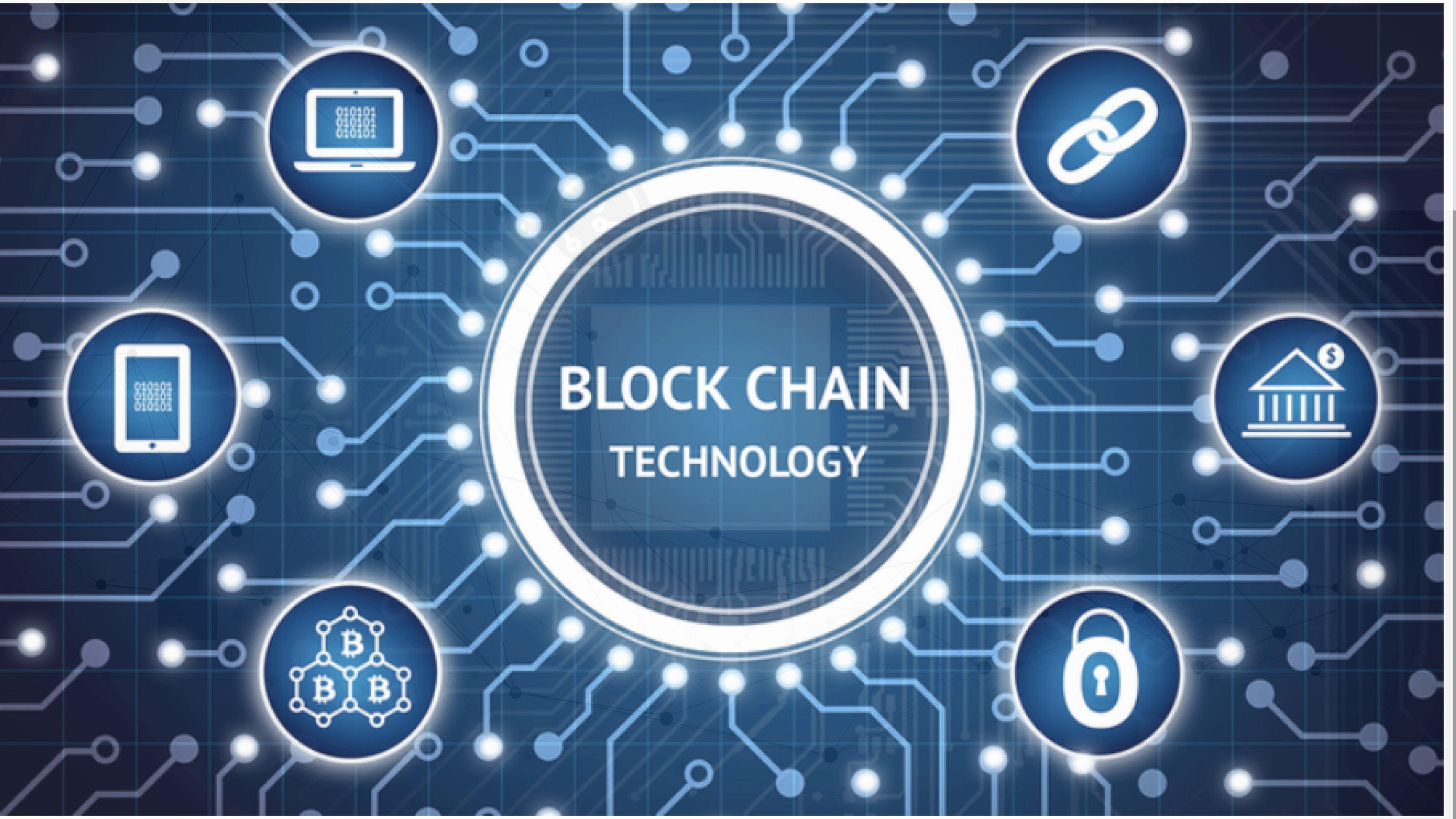

BLOCK CHAIN
TECHNOLOGY

CRYPTOCURRENCY

A cryptocurrency is a digital currency, which is an alternative form of payment created using encryption algorithms. The use of encryption technologies means that cryptocurrencies function both as a currency and as a virtual accounting system. To use cryptocurrencies, you need a cryptocurrency wallet.

