Hewlett Packard Enterprise

VNUG Blockchain

Paul Denzinger, Advanced Technology Center, HPE

VNUG 2023

AGENDA

- The problem space
- Distributed ledgers
- Blockchain
- Satoshi Nakamoto
- Bitcoin vs Blockchain
- Blockchain details
- Use cases
- Smart contracts

CHALLENGE – THE PROBLEM SPACE

Imagine you had an important app used by millions of users across the world that needed to log its activity.

The log file contains critically important information.

Now, create a transaction log file with the following characteristics:

- Can be written to by any instance of the app, from anywhere, at any time, without explicit user permissions
- Is protected from malicious intent (data corruption, hacking, etc.), and is immutable from unauthorized changes
- Can be read by anyone to view the transaction activity and balances, but preserves anonymity of participants and their transactions
- Maintains the correct sequence of all transactions, regardless of when and where they occurred
- Is scalable/elastic, in real-time
- Is replicated/distributed and resilient across outages, and is always available
- Manages and coordinates changes to all of its replicas from all of the app instances
- Relies on decentralized management – no single point of control/management/authorization

These are generally the principles used by distributed ledgers and specifically by Blockchain

DISTRIBUTED LEDGER TECHNOLOGY AND BLOCKCHAINS

Distributed Ledger Technology

- The combination of infrastructure and protocols that allow simultaneous access, validation, and record keeping across a networked database

DLT is the technology that blockchains are built on

- All blockchains are implemented using DLT but not all DTLs are blockchains
- There are multiple types/implementations of blockchains – the most popular being the blockchain that powers Bitcoin
- Bitcoin is an application that provides a digital currency (crypto-currency); blockchain is the technology that makes it work
- Blockchain technology forms the underpinnings of Bitcoin, as well of other types of digital currencies*
- While the implementation details for each type of blockchain differ somewhat, the overall objectives are the same
- Blockchains can also be used for purposes other than crypto-currencies

- Many people use the term, *blockchain*, without clarifying whether they mean the specific technology, or the crypto-currency being used, which can be confusing – so beware.

* Top 100 Crypto Coins by Market Capitalization https://coinmarketcap.com/coins/

WHY WAS BLOCKCHAIN DEVELOPED?

Created by a person or a group, under the name (or pseudonym) of Satoshi Nakamoto* in 2008

Blockchain functions as the public distributed ledger for Bitcoin (also developed by Nakamoto) cryptocurrency transactions

A small team of developers collaborated with Nakamoto to build and deploy the blockchain and Bitcoin**

Nakamoto was primarily trying to solve the problem of creating a decentralized and trustless digital currency system.

The key problem he aimed to address was the reliance on centralized financial institutions and intermediaries for processing transactions and issuing currencies.

That also carries over into government oversight and regulations vs privacy rights and the "freedom to transact" for individuals.

* Paper: *Bitcoin: A Peer-to-Peer Electronic Cash System* https://bitcoin.org/en/bitcoin-paper

** https://bitcoinmagazine.com/technical/what-happened-when-bitcoin-creator-satoshi-nakamoto-disappeared

WHAT IS SIGNIFICANT ABOUT BLOCKCHAIN?

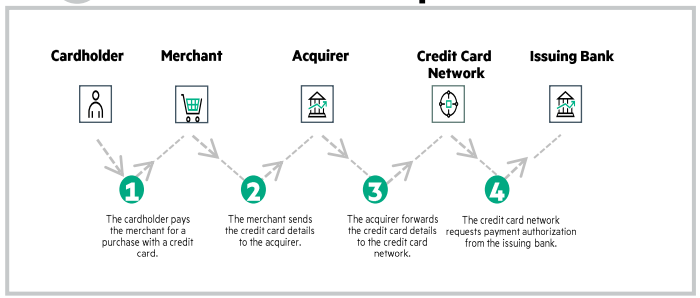
Blockchain is significant for several important reasons, including:

- It solves the problem of "double spending" inherent in digital currencies
  - Unlike physical currency, digital currency can be replicated any number of times and spent more than once, outside of the oversight of a central trusted authority
  - Blockchain solves this problem through its decentralized transaction confirmation, verification, and consensus mechanisms
- With blockchain, participants can engage in peer-to-peer transactions, without the need for a central authority to monitor and facilitate transactions, with privacy and immediacy
- In addition to facilitating e-commerce and exchange of digital currencies, it is also adaptable to more general purposes
  - Smart contracts, supply chain, provenance validation, tokenization, etc.

