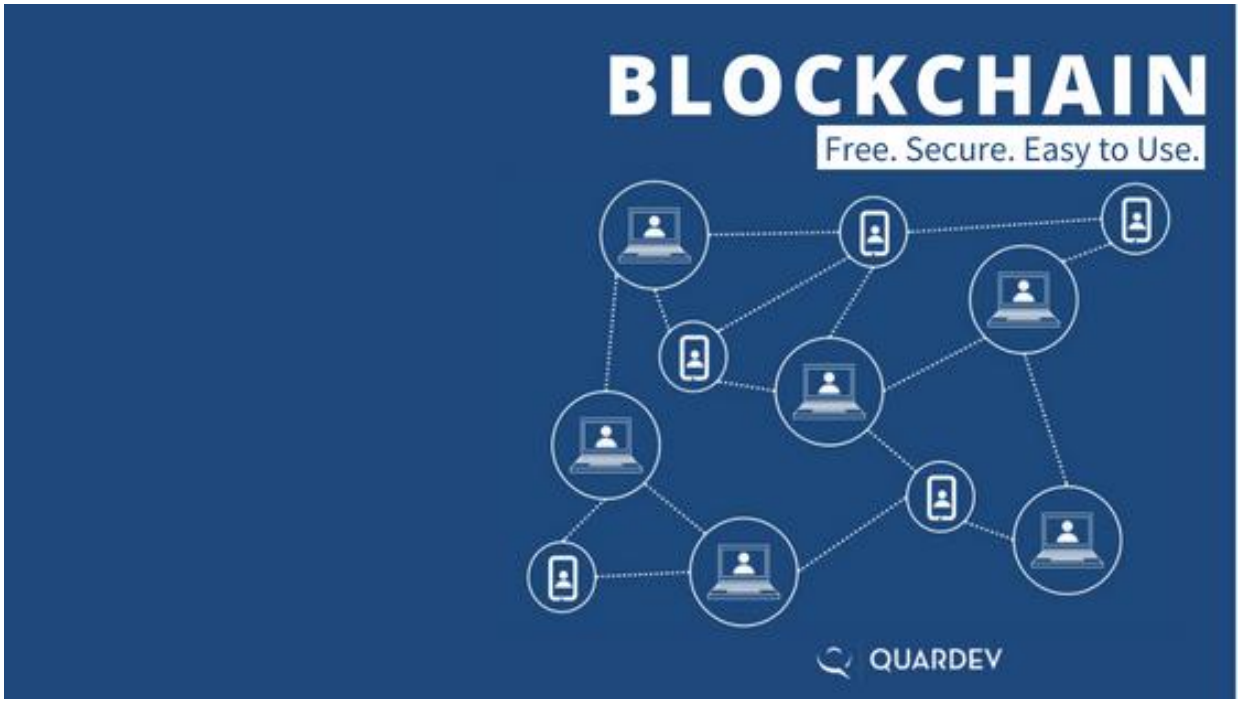

QUARDEV
Integrity, Service, Solutions

QUARDEV
Integrity, Service, Solutions

Quardev

•Blockchain Technology Overview

- Parke Blake
- James Frazier



Blockchain is a secure distributed ledger

QUARDEV
Integrity, Service, Solutions

Blockchain Overview

- **Blockchain**

- Why blockchain was developed
- History of Blockchain
- Structure of Blockchain
- Uses for Blockchain
- Who is investing in BC
- Potential challenges with BC
- Links to use BC today
- Q & A

QUARDEV
Integrity, Service, Solutions

Problems solved with blockchain technology

Need for a peer to peer transaction. That is, no need for a central authority.

Single digital asset; no double spending.

Transactions are transparent; all participants have the exact same record of the transaction.

