BR.
THE BLOCKCHAIN REVIEW

Bitcoin White Paper Made Simple

A guide to understanding the Bitcoin white paper for people without an advanced degree in computer geekery

CONTENTS

WTF

Most of us regular folk have been scratching our heads in utter bewilderment ever since the release of the Bitcoin White Paper in 2008. I mean common. WTF is going on, right?

Take a look at this...

> *To implement a distributed timestamp server on a peer-to-peer basis, we will need to use a proof-of-work system similar to Adam Back's Hashcash [6], rather than newspaper or Usenet posts. The proof-of-work involves scanning for a value that when hashed, such as with SHA-256, the hash begins with a number of zero bits. The average work required is exponential in the number of zero bits required and can be verified by executing a single hash. For our timestamp network, we implement the proof-of-work by incrementing a nonce in the block until a value is found that gives the block's hash the required zero bits. Once the CPU effort has been expended to make it satisfy the proof-of-work, the block cannot be changed without redoing the work."*

Yep. This is not a drill.

That's a real excerpt from the Bitcoin White Paper. In fact, it addresses one of the most important elements in Bitcoin.

But let's be honest.

If you're like most people without an advanced degree in computer science or engineering, the excerpt above is just one of many examples that makes you feel overwhelmed, frustrated and bamboozled.

Don't worry though. You're not alone.

The Intrepid team has heard your distress calls, and we're here to help.

Who should read this guide?

This guide will break down the Bitcoin white paper so that people without an advanced degree in computer geekery can understand what Bitcoin is, how it works and the problems it solves. By extension, you will also gain a better understanding of blockchain, the underlying technology that enables Bitcoin to operate. If you have a general idea about Bitcoin but just can't seem to make sense of it all, this guide is for you.

The guide is **not** for people with advanced knowledge of Bitcoin nor will it make you an expert. With this in mind, we will be leaving out some of the more hardcore technical elements that are irrelevant to you gaining a fundamental understanding. We will also be expanding on some concepts where needed.

Why should you care?

That's easy. The Bitcoin white paper is one of the most important documents to get your head around if you want to understand what cryptocurrencies are and how they work.

The Bitcoin white paper is not only considered the most seminal piece of work in the cryptocurrency movement, it also gave birth to a transformative technology called blockchain.

If you can digest the central concepts in the Bitcoin white paper, the broader decentralized revolution, which involves hundreds of different cryptocurrencies and other types of blockchain-based applications will begin to make a lot more sense.

Background

It's late 2008, and the global financial crisis is causing shock waves around the world. Anger at the worldwide banking industry, governments and other centralized authorities has reached fever pitch.

Enter a mysterious figure named Satoshi Nakamoto, whose real identity continues to remain shrouded in mystery to this day.

Satoshi authors and releases a white paper titled Bitcoin: A Peer-to-Peer Electronic Cash System. The paper shared the workings for a new digital currency system that didn't rely on banks to facilitate transactions or governments to create and disseminate the currency.

Shortly after its release it is studied by members of the Cypherpunk group and found to be extremely promising. In January 2009, the first transaction takes place between Satoshi and Hal Finney, a developer and prominent member of the Cypherpunk movement.

And the rest is history. Today, almost everyone has heard about Bitcoin and its value has skyrocketed. Even more profoundly, the Bitcoin currency along with its core blockchain operating technology has managed to propel a decentralized revolution around the world. For a complete timeline of Bitcoin from 2007 onwards, visit http://historyofbitcoin.org/ .

A quick note before we begin:

The Bitcoin White paper can be split into four main sections:

- Abstract - An overview of the entire paper (Not important, we will skip this)
- Section 1 - Introduction - Problems with digital transactions & introduction to the Bitcoin solution
- Sections 2 - 11 How the Bitcoin system works
- Section 3 - Conclusion - Summary of the key features proposed in the paper

This guide will examine each section (except the abstract) and follow the same order as the Bitcoin paper.