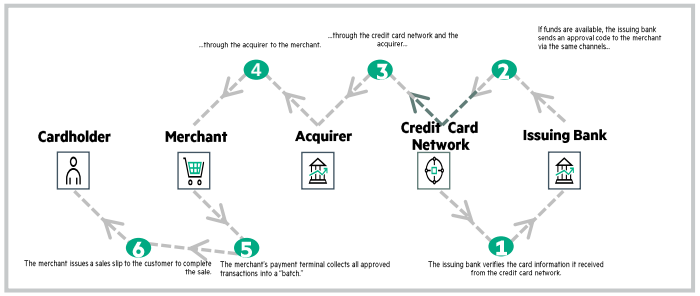
TYPICAL FINANCIAL TRANSACTION TODAY

16 Steps, 6+ Parties, ~7 Days – (Now, typically 2-4 days)

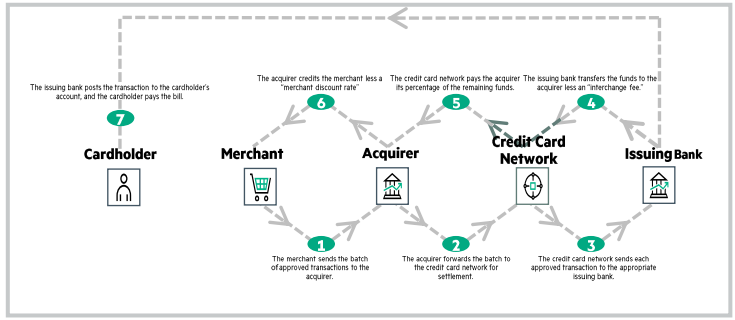
1 Authorization - 4 step

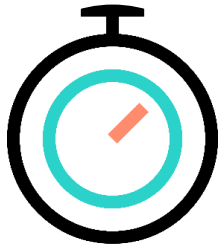


2 Authentication - 5 step



3 Settlement - 7 step





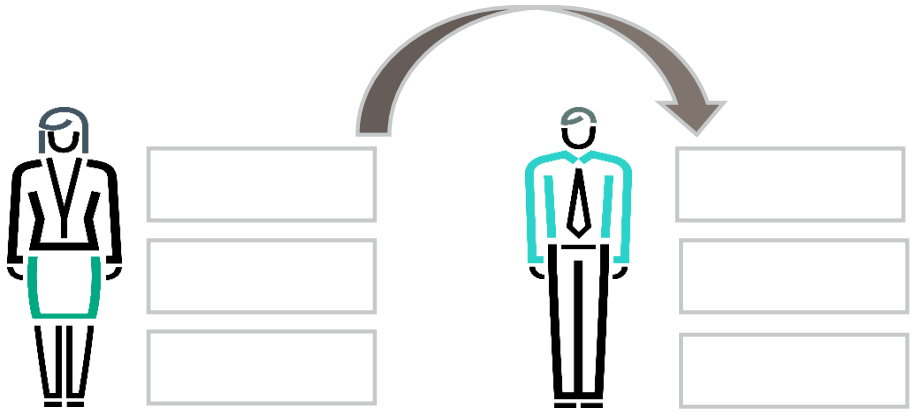
Can I reduce Time?

Can I Simplify?

Can I reduce Cost?

Source: How Credit Card Transaction Processing Works: Steps, Fees and Participants, Odysseas Papadimitriou, WalletHub CEO, Payment risk committee report

TYPICAL FINANCIAL TRANSACTION ON BLOCKCHAIN



Speedy – in minutes

+

Simple and efficient – 1 step , 2 parties

+

Lower Transaction costs

+

Self Auditing and Transparent

+

Ability to create trusted networks

MANY WAYS TO USE BLOCKCHAIN

Peer-to-peer “trustless” transactions

Participants can directly exchange assets, such as cryptocurrencies, without the need for intermediaries like banks or payment processors, or a central authority

Cross-border payments and micropayments

Participants can facilitate cross-border payments and remittances with reduced fees and faster settlement times.

Blockchain enables cost-effective micro-transactions, allowing participants to send or receive tiny amounts of value that might be impractical with traditional payment systems.

Decentralized immutable record keeping

Participants can maintain a shared, tamper-proof ledger without relying on a central entity, enhancing transparency and reducing the risk of fraud.

Voting and governance

Blockchain enables transparent and tamper-resistant voting systems and decentralized governance models for organizations and communities.

Tokenization of assets

Participants can tokenize real-world assets, such as real estate or artwork, making them more liquid and accessible for investment and trading.

Smart contracts

Participants can create self-executing contracts that automatically enforce predefined conditions, reducing the need for intermediaries and manual oversight.

Supply chain transparency

Participants can track and verify the origin and movement of goods throughout the supply chain, reducing fraud and ensuring product authenticity.

Provenance validation

Prove the history of ownership of artwork, jewelry, music, research, etc. – Any product of value that is subject to forgery.

WHAT DATA IS CONTAINED IN A DISTRIBUTED LEDGER?

