phillip might send Dip 10 Bitcoin. All of these transactions are also added to their sheet until they are full.

Miners

Once a page is full, a subset of the peer network validates the transaction sheet and performs the process of "sealing" the page before it can be added the folder.

The seal ensures the page can never be changed from this point forward. To accomplish this, the special peers solve the following puzzle:

"What nonce when combined with ***both*** *the* ***sheet to be sealed*** *and the* ***hash value of the previous page*** *produces a hash value with three leading zeros?"*

The first special peer to find the nonce broadcasts it to all peers. The entire P2P network then validates the nonce is correct. If 51-percent of the peers agree, the entire network seals the page with the nonce and adds the page to the folder.

Sealing a page means appending the nonce to a special location on the page and storing the hash value of the previous page as a reference in the page.

Because the nonce takes into account the current page and the hash value of the previous page, each page is now linked cryptographically to the previous page in a change-sensitive fashion. Therefore, a single change to any page, will break the entire chain of pages or blocks.

This ensures the integrity of the entire blockchain.

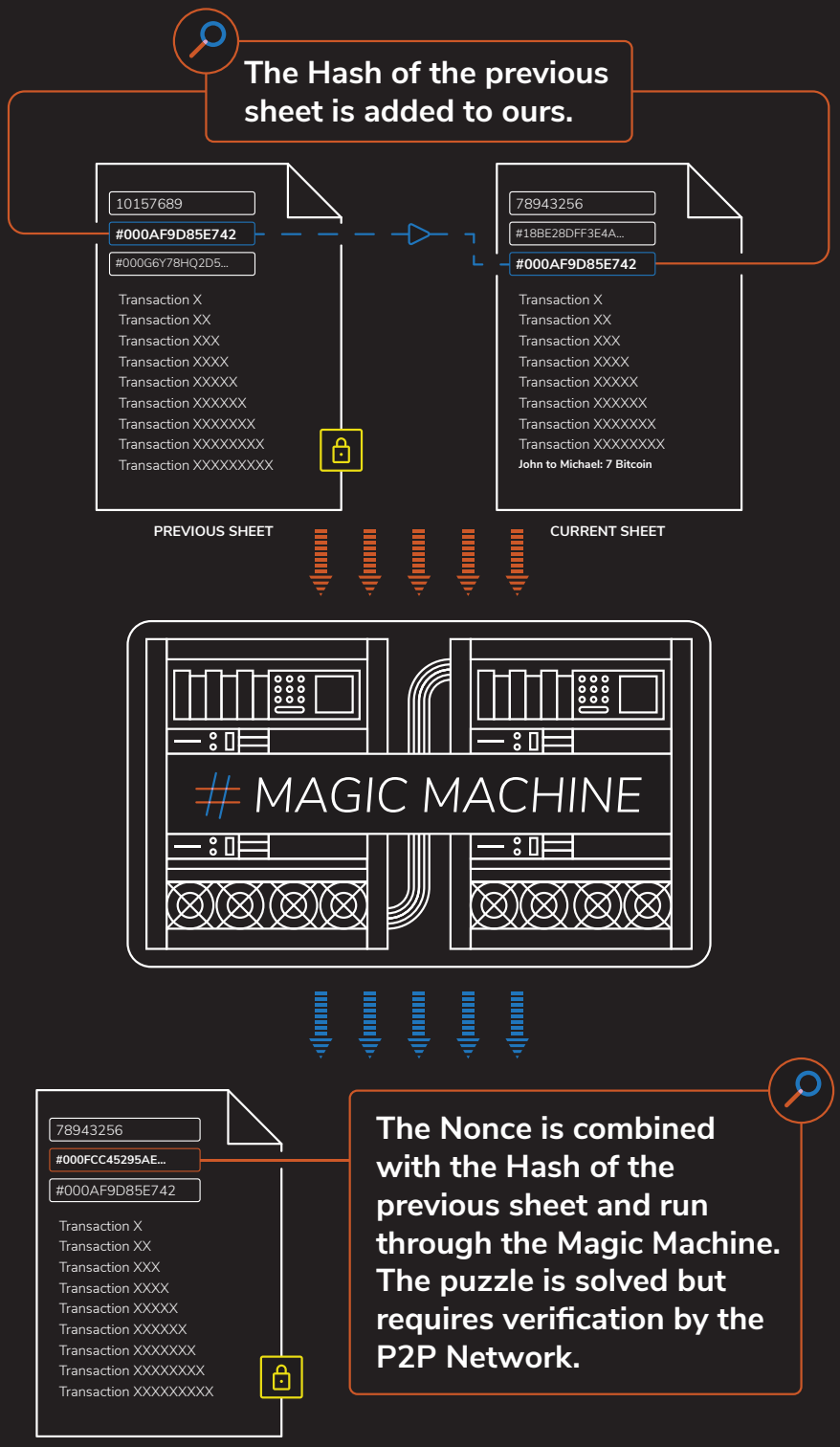


FIGURE 7: LINKING THE HASH TO THE PREVIOUS SHEET

Let's say one of the peers was malicious and decided to tamper with the transaction between John and Michael. For example, instead of sending 0.2 Bitcoins from John to Michael, Phillip records the transaction as John sending 0.2 Bitcoins to Phillip himself.

To do this, he would have to recalculate every nonce in the folder and convince 51-percent of the network to agree with him. More importantly, he'd have to expend a great deal of energy and somehow get the rest of the peer network to collude with him.

This 51-percent vote is a consensus algorithm that involves multiple peers in the network. This is like having a jury of peers validate the integrity of the folder, its pages, and each transaction within.

Satoshi accomplished his goal. Ownership of Bitcoin is accomplished without the need for a middle man.

Why do these special peers perform this compute intensive work?

Satoshi created an elegant way to encourage a special subset of peers in his network to expend energy and help secure the network.

Once a page is full and ready to be sealed, the special subset of the peers attempts to solve the required computer puzzle. The first one to present their proof-of-work (the nonce) is awarded some Bitcoin that is created from thin air, like a digital mint. In this way, the special-peers are said to have **mined** the new Bitcoin.

As such, these special-peers are known as **Miners**.

