

Demystifying Blockchain for Telecom

Alexander F. L. Sand, Eversheds Sutherland

May 10, 2018



Agenda

- Bitcoin Basics
- Bitcoin vs Blockchain
- What is a Blockchain?
- A Distributed Network
- Building the Chain
- Powering Transactions
- Creating Consensus
- Smart Contracts
- ICOs
- Promises of Blockchain
- Risks of Blockchain

Presenter



Alexander F. L. Sand
Associate
Eversheds Sutherland
alexandersand@eversheds-sutherland.com
+1 212 287 7019

What You May Have Heard About Bitcoin

Bitcoin Basics

Some Basics on Bitcoin

Where do you get Bitcoin?

- There are companies that specialize in buying and selling bitcoin. They operate exchanges that offer exchange rates between USD/BTC and other digital currencies, similar to exchanging money at an airport.

What gives Bitcoin value?

- Like many investments, Bitcoin's value derives from people's willingness to accept it as having value. The fact there are liquid markets that are constantly willing to exchange money for Bitcoin means it has value. What gives gold value?

Where do you keep Bitcoin?

- Bitcoin only exists as a balance on a shared ledger, so you can't really hold Bitcoin in your hand like you can a dollar. What you can hold is the code that proves you own the balance of bitcoin associated with an address. Software and services that help you store this code and make it easy for you to transfer Bitcoin are called a bitcoin "**wallet**."

Bitcoin Basics

Criminality

True or False?

Bitcoin is mostly used
for criminal activity.

Bitcoin and Criminality

- Bitcoin did prove popular on “dark markets” in its early days.
- Enables users to provide instant payment anywhere in the world.
- As it would be to any internet business, this is useful if for selling illegal things on the internet, and has the added benefit of not having to deal with banks.
- Also was often billed as being “anonymous” and so buyers and sellers thought it would be safer to use Bitcoin than another form of payment.

Bitcoin and Criminality

- Turns out Bitcoin isn't nearly as anonymous as people thought.
- Law enforcement has been able to shut down multiple dark markets and arrest their operators across jurisdictions.
- In the most famous case, Ross Ulbricht, who had run the "silk road" dark market, was arrested by the FBI in San Francisco. He received a life sentence.
- Cash will always be king for crime.

Bitcoin vs. Blockchain

What's the difference?

Bitcoin

- The first “cryptocurrency”
- A distributed electronic payment system that does not rely on central banks or other counterparties
- Enables global peer to peer payment with no single central depository or processor
- Powered by the first ever blockchain