A ledger is simply a record of transactions:

- Shows the chronology (time sequence) of who sent and received money or other assets of value.
- For NonStop users, you can think of the TMF audit trail as a ledger of business transactions against a NonStop DB.
- A ledger differs from a DB in that a DB shows the current state of all txs, while the ledger shows the chronological order of txs
- A ledger is a essentially a replica of a DB – the current state can always be reproduced

Transaction	Date	Description	Payment	Deposit	Balance
0001	01-01-2023	Payment received		$1000	$1000
0002	02-12-2023	Payment made	$100		$900
0003	02-27-2023	Payment made	$150		$750
0004	08-03-2023	Payment received		$5000	$5750

Account table
Account Number ...
Account Owner ...
Account Status ...
Account Balance ... $5750

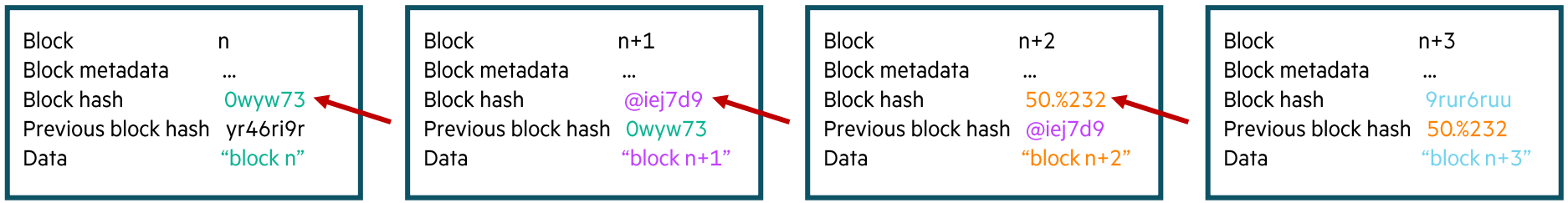
Distributed ledger replicated and synchronized

WHAT DATA IS CONTAINED IN A BLOCKCHAIN?

A ledger in the context of blockchain typically contains information about transactions and other relevant data, in addition to metadata required by the specific blockchain implementation used.

For a cryptocurrency-based blockchain (like Bitcoin), the blockchain will typically contain:

- Sender's address – The address of the party initiating the transaction.
- Recipient's address – The address of the party receiving the transaction.
- Amount – The quantity of the cryptocurrency or asset being transferred.
- Timestamp – The time when the transaction occurred.
- Digital signature – A cryptographic signature that proves the transaction's authenticity and origin.
- The "nonce" (Bitcoin) – A very special number used for proof-of-work (PoW) and validation
- Previous block hash – In some blockchains, like Bitcoin, each block references the previous block's hash to create a chain of blocks.
- Pertinent metadata – used by the particular blockchain



Chain of blocks

CATEGORIES OF BLOCKCHAIN

Two broad categories of blockchain

- Permissionless
  - Anyone can connect to the blockchain (via an app) – no pre-approval or permission is required
  - Bypasses/avoids central authorities and regulation
  - Bitcoin and most other cryptocurrencies use permissionless blockchains
  - With a Bitcoin blockchain:
    - Anonymous users can connect to the network, download the entire blockchain, create a wallet and conduct transactions, or act as a "miner" (validator or transactions) to earn bitcoin as payment
    - The validation process – known as "proof of work" (PoW) is very costly and energy inefficient, but is required to protect the integrity of the blockchain
- Permissioned
  - Participants require pre-approval and explicit permission to use the blockchain (e.g., a consortium of organizations)
  - KYC (know your customer) and similar requirements result in less privacy and transparency
  - Sacrifices some anonymity and decentralization in return for protections against maliciousness and better performance
  - The choice of most businesses, governments, and financial institutions
  - With a permissioned blockchain:
    - There are a limited number of validator nodes, usually preselected by the organization
    - The validation process is typically much more efficient and faster, and is usually based on "proof of stake" (PoS)

Blockchains may also be public or private, but those tend to conform to permissionless and permissioned, respectively

KEY OBJECTIVES OF THE BLOCKCHAIN ARCHITECTURE

Decentralization

- Remove the need for a central authority or intermediary.

Security

- Use cryptographic techniques to protect data and transactions

Immutability

- Prevent alteration of recorded data once it's added

Availability

- Use replication to maintain availability and resiliency

Trustlessness

- Allow participants to transact without needing to fully trust each other – “trust” is inherent in the blockchain