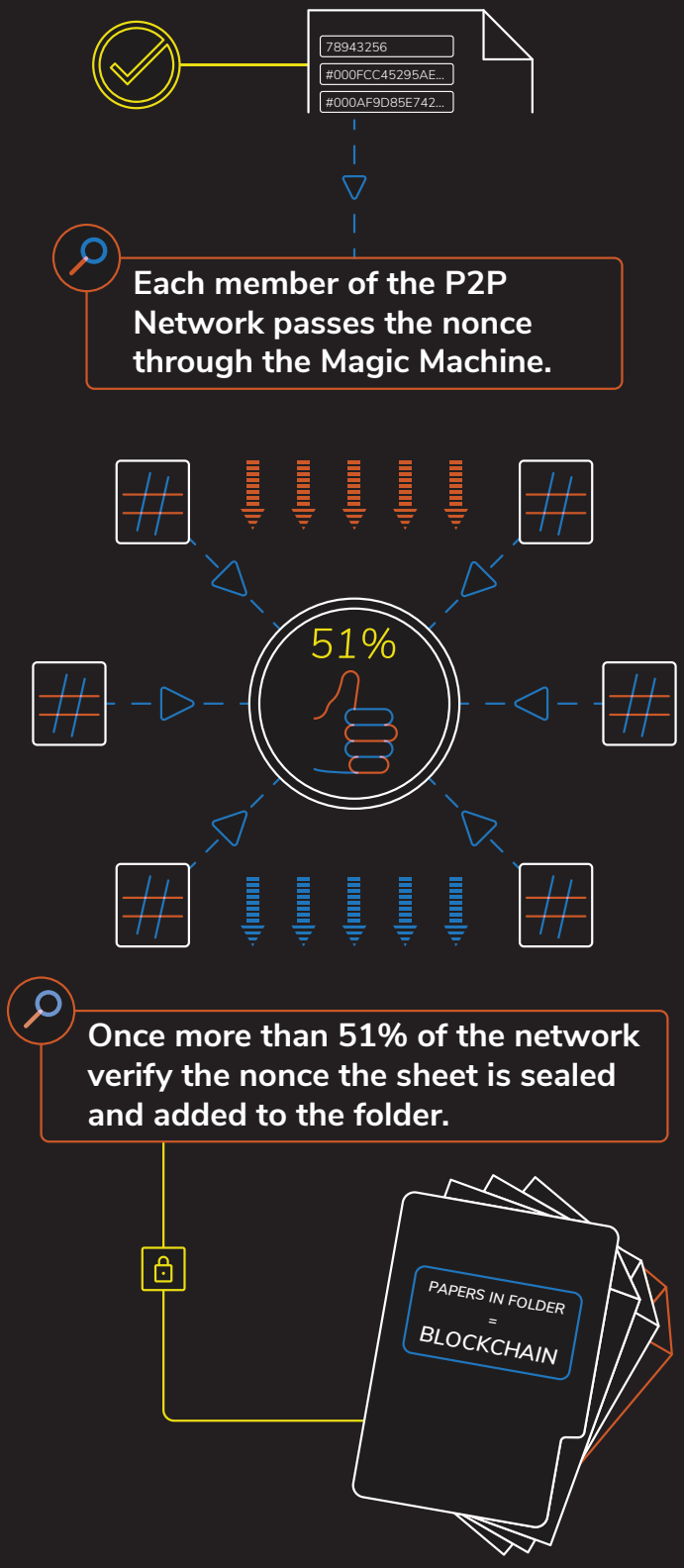


FIGURE 8: THE P2P NETWORK REACHES CONSNSUS AND ADDS THE SHEET TO THE FOLDER.

Blockchain: A Decentralized Integrity Platform

To create Bitcoin, Satoshi combined a peer-to-peer network with cryptographic technology to create a distributed ledger that maintains its integrity through a simple consensus algorithm.

More importantly, he accomplished this without the need for a central authority nor the need to trust any of the participants in the network.

Satoshi's blockchain is therefore an elegant suite of technologies to create a peer-to-peer network that supports the ownership of a digital currency – Bitcoin. The Bitcoin network is secure, has no limit to its size, and unlike a central bank has a limit to the total number of Bitcoins that will ever be minted – 21 million.[11]

Over the years as Satoshi's design has been examined, it's become clear that blockchain is useful for achieving and maintaining integrity in any distributed system.

Satoshi Nakamoto, whose identity remains a mystery, created something bigger than Bitcoin.

He created a new way to manage the ownership of any digital asset without the need for a middleman or trusted peer network.

The underlying technology to the Bitcoin network has unleashed one of the greatest opportunities for innovation in the past decade.