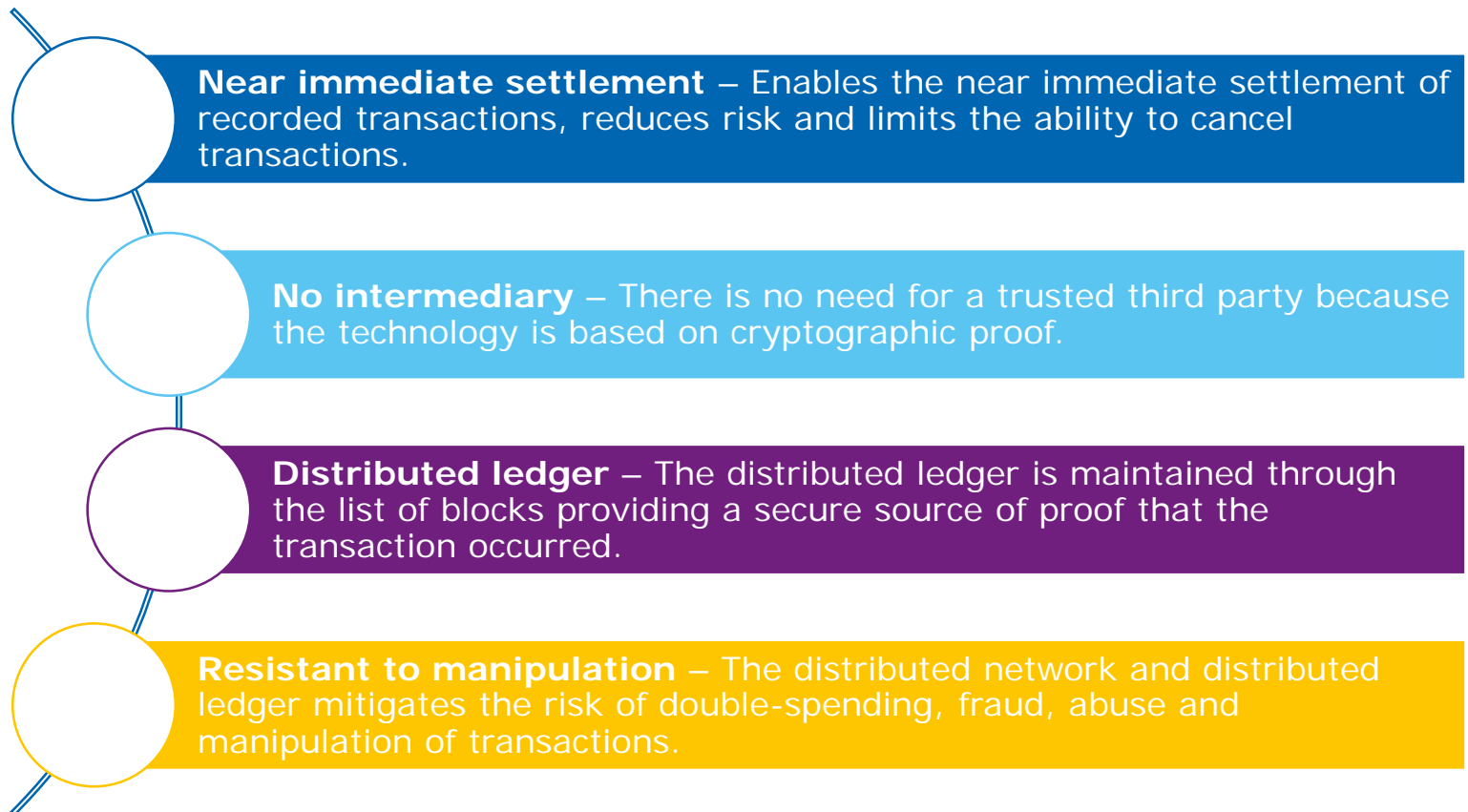
Blockchain

- The technology underlying bitcoin and many other projects
- A new system to arrange, process, store, and share information electronically
- Leverages existing and widely used cryptography
- Just one kind of “distributed ledger technology”

Blockchain

Capabilities

Blockchain is a digital ledger system for recording business transactions and events.



There is nothing magical about the blockchain

It is a database or ledger



Blockchain

A Distributed Ledger

What is a distributed ledger?

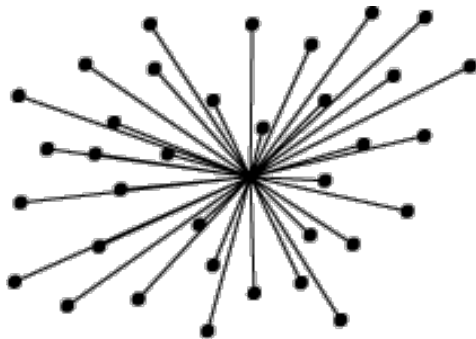
- An asset database shared across a network on multiple sites or geographies.
- All participants can have access to the ledger via a copy or connection to other databases.
- Any changes made on any one of the ledgers will be reflected on all ledgers.
- It's a technological means of keeping accurate and updated records in multiple locations.

Blockchain

Types of Networks

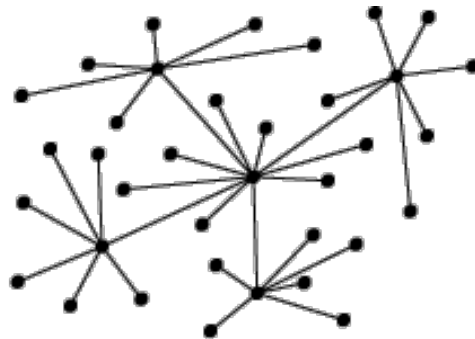
Centralized

- One authority/failure
- Easy to maintain
- Can be unstable
- Slow scalability/evolution



