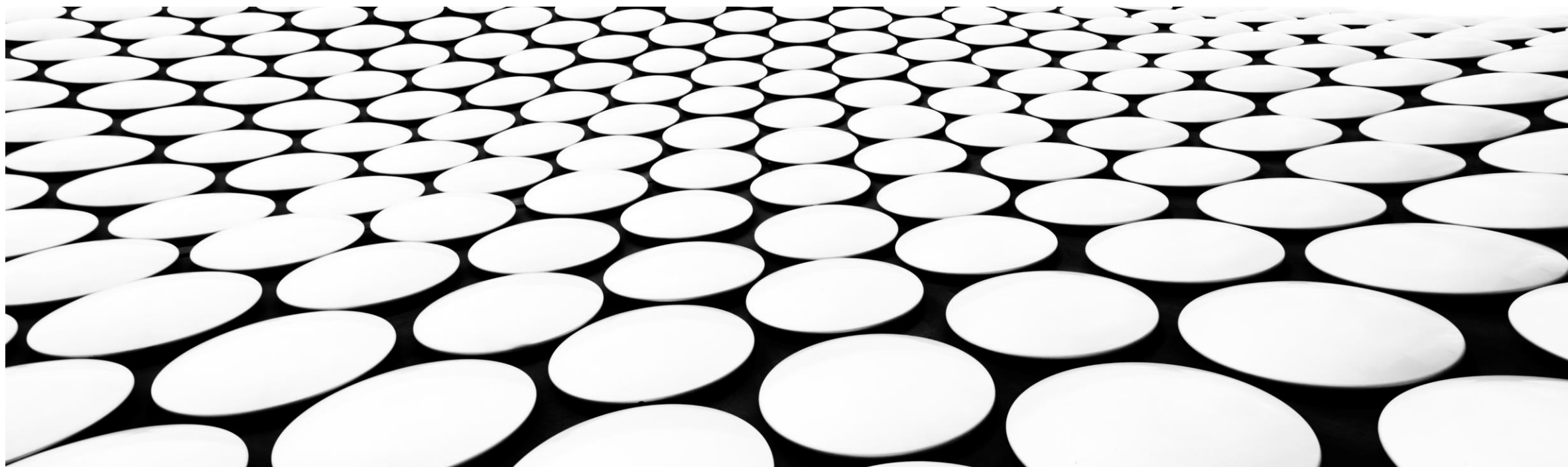

WHAT IS CRYPTOCURRENCY AND WHY SHOULD YOU CARE?

BY HASSAN AL-SAFFAR



The background features a complex, abstract composition of overlapping geometric shapes. A prominent feature is a large, bright blue shape that forms a grid-like structure with several rectangular cutouts. One of these cutouts is filled with a solid orange color. The overall effect is a layered, architectural look with sharp lines and a limited color palette of blue, orange, and white.

DISCLAIMER

I AM NOT A FINANCIAL ADVISOR!

This is not
investment
advice

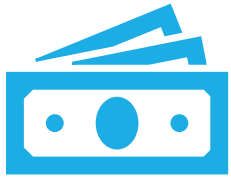
This is purely
informational



WHAT IS CRYPTOCURRENCY?

- Decentralized Digital Cash that allows money to be sent anywhere in the world at anytime
- No one entity controls crypto it is owned by the people – the technology is open source and accessible to anyone with an internet connection
- To buy and sell crypto you can download software on your phone and/or computer

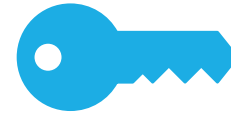
WHY IS IT CALLED CRYPTOCURRENCY?



It is a combination of cryptography and currency



Cryptography is the use of math to hide information from people not intended to see it and protect the confidentiality and integrity of data.



The use of Digital Cryptography Technology is what makes this platform secure

Symmetric (Private-Key) and Asymmetric Encryption (Public-Key)

Digital signatures

WHY SHOULD YOU CARE?

