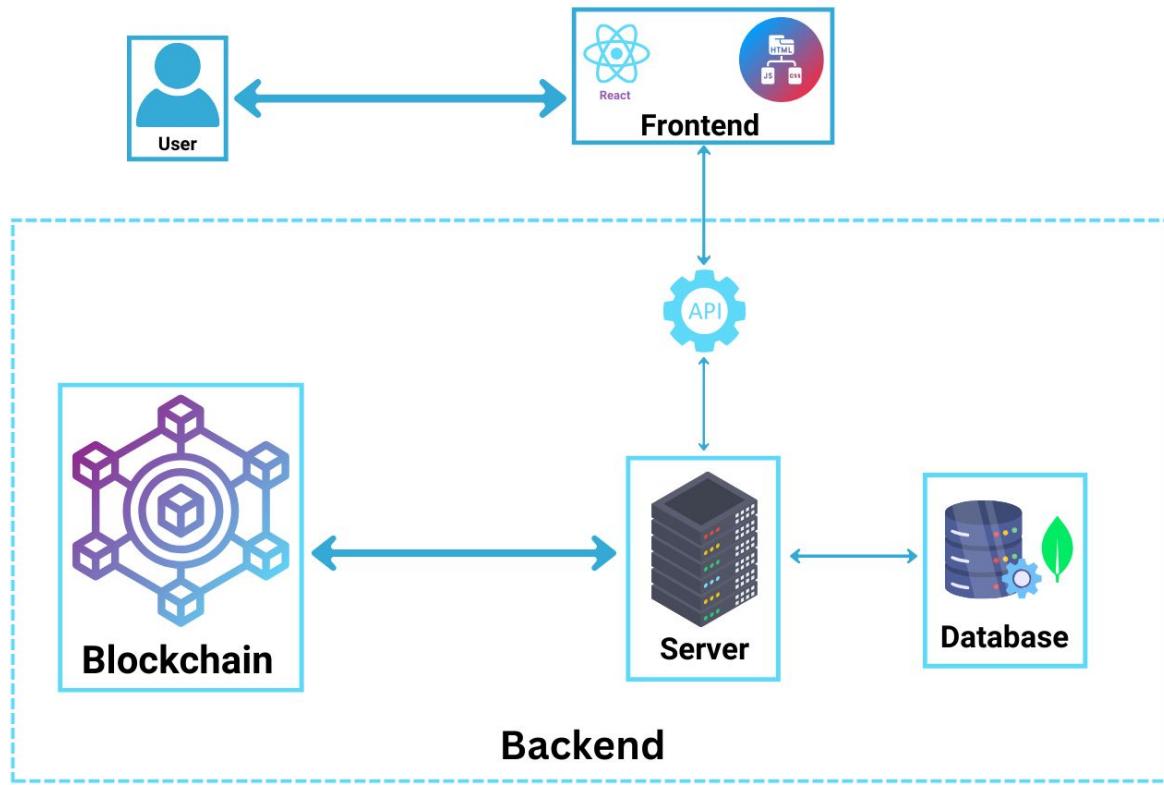


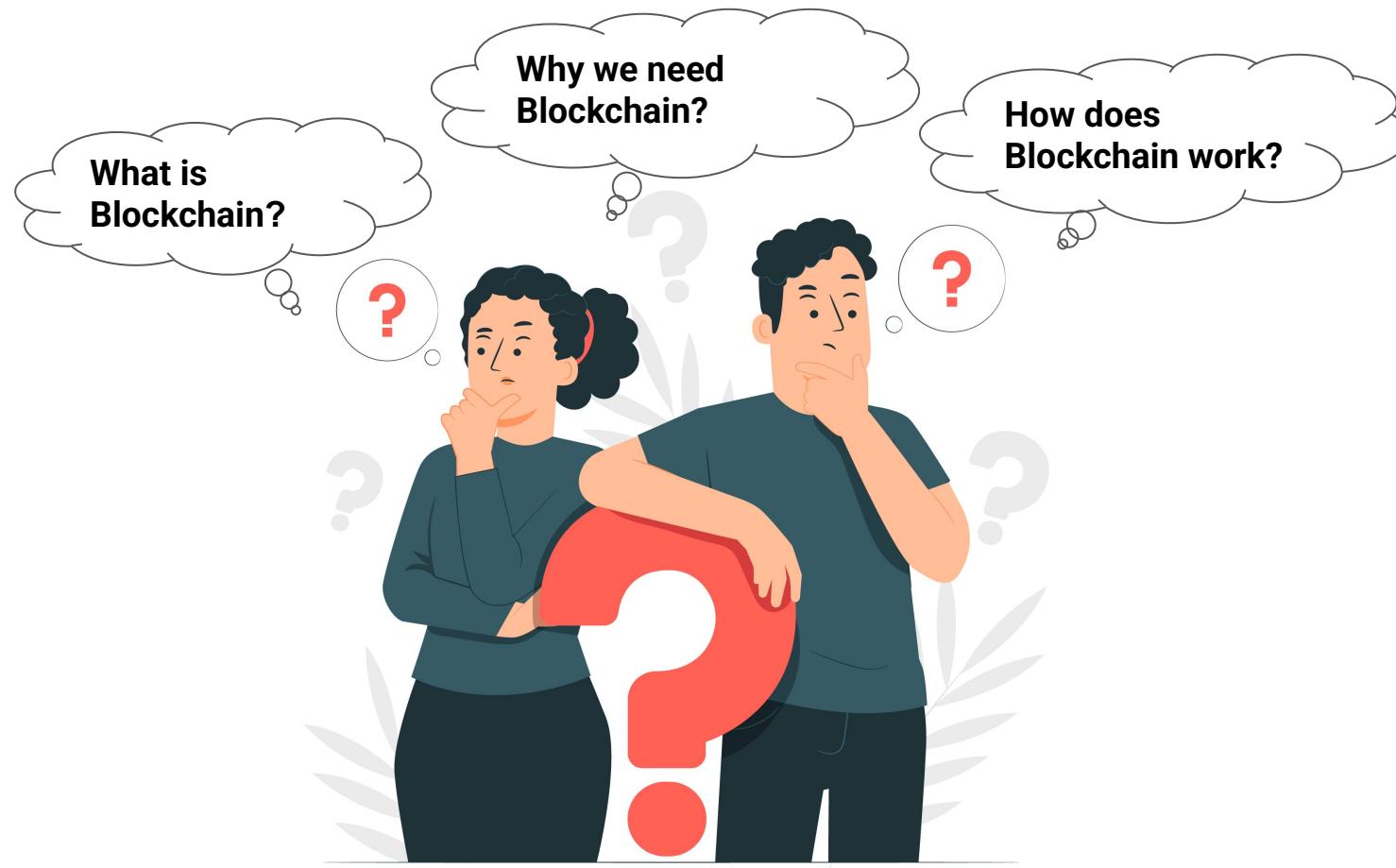
# Introduction to Blockchain

# Development Architecture



# Agenda

- Blockchain Introduction
- Consensus algorithms
- Types of Blockchains
- Application areas