Consensus

- Reach agreement on the validity of transactions through consensus mechanisms

Efficiency

- Streamline processing by automating verification and reducing intermediaries

Transparency

- Enable all participants to see the same shared data

Auditing and traceability

- Provide a transparent and traceable record of transactions

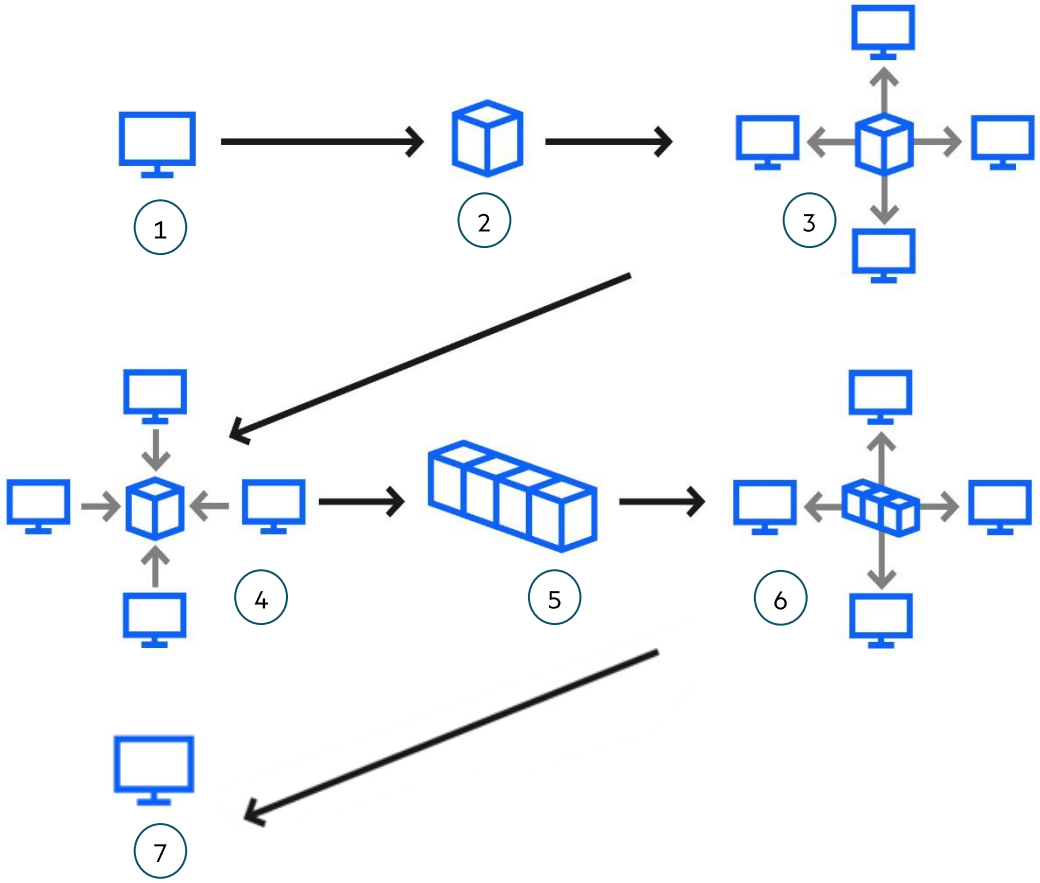
Fraud reduction

- Minimize the risk of fraud due to the tamper-proof nature of data

GENERAL OPERATION OF HOW THE BLOCKCHAIN WORKS

You interact with a blockchain indirectly through an app which calls the necessary functions via an API

1. Transaction started
2. TX data is packaged into a block
3. The block is replicated to the blockchain miners/validators
4. The block is approved via consensus (PoW or PoS)
5. The block is added to the chain
6. And distributed to all nodes in the network
7. The Tx is completed



WHY USE A NETWORK OF NODES?

Using multiple validator nodes in a network addresses the following objectives:

Availability

- Since all data and functionality are replicated to all nodes

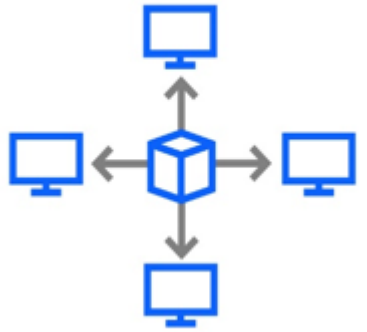
Decentralization and trustlessness

- Which replaces a single trusted authority with multiple, independent, and distributed validators

Consensus and immutability

- Validators work concurrently on PoW or PoS and all results are verified by independent nodes to prevent “bad actors” from corrupting or compromising the blockchain
- The only way to compromise the blockchain is for a majority of validators to be hacked at the same time, in the same way, which is highly unlikely

➔ the 51% attack problem



Distributing this functionality across a network of cooperating nodes is key to the integrity of the blockchain!

A LOOK INTO KEY FEATURES OF THE BITCOIN BLOCKCHAIN

Immutability, proof-of-work, the “nonce” and “difficulty target”, consensus, and blockchain eventual consistency.

Each blockchain is similar in its operation, but different in its implementation. This section takes a look into a few of the more interesting and unique aspects of the Bitcoin blockchain.

For an excellent and detailed description of blockchain functionality, consult the book: *Mastering Bitcoin*, by Andreas A. Antonopoulos (O’Reilly Books)

DISTRIBUTED AND REPLICATED FUNCTIONS

Bitcoin uses a peer-to-peer network of nodes:

- A flat network structure – no hierarchy
- All nodes are equal – “no special” nodes

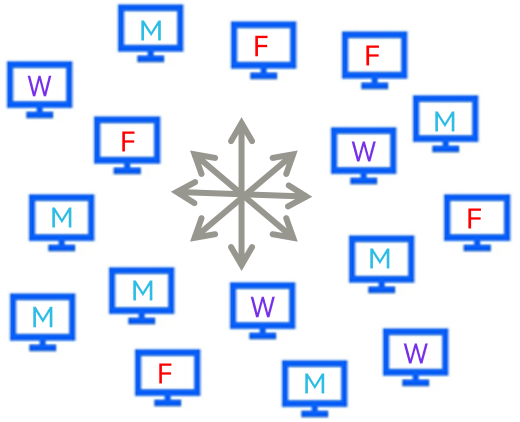
Bitcoin nodes can serve different roles, including:

Wallet (W)

Blockchain DB (F)