Permission less

- No one has control over your money but you

Censorship-resistant

- The design of the network makes it almost impossible for bad guys to attack it

Cheap and fast

- Money can be sent in almost an instant and at a cheaper cost




WHAT IS BITCOIN?



FIRST LET'S UNDERSTAND SOME CONCEPTS



WHAT IS DIGITAL CRYPTOGRAPHY



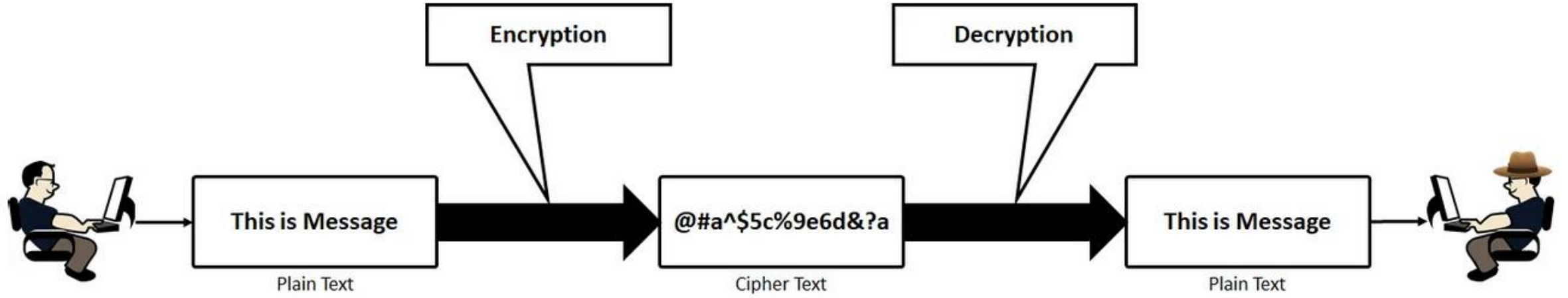
**USES THE POWER
OF MATHEMATICS
TO HIDE
INFORMATION**

Keeps information in use, transmission and storage unreadable to those not allowed to see it.

Converts plain text to cipher text. Cipher text can only be converted to plain text by those who have the keys.

These keys are what proves a person's authenticity, identity and allows verification by anyone.

This is what keeps information on the internet secure and you use it everyday without knowing it.