# DEFINING A CHAIN

**WHAT ?**

BLOCKCHAIN  
TECHNOLOGY IS A  
**DECENTRALIZED**  
**DISTRIBUTED**  
**IMMUTABLE**  
**LEDGER** TECHNOLOGY

**WHY ?**

A REAL TIME OPEN  
LEDGER FOR RECORDING  
ANY TYPE OF  
TRANSACTION/DATA  
WITH NO SINGLE OWNER

**WHEN ?**

CAME IN A  
DOCUMENT  
OR **WHITEPAPER**  
PUBLISHED BY SATOSHI  
NAKAMOTO

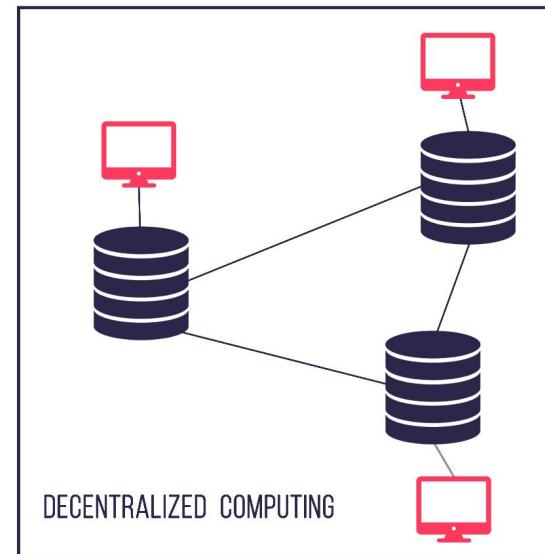
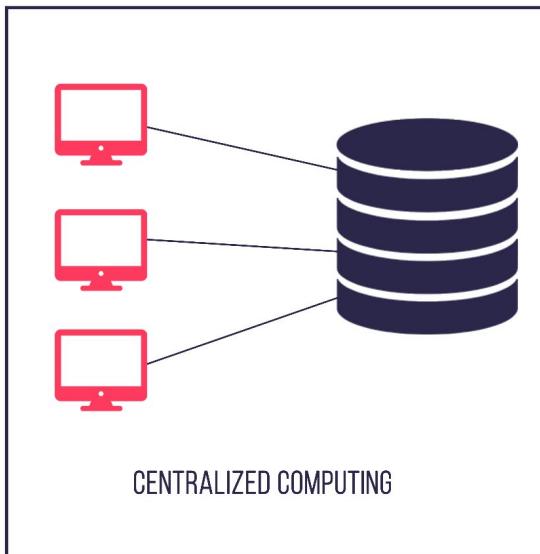


# CENTRALIZED



# DECENTRALIZED

# Decentralized Computing



2008



**"Bitcoin: A peer to peer electronic cash system" by an anonymous entity called Satoshi Nakamoto**

2009



Satoshi launches Bitcoin as an alternative to current financial system

2010



Laszlo Hanyecz bought 2 pizzas for 10,000 bitcoins (BTC). As per current price, it amounts to 29366956230 INR (Nov, 2023)

2023



**Bitcoin consumes an estimated 150 terra watt- hours of electricity annually, more than the annual consumption of Netherlands**

# The Bitcoin Whitepaper

- The idea was published in 2009 by an pseudonymous person/group of people, named **Satoshi Nakamoto**.

Goal with Bitcoin was:

- To create a **trustless** system, using cryptography
- Solve double-spending problem of previous digital currencies
- Create digital assets that can be owned, with proof of ownership

## 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.



# WHAT LIES UNDER THE HOOD ?



# Bitcoin / bitcoin / blockchain

## **Bitcoin**

A protocol for a decentralized peer-to-peer network that creates consensus without needing a central authority to provide trust.

## **bitcoin**

The currency (token) issued as a reward in the proof-of-work mining process.

## **blockchain**

The public ledger where the network records (transactions) are written.