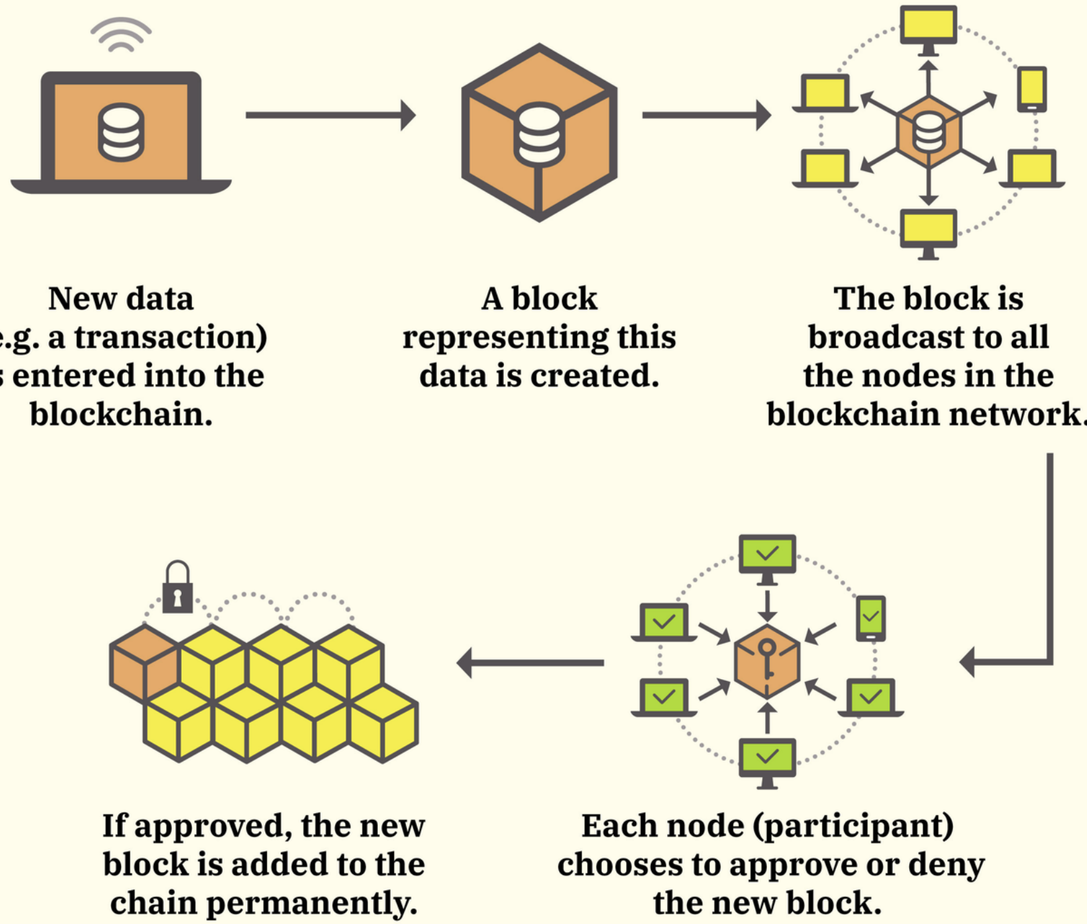
examples:

- Bitcoin
- Ethereum
- Litecoin
- Tether

BLOCKCHAIN TECHNOLOGY

Blockchain technology is a decentralized, distributed ledger that stores the record of ownership of digital assets. Any data stored on blockchain is unable to be modified, making the technology a legitimate disruptor for industries like payments, cybersecurity and healthcare.

Blockchain Process



Who Invented?