Mining (M)

Routing



- All nodes perform routing, validate and propagate transactions and blocks, and participate in discovery
- Full blockchain nodes maintain the blockchain DB
- Mining nodes create new blocks and “mine” bitcoins, and maintain the blockchain DB

The blockchain is not replicated using a replication utility

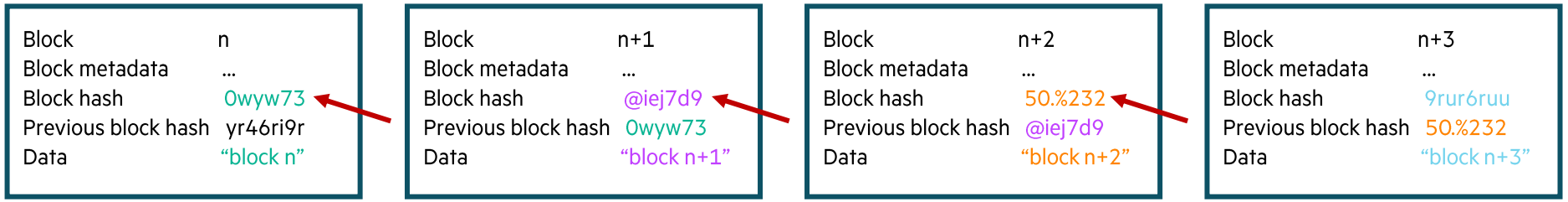
Each minor maintains its own complete copy of the blockchain as a sequential file.

Consistency across these copies is maintained through consensus.

HOW IS IMMUTABILITY ACHIEVED?

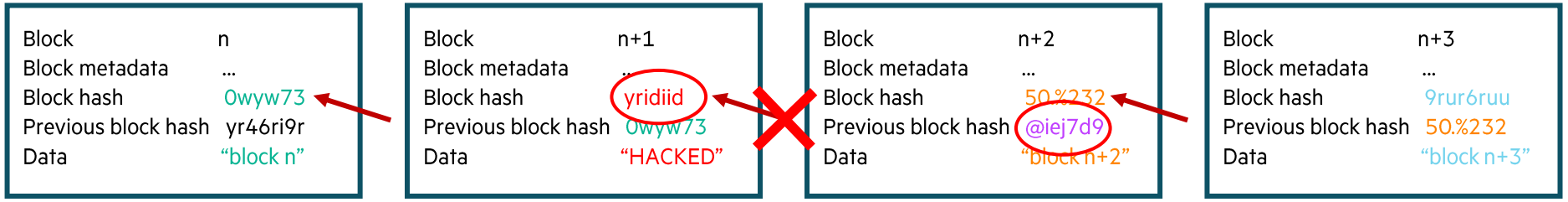
Chain of blocks (based on Bitcoin's blockchain)

The header of each block maintains a hash of its content (which includes the hash of the preceding block), plus the hash from the preceding block, as well as other metadata, which includes the "nonce" that is a critical component of PoW:



Chain of blocks

If data in a block were to be modified, its hash would have to be recomputed, and in the following block, the previous block hash would need to be recomputed, and then the block hash would need to be computed. This would continue all the way to the top of the block chain. Producing a new hash involves the nonce, and is "labor intensive" – hard to do quickly:



Corrupted chain of blocks -- Discovered & rejected

WHAT IS “PROOF OF WORK” (POW)?

PoW is a mechanism to reliably add transactions to the blockchain while protecting it from bad actors.

- Some form of PoW is used by most public, permissionless blockchains & cryptocurrencies, including Bitcoin.

Bitcoin relies on consensus from multiple “miners” within the public network to:

- Do “mining” – create new bitcoins
- Perform the PoW computation to create new blocks
- Validate transactions
- Insure there is no “double spending” of digital currencies

The PoW process is what secures the bitcoin system and enables network-based consensus without relying on a central authority.

WHAT IS "PROOF OF WORK" (POW)? … MORE

- The PoW algorithm is deliberately made difficult to perform, to deter spammers/hackers -- the is the process of "mining" bitcoins
- It involves executing expensive mathematical operations (hashes) that must be performed numerous times until the solution is found
- It is executed concurrently by all miners in the network – miners compete against one another to be first to complete the challenge
- Miners must use special HW to attain the processing speeds required
- The first miner to solve the problem "wins" and is awarded an amount of bitcoin as an incentive to participate*
- The winning miner also receives a fee from user transactions as a payment for services

The miner distributes the newly validated block to other nodes that independently confirm the computation (PoW), add it to the blockchain, and abandon their own efforts to mine the block.

Mining is what validates and clears transactions and secures the system, without relying on a central authority.

*In Nov 2021, the reward was 6.25 BTC, and at a price of $50K/BTC that works out to ~$312K for 1 block!
In Mar 2022, the price of BTC was $39K, which would earn "only" ~$244K.