How Cryptography Works

CRYPTOGRAPHY BASICS

- Key Cryptography
- Hashing
- Digital Signatures

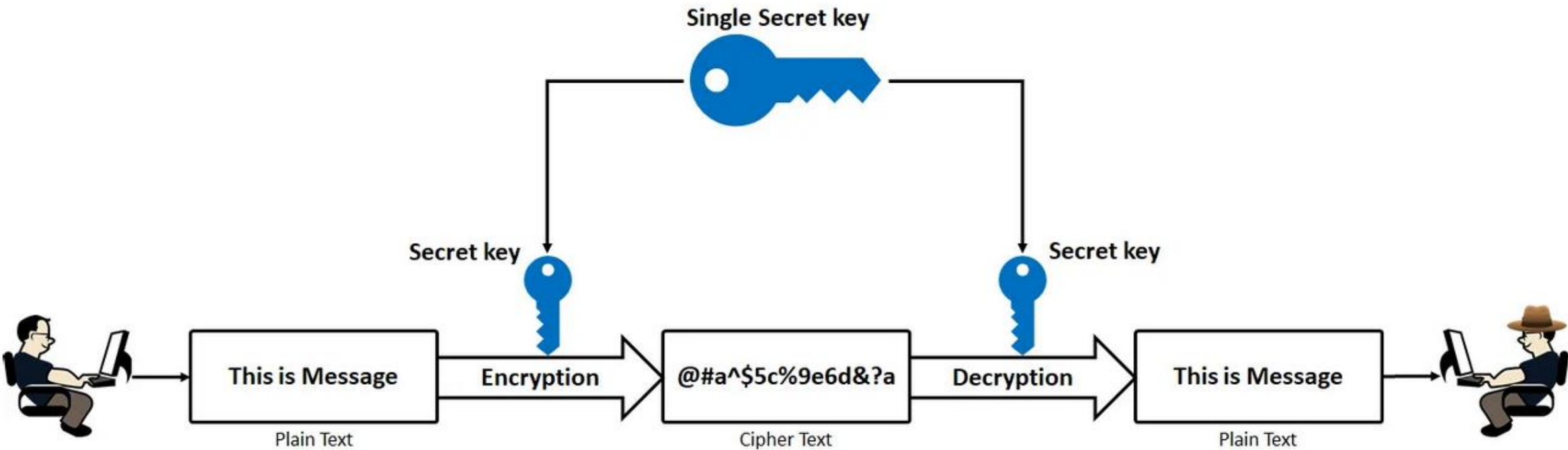
TYPES OF CRYPTOGRAPHY



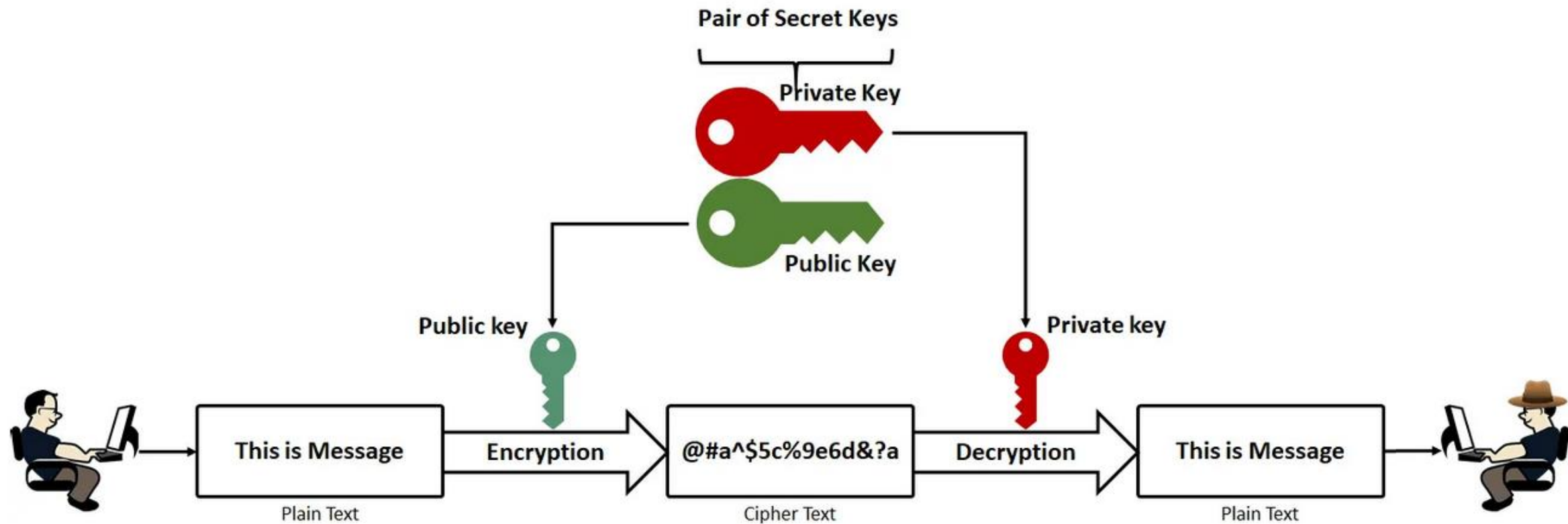
Symmetric Key Cryptography



Asymmetric Key Cryptography



Symmetric Cryptography



Asymmetric Cryptography



WHAT IS HASHING?



HASHING EXPLAINED

- Mathematical process for recording any data into a single bit string.
- Works by inputting data into an algorithm called a hashing function that produces a signature.
- This function is one way meaning it cannot be reversed.
- This ensures its integrity because any small change creates a different output, which we nerds call, a message digest.