The first decentralized blockchain was conceptualized by a person (or group of people) known as Satoshi Nakamoto in 2008.

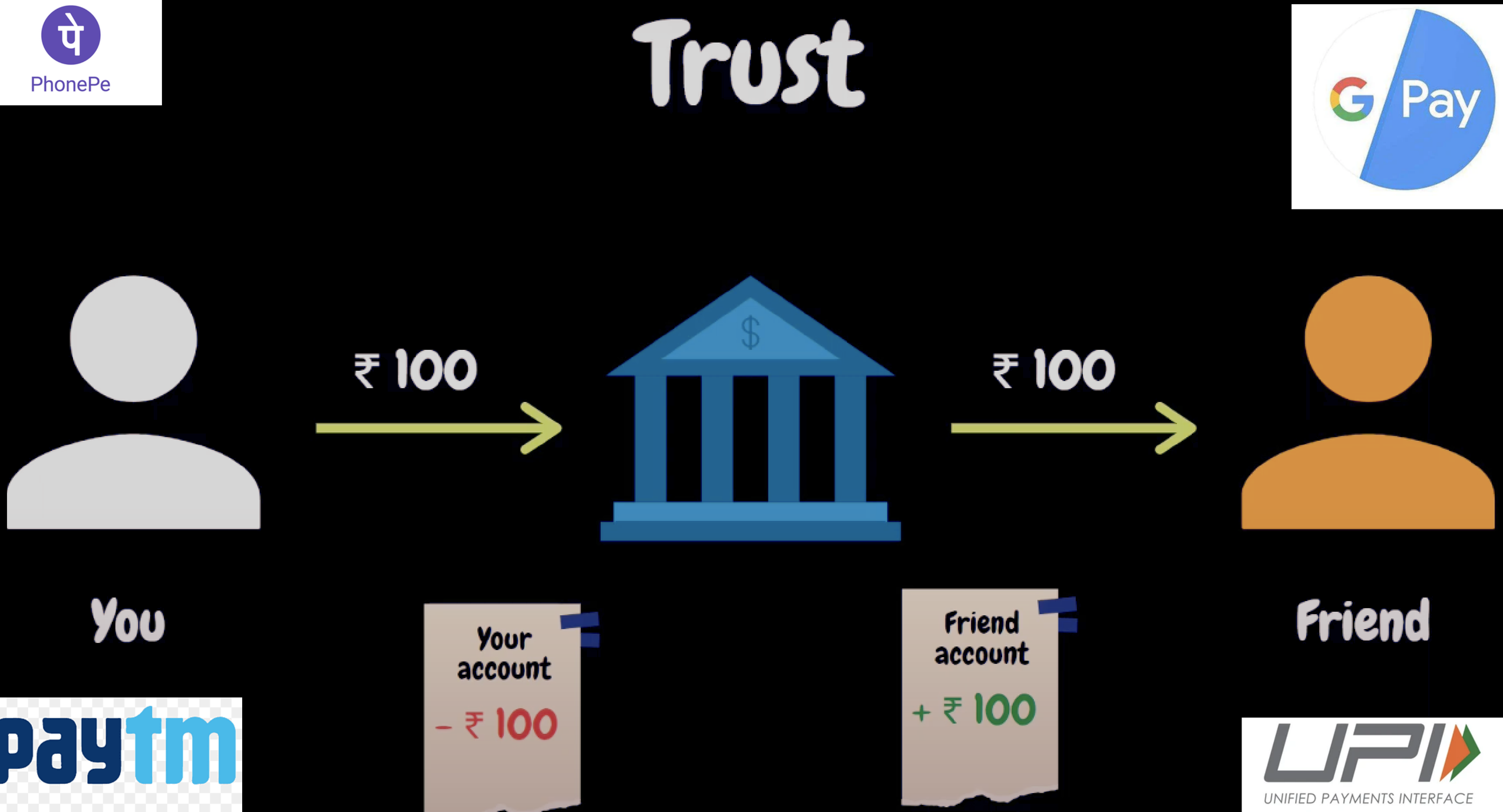
Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

PhonePe

Trust



G Pay

paytm

UPI
UNIFIED PAYMENTS INTERFACE

LEHMAN BROTHERS

Lehman Brothers Inc. was an American global financial services firm founded in 1850.[2] Before filing for bankruptcy in 2008, Lehman was the fourth-largest investment bank in the United States (behind Goldman Sachs, Morgan Stanley, and Merrill Lynch), with about 25,000 employees worldwide.