# BREAKING IT DOWN...



PAGES

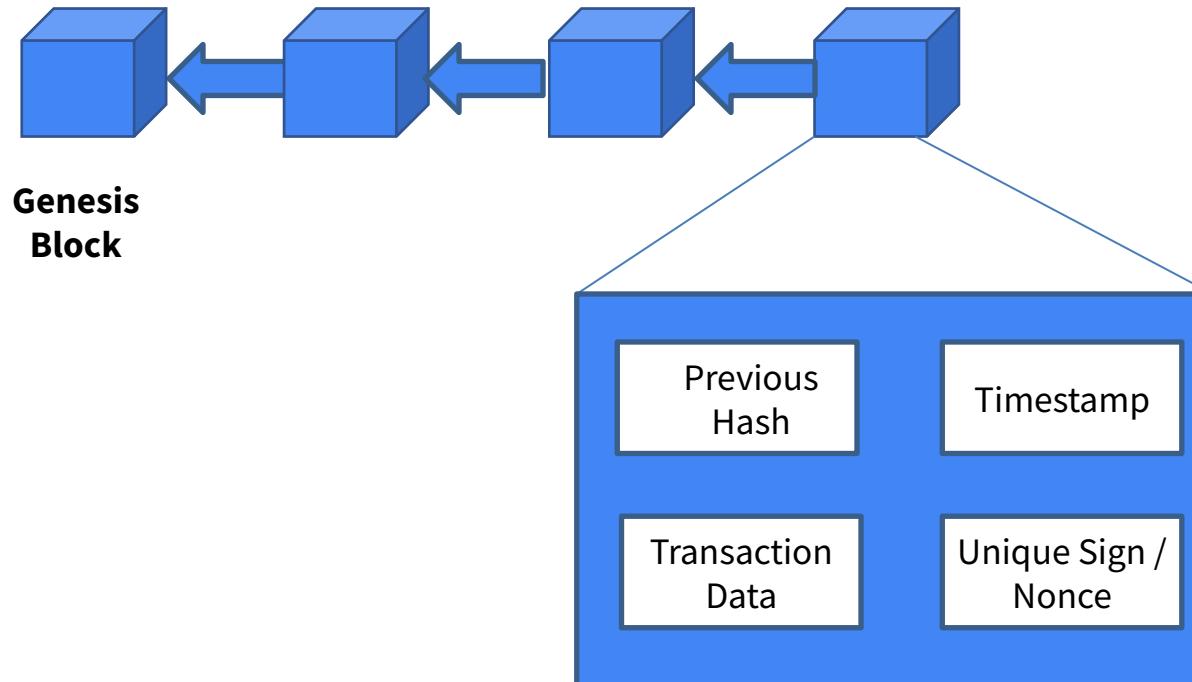


BOOKS

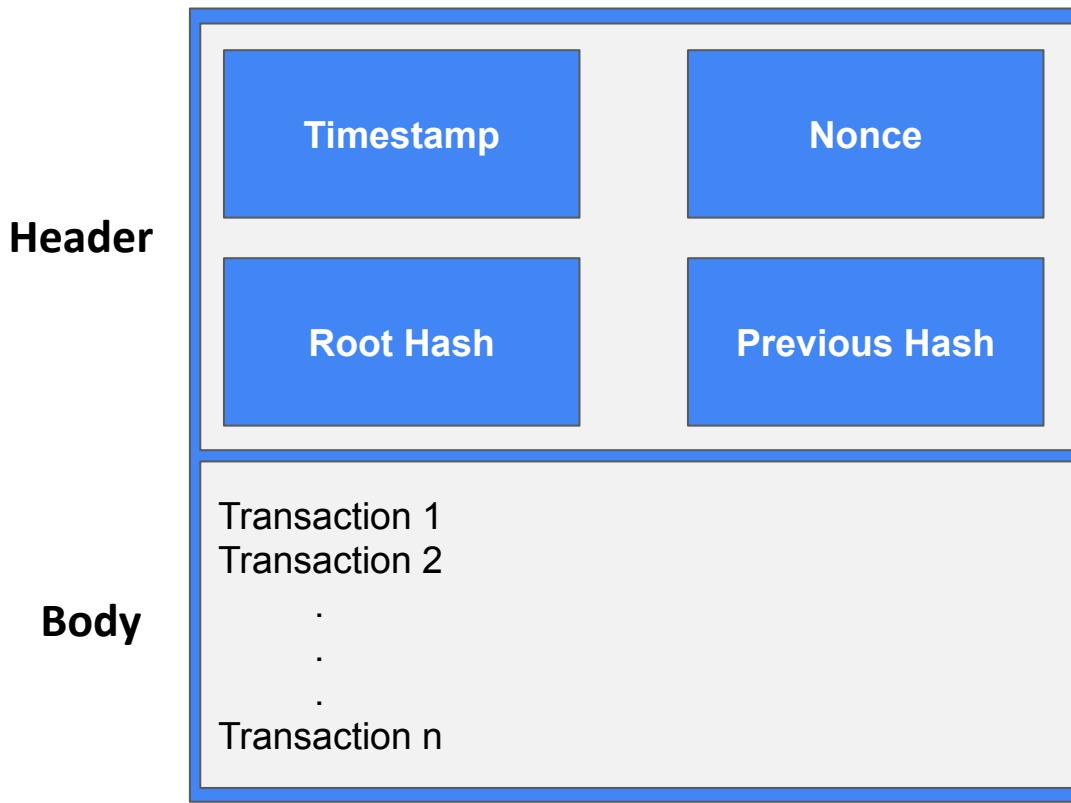


EVERYONE KEEPS A COPY

# Blockchain

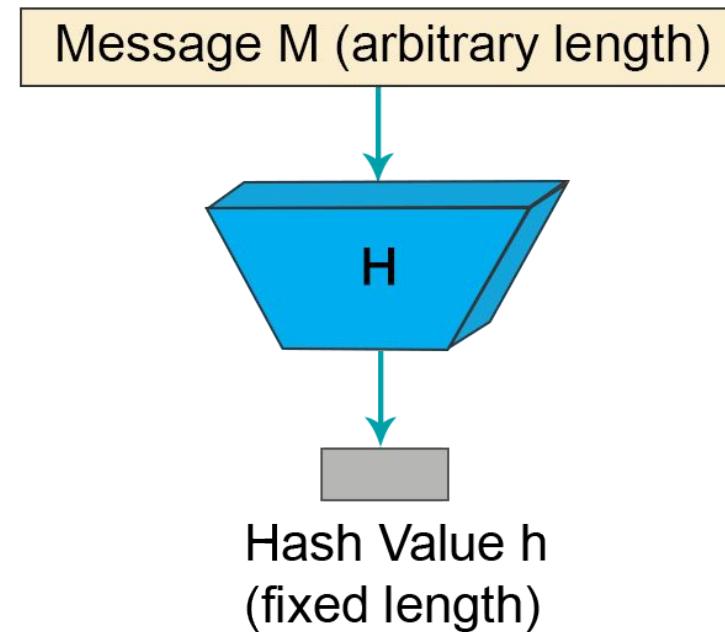


# Block



# Hash

- A mathematical function - turns data into a hash
- Takes the input data and turns it into an output of a fixed length
- Same hash for same input
- If even one character in the input text or data is changed, the output hash will change
- One-way function
- Eg:- SHA256.