DIGITAL SIGNATURES EXPLAINED

A hash function is used to create a message digest from the private key. This is the signature.

- Ensures message is from the sender
- Proves information was unaltered

This ensures:

- Message authenticity
- Integrity
- Non-repudiation



CURRENCY



THE FIRST DIGITAL CURRENCY

WHAT MAKES
IT DIFFERENT
FROM FIAT
CURRENCY?

WHAT IS FIAT CURRENCY?

Government issued money that is not backed by any physical commodity.

It derives its value from its issuing government and dependant on the strength of the government.

Before currency was backed by precious metals such as gold and silver, fiat gives the government more control over its currency/economy and economic growth is not as limited.

PROS AND CONS

Scarcity

Cost

Responsiveness

International
Trade

Convenience

No intrinsic
value

Historically risky

FIAT VS CRYPTOCURRENCY

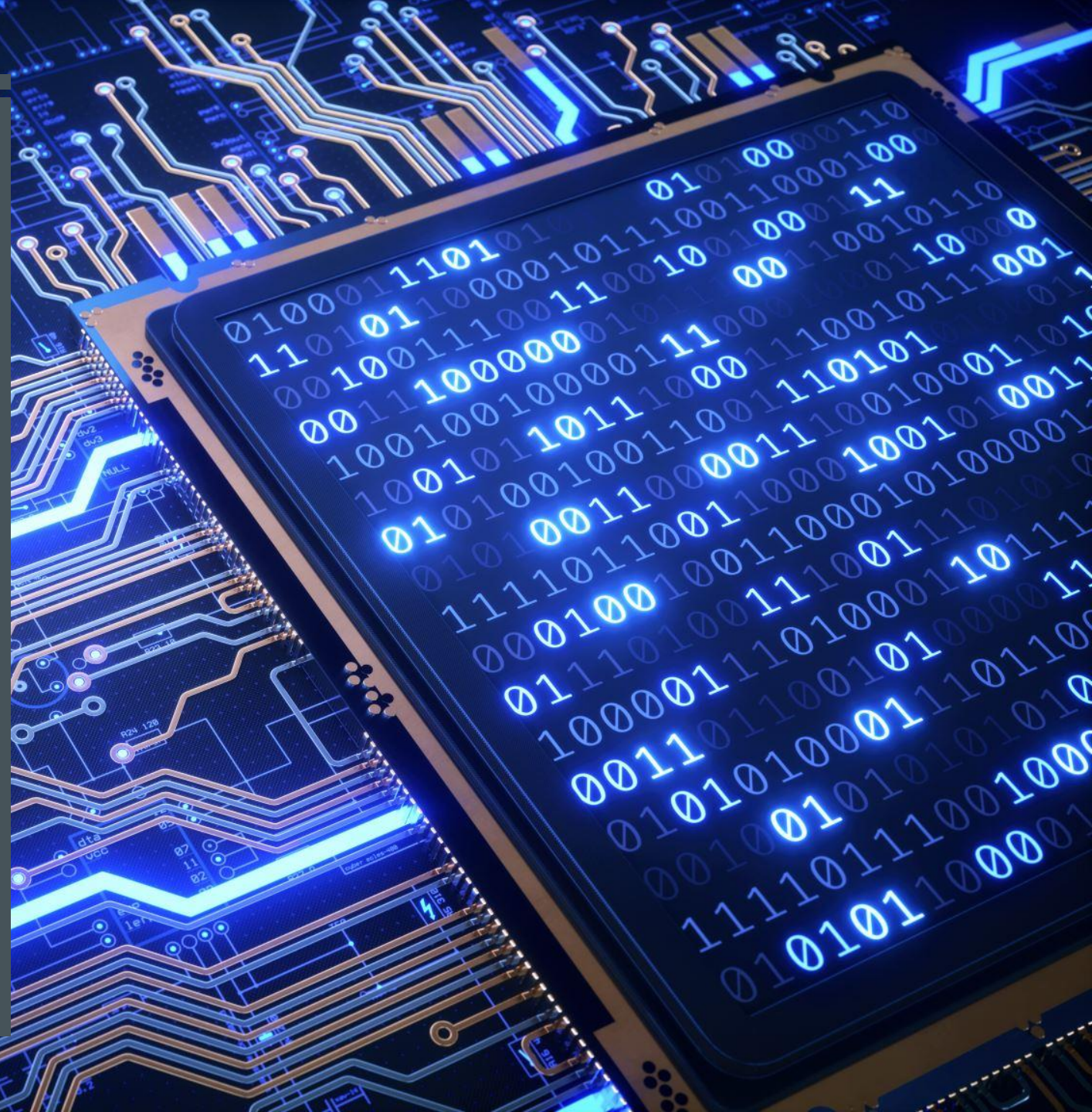
- Neither is backed by a physical commodity
- Fiat is centralized and controlled by the government, crypto is decentralized.
- The technology that makes crypto work is a distributed digital ledger called **blockchain**