Introduction

In the introductory section, Satoshi argues that digital transactions are too reliant on financial institutions and other intermediaries due to something called the double-spending problem. This reliance means that digital transactions are expensive and slow.

To overcome the double spending problem, Satoshi proposes a new system called Bitcoin which enables people to conduct direct electronic bitcoin payments without needing to rely on costly intermediaries.

What you need to know

Historically, when it comes to transacting money or anything of value, people and businesses have relied heavily on intermediaries like banks and governments to ensure trust and certainty.

Middlemen perform a range of critical tasks that help build trust into the transactional process. Things like payment authentication & record keeping.

The need for intermediaries is especially acute when making a digital transaction.

That's because the internet today is an internet of information, where information is copied and distributed around the world.

Think video, email, any digital file.

For example. When you read an email, you are actually looking at a copy of the original. The person who sent you the email has the original email while you have a copy.

This may seem obvious, but when you spend money

online, you are not sending physical currency notes. Only data, which represents the transaction of currency (USD, YEN, POUNDS, etc.) is getting sent. So, money in the digital world is just another piece of data like an email or any digital file.

Until now, in this Internet of information, it has been impossible to store, move and transact money or anything of value without relying on an intermediary.

That's because there's a big problem.

Things don't work so well if you can send someone $100 online, yet still, have that original $100 under your name. That would mean you could just keep spending that $100 as many times as you wanted. The money would become meaningless.

This problem doesn't exist in the physical world. After a person spends physical currency like US dollars, they no longer have that cash (the actual notes) in their possession. They can't, therefore, spend the same money over and over.

The digital world is a different beast. Intermediaries like banks are needed to facilitate transactions and solve the double spending problem thus creating trust between parties. They do this by ensuring the records of who owns what is up to date at any given time.

For example, if you spend $100, banks ensure that your account balance decreases by $100 and the account of the person or organization you transacted with increases by $100. No double spending can occur.

The reliance on intermediaries to facilitate online transactions and prevent double spending has two main disadvantages:

- Non-reversible transactions are not possible as intermediaries like banks have to mediate any disputes that arise. With the possibility to reverse a transaction through mediation, the need for trust between parties increases as does the need for trusted intermediaries.
- The cost of financial institutions to resolve disputes and deal with fraud (mediate) increases transaction costs, thereby, making small or micro-transactions impractical. Think about it. Why would anyone digitally transfer or spend $1 if the transaction costs worked out to be even greater than the amount being transferred or spent?

To overcome the double spending problem which results in a reliance on intermediaries and a whole new set of issues (inability to make non-reversible transactions, increased costs, etc.), Satoshi proposes a new electronic payment system that relies on sophisticated computer encryption (cryptography) instead of the trust generated by expensive and slow intermediaries.

As Satoshi puts it,

> *No mechanism exists to make payments over a communications channel without a trusted party. What is needed is an electronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with*

each other without the need for a trusted third party.

Why is this section important?

This section discusses the main problems with digital transactions today. It also briefly introduces Satoshi's solution to solve this problem.

You probably carry out online transactions all the time, but you may not have realized the central role intermediaries play in your transactions. After reading the introductory section, you should have a good idea about the nature of the double spending problem and the flow on issues it creates. You should also understand that it is the double spending problem which Satoshi seeks to solve with the Bitcoin peer to peer system.

Transactions

This section introduces the technology that enables Bitcoin to operate - You may have heard about it. It's called Blockchain!

What you need to know

From the start, it's important to clarify that a though Satoshi refers to 'coins' throughout the paper, there are no physical bitcoins.

They don't exist, anywhere.

There are only records of bitcoin transactions (data) which get stored in a big digital ledger called a blockchain. Yes! A blockchain!

The ledger history of transactions (i.e., the Bitcoin blockchain) is the actual currency.

What is a blockchain?