Paypal/SquareCash/etc
Visa/Mastercard/Amex/etc
Bank

QUARDEV
Integrity, Service, Solutions

Problems solved with blockchain technology

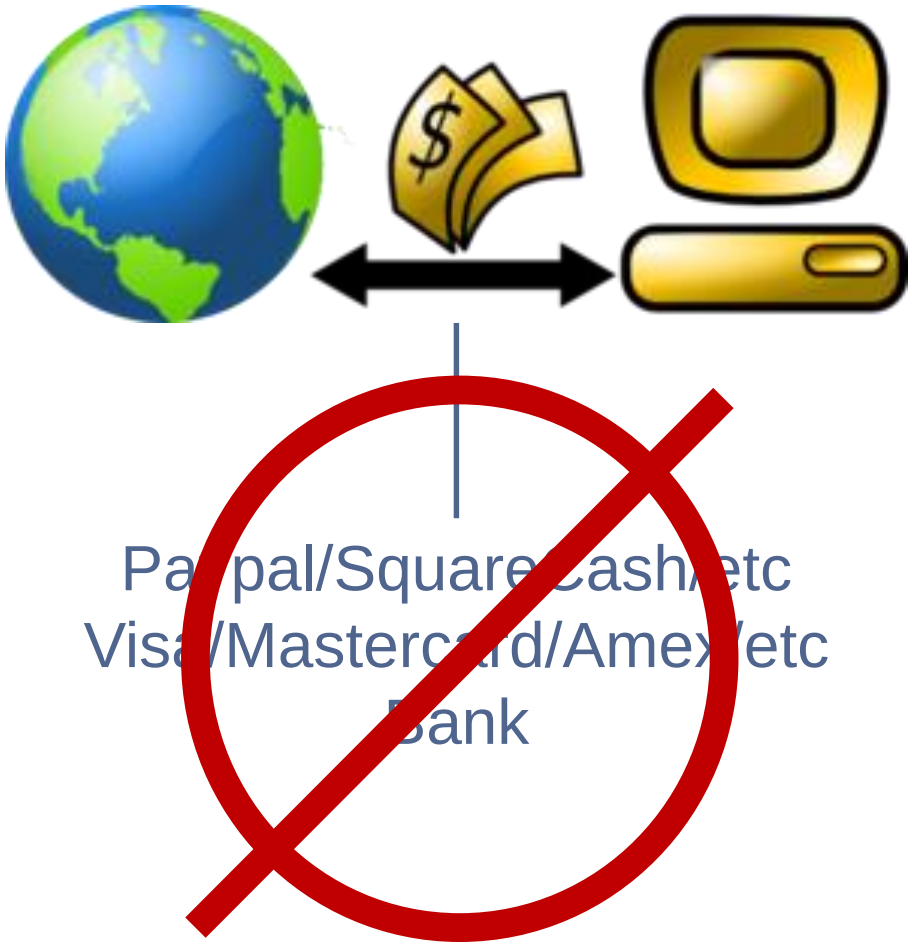
Need for a peer to peer transaction. That is, no need for a central authority.

Single digital asset; no double spending.

Transactions are transparent; all participants have the exact same record of the transaction.

With no central authority, must be:

- Self maintaining
- Secure and immutable

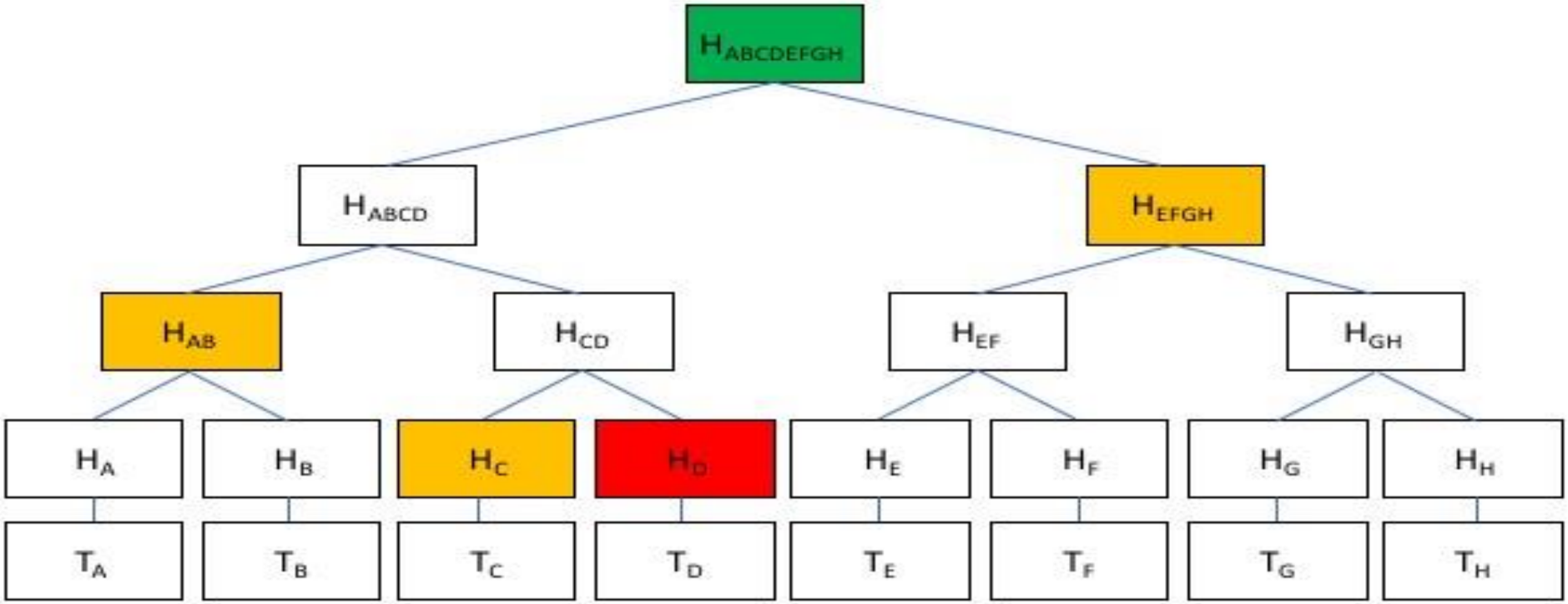


History of Blockchain

1991: The first work on a cryptographically secured chain of blocks was described by Stuart Haber and W. Scott Stornetta.

1992: Bayer, Haber and Stornetta incorporated Merkle Trees into the design, which improved efficiency by allowing several documents to be incorporated into one block.

Merkle Tree



Source Investopedia

History of Blockchain

2008: The first Blockchain was conceptualized by a person (or group of people) known as **Satoshi Nakamoto**. There is a fascinating story about how people have try to identify Nakamoto.

2009, January 3rd: The “Genesis” (first) block is created and time stamped for Bitcoin.

It was implemented the following year by Nakamoto as the core component of the cryptocurrency Bitcoin, where it serves as the public ledger for all transactions of the ledger.

2014-2017: The bitcoin file size grew from 20 gigabytes to over 100 gigabytes.

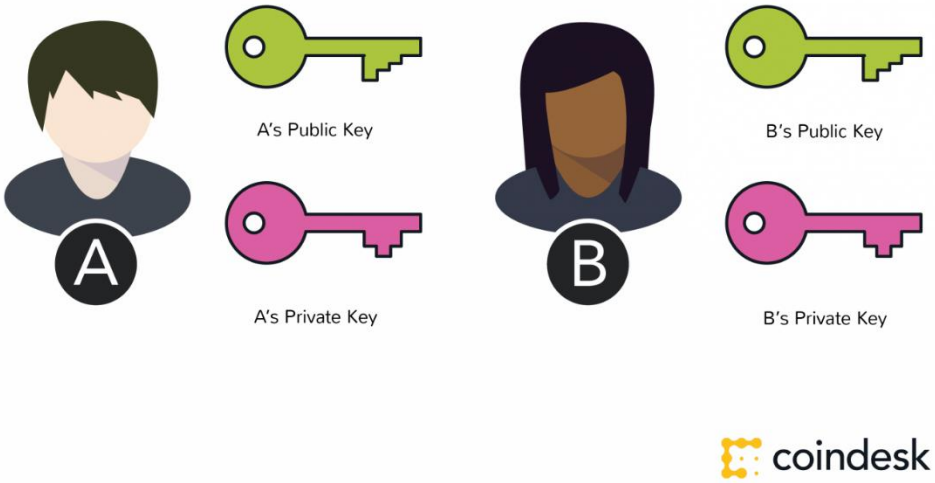
History of Blockchain

2014: The term Blockchain 2.0 is coined, referring to new applications of the distributed Blockchain database. 2.0 allows programable Blockchains (smart contracts etc.)