WHAT IS BLOCKCHAIN?

DIGITAL DATABASE

- Append-only
- Each block is cryptographically linked, a new block must contain a digital fingerprint of the last block.
- Immutable – if there is a change then the finger print will change and since each block is linked by a fingerprint of the last block every block is changed. Everyone will notice this ensuring the integrity of the digital ledger.



ITS NOT AS COMPLICATED AS YOU THINK!

- We can create a blockchain together with a piece of paper and a pen.
- Start by creating a table of balances and everyone holds an identical copy. This is the decentralization.
- Everyone agrees on the data in the block and signs it. This is the consensus.



BLOCKCHAIN EXPLAINED



Each party records their changes in their balance and any transactions made. Everyone holds a copy.



These changes are then verified by everyone else and as long there is a majority. The new information is appended to the block.



Once enough data is in the block. A new one is made and is linked to the previous block.



This makes it difficult to go back to a previous block and change information.

WHAT STOPS PEOPLE FROM CHEATING THE SYSTEM?

- Anyone can download software, get a copy of the digital ledger, write blocks and attempt to cheat? Right?
- What if I want to write a block that says bob sent me a million dollars?

WRONG!

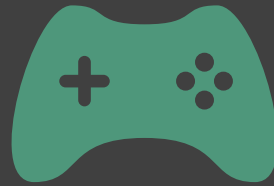


ITS ALL ABOUT MATH!

RULES DEFINED BY MATHEMATICAL CONSTRAINTS



Cryptography



Game Theory



Consensus Algorithm

A network of colorful sticks (yellow, orange, green, blue, red) connected by small yellow connectors, forming a complex, interconnected structure on a purple background. The sticks are arranged in a way that suggests a mesh or lattice, with some sticks crossing each other. The overall appearance is that of a physical model of a network or a complex system.

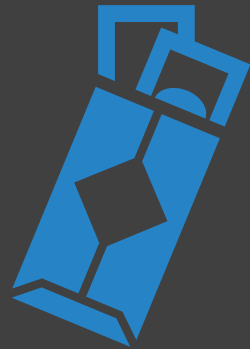
WHAT IS A BLOCKCHAIN CONSENSUS ALGORITHM?

CONSENSUS ALGORITHMS

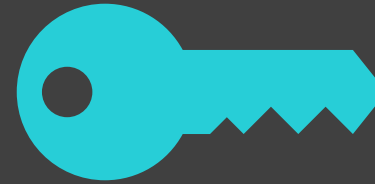
Allows machines and users to coordinate in a distributed setting and agree on a source of truth.

Fault tolerance in a system where users don't trust each other and can agree with each other.

CONSENSUS ALGORITHMS AND CRYPTO



Users' balances are recorded in a database (blockchain), everyone must maintain an identical copy.