A blockchain is a type of distributed ledger or decentralized database that keeps continuously updated records of digital transactions (who owns what). The Bitcoin blockchain is designed as a write once read only database where records can only ever be added, not edited or deleted.

Rather than having a central administrator like a traditional database, (think banks, governments), a blockchain has a network of replicated databases, synchronized via the internet and visible to anyone within the network.

The relationship between Bitcoin and Blockchain is best summed up by Sally Davies, FT Technology Reporter:

> *[Blockchain] is to Bitcoin, what the internet is to email. A big electronic system, on top of which you can build applications. Currency is just one.*

How does this decentralized network made up of strangers spread across the world (the Bitcoin blockchain) overcome the double spending problem?

It does this by publically announcing all transactions to the network. As Satoshi states:

> *The only way to confirm the absence of a transaction is to be aware of all transactions. In the mint based model, the mint was aware of all transactions and decided which arrived first. To accomplish this without a trusted party, transactions must be publicly announced.*

What about privacy and security?

When people hear that all transactions are publically announced, a typical response is - that's an abuse of my privacy and security! I don't want my transaction history and identity presented to the world.

Don't worry. While it's true that all transactions are publicly announced, transactions use cryptography instead of relying on centralized intermediaries to provide security and privacy.

WTF is cryptography?

Cryptography is just a form of encryption that involves the creation of codes to allow information to be kept secret. It is the cryptographic element of Bitcoin which turns a transaction message into a format that is unreadable to an unauthorized user.

So even though Bitcoin transactions can be viewed by anyone on the network, they are pseudonymous. When you send and receive bitcoins, it's like writing under a screen name, pen name, alias or whatever you want to call it. This alias which comes in the form of a jumbled bunch of characters is not linked to your identity.

That's interesting, tell me more

A Bitcoin transaction is a signed piece of data that allows a transfer of ownership of a specified amount of bitcoin to an assigned address. Transactions do not get signed in a traditional sense with a pen and paper. Instead, transactions are authenticated through the generation of some code that is unique to each party and transaction.

Bitcoin digital signatures are like mathematical mechanisms that authenticate transactions. They use something called public key cryptography which is a system that uses pairs of connected keys.

A public key is publicly visible on the network, and a private key is known only to the owner of a Bitcoin. It is these paired keys or digital signatures that ensure transactions are secure, authentic and private.

Here's a look at the transaction process in a nutshell:

A sender generates a private and a public key. They then digitally sign a transaction message which ensures the transaction is authentic and non-repudiable and send their public key along with the signature and message to the Bitcoin network.

But what happens if members of the network use different transaction timelines? Members are spread around the world so won't people be able to double spend their bitcoins? How do participants in the Bitcoin network agree on a single history of the order in which transactions were received?

To avoid these issues, members of the network agree to a single transaction timeline and process transactions according to their timestamp. More about this in the next section.

Why is this section important?

Most of you will have heard about blockchain technology but wondered where it fits into the whole Bitcoin thing. Now you can understand the relationship between Bitcoin and Blockchain and see why they are so often confused or used as interchangeable terms.

Timestamp Server

In section three, Satoshi goes into more detail about how the decentralized Bitcoin network overcomes the double spending problem. He proposes a specific software that is used to digitally timestamp data called a timestamp server.

What you need to know

Even though the majority of the network agree to run on a single timeline, for a decentralized system like Bitcoin to operate without any central intermediary, there needs to be a way for the network to agree about which order transactions are generated in. That means each transaction needs to get stamped with a precise time on it.

Think about it. Without the network running on a single timeline and each transaction getting timestamped, how does a new recipient of bitcoins know and trust that the previous owner did not sign any earlier transactions? In the Bitcoin network there is no central intermediary to confirm if a transaction or previous transactions have been double spent.

The solution

The timestamp server is a piece of software that timestamps transactions when they occur. It takes a small section of the transaction data and digitally timestamps it to create a hash.

What's a hash?