Hash demo - <https://andersbrownworth.com/blockchain/hash>

# Hash Example

**SHA 256**

Input

from: person1

to: person2

amount: **5000**

Hash

A1BA93299F5836B8A58543CAD52B8818F0C95F12991635609B0F7CAAF6388A58



# Hash Example

SHA 256

## Input

from: person1

to: person2

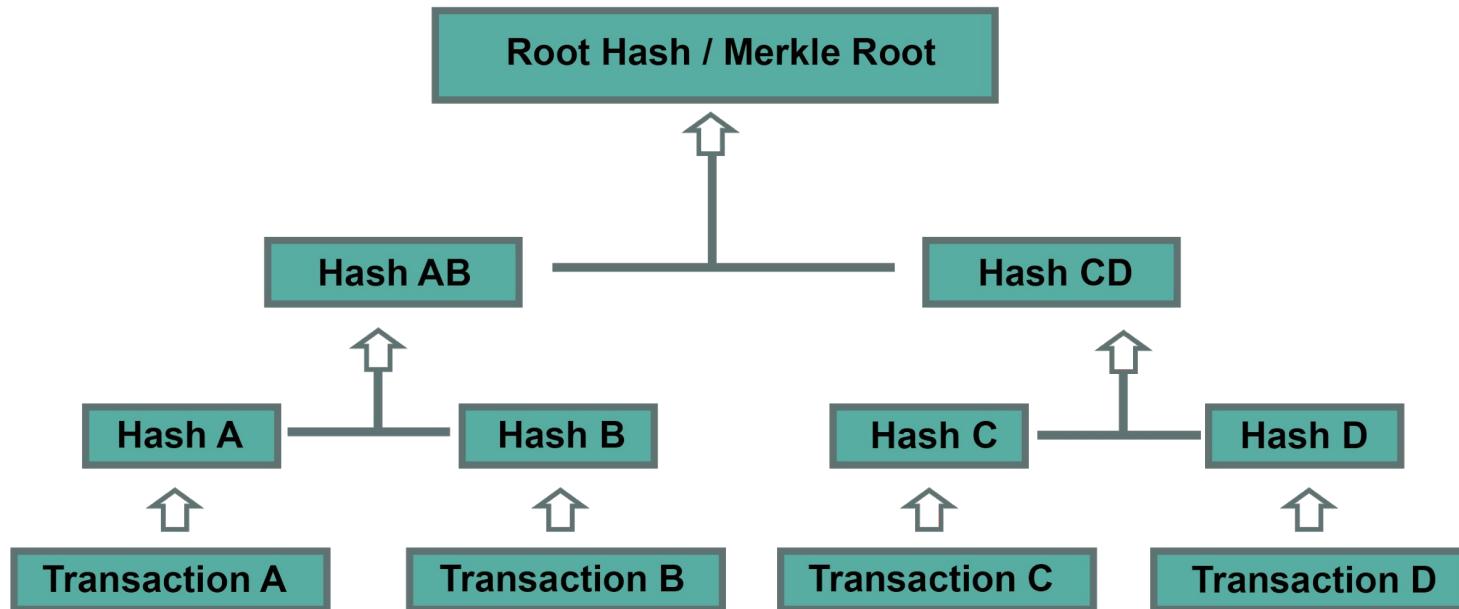
amount: **5001**

## Hash

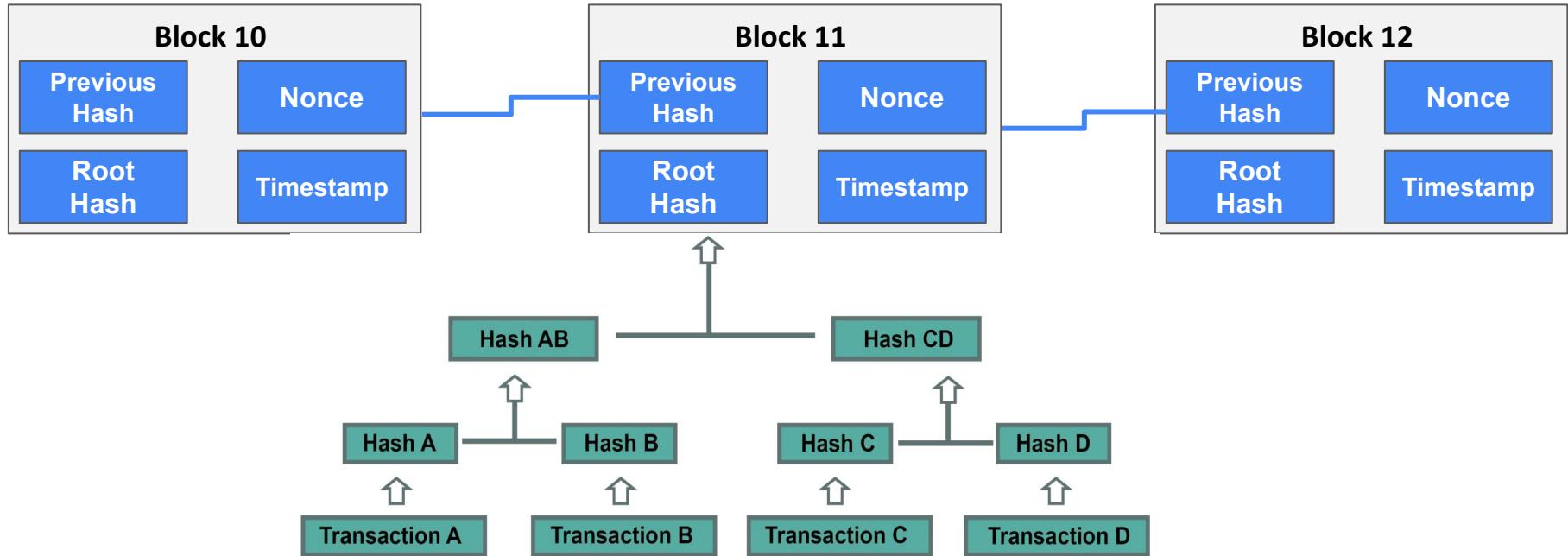
C677256A3CD1F73CD4476204BCA19050E0A11AB11FAEBF14CD7B37FB696F73C5



# Merkle Trees

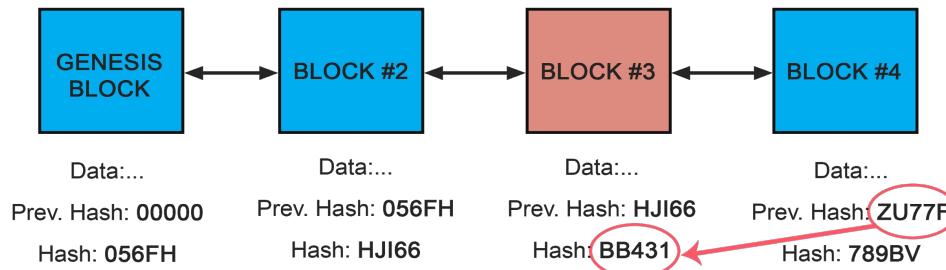


# Hash Chain



# Tamper Proof

- Each block in the chain contains transaction data.
- Is cryptographically hashed.
- The blocks of hashed data draw upon the previous-block in the chain
- This ensures all data in the overall "blockchain" has not been tampered with and remains unchanged.
- Hacker would need to change the block containing that record as well as those linked to it to avoid detection.