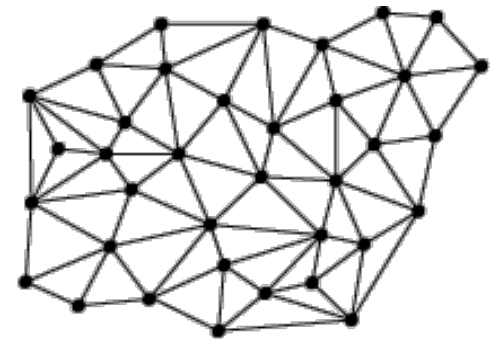
Decentralized

- Several authorities
- More stable
- Medium scalability
- Quicker evolution



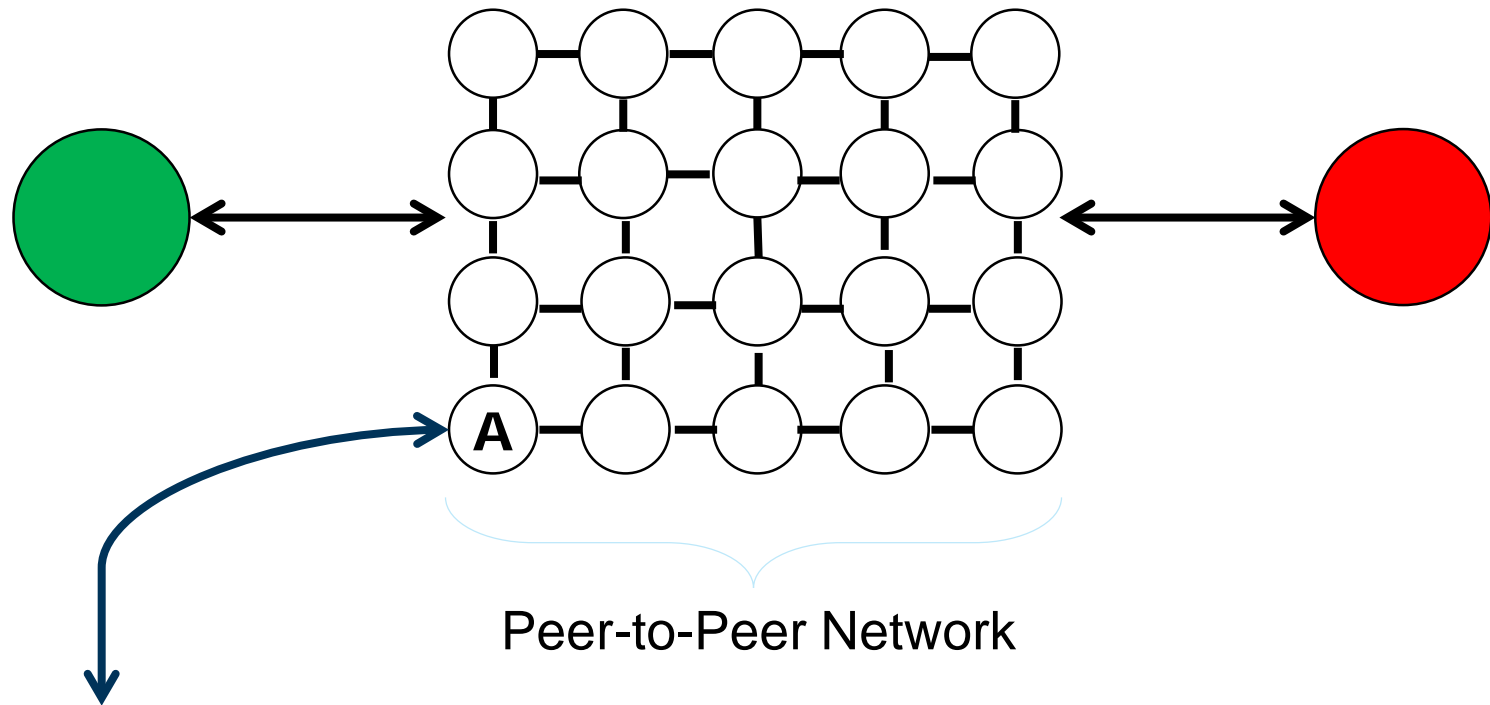
Distributed

- No central authorities
- Quicker evolution
- Infinite scalability
- Difficult to maintain
- Most resilient



Blockchain

A Peer-to-Peer Distributed Network



A Node = Individual Server

Each node has an entire copy of the database (with records of all of the transactions) which the node continually updates and reconciles with each other node in the network. The result is a “distributed ledger.”

Blockchain

A Function of the Network

Validation

- Anything that happens on a blockchain is a function of the entire distributed network as a whole.
- Each node has a copy of the blockchain (all logged transactions), and every copy must be consistent with all other copies; otherwise the transaction will not be incorporated into the blockchain.

Blockchain

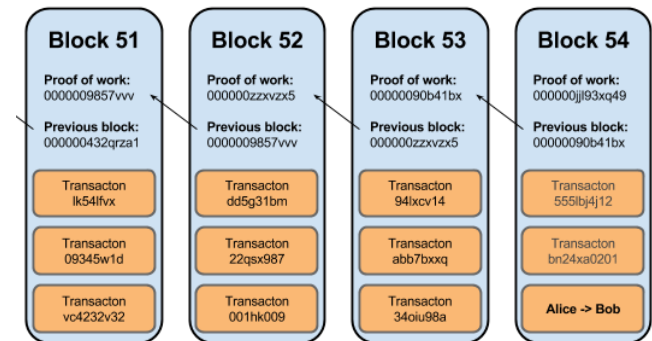
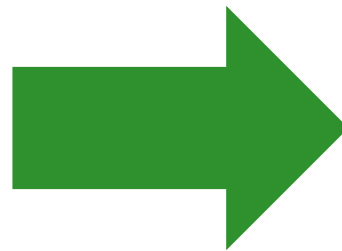
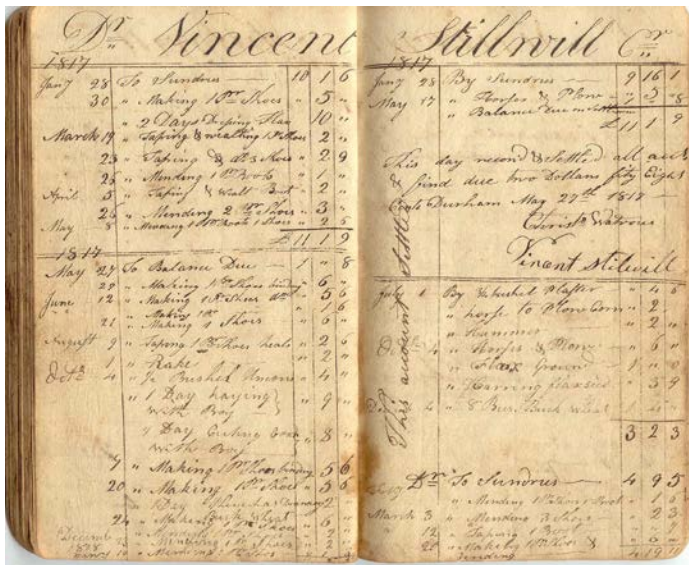
What is it really?

Some ways to think about Blockchain?

- The great chain of being sure about things
- Single source of truth with many copies
- A tool for organizing, tracking, and using large sets of ever-changing data

Blockchain

What is a block?



If a blockchain is a ledger then a block is a page of that ledger

Blockchain

What is a block?

A block contains:

A record of some or all recent transactions broadcast to the network but not yet confirmed (at least one transaction, but may contain thousands);

A unique identifier (the "hash") for the current block; and

A reference to the unique identifier (the hash) from the previous block in the chain.

The ledger is kept through the long list of blocks, known as the blockchain.

Blockchain

Building the Chain

If anyone can write a page in the ledger, how do we make sure they all work together?

Blockchain

Hashing – A Cryptographic Fingerprint

A one-way function that is not reversible.