A cryptographic hash is an algorithm that takes an input and turns it into an output of a fixed size. It looks like a line of jumbled up numbers and letters. There are many types of cryptographic hashes. Bitcoin, for example, uses a hashing algorithm called SHA-256.

Here's an example:

INPUT: Hello

OUTPUT: 2cf24dba5fb0a30e26e83b2ac5b9e29e1b

161e5c1fa7425e73043362938b9824

What happens after the hash is created?

- The timestamped hash is made publicly available for everyone in the network to view.
- The Bitcoin network processes each transaction in order of their respective timestamped hash.
- The hash serves as a complex computer problem that needs to be solved by miners before a transaction can be added to the blockchain for eternity.
- Each time stamp includes the previous transaction timestamp thus forming a chain of transactions aka a blockchain.

An important note

If the same coin is sent to multiple recipients only the first recorded transaction will be accepted. The transactions with later timestamps are rejected. Because the entire Bitcoin network agrees to the same transaction timeline, there are no discrepancies.

Why is this section important?

If you ever wondered how members of the Bitcoin network agree on a single history of the order in which transactions were received and overcome the double spending problem, this section has the answers.

Proof of Work

Section four is **SUPER** important. It focuses on how the Bitcoin network deters denial of service attacks and other service abuses.

What you need to know

For a decentralized system like Bitcoin to operate without any central intermediary, there needs to be a way for the network to agree about which transaction records are valid and deter any abuse of service attacks like spamming.

Although we have already learned how the Bitcoin network agrees to the order of transactions, it will help your understanding of Proof of Work if quickly go over it again.

When transactions are publically broadcast on the Bitcoin network, they do not come in the order in which they get generated. Transactions get passed from node to node in the network, but there is no guarantee that the order in which they are received at each node is the same order in which the transactions were generated.

To agree to the order of transactions, decentralized networks like Bitcoin use Blockchain technology which places transactions in timestamped blocks (groups).

All transactions in a specific block are deemed to have occurred at the same time, and each block gets linked to a chain of other timestamped blocks in chronological order.

But a big problem still remains.

If multiple blocks can be created at the same time, and blocks travel through the network arriving at different points in the network at different times, how does the network agree which additions to the ledger are valid?

Any member of the network can still collect unconfirmed transactions, create a block and send it out to the network in an attempt to add it to the validated chain of blocks (the Bitcoin blockchain).

If an ill-intentioned member of the network sends out a bunch of unconfirmed or illegitimate transactions to add to the blockchain, it could clog up the entire system by monopolizing the network's computing power, preventing the validation of real transactions from occurring.

Introducing Proof of Work (PoW)

Proof of Work aka mining is performed to facilitate transactions on the blockchain and discourage bad actors from spamming the network by sending out fraudulent or illegitimate transactions. It involves miners (members in the network with high levels of computing power) to prove that a specified amount work has been completed.

These miners must solve complex mathematical puzzles that are difficult to solve yet easy to verify. Solving these problems demands lots of expensive computational effort (lots of hardware equipment

and electricity usage), so fraudulent transactions become infeasible. They are just not worth it!

Miners that successfully solve the PoW puzzle and update the blockchain get a reward of bitcoins. (This is how new bitcoins get made) The network picks the longest valid chain with the highest amount of work as the correct chain. Consensus is reached!

Think about PoW as a system that adds a penalty or cost to members who try to present an alternate history of transactions to the network.

What does Proof of Work actually involve?

A Proof of Work problem is based on something called a cryptographic hash function. In Bitcoin, miners put new blocks of transactions through an algorithm that turns a large amount of transaction data into a fixed length aka a hash. (Remember we looked at hashing in the previous section.)

The Bitcoin network demands that a block's hash has to look a certain way. If the hash doesn't fit the required format, then the puzzle remains unsolved. It usually takes many attempts to find the solution, and as stated before, it takes a lot of computing power. Every time a miner successfully creates a hash that fits the required format, they get a reward of bitcoins, and the blockchain is updated.