# Entering the Blockchain Network





**Bitcoin**  
A public deposit box  
  
Anyone can deposit

**Private Key**

Like a very long PIN,  
only the owner can unlock

**A Bitcoin Address**

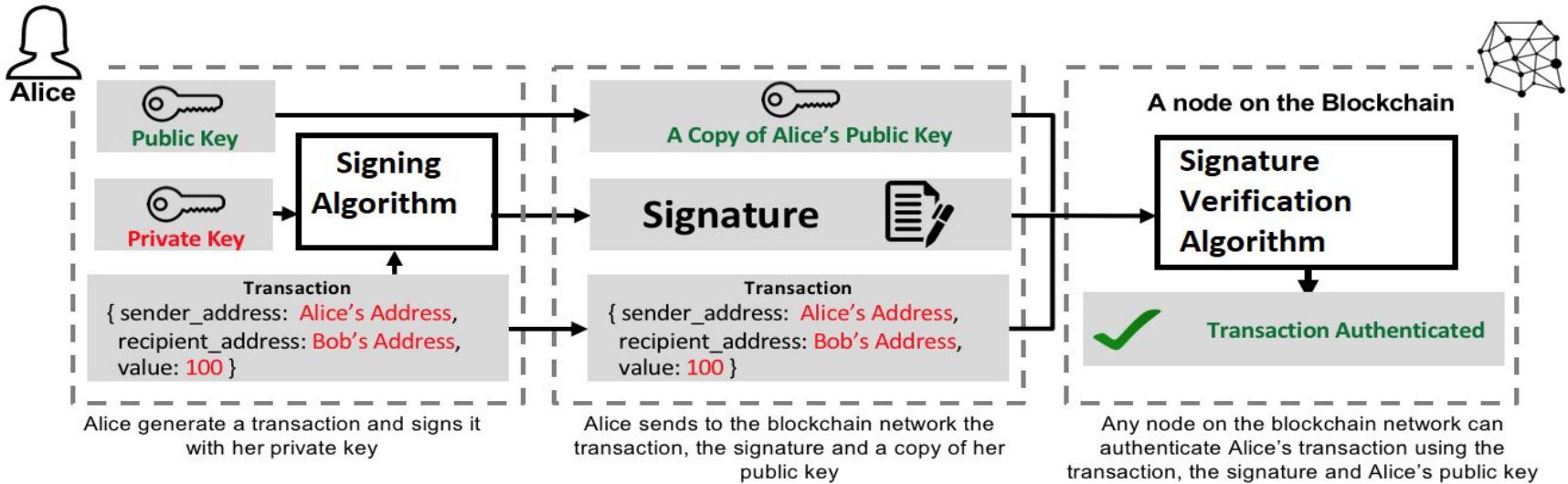
Used to identify where  
to deposit the payment

# Bitcoin Address



37LRvHjJdhdEergQEJEduREAtuRBF8dLL7

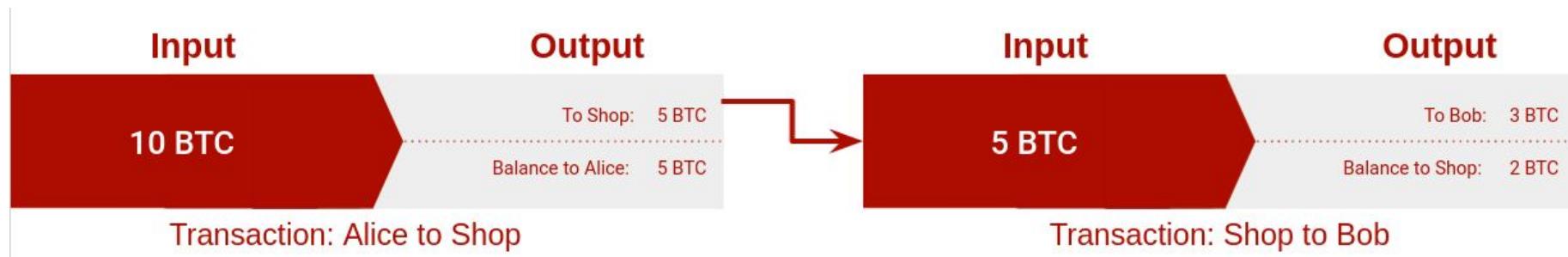
# Authentication of Transaction



Authentication Process for Transactions on the Blockchain

source:<http://adilmoujahid.com/posts/2018/03/intro-blockchain-bitcoin-python/>

# Transaction - UTXO



# Consensus

## Dictionary

Search for a word



### consensus

/kən'sensəs/

*noun*

a general agreement.

"there is a growing consensus that the current regime has failed"

Similar:

agreement

harmony

concord

like-mindedness

concurrence



Translations, word origin and more definitions

Definitions from Oxford Languages

Feedback

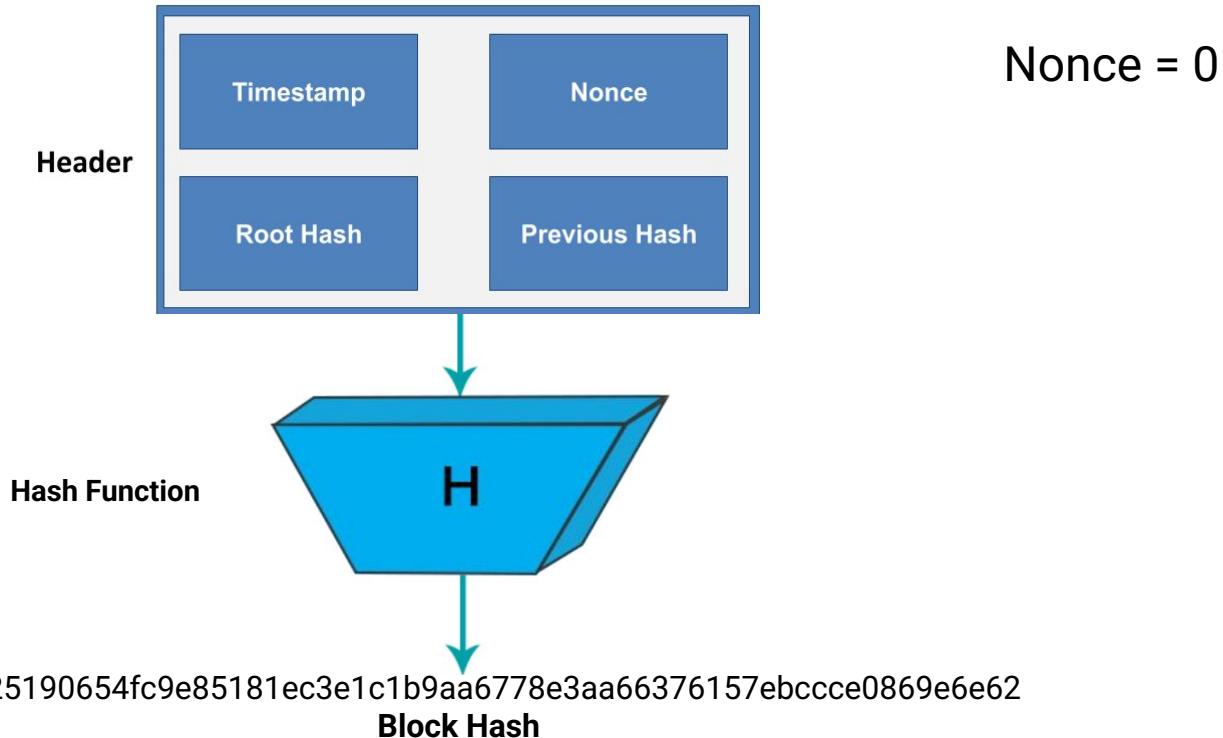


# Proof of Work

- Transactions are bundled together into a block
- Miners verify that transactions within each block are legitimate
- To do so, miners should solve a mathematical puzzle known as proof-of-work problem
- A reward is given to the first miner who solves each blocks problem
- Verified transactions are stored in the public blockchain