This resulted in lack of trust among peoples about concept of banks

Ledger

B pays A ₹ 2,500

C pays A ₹ 2,500

D pays A ₹ 2,500

A pays C ₹ 1,000

B pays C ₹ 1,000

D pays C ₹ 1,000

Month end Settlement

A ₹ 6,500

B ₹ 3,500

C ₹ 500

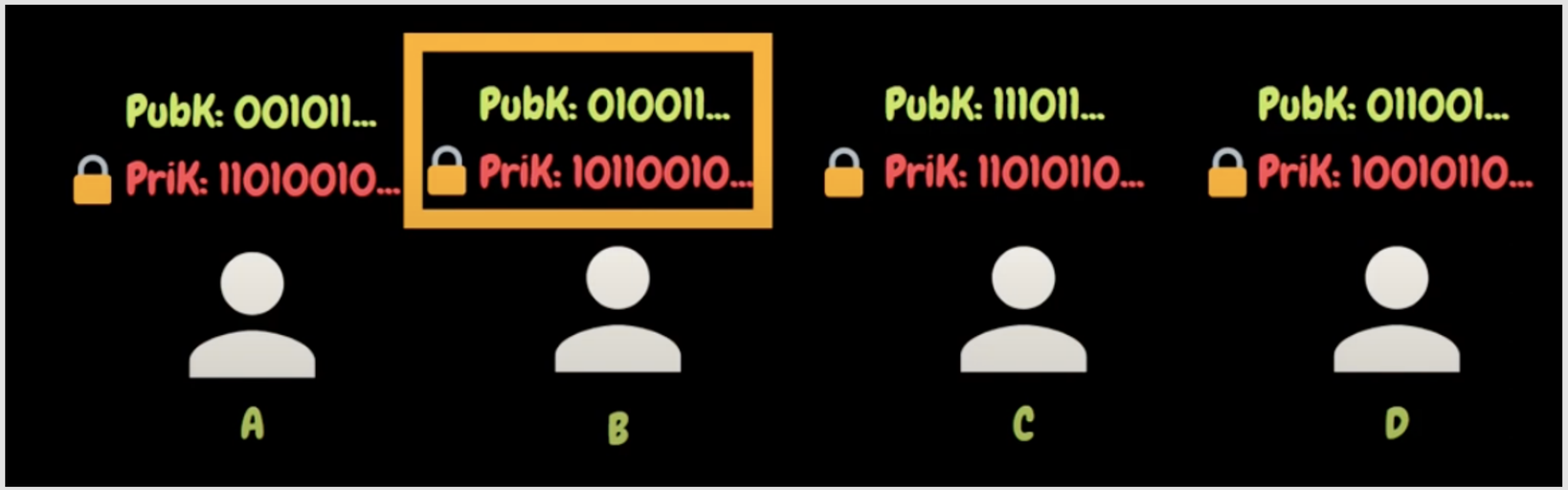
D ₹ 3,500

Limitations

- Everyone can add lines ⟶ Digital signature
- Month End Settlement ⟶ Restricting Payment
  Overloading

Digital Signature

A digital code (generated and authenticated by public key encryption) which is attached to an electronically transmitted document to verify its contents and the sender's identity.