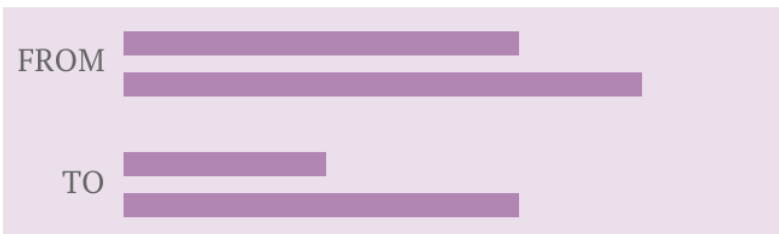
```
thedeadrobot 21:02:05 | ~ | 🐼 > echo "Hello" | md5
09f7e02f1290be211da707a266f153b3
thedeadrobot 21:02:06 | ~ | 🐼 > echo "hello" | md5
b1946ac92492d2347c6235b4d2611184
thedeadrobot 21:02:11 | ~ | 🐼 > echo "Hello" | md5
09f7e02f1290be211da707a266f153b3
thedeadrobot 23:06:08 | ~ | 🐎 > █
```

Each transaction has a unique fingerprint that cannot be changed.

TRANSACTION RECORD
ALICE > BOB

Hash
function

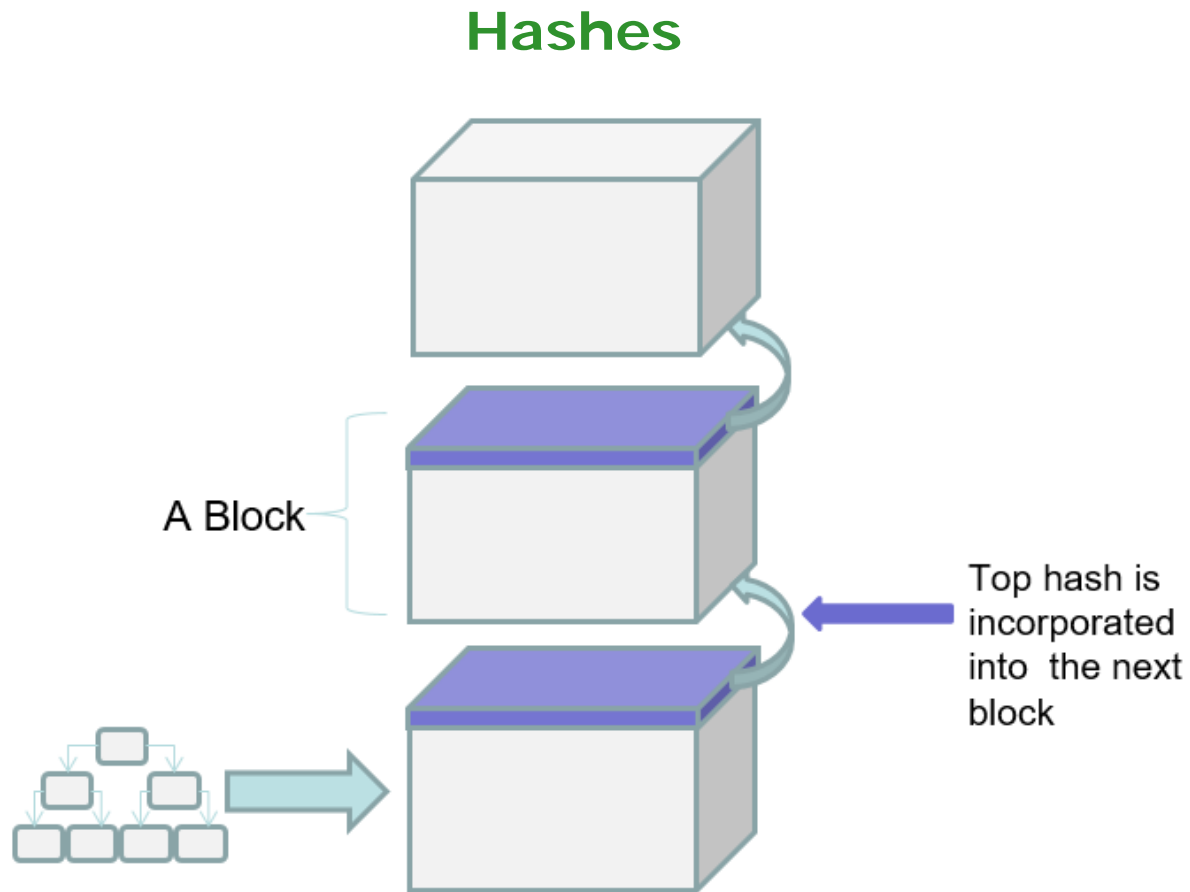
Hash
(unique ID)



```
d7a8fbb307d78094
69ca9abcb0082e4f
8d5651e46d3cdb76
2d02d0bf37c9e592
```


Blockchain

Building the Chain



Blockchain

Powering Transactions

If anyone can submit a transaction, how do we know the person submitting the transaction has authority to initiate the transaction?

Blockchain

Transactions Powered by Cryptography

Public-key cryptography powers transactions

Blockchain relies on public-key cryptography: It is built on pairs of public and private keys.

Every account on the ledger has an "address" (public key or account number).

Only the owner of the account gets the corresponding private key.

The public and private keys are mathematically linked.

It is computationally easy to derive a public key from the private key, but hard to derive a private key from the public key.

Blockchain

Transactions Powered by Cryptography

Public-key cryptography powers transactions

The public key is used as an account number that holds assets.

The private key is used to prove ownership of the assets associated with the public key.

The owner of the account mathematically signs a transaction with the private key to authorize the transaction in the account.

The private key never needs to be shared or shown to anyone else.