Public key cryptography ensures users cannot spend each others' coins but... there still needs to be a single source of truth

COMMON TRAITS OF CONSENSUS ALGORITHMS

Users must provide some sort of stake to gain a reward

- Something of value that the user must put forward to participate
- If they cheat, they lose their stake
- Examples: Computing power, cryptocurrency, reputation

Transparency

- Costly to produce new blocks
- Easy for everyone else to validate

TYPES OF CONSENSUS ALGORITHMS





PROOF OF STAKE AND PROOF OF WORK



PROOF OF WORK

- The god father of blockchain consensus algorithms
- First implemented in Bitcoin but has been around for some time
- In proof of work, validators called miners hash the data they want to add until they produce a specific solution.

HASHING REVIEW

It's a digital fingerprint a fixed string of characters that is created when data is ran through a hashing function

The same data will always give the same output, if the data is changed in anyway the hash will be different.

The output will not tell you anything about the data fed into the function, providing proof that you knew about the information.

This allows other to validate when the data is revealed since it will give the same hash

HOW PROOF OF WORK GIVES VALIDITY TO NEW BLOCKS

The protocol sets out the conditions that will make the next block valid.

- Example a block with a certain hash that will be considered valid

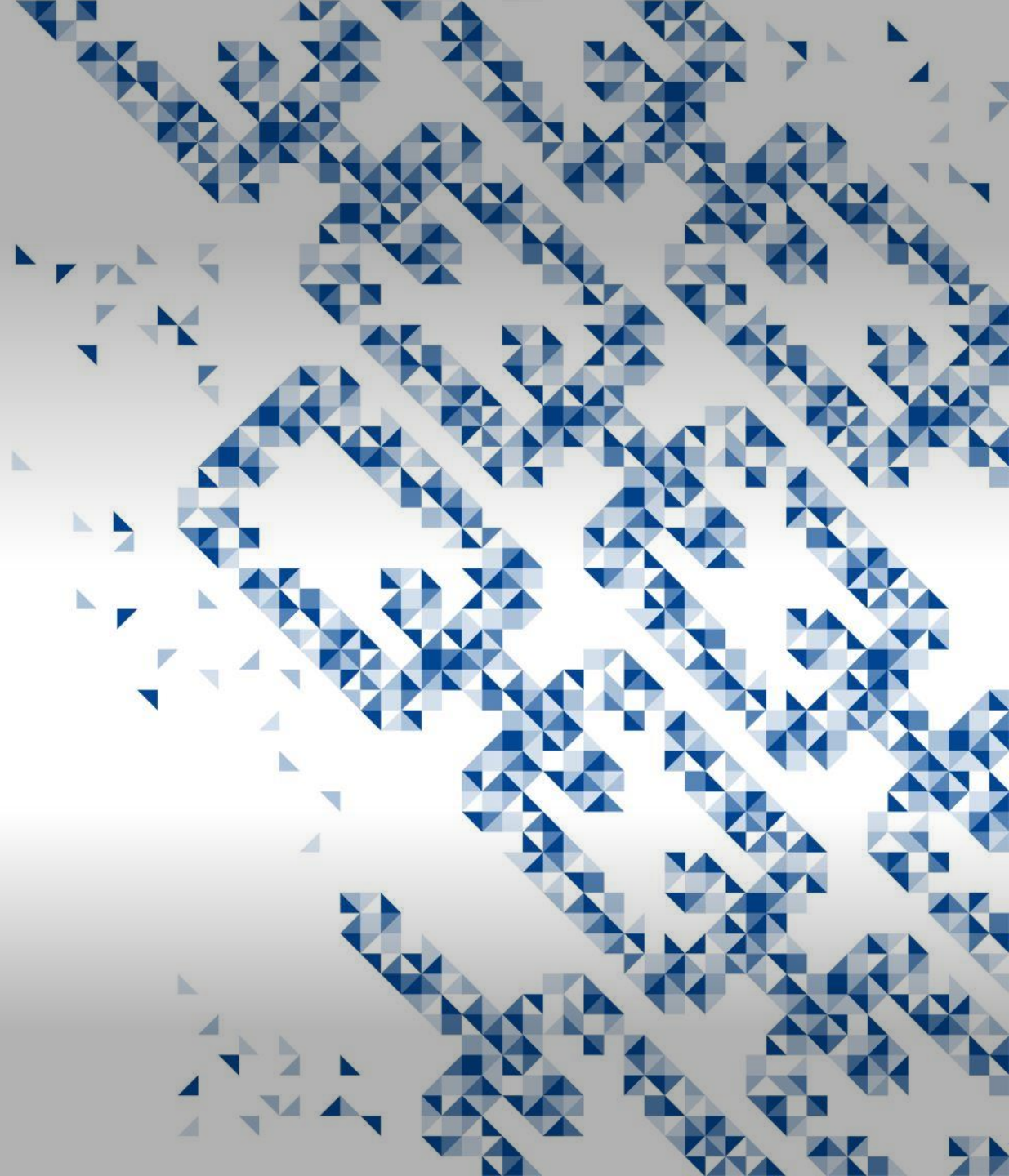
Since this number is unknown miners have to brute force inputs to become the first to obtain that hash.