In the original Nakamoto papers, the words block and chain were used separately, but were eventually popularized into a single word in **2016**.

2016: The Global Blockchain Forum is established to help establish industry standards.

Blockchain Transaction



Digital signatures are used to identify users. User "A" uses its private key to identify itself and then along with its public key, announces a transaction request with "B" using the public key for "B." The keys are used to create the digital signatures.

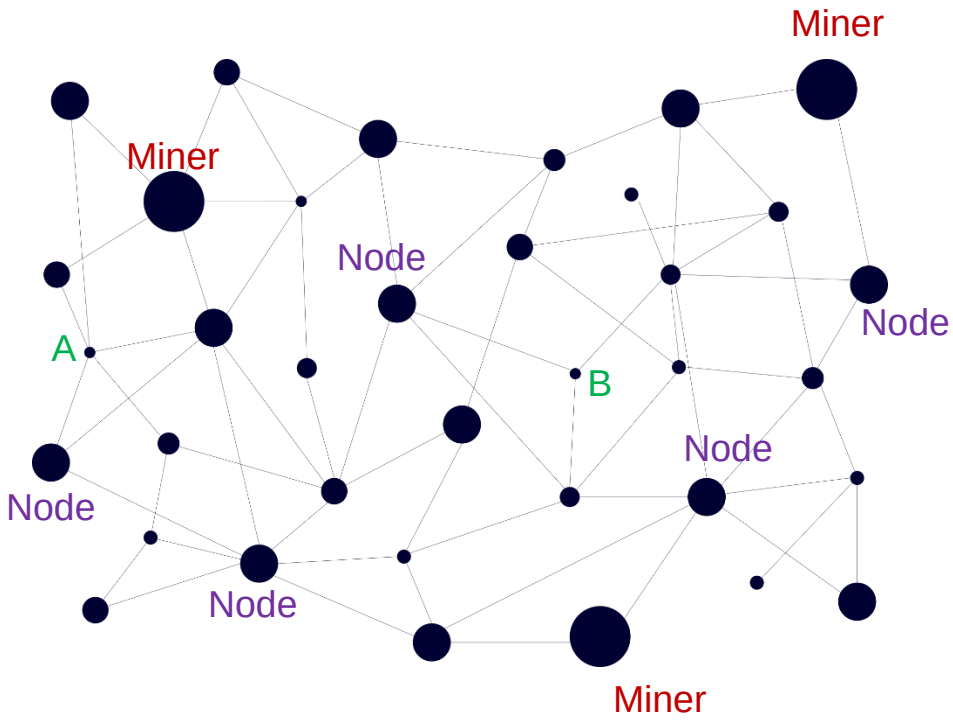
QUARDEV
Integrity, Service, Solutions

Blockchain Transaction

Nodes within the network called miners validate transaction details and create a record of the transaction by adding it to a block candidate.

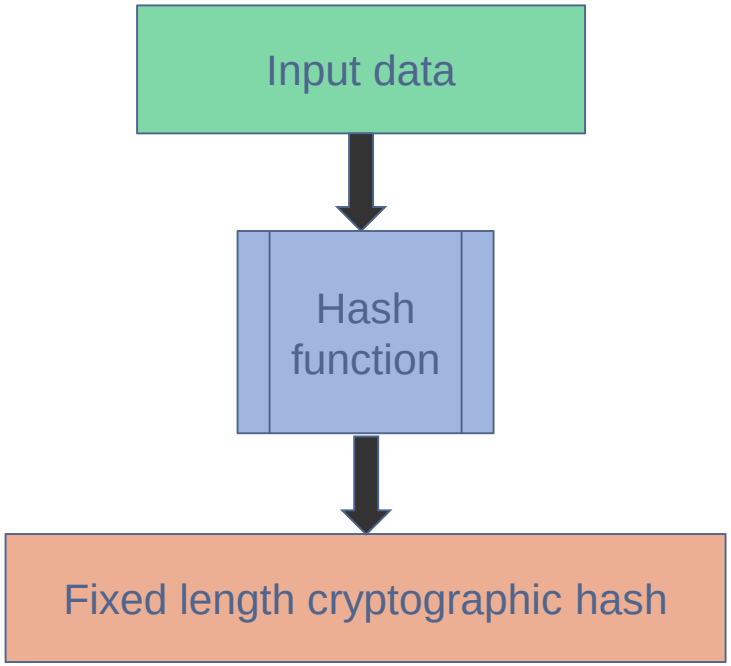
When complete, the miner broadcasts the block candidate to the blockchain network.