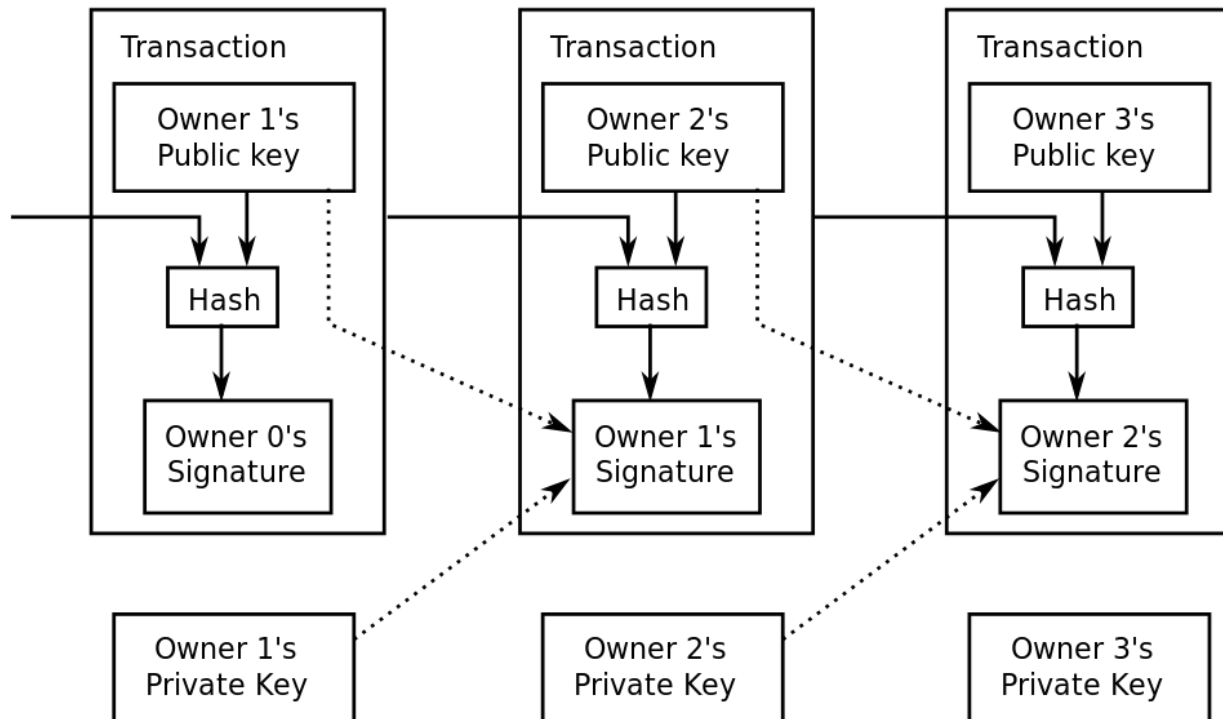
Everyone else on the chain can mathematically prove that whoever authorized the transaction had the private key, and therefore it is a valid transaction.

Whoever holds the private key, owns the account (like a bearer bond.)

Blockchain

Powering Transactions

Asymmetric Keys – Public and Private Keys



Any transaction not properly signed will be rejected by the network.

Blockchain

Powering Transaction

True or False?

Blockchain
transactions are
anonymous.

Blockchain

Powering Transactions

Pseudonymous transactions:

Sending and receiving an asset is similar to writing under a pseudonym.

On blockchain, the owner of an asset is identified by their address.

If your address is linked to you, then every transaction involving your address will also be linked to you.

Your address is a version of your public key.

Blockchain

Building Consensus

If anyone can submit a new page to the ledger at any time, how do all the parties agree which pages are valid?

Blockchain

Building Consensus

Why consensus?

In a centralized network, no need for consensus; it is done by the central authority.

In a distributed or decentralized network, how do you agree on what is true?

Anybody could try to manipulate or attack the network for personal gain by submitting false transactions.