Why is this section important?

Proof of Work aka mining is used to facilitate transactions on the Bitcoin blockchain and prevent attacks from dishonest members. Although Proof of Work is not a new idea, the way Satoshi used it in combination with digital signatures, and P2P networks is groundbreaking. It is Satoshi's combination of these existing concepts that provide the main innovation in the Bitcoin white paper.

Network

Section five of the Bitcoin white paper addresses the steps involved in running the network.

What you need to know

The steps involved are as follows :

- New transactions are broadcast to all computers (nodes) in the network.
- Each node collects new transactions into a block of transactions.
- Each node works on finding a difficult proof-of-work for its block.
- When a node solves the mathematical problem (proof-of-work), it broadcasts the block to all nodes.
- The network nodes only accept the new block if all transactions in it are valid and not already spent.
- Nodes then move on and start creating the next block in the chain.
- Repeat above steps.

If two nodes broadcast different versions of the next block simultaneously, the network nodes consider the longest chain to be correct and will keep working on extending it. Any nodes that are switched off and fail to receive a new block will be updated when they connect back to the network.

Why is this section important?

Bitcoin is reliant on a network of nodes and a consensus mechanism (PoW) to keep members of the network (nodes) honest and incentivized. By understanding the steps involved in running the network, you can get a better overall picture of how Bitcoin works. As you can see, the process of running the network is relatively simple.

Incentive

In section six of the Bitcoin white paper, Satoshi looks at how to incentivize members/nodes to support the network and carry out the expensive and time-consuming task of PoW, aka mining.

What you need to know

Bitcoin mining is an expensive and time-consuming task. To incentivize members to support the network a reward is given in the form of bitcoins.

The first transaction in a block creates a new coin which is owned by the person (node/miner) who solved the puzzle and subsequently created that particular block.

> *”This adds an incentive for nodes to support the network, and provides a way to initially distribute coins into circulation, since there is no central authority to issue them.”*

Unlike traditional currencies like the US dollar, Bitcoin doesn’t have a central bank to ‘print’ or produce more currency. To introduce more bitcoins into the network and motivate people to keep the system honest, miners are rewarded with new bitcoins.

Transaction fees which are additional charges added to transactions are also used to incentivize miners to keep the network operating smoothly. Once a

predetermined number of coins (21 million to be precise) have entered circulation, the incentive will then transition entirely to transaction fees.

Why is this section important?

Ever heard the term crypto-economics? The term refers to the study of economic interactions in adversarial environments. It's all about incentives and disincentives.

In adversarial P2P environments like Bitcoin, where there are no central intermediaries to keep bad things from happening, there needs to be a set of incentives and penalties to keep things running smoothly. Without a way to incentivize members, the Bitcoin network would not be able to operate.

Reclaiming Disk Space

This section is all about saving space!

What you need to know

Think about the history of transactions that have ever occurred on the Bitcoin blockchain since its inception in 2009. That's a lot of transaction data!

Think about what happens when your computer gets low on disk space. Standard processes begin to slow down, and your computer runs painfully slow, right?

Well, to save disk space and keep Bitcoin usable, Satoshi proposes old transactions get discarded after a set amount of time.

But, Satoshi isn't proposing to delete past transactions altogether. To maximize disk space and keep the entire history of the Bitcoin blockchain intact, Satoshi recommends keeping a trace or root of a transaction so that the blockchain can remain unbroken but at the same time have more space.

It's kind of like data compression where all the number of bits needed to represent data is reduced to save storage space and speed things up.

To facilitate this without breaking a block's hash, transactions are hashed in a Merkle Tree. A Merkle tree is just a hash based data structure that allows the efficient and secure verification of large amounts of data.

Why is this section important?

Bitcoin may appear all-powerful, but it has constraints just like any other network or system. Memory allocation is a critical factor in determining the Bitcoin network's storage capacity and speed of transactions.