DISTRIBUTED, EMERGENT CONSENSUS

Consensus among the miners is not achieved explicitly

Consensus is an *emergent* characteristic from thousands/millions of independent miners engaging in the same simple processing rules to mine blocks (POW)

There is no dependence on a central authority

Consensus emerges from the interplay of four processes that occur independently across the blockchain network:

- Verification of every transaction by every full node
- Aggregation of transactions into blocks validated through POW by mining nodes
- Verification of the new blocks by every node and assembled into a chain
- Selection of the chain with the most cumulative computation (i.e., longest chain) via POW, by every node

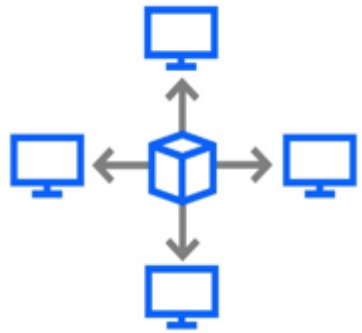
HOW DOES "PROOF OF WORK" (POW) WORK?

PoW made simple…

- A hash is computed from the block "data" using a "nonce" and a "difficulty target"

  (A nonce is "a Number used ONCE")
- If the hash result is less than the difficulty target number, then the mining is successful and complete
- If it is not, the nonce is incremented by 1, and the hash/comparison is repeated

This continues until the miner is successful, or until it receives notice that another node solved the problem



PoW is performed concurrently by all miners in the network

Where do these values come from? … the block header:

Among other items, the block hearer contains:

- The previous block hash
- The current block hash
- The starting "nonce value" (which is 0)
- The "difficulty target" value

Once a "winning" nonce value is found, it is kept in the block header for later verification

This design makes it easy for other nodes to verify the PoW work – this is why it is called, "Proof of Work"

The "work" part is made deliberately intensive for protection against hackers, while the "proof" part is very simple and fast to verify.

THE REASON FOR THE NONCE AND "DIFFICULTY TARGET"

Remember, PoW is meant to be "hard" to do, but easy to verify.
So the challenge becomes, how to accomplish this?

Given the same input, a hash function always produces the same result.
But by changing the nonce – by even the value of 1 - the hash function produces a completely different result – it effectively generates a pseudo-random number.

Next, in order to "win" (solve the problem), the hash result must be less than (<) the "difficulty target" number.

This forces the miner to repeat the hash function numerous times (each time with a different nonce value) until the comparison is satisfied, or solved by another node.

The "difficulty target" number is chosen to force the solution to take ~10 mins on average. Using a lower value causes the solution to take longer, while a larger value causes the solution to complete more quickly.

To keep pace with faster HW technology over time, the blockchain is designed to adjust the difficulty target dynamically to keep the solution time at ~10 mins.

With the "winning" nonce value, the hash result can be quickly reproduced by an independent validator to verify the PoW solution.

Hash (11111111 + 0) = 2324
Hash (11111111 + 1) = 9934
Hash (11111111 + 2) = 0213
Hash (11111111 + 3) = 7377
…
The nonce "randomizes" the result.

A large difficulty target can be solved with many more solutions than a smaller value, and thus more quickly:

When the target = 9999,
99.9% of the possible hash values solves the problem, and a solution is quickly found.

When the target = 0000,
Only 0.01% of the possible hash values solves the problem and takes many more tries (and more time) to find a solution.

Even though the nonce increases sequentially, the resulting hash values do not – they are effectively random values.

“PROOF OF WORK” EXAMPLE

A miner receives a block to process:

Solution attempt 1:

Hash (“block hash” + “prev block hash” + “0”) = 6595

6595 > 100, so increment nonce by 1, and repeat

Solution attempt 2:

Hash (“block hash” + “prev block hash” + “1”) = 0556

0556 > 100, so increment nonce by 1, and repeat

…

Solution attempt 5,053:

Hash (“block hash” + “prev block hash” + “5052”) = 0023

0023 < 100, mining is complete, so miner can distribute the block

The miner distributes the block for verification

Block	n
Block hash	1111
Previous block hash	5555
Nonce	0
Difficulty target	100

Nonce = 0
Hash (“block hash” + “prev block hash” + “nonce”) = hash-result
If hash-result < target, then win
Otherwise, increment nonce by 1, and repeat

In real life, there are typically millions of hashes required to produce a solution!

VERIFYING “PROOF OF WORK” EXAMPLE

A node receives a “winning” block to verify:

Compute verification:

Hash (“block hash” + “prev block hash” + “5052”) = 0023

0023 < 100, so this block PoW is independently verified

The “winning” block is propagated to other/all miners and is eventually written into the blockchain

Block	n
Block hash	1111
Previous block hash	5555
Nonce	5052
Difficulty target	100

← “Winning” nonce

Nonce = 0

Hash (“block hash” + “prev block hash” + “nonce”) = hash-result

If hash-result < target, then block PoW is verified

Otherwise, reject

HOW IS EMERGENT CONSENSUS USED TO MAINTAIN THE BLOCKCHAIN?