Nodes verify the block candidate, then add that information to the blockchain once a consensus has been reached between nodes that all criteria have been met.



Cryptographic Hash

1. No matter how many times input run through algorithm, same hash results (deterministic)
2. Given a hash result, it is impossible to determine original input (pre-image resistance)
3. Even very small changes affect results
4. Given two different inputs, it's impossible for their hashes to be equal



Mining Process

Hash of previous block (pointer) combined with current input data and hashed

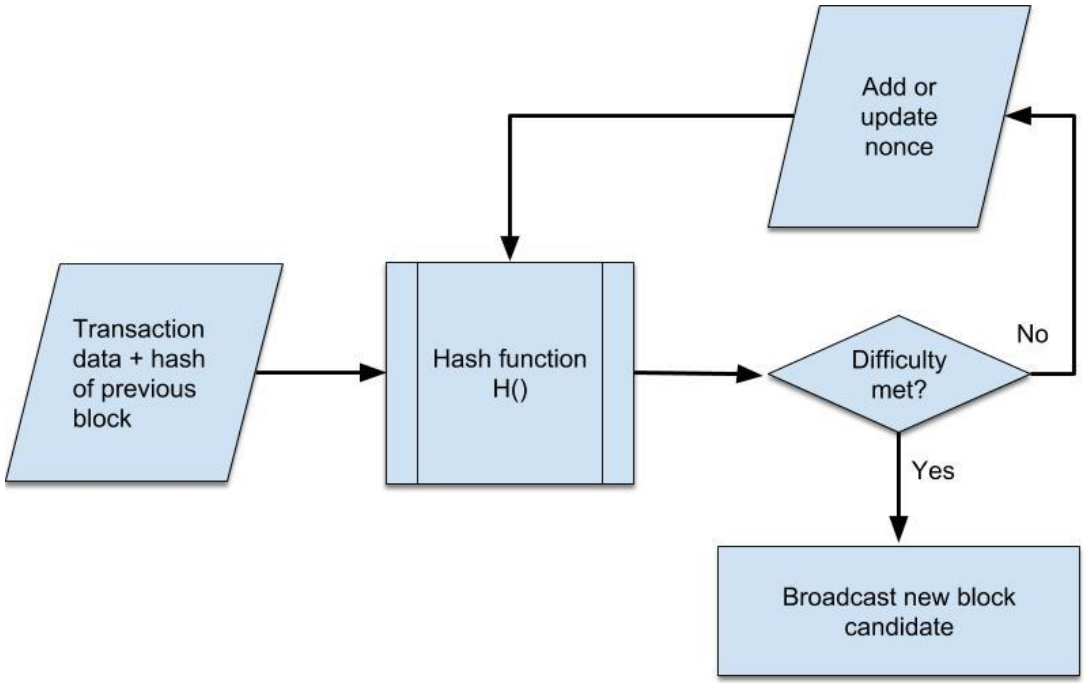
Nonce added to that and hashed

Result compared to required difficulty level

If criteria met, new block candidate announced to nodes

If criteria not met, nonce updated and rehashed.