While it's not critical for you to understand this section in depth, the main takeaway is that storage capacity is an issue in the Bitcoin network. To save space, a particular method of structuring data is used called Merkle Trees.

Simplified Payment Verification

Section eight is all about payment verification.

What you need to know

You don't have to be a miner that helps verify transactions to make Bitcoin transactions.

It's also possible to just send and receive bitcoins with a simple Bitcoin wallet.

Most members of the Bitcoin network around the world do not operate full payment verification nodes and don't have massive supercomputing power at their fingertips. Most people just own a simple light wallet aka a simplified payment verification node.

What's the difference?

Whereas Full Payment Verification wallets, also called thick or heavyweight wallets, require a complete copy of the blockchain and can verify transactions, Simplified Payment Verification wallets, also called thin or lightweight wallets, do not have a full copy of the blockchain and cannot check whether transactions are valid.

They can however securely determine whether or not a user has received transactions.

Why is this section important?

Nothing is stopping you from going online right now, buying some bitcoins and beginning to send and receive bitcoins to and from your wallet. Well

nothing except maybe regulations, but that is a whole different discussion.

Bottom line. You don't need to be a computer geek with thousands of dollars of equipment to get involved in the Bitcoin revolution. It's pretty easy!

Combining and Splitting Value

Don't be scared of the title. This is one of the easier sections to understand.

What you need to know

Have you ever wondered how varying amounts of bitcoins get handled when they are transacted?

As you may know, bitcoins can be split up, so it's not only possible to transact in full Bitcoin denominations.

Think about it like dollars and cents.

When you go to the local store, it's possible to pay for an item in a variety of ways right? 10 or 20 cent coins for example. You don't just have one dollar coins or notes in your wallet.

Just like traditional currencies such as the US dollar, bitcoins can be split into 'cents.' Whatsmore, they can also be combined to form larger transactions.

An example

You walk into a store and want to purchase something for $50. It would be inefficient for you to hand over $1 coins/notes to the shop attendant. It would also be inefficient for the store owner to individually process each of these $1 transactions independently 50 times!

It's much easier to just hand over a $50 note in one quick and easy transaction.

In bitcoin, a coin can be both split into multiple parts before being passed on and combined to make

a larger amount, thus ensuring practicality and efficiency in the network.

Why this section is important?

The way bitcoins get processed impacts the efficiency of the bitcoin network. By enabling the value of coins to be split and combined, the network can remain relatively efficient.

Privacy

Yes, you guessed it!

This section is all about privacy.

What you need to know

In the traditional banking model, privacy is achieved by limiting access to transaction information to the parties involved and the trusted third party.

In Bitcoin, however, there is no central intermediary like a bank. Instead, new transactions are broadcast to the network so all members can check that no fraudulent activities like double spending are taking place.

But what about the privacy of people making transactions?

This is where public key cryptography comes to the rescue. Transaction information is encrypted so members of the network only see a random bunch of letters and numbers.

No party that intercepts a transaction message will be able to read it. Only the holder of the private key can make sense of the message contents.

Why is this section important?

As the world digitizes at a rapid speed, data privacy has become a significant concern. Data breaches have impacted companies & government agencies around the world. From Yahoo, Sony and Target

to the NSA and US Department of Defense, sophisticated hackers are stealing highly sensitive data on an unprecedented scale.

If a breach of the Bitcoin network occurs, your address and transaction information cannot be easily linked to your identity.

Calculations

Caution: Geek porn ahead! Section ten is not for the average punter.

What you need to know

This section is getting well into the weeds. Understanding it is not only **unnecessary**, but it could also be detrimental to your mental health. Jokes aside, it will only serve to confuse you so we will skip right over it and head to the conclusion.

Take a look at this excerpt and you will see what we're talking about.