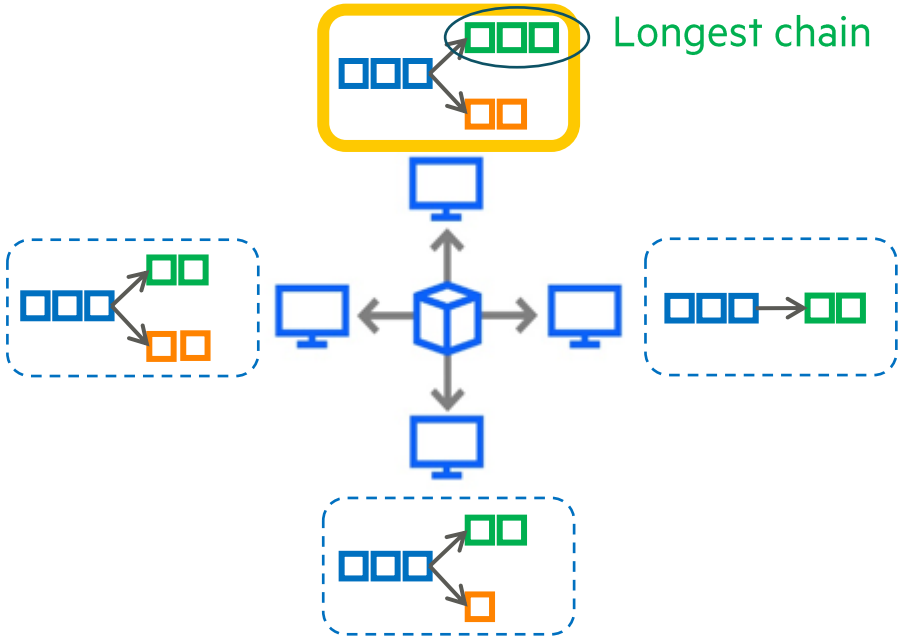
Because the blockchain is decentralized the different copies are not always consistent.

- Timing issues can cause blocks to arrive in a different order at the various nodes
- Temporary forks can develop at different nodes

Because emergent consensus is used, there is no central arbitrator to decide which fork/chain is the “official” representation of the blockchain.

Instead,

- Each node resolves this independently, and consistently, by always choosing the chain with the greatest amount of accumulated “difficulty” (hashes), which is the “longest” chain
- Over time, as miners distribute new block solutions and extend chains, all copies of the blockchain eventually converge to the same state (i.e., eventual consistency), based on the longest chain solution. Miners working on shorter chains stop their work and converge on the new, longer chains.



In practice, forks are almost always resolved within one block.

The 10-min rule is designed to allow sufficient time for these forks to resolve before becoming too complex.

ALTERNATIVES TO POW

PoW vs Proof-of-Stake (PoS)

- PoS is a much more energy efficient method for maintaining the blockchain and is the main alternative to PoW
- Block validation is performed by “stakeholder” nodes
  - These are owners of nodes that place coins in collateral (put up a “stake”) for the privilege of validating blocks
  - There is a minimal number of coins required as an “entry fee”
  - Validators earn a fee for processing blocks
  - Validators that put up large stakes have a greater opportunity to validate more blocks, and earn more in fees
  - Bad actor validators risk loosing their entire stake, which is the disincentive for maliciousness
  - PoS works because validators are willing to back up their work with their own money

- Under PoS:
  - Validators are chosen at random for each block
  - Blocks and transactions are validated by multiple validators concurrently
  - When a certain number of validators verify and agree a block is valid, it is added to the blockchain
  - There are various implementations, with some requiring a quorum of validators to agree on the outcome

- Specific implementation details are dependent on the vendor’s blockchain being used

SMART CONTRACTS

A good application of blockchain (and DLT) technology

SMART CONTRACTS

Blockchain smart contracts:

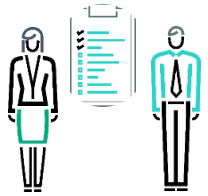
- Program code that carries out the terms and conditions of a contract are stored on the blockchain and run automatically when certain conditions are met
- Benefit from the characteristics of blockchain
  - Immutable, trust factor, transparent, verifiable, secure, efficient, automatic, etc.

Smart contracts pre-date blockchain

- "Computerized transaction protocols that execute terms of a contract", Nick Szabo, 1994

Ethereum blockchain is the most popular platform for SCs, but also supported by Bitcoin blockchain

Some companies, such as R3 Corda, provide SCs using DLT (not a blockchain)



- Contract created between two parties
- Both parties remain anonymous
- Contract is stored on a blockchain or ledger