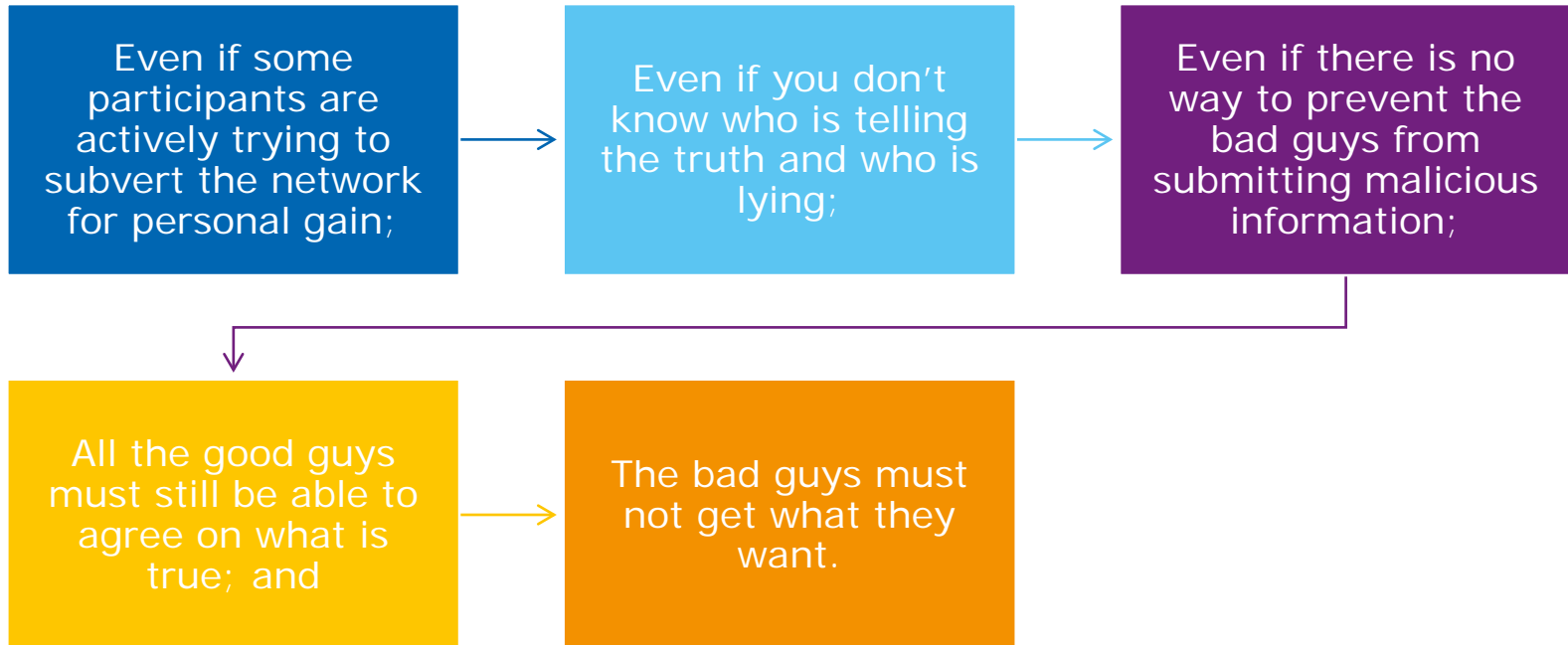
Goal: the aim of the consensus approach is to secure the network, predominantly through economic means: it should be too expensive to attack the network, and more profitable to help protect it.

Blockchain

Building Consensus

Fault Tolerance

- In other words...



Blockchain

Fault Tolerance and Blockchain

BFT is essential on a blockchain

- Most traditional distributed computing environments have central configuration databases or authorities that can fix things in the event of a Byzantine failure.
- On a blockchain, because there is no central authority, transactions are confirmed based on community consensus alone, which is what makes it so powerful.
- Most blockchain technology, including Bitcoin, has relied on a concept called proof of work (PoW).
- Under this model, anyone who wants to add to the blockchain must perform a work-intensive task using information from the existing blockchain in order to add new information.
- In the case of Bitcoin, PoW is produced using a hashing algorithm that, by its nature, takes a fair amount of time to execute.

Blockchain

Consensus in Bitcoin

Proof of Work

- In a PoW system, data can't be added to the blockchain without a significant time investment on the part of the party adding the data.
- This provides a practical protection against manipulation of the blockchain because, in order to undermine group consensus, a malicious party would need to invest a great deal of time producing sufficient PoW to exert a meaningful influence on the blockchain.
- On a blockchain that is sufficiently large, the PoW requirement effectively provides BFT.
- This approach also has a limitation. It requires the expenditure of a large amount of computational effort for no purpose other than fault tolerance.

Blockchain

Consensus in Bitcoin

Mining for Bitcoins

- Computers compete to find a hash with specific properties.
- The computer that finds the answer first—the proof that it has done the necessary work—is allowed to add a new block of transactions to the blockchain.
- It is rewarded with a tranche of newly minted bitcoins (currently 12.5 BTC per block, or roughly every 10 minutes), plus all of the small transaction fees users have paid to send coins.
- In addition to building consensus, this also serves to incentivize participation, which makes the blockchain bigger, and which makes the blockchain more secure.

Blockchain

Building Consensus

Consensus Concepts:

Proof of Work

Proof of Stake

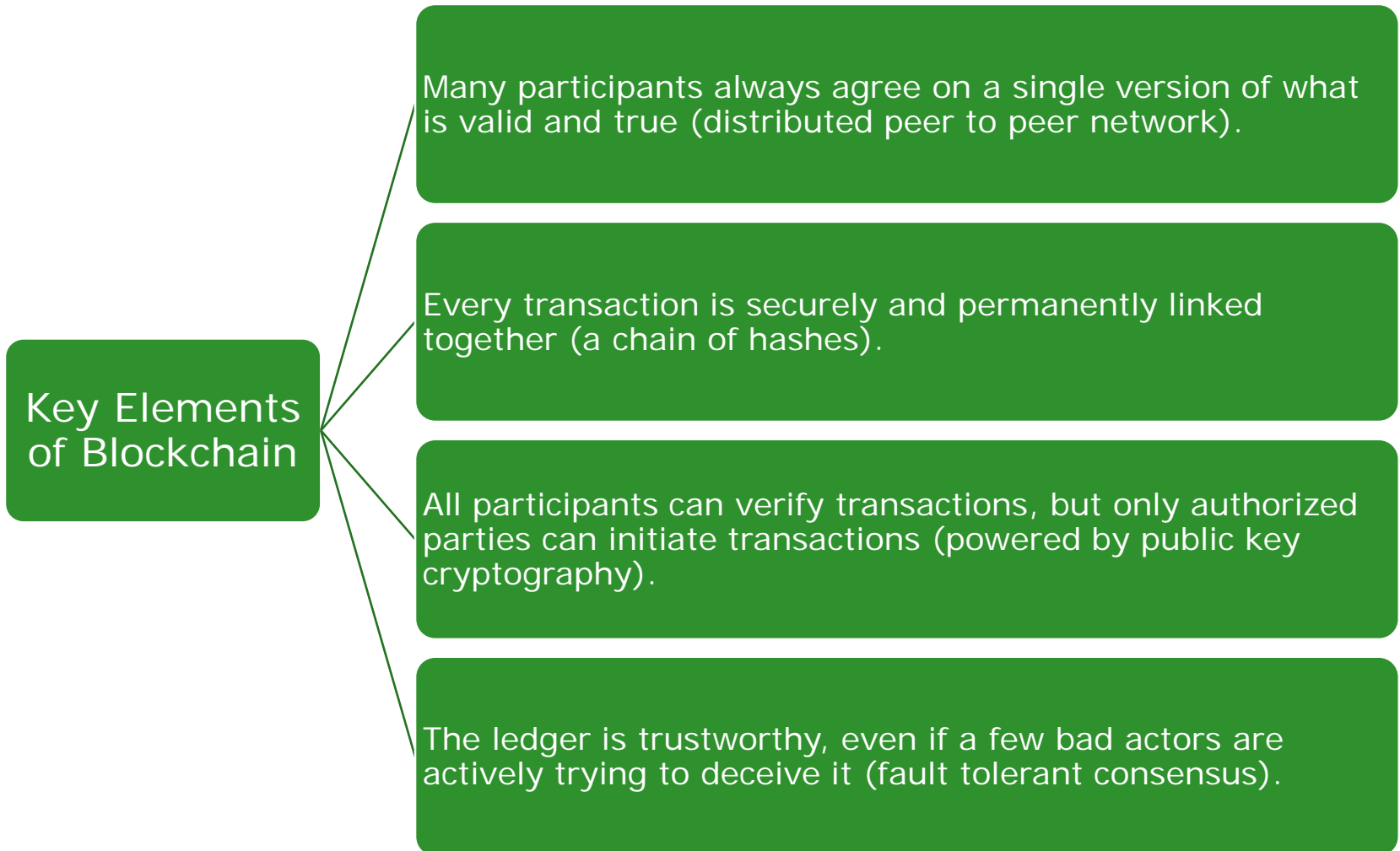
Leased Proof of Stake

Delegated Proof of Stake

Proof of Importance

Blockchain

Recap of What Makes It Work



Blockchain

Promises of a Blockchain

Potential Benefits of Blockchain:

*Reduce
choke-points*

Ability to verify and process transactions without third-party involvement.

*Data
reconciliation*

The information is transparent and the data is complete, accurate and consistent across all locations and databases.

Data Access

Data from many sources can be instantly available across the network

*Automated
transactions*

Transaction processing can be nearly instantaneous and can leverage automation.

*Cost
reduction*

Costs associated with third-party intermediaries, governance and audits can be greatly reduced.

Blockchain

A Tool for Business

Public vs. Private

Public blockchain means anyone can join and see transaction records.

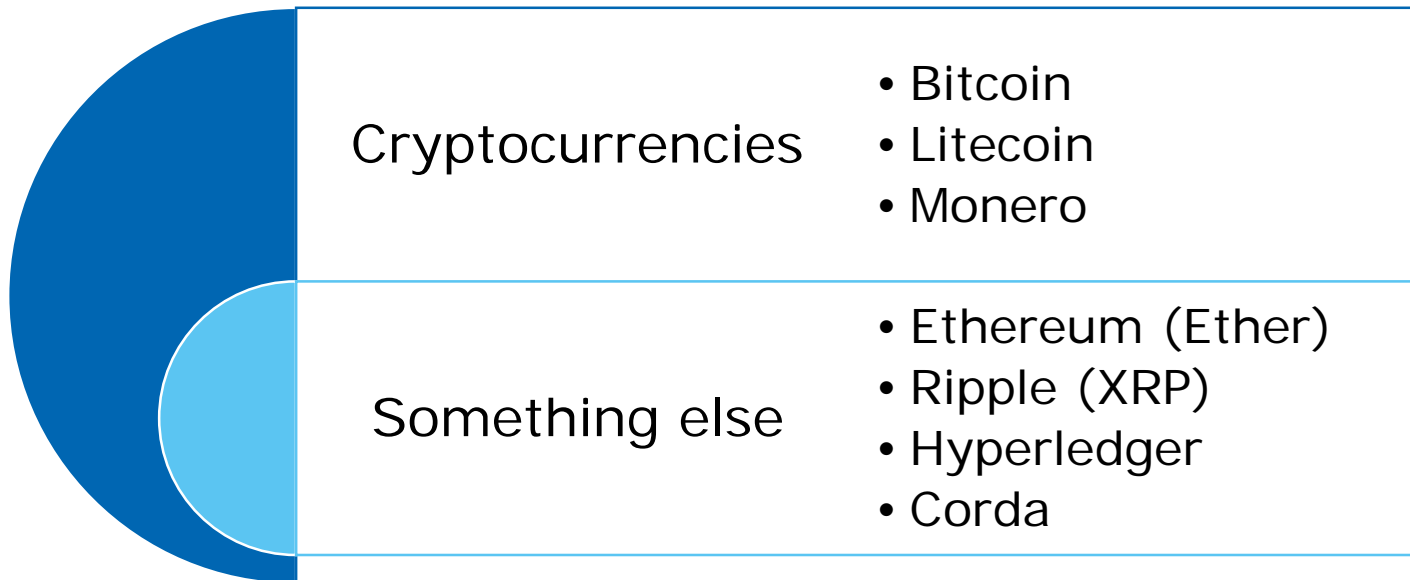
Private blockchain means only those who are authorized may join or see certain information.

In many cases, businesses will set up a private blockchain for increased privacy and security.