The hash is known but the inputs to gain the hash are not, hashing functions are called one way or trap door functions. Easy to determine the hash when the inputs are known but hard to determine the inputs with only the hash.

Once validated they can write the new block in the chain and are awarded coins.

The stake when mining is the cost of the hardware needed and electricity.

BITCOIN



WHO INVENTED BITCOIN? NO ONE KNOWS...

It was invented by a person who goes by the alias Satoshi Nakamoto.



Satoshi published a document in 2008 outlining the working of the system and released months later.

**WHAT MAKES IT
SO INNOVATIVE?**

Decentralized

Censorship resistant

Secure

Borderless



BITCOIN EXPLAINED

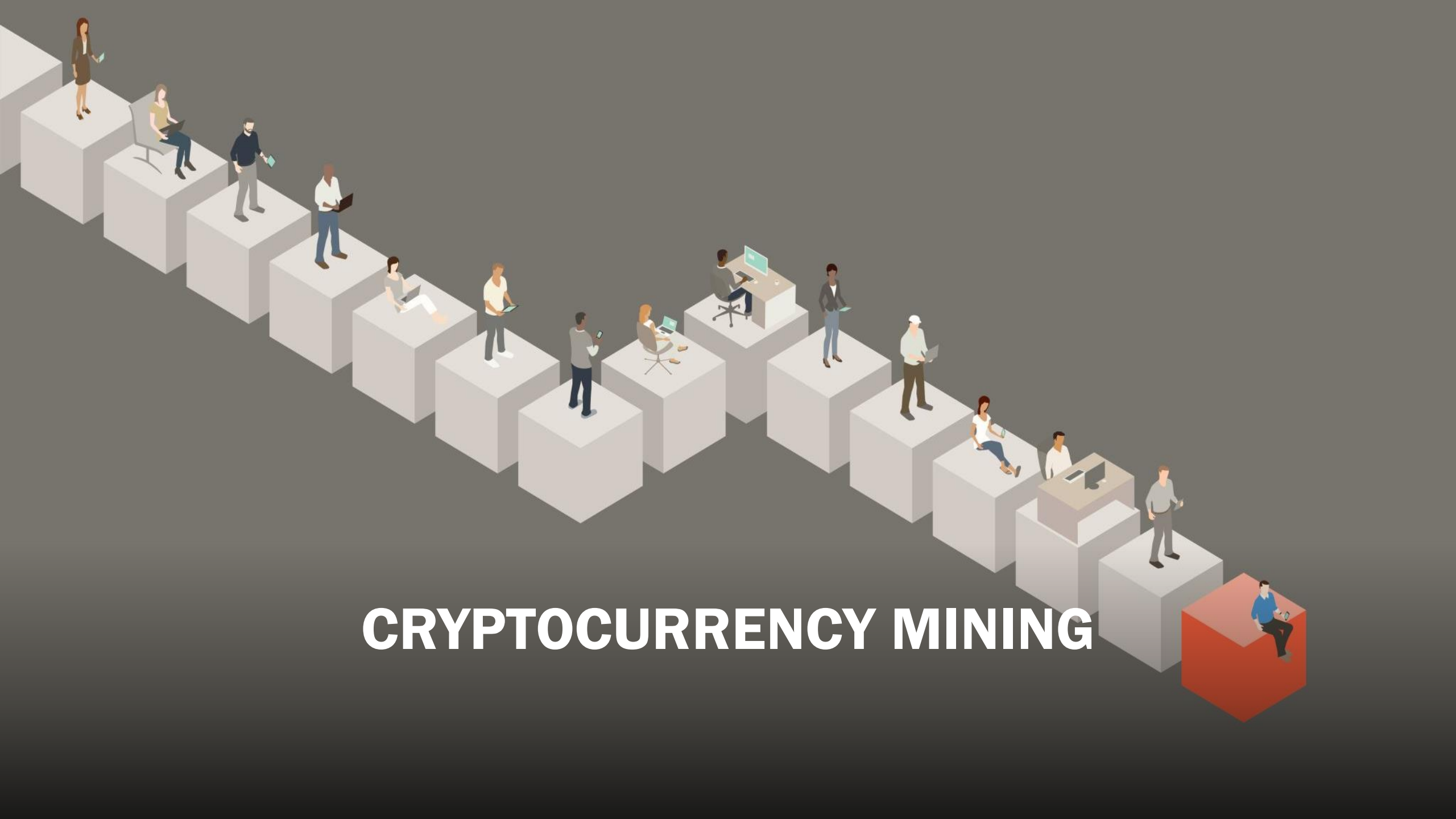
Digital money that runs on a distributed network of computers