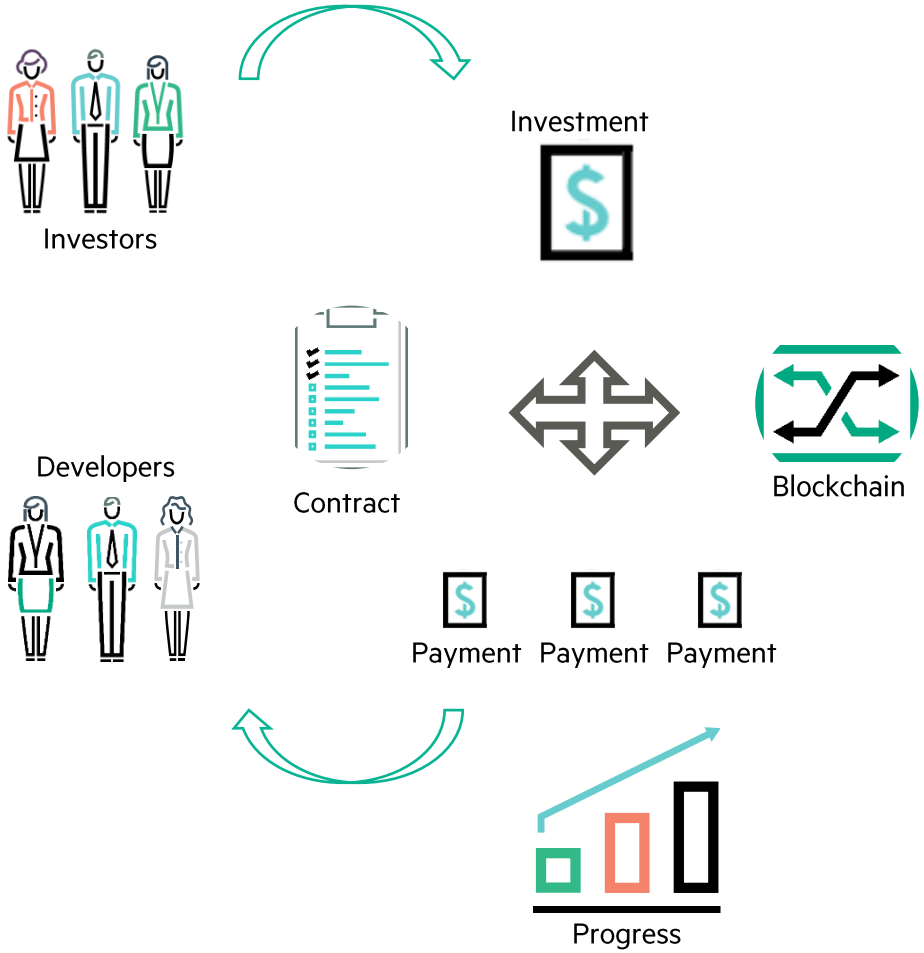
- A triggering event occurs, i.e. deadlines, transaction event, etc.
- The contract self-executes the embedded code

- Regulators and users can analyze the details & conditions
- Input into data analytics for better results

SMART CONTRACT EXAMPLE

Blockchain-based crowd funding of projects

- A contract is written to attract funding for the creation of a new, cool product, and is placed on the blockchain
  - Money invested will be entrusted so that it is only distributed to the developers upon satisfactory delivery of key milestones
  - A contract is written that provides the details, and knows about bank accounts, and terms of product delivery, etc.
  - The program code implements the details of the contract
- Investors can confidently contribute money, knowing their investments are protected
- As key features of the new product are produced and pass the conditions as stated in the contract, funds are automatically transferred to the development team
- If not, funds are returned to the investors and any penalties applied

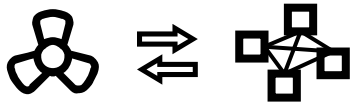


ONE VERY COOL EXAMPLE

Encrypted microchips are used to give automated delivery drones a unique identity on the blockchain which IoT applications can use to allow or restrict drone access to locations such as a home or warehouse.

https://news.bitcoin.com/chronicled-demo-blockchain-drone/
https://www.youtube.com/watch?v=bdK4kXEh9j8

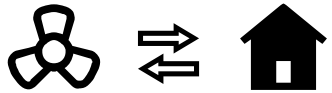
COOL EXAMPLE SYNOPSIS



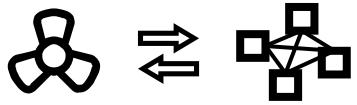
Drone and smart Window pre-register with blockchain to deliver and receive medication at a specific address

Bed-ridden customer refills Rx from smart phone

Pharmacy prepares Rx for delivery by Drone



Drone locates and verifies address of home and delivery instructions via blockchain



Drone electronically “knocks” on Window via Bluetooth
Window checks the blockchain to verify Drone

Window opens; Drone makes delivery

One very satisfied customer

REFERENCES

Satoshi Nakamoto:

Paper: ***Bitcoin: A Peer-to-Peer Electronic Cash System*** https://bitcoin.org/en/bitcoin-paper

https://bitcoinmagazine.com/technical/what-happened-when-bitcoin-creator-satoshi-nakamoto-disappeared

How it works:

https://en.wikipedia.org/wiki/Blockchain

https://en.wikipedia.org/wiki/Distributed_ledger

https://www.investopedia.com/terms/b/blockchain.asp

Lots of great content and articles:

https://www.investopedia.com/blockchain-4689765

Top 100 Crypto Coins by Market Capitalization :

https://coinmarketcap.com/coins/

For an excellent and detailed description of blockchain functionality, consult the book:

"Mastering Bitcoin", by Andreas A. Antonopoulos (O'Reilly Books)

EVRY Financial Services white paper: *"Blockchain Powering The Internet of Value"*, 2015

https://www.finyear.com/attachment/637653/

THANK YOU!

For more information send email to paul.denzinger@HPE.com