=z q p To get the probability the attacker could still catch up now, we multiply the Poisson density for each amount of progress he could have made by the probability he could catch up from that point: ∑ k=0 ∞ k e - k! · { q/ p z-k if k≤z 1 if kz} Rearranging to avoid summing the infinite tail of the distribution... 1-∑ k=0 z k e - k! 1-q/ p z-k Converting to C code... #include double AttackerSuccessProbability(double q, int z) { double p = 1.0 - q; double lambda = z * (q / p); double sum = 1.0; int i, k; for (k = 0; k <= z; k++) { double poisson = exp(-lambda); for (i = 1; i <= k; i++) poisson *= lambda / i; sum -= poisson * (1 - pow(q / p, z - k)); } return sum; } 7 Running some results, we can see the probability drop off exponentially with z. q=0.1 z=0 P=1.0000000 z=1 P=0.2045873 z=2 P=0.0509779 z=3 P=0.0131722 z=4 P=0.0034552 z=5 P=0.0009137 z=6 P=0.0002428 z=7 P=0.0000647 z=8 P=0.0000173 z=9 P=0.0000046 z=10 P=0.0000012 q=0.3 z=0

P=1.0000000 z=5 P=0.1773523 z=10 P=0.0416605 z=15 P=0.0101008 z=20 P=0.0024804 z=25 P=0.0006132 z=30 P=0.0001522 z=35 P=0.0000379 z=40 P=0.0000095 z=45 P=0.0000024 z=50 P=0.0000006 Solving for P less than 0.1%... P < 0.001 q=0.10 z=5 q=0.15 z=8 q=0.20 z=11 q=0.25 z=15 q=0.30 z=24 q=0.35 z=41 q=0.40 z=89 q=0.45 z=340

Why this section is important?

It's not. Don't get bogged down in this, you will get lost. Seriously, move along.

Conclusion

Congratulations! If you have lasted all the way to the end, you should now have a fundamental understanding of Bitcoin and Blockchain, the underlying technology that enables it to operate. In the final section, Satoshi summarizes the key points addressed throughout the white paper.

Here are the key takeaways :

- To overcome the double spending problem which results in reliance on intermediaries and a whole new set of problems (inability to make non-reversible transactions, increased costs, etc.) Satoshi proposes a new electronic payment system that relies on complex computer encryption (cryptography) instead of the trust generated by intermediaries.
- A blockchain is a type of distributed ledger or decentralized database that keeps continuously updated records of digital transactions (who owns what). It is the underlying technology that enables Bitcoin to operate.
- Instead of relying on centralized intermediaries to provide security and privacy, Bitcoin transactions use cryptography. Transaction information can't be linked to any identify because it is encrypted. Members of the network only see a random bunch of letters and numbers.
- For a decentralized system like Bitcoin to operate without any central intermediary, there needs to be a way for the network to agree about which

order transactions are generated in (to prevent double spending) and which transaction records are valid (to deter any abuse of service like denial of service attacks and spamming).

- Proof of Work aka mining is performed to facilitate transactions on the blockchain and prevent abuse of service attacks. It involves miners (members in the network with high levels of computing power) to prove that a specified amount work has been completed.
- To incentivize members to support the network and carry out the expensive and time- consuming task aka mining, a reward is given in the form of bitcoins.
- To maximize disk space and keep the entire history of the Bitcoin blockchain intact, the Bitcoin network keeps a trace or root of transaction data.
- You don't have to be a miner that helps verify transactions to be involved in the Bitcoin network. It's also possible to send and receive bitcoins with a simple Bitcoin wallet.
- A bitcoin can be both split into multiple parts before being passed on and combined to make a larger amount, thus ensuring practicality and efficiency.

BR.

About Blockchain Review

The Blockchain Review provides curated insights from industry insiders on cryptocurrency and blockchain technology, and how it's impacting business and society. Find simple and easy to understand advice for founders, developers, and investors, on how to startup, grow, and succeed in a changing world shaped by emerging technology and innovation.

Visit www.blockchainreview.io