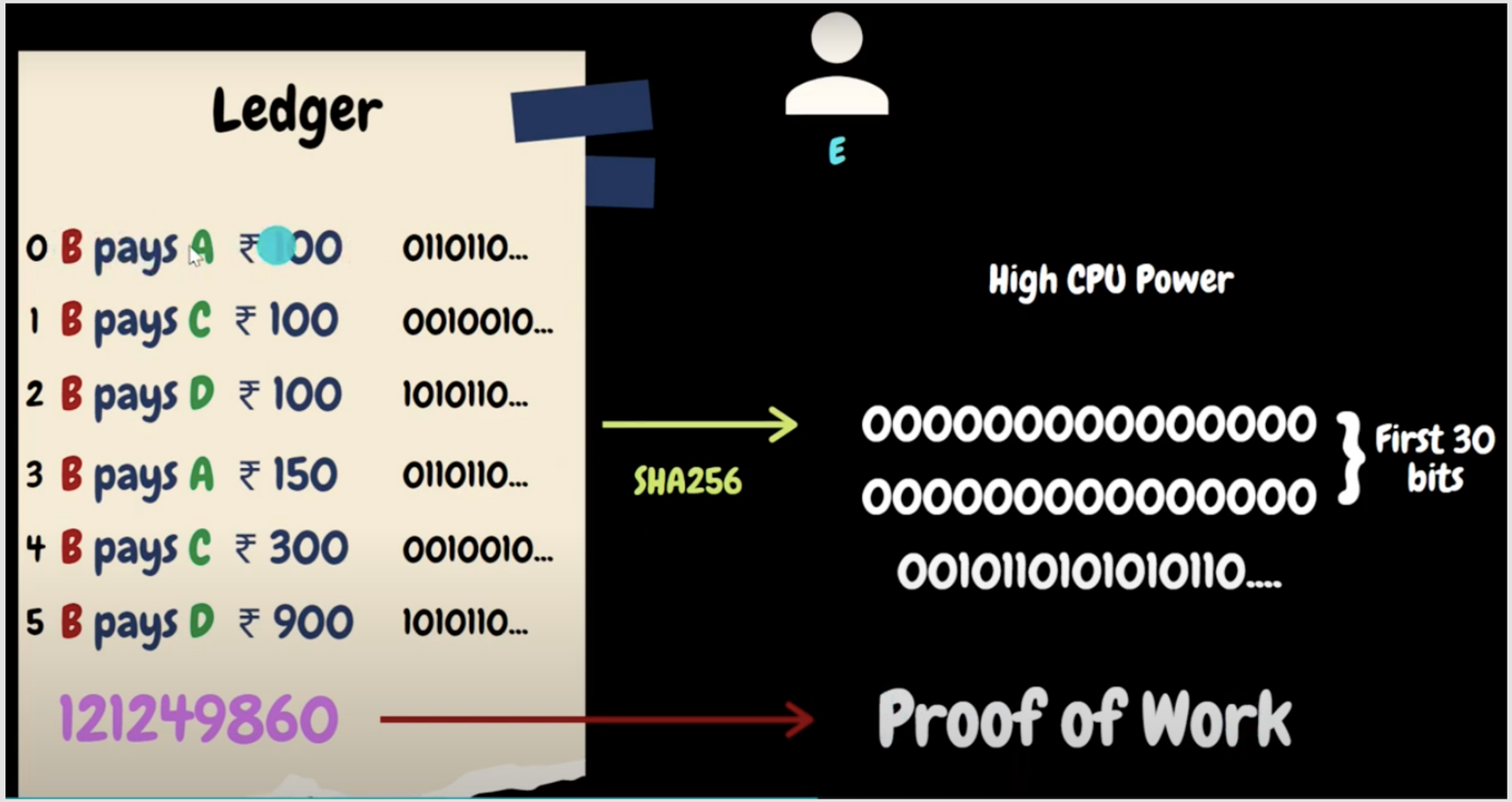


256 **bits**

Sign			Verify		
Input	→	Output	Input	→	Output
Message Private Key		Signature	Message Signature Public Key		True False