# The Puzzle



# Solution

## Block Hash\*

9740a25190654fc9e85181ec3e1c1b9aa6778e3aa66376157ebccce0869e6e62

compared to

## Threshold value\*

**IF Block Hash > Threshold**  
Increment Nonce value &  
Repeat hashing

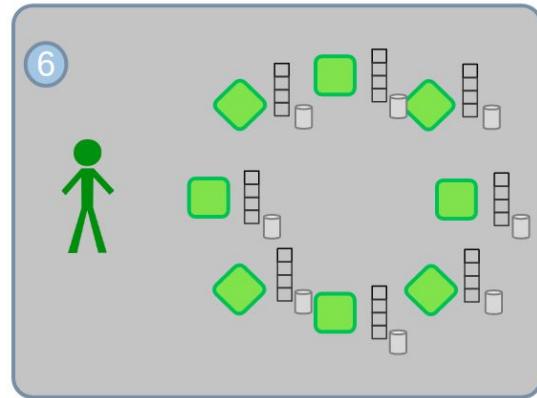
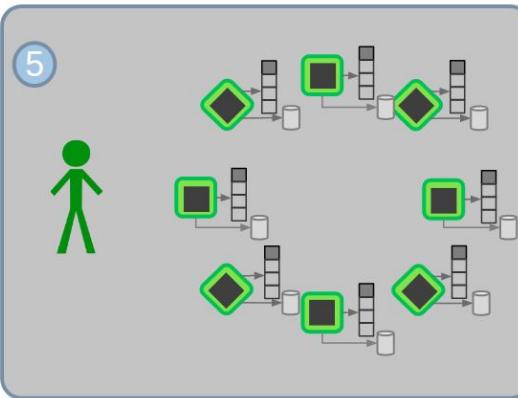
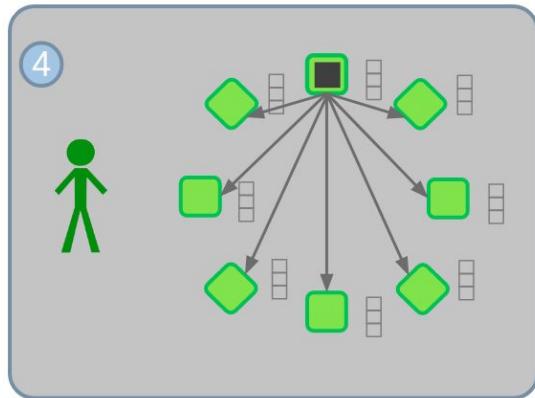
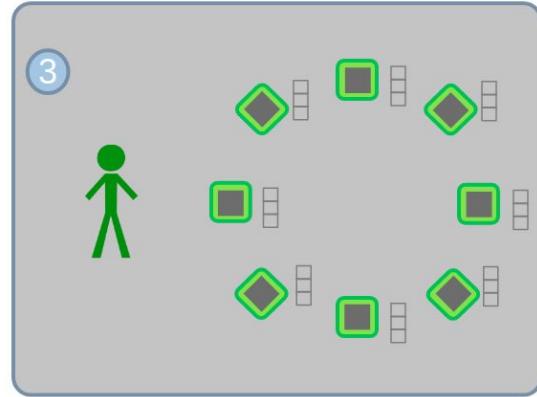
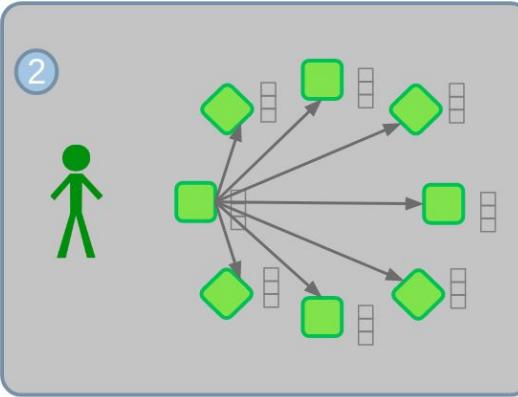
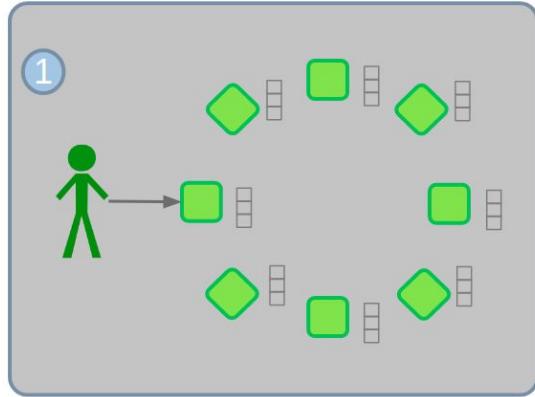
# IF Block Hash < Threshold

## Result Found

## Sample result\*

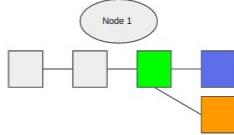


# Transaction Flow - Blockchain Network

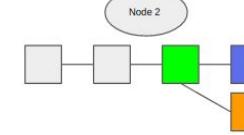
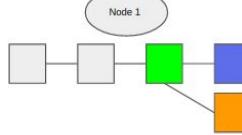


# Fork Resolution

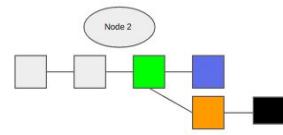
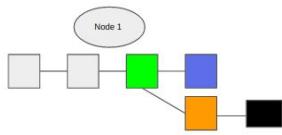
1



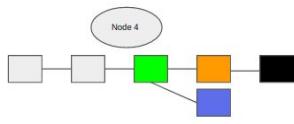
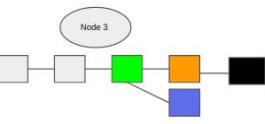
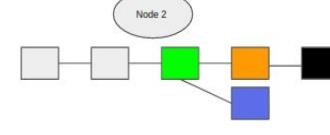
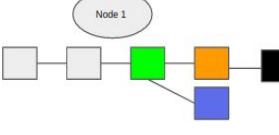
2