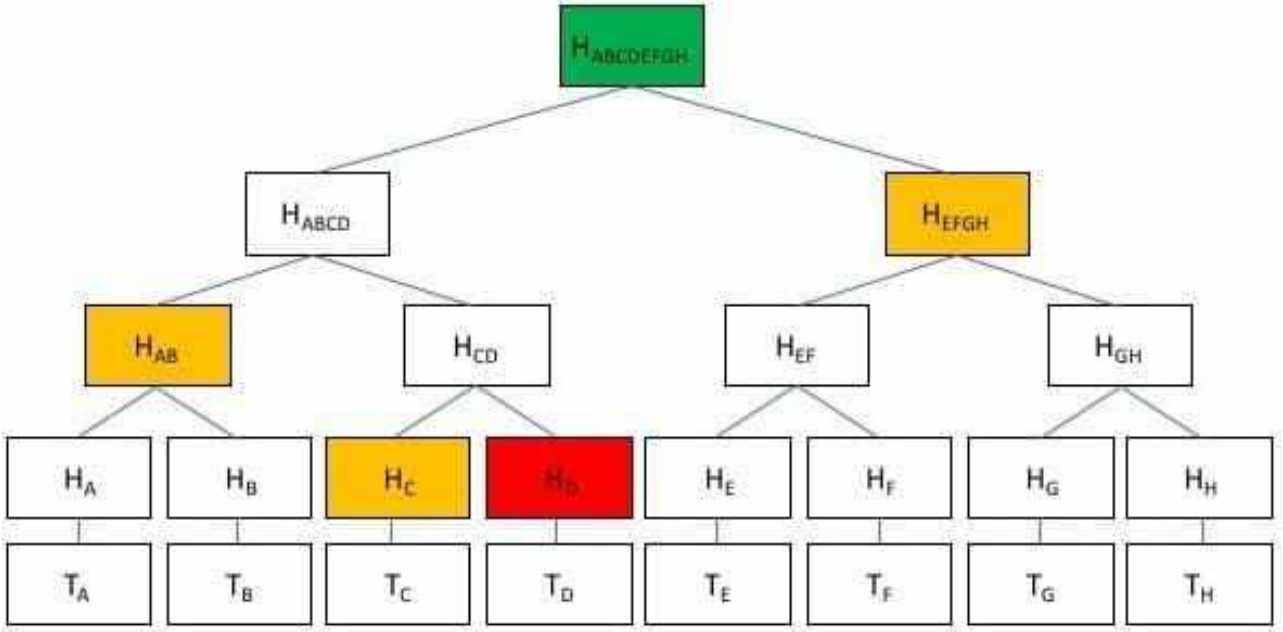
Rinse repeat.



QUARDEV
Integrity, Service, Solutions

Merkle Tree

- Data structure of transaction hashes
- Each parent is a hash of children
- Root is a hash of all contained hashes
- Simplifies verification of transactions



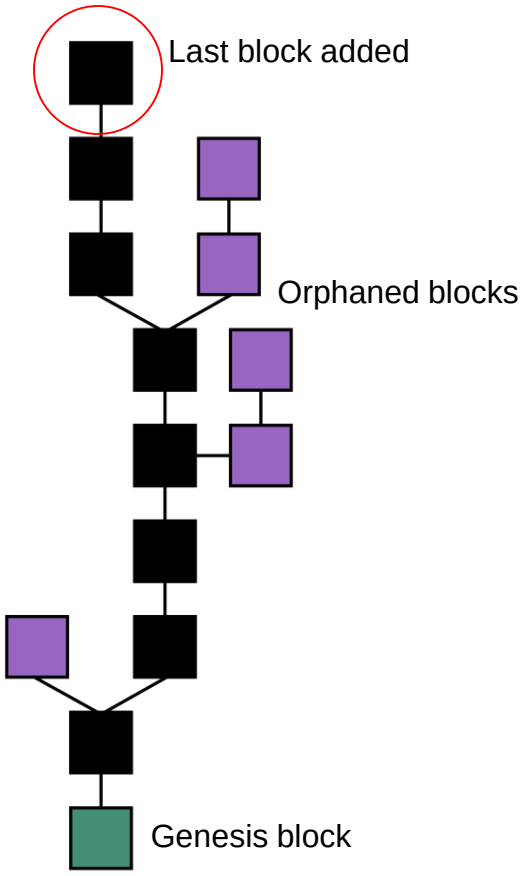
Source Investopedia

Adding a block to the Chain

Following announcement of new block candidate, nodes verify candidate.

If node consensus is achieved, the new block is added to the chain

Miners stop work on last block, return open transactions to pool, and begin work on next block.



Original source Wikipedia

Public vs. Private Blockchain

Public

No central authority
Decentralized

Distributed

Transparent; public data can be viewed

Private or Permissioned

Central authority
Administration layer

Distributed

Data is private

Easier to implement

Fewer transactions, so better performance

What kinds of things is Blockchain being used for today?