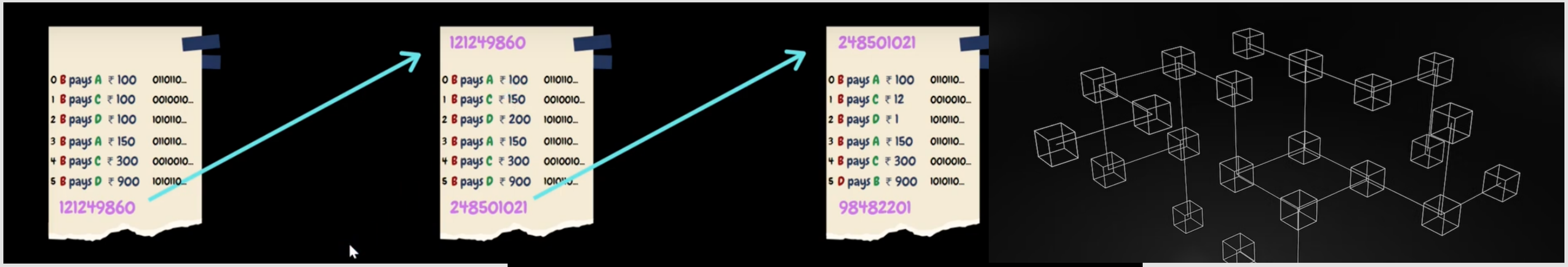
Proof of Work

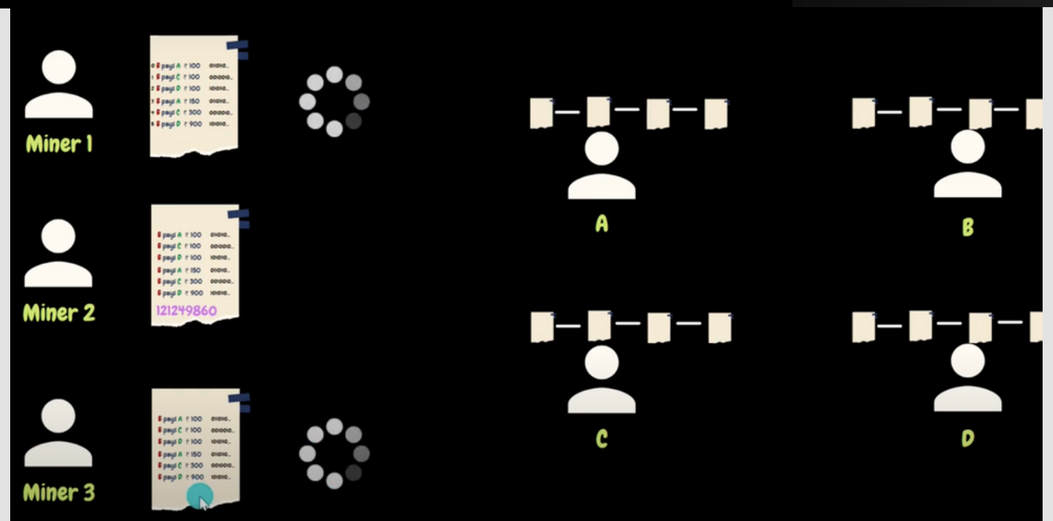
Proof of work (PoW) is a decentralized consensus mechanism that requires network members to expend effort in solving an encrypted hexadecimal number. Proof of work is also called mining, in reference to receiving a reward for work done.



Bitcoin Mining

Blockchain "mining" is a metaphor for the computational work that network nodes undertake to validate the information contained in blocks. So, in reality, miners are essentially getting paid for their work as auditors.





Pros and Cons of Blockchain Technology

Advantages	Disadvantages
Data is Immutable	Cost of Implementation
Transparency	Low Performance
Free from Censorship	Modifying Data is Hard
Traceability	High Energy Usage
Low Transaction Fees	Private Key Recovery
Heighten Security	Prone to Illegal Activity

November 2023

THANKYOU