3

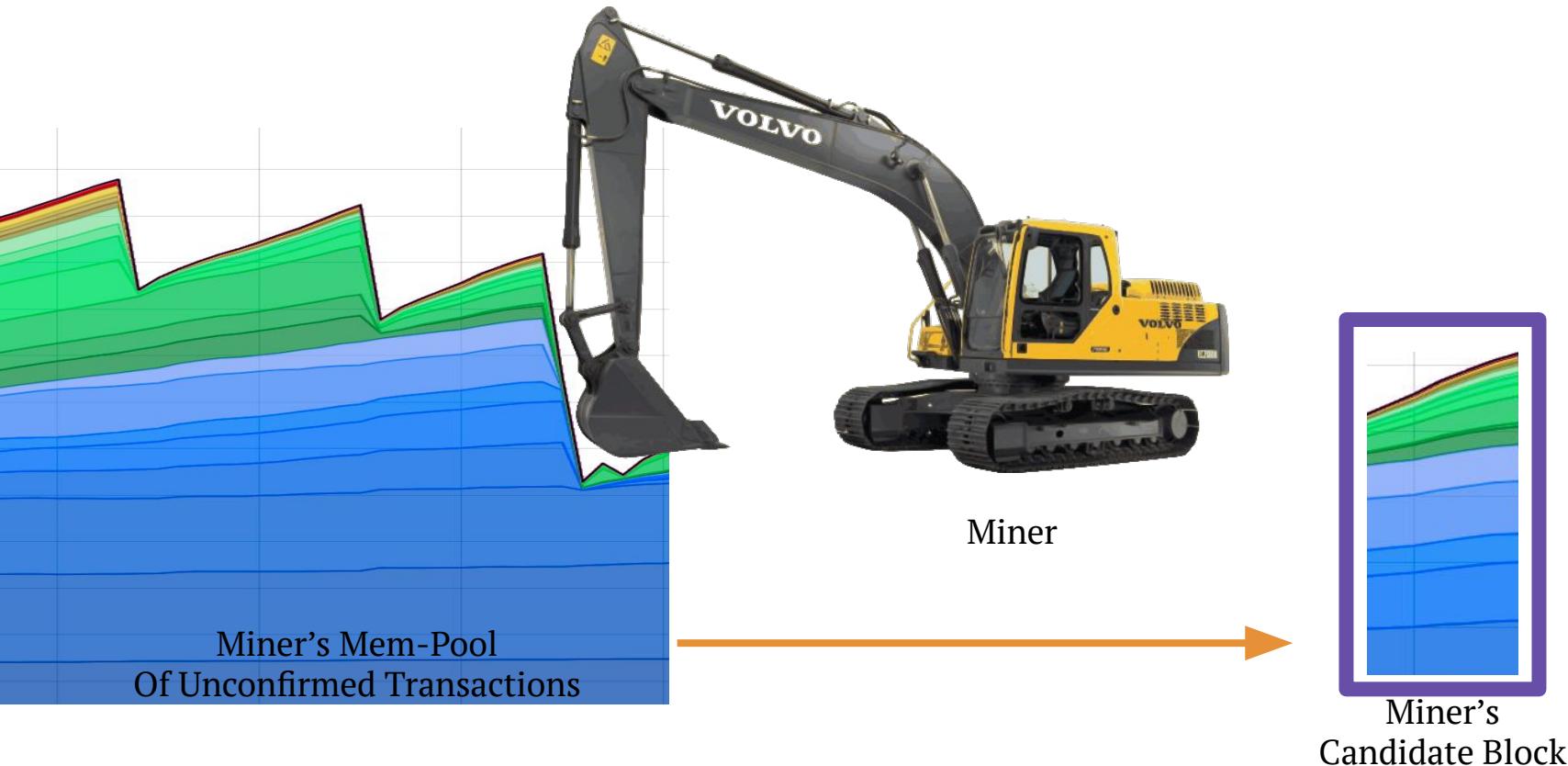


4





# Miners Add Transactions to Blocks



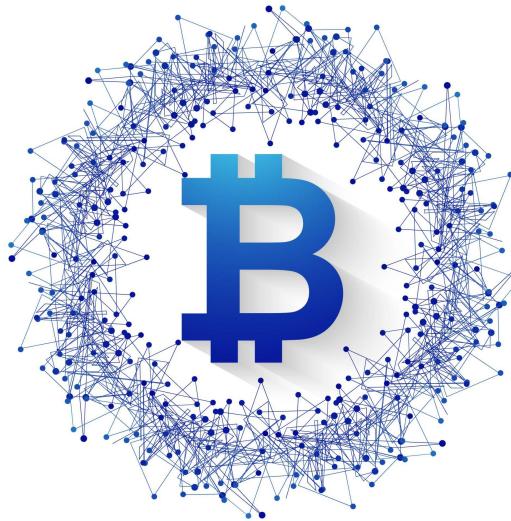
# Mining Incentives

Miners currently receive two types of rewards in return for the security provided by mining:

- (1) new coins created with each new block, and
- (2) transaction fees from all the transactions included in the block.

**Bitcoin Halving:** Regulating the supply to deal with inflation

# Where Bitcoin Network fell Short ?



Was meant only for bitcoin



Cannot perform complex computation

# The Smart Contract

- A smart contract is a computer protocol intended to digitally facilitate, verify, or enforce the negotiation or performance of a contract.
- Smart contracts allow the performance of credible transactions without third parties.
- These transactions are trackable and irreversible.



# Programmable Blockchain

Vitalik Buterin (OP)

Sr. Member



Activity: 330

Merit: 394

## [ANN] Ethereum: Welcome to the Beginning

January 23, 2014, 11:33:17 AM

Merited by BayAreaCoins (10), tk808 (10), notbatman (8), suchmoon (7), IncludeBeer (7), Kda2018 (7), Abiky (5), nutildah (5), alani123 (5), redsn0w (5), klintay (5), dragonlinux (5), zork (5), somacoin (5), vapourminer (4), Mrpumperitis (3), goldcoinminer (3), Cloudpost (3), Northa (3), OmegaStarScream (2), pangu (2), julerz12 (2), PuertoLibre (2), bitcampaign (2), V1saya (2), batang\_bitcoin (1), Jcga (1), Husna QA (1), wmaurik (1), Raja\_MBZ (1), mandor (1), Eastereg69 (1), bubbalex (1), kopisu (1), HBKMusIK (1), FreedomCoin (1), Financisto (1), Tyr808 (1), iwantmyhomepaidwithbtc2 (1), CrowdFunder (1), tammuz (1), safexscam (1), NeStore (1), gabbelo (1), heyspongebob (1), Neo Baudrillard (1) #1

### Welcome to the New Beginning

When the grand experiment that is bitcoin began, the anonymous wizard desired to test two parameters- a trustless, decentralized database enjoying security enforced by the austere relentlessness of cryptography and a robust transaction system capable of sending value across the world without intermediaries. Yet the past five years years have painfully demonstrated a third missing feature: a sufficiently powerful Turing-complete scripting language. Up until this point, most innovation in advanced applications such as domain and identity registration, user-issued currencies, smart property, smart contracts, and decentralized exchange has been highly fragmented, and implementing any of these technologies has required creating an entire meta-protocol layer or even a specialized blockchain. Theoretically, however, each and every one of these innovations and more can potentially be made hundreds of times easier to implement, and easier to scale, if only there was a stronger foundational layer with a powerful scripting language for all of these protocols to build upon. And this need is what we seek to satisfy.