QUARDEV
Integrity, Service, Solutions

Data Storage

- In cloud data storage
- No central repository needed, (no single provider, point of failure)
- **Storrj.io** doing this now, and will pay you for storage space

Smart Contracts

- Contract with some code built in
- Standard contract tell you what should happen next
- Smart contract validates, then execute the next steps

What kinds of things is Blockchain being used for today?

QUARDEV
Integrity, Service, Solutions

Decentralized Notary

- Verifies documents
- Confirms the existence of something with a time stamp
- Provable in Court of Law
- Originstamp.org does this for free today, you're welcome to check it out

What kinds of things is Blockchain being used for today?

QUARDEV
Integrity, Service, Solutions

Supply Chain Management

Current challenges:

1) Lack of transparency
2) Distribution complexity
3) Makes; verification, sourcing and investigation difficult

With Blockchain:

1) All transfers are registered on the ledger (you might argue that the universal use of a common ERP system could solve this, but you lose the other benefits of the distributed network)
2) Products are tagged, marked and easily identified along any point in the distribution chain
3) Provides transparency, reduces complexity, allows verification, with no single authority in control

What kinds of things is Blockchain being used for today?

QUARDEV
Integrity, Service, Solutions

Food Traceability

Similar to Supply Chain benefits, with specific advantages in:

1) Reducing the time it takes to track any package

2) Reduction of shipping costs

3) Improved product safety. Example: Finding the source, and reducing the spread of an e-coli outbreak would be greatly expedited.

What kinds of things is Blockchain being used for today?

QUARDEV
Integrity, Service, Solutions

Healthcare

Patient records challenges:

1) Many disparate systems in place
2) Delayed treatment
3) Not receiving treatment
4) Wrong treatment

Blockchain:

1) Can become the glue that hold multiple highly fragmented systems together

Many hurdles to overcome:

1) Modifying existing monolithic systems
2) Adopting and standard communications protocol
3) This is in development, but this will be a slow adoption. Even so, the benefits are so clear, effort are underway to make this happen.

What kinds of things is Blockchain being used for today?

QUARDEV
Integrity, Service, Solutions

Voting

Relatively simple application, one vote, one person.

Provides validation of the electoral process.

What's the worst that could happen???

Who is investing in Blockchain?

QUARDEV
Integrity, Service, Solutions

The New York Times reports that in the first quarter of 2018, VCs have put ½ a billion dollars into 75 different Blockchain projects. That's more than double what they raised in the 4th quarter of 2017

All of the "Big-Four" accounting firms have Blockchain initiative:

1) Ernst & Young
2) PwC
3) Deloitte
4) KPMG

Who is investing in Blockchain?

QUARDEV
Integrity, Service, Solutions

As well as:

IBM

Microsoft

Oracle

Amazon

Google

JP Morgan Chase

Bank of America

Bill and Melinda Gates Foundation

Who is investing in Blockchain?

QUARDEV
Integrity, Service, Solutions

- E&Y has gone so far as to develop cryptocurrency wallets for all of their Swiss employees, and have installed a Bitcoin ATM in the Swiss offices.
- India's Icici Bank onboarded more than 250 corporate customers for domestic and international financial transactions.
- Delaware is updating its laws to allow Blockchain technology to be used for record keeping and electronic transmissions in Banking and Insurance industries.
- Wyoming and Colorado are doing the same.

QUARDEV
Integrity, Service, Solutions

Challenges

- Keeping track of private key
- Performance
- Energy use / Environmental cost
- No blockchain regulations which may be needed in highly regulated industries
- Public perception/adoption; complexity complicates understanding
- Initial cost
- Integration with legacy systems
- Established services may have vested interest in blockchain failure
- Bugs in node code

QUARDEV
Integrity, Service, Solutions

For Experimenters

Medium.com, Programmers Blockchain with Kass:
Creating Your First Blockchain with Java, Parts 1 and 2

Azure:
https://azure.microsoft.com/en-us/solutions/blockchain/

IBM:
https://www.ibm.com/blockchain/getting-started.html

AWS:
https://aws.amazon.com/blockchain/

Openchain (open source)
https://www.openchain.org/

Multichain (open platform):
https://www.multichain.com/

Blockchain Technology Q & A

QUARDEV
Integrity, Service, Solutions

- Parke Blake
- James Frazier