Often referred to as, digital currency, decentralized public ledger, protocol, it is all of these.

Bitcoin is the name of the peer-to-peer currency.

Blockchain tech is what bitcoin uses to record data about transactions etc. They are different.

The protocol Bitcoin is governed by is called Bitcoin Core and is open source.



CRYPTOCURRENCY MINING

WHAT IS CRYPTOCURRENCY MINING?

The process in which transactions between users are verified and added to the blockchain.

How new coins are introduced into the supply.

Records of transactions are recorded into a candidate block which is hashed.

The protocol will dictate a hash that must be a certain value determined by the protocol.

Once this is found it is presented to the network and is validated.



WHY IS BITCOIN SO VALUABLE?

How Many Bitcoins Are There?



18,699,737.5

Total BTC in Existence



2,300,262.5

Bitcoins Left to Be Mined



89.046%

% of Bitcoins Issued



900

New Bitcoins per Day

**HOW MANY
BITCOINS
WILL EVER
EXIST?**

21 MILLION

SOMEWHERE
AROUND 3 TO 4
MILLION

**HOW MANY HAVE BEEN
LOST?**

WHEN WILL THE LAST BITCOIN BE MINED?

- Sometime around 2140
- The block rewards called halving's, divides the block rewards in half every four years.
- Currently the reward is 6.25 Bitcoin

BITCOINS USE CASE AS AN INVESTMENT



STORE OF VALUE

ITS VALUABLE BECAUSE OF ITS SCARCITY

LIQUIDITY



IT CAN BE EASILY BE CONVERTED TO OTHER FORMS OF CURRENCY

HEDGE AGAINST INFLATION

- Investors like me believe its value will go up in time protecting your earned value against inflation

CONCLUSION

1

Bitcoin has opened the door for a new paradigm of decentralized finance

2

With other iterations of this underlying technology, It has created a new wave of decentralized services

3

A shift towards a decentralized internet of applications/commodities as newer generations loose faith in our traditional institutions

THANK YOU