The excitement about the blockchain is based on its ability to serve as a tool for achieving and maintaining integrity in purely distributed peer-to-peer systems that have the potential to change whole industries due to disintermediation."[12]

By removing the need for a middleman, one lowers potential security concerns from hacking to corruption as well as speeding up manual processes that are antiquated and can take too long."

GS Equity Research, 2015

Sources

[1] Popper Nathaniel, *Digital Gold: Bitcoin and the Inside Story of the Misfits and Millionaires Trying to Reinvent Money*, Harper Collins, New York, May 19, 2015

[2] Nakamoto, Satoshi, *Bitcoin: A peer-to-peer electronic cash system*, www.bitcoin.org, 2008.

[3] https://coinmarketcap.com/

[4] Marketcap with Prices Of Cryptocurrencies Like Bitcoin & Ethereum https://www.ccn.com/marketcap/

[5] Schonfeld, Erick. Shawn Fanning And Sean Parker Talk About Airtime And "Smashing People Together". TechCrunch. June 4, 2018

[6] https://www.pcworld.idg.com.au/article/22380/requiem_napster/

[7] Drescher, Daniel, Blockchain Basics: A Non-Technical Introduction in 25 Steps, Germany, 2017

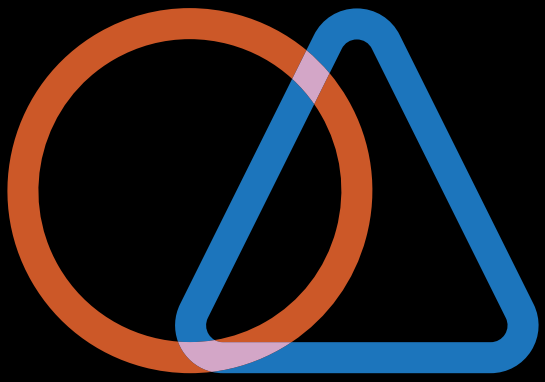
[8] https://en.bitcoin.it/wiki/SHA-256

[9] Drescher, Daniel, Blockchain Basics: A Non-Technical Introduction in 25 Steps, Germany, 2017

[10] https://www.coindesk.com/price/

[11] https://bitcoin.org/en/faq

[12] Drescher, Daniel, Blockchain Basics: A Non-Technical Introduction in 25 Steps, Germany, 2017



Visit
www.solunacomputing.com
for more information.