Ethereum is a modular, stateful, Turing-complete contract scripting system married to a blockchain and developed with a philosophy of simplicity, universal accessibility and generalization. Our goal is to provide a platform for decentralized applications - an android of the cryptocurrency world, where all efforts can share a common set of APIs, trustless interactions and no compromises. We ask for the community to join us as volunteers, developers, investors and evangelists seeking to enable a fundamentally different paradigm for the internet and the relationships it provides.

### Who is Behind Ethereum?

Our primary core devs are:

- Vitalik Buterin → Inventor of Ethereum, protocol developer and researcher
- Gavin Wood → Lead C++ developer
- Jeffrey Wilcke → Lead Go developer

# Evolution of Chain



## The Currency

The implementation of distributed ledger technology led to its first and obvious application:  
**Cryptocurrencies**



## Smart Contracts

An extension of blockchain into privacy, smart contracts and the emergence of non-native asset blockchain tokens and capabilities



## Decentralized Applications

Adoption to mainscale applications, blockchain scaling. Improves speed without sacrificing security

# Blockchain Variants

## Permission-less

- Anyone can join the network and participate in consensus
- No need to prove identity.
- Proof of Work and Proof of Stake are some of the consensus used.
- Eg: Bitcoin and Ethereum



## Permissioned

- Only a restricted set of users have the rights to validate the block transactions
- Paxos, Raft, PBFT consensus : Only approved actors participate in consensus
- Eg: Hyperledger Fabric, Corda



# Blockchain Vs Database

Feature	Blockchain 	Database
<b>Data Integrity</b>	Immutable – once data is added, altering it is very difficult.	Mutable – data can be updated or deleted.
<b>Control</b>	Decentralized; no single entity has control.	Centralized; administered by database admins.
<b>Trust Mechanism</b>	Consensus algorithms and cryptographic proofs.	Access control and trust in the database system.
<b>Redundancy</b>	Data stored across multiple nodes; high redundancy.	Often single points, but can be backed up/cloned.
<b>Security Model</b>	Trustless – doesn't rely on a central authority.	Trust-based – relies on security protocols & admins.
<b>Use Cases</b>	Cryptocurrencies, transparent ledgers, smart contracts.	General data storage, CRUD operations, reporting.



# Why Industry loves Blockchain ?



Traceability



Universal record



Enhanced  
Security &  
Availability



Third party elimination



Auditability

# Where does the chain fit ?



## DIGITAL IDENTITY

A SELF SOVEREIGN ID CAN BE USED TO VERIFY IDENTITY WITHOUT NEEDING AN INDIVIDUAL TO PRODUCE NUMEROUS DOCUMENTS



## SUPPLY CHAIN MANAGEMENT

BLOCKCHAINS ALLOW MULTIPLE PARTIES TO ACCESS A DATABASE TO ACT AS THE SINGLE SOURCE OF TRUTH. RECORDED TRANSACTIONS ARE IMMUTABLE, ARE APPEND ONLY AND PROVIDE A TIME STAMPED AUDIT TRAIL .



## HEALTHCARE

USING BLOCKCHAIN TECHNOLOGY TO RECORD PATIENT INFORMATION ON A DISTRIBUTED LEDGER CAN ALLOW DIFFERENT STAKEHOLDERS CONDITIONAL ACCESS TO A SINGLE SOURCE OF TRUTH

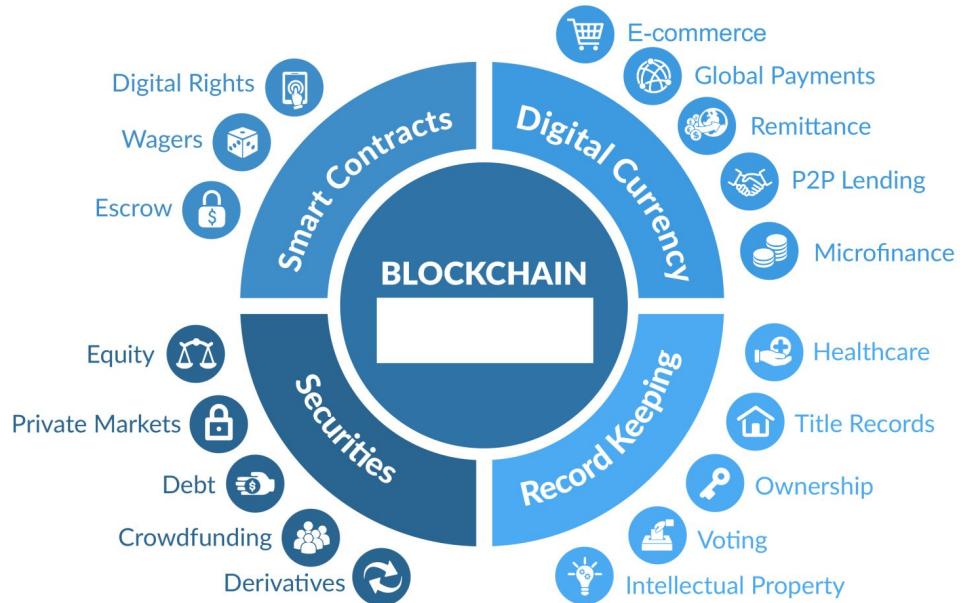


## REAL ESTATE

BLOCKCHAIN ALLOWS PEOPLE TO TRANSFER FUNDS, PROPERTY TITLES AND DATA IN A MORE PEER-TO-PEER MANNER THAT IS DIGITAL AND OPEN SOURCE

# Value of Blockchain

- Distributed environment.
- Trust-free consensus based transactions.
- Auditable public ledger system.
- Resilient systems.
- Reduction in cost and complexity.
- Trace intruders and attackers.



# Queries?