Blockchain

Many Different Flavors

There are many different blockchain and distributed ledger products:



Blockchain

Smart Contracts

What is a Smart Contract:

- A smart contract is basically just computer code.
- Today's legal contracts have no real relationship with the computer code that executes them.
- Smart contracts are when business terms are recorded in code instead of legal language.
- Some think they could replace written contracts.
- Alternatively, can think of as a way to automate performance of contractual obligations.

Blockchain

Smart Contracts

What is a Smart Contract:

- Transactions are really just changes.
 - E.g. State 1 = Alice has \$10, and Bob has \$5. Alice pays Bob \$5. State 2 = Alice has \$5 and Bob has \$10.
- This change of state can be anything, not just value transfer.
 - (E.g. Has Alice Filed an insurance claim in the last 12 months? What is Alice's credit rating? What is Alice's mailing address?)

Blockchain

Smart Contracts

What is a Smart Contract:


- Transactions can be caused by an action in code so they happen automatically.
- Instead of manually recording or triggering a transaction, code that sits on top of a blockchain can automate the change.
- That change will then be replicated instantly across the entire blockchain network.

Blockchain

Smart Contracts

Smart Contract Example:

A customer buys a new car, and needs immediate proof of insurance to drive the new car off the lot.



The customer could fill out a form online, select policy features, provide payment, and submit contact information.




The payment verification and results of the credit check could then be automatically fed directly into a smart contract.


Blockchain

Smart Contracts

If the payment clears and the credit check matches pre-defined characteristics, the smart contract could then immediately generate and send proof of insurance to the customer.




Simultaneously, the record generated of the customer's transaction could be instantly propagated and accessible across enterprise systems.



Every other database (node) connected to the blockchain network would immediately have an immutable and accessible record of all that policy and transaction information

Beneficiary, date and time of issuance, when payment was received, when coverage became active, etc.



All without human involvement.

Blockchain

Smart Contracts

What is a token?

- A token is any crypto-asset that lives on a blockchain that supports multiple assets, most commonly Ethereum.
- These are the “different blockchains” or “crypto-assets” that we mentioned.
- The tokens do not have to be set up to function like currency, like bitcoin is.
- A token can represent pretty much anything, and can have any desired feature.
- For example, a token can function as a security, including automated distribution of dividends.

Blockchain

Other Kinds of Blockchain Products

What is an ICO?

- An “Initial Coin Offering” is selling a Cryptocurrency in order to raise funds to support a blockchain startup.
- The funds you pay for the token are used to build the platform/service associated with the token.
- The token entitles buyers to a share of future profits.
- It may also enable buyers to interact or use the platform/service once built.
- Unsurprisingly, the SEC is now regulating these as securities.

Blockchain

Recap of What Makes It Work

Key Elements of Blockchain

```
graph LR; A[Key Elements of Blockchain] --- B[Many participants always agree on what a single version of what is valid and true (distributed peer to peer network).]; A --- C[Every transaction is securely and permanently linked together (a chain of hashes).]; A --- D[All participants can see and verify transactions, but only authorized parties can initiate transactions (powered by public key cryptography).]; A --- E[The ledger is trustworthy, even if a few bad actors are actively trying to deceive it (fault tolerant consensus).];
```

Many participants always agree on what a single version of what is valid and true (distributed peer to peer network).

Every transaction is securely and permanently linked together (a chain of hashes).

All participants can see and verify transactions, but only authorized parties can initiate transactions (powered by public key cryptography).

The ledger is trustworthy, even if a few bad actors are actively trying to deceive it (fault tolerant consensus).

Blockchain

Possibilities in Life Insurance

Potential uses for blockchain in Telecommunications:

Payment settlement for inter-carrier voice traffic (clearinghouse for wholesale voice market).

Prevention of roaming fraud.

Blockchain

Possibilities in Life Insurance

Example 1: Clearinghouse for Wholesale Voice Market

- Today, inter-carrier payment settlement for wholesale voice can still be a fairly manual process.
- Each carrier involved separately must determine which calls require outgoing or incoming payment, determine payment amounts and destinations, and then reconcile the information with each carrier involved.
- Colt and PCCW Global developed a POC blockchain solution that automates this process earlier this year.
- Call records were recorded on a Private bilateral blockchain, which were then reported to a public blockchain.
- Smart contracts were then used to rate call detail records, resolve disputes, and record the settlement transactions.
- Tens of thousands of call records were analyzed and settled in minutes.
- The same process was previously manual and would take weeks or months.

Blockchain

Possibilities in Life Insurance

Example 2: Preventing Roaming Fraud

- Related to the clearinghouse and settlement example, being able to quickly identify and track subscribers across networks can assist with combating fraud.
- A permissioned blockchain could be implemented between every pair of operators. Nodes from both operators could act as miners, verifying the validity of each roaming event reported to it by the other operator.
- When a subscriber makes a call on a visiting network, the visiting network would immediately report the call as a transaction on the blockchain containing the call detail records to the home network.
- The home network would instantly mine the transaction to validate the CDR information.
- If the information is fraudulent, and the home network has no corresponding subscriber, the call can be denied.

Some Risks to be Aware of

Data security – You need to know what data you have, where it is, and who has access to it.

Blockchain offers immutability, but this also means it is harder to undo mistakes. Transactions are irreversible.

All blockchain transactions are traceable back to genesis. This can both be good and bad. How much information are you sharing with your competitors and counterparties?

Regulatory risk – While you may be able to build it, that doesn't mean regulators will allow you to do it.

IP – Who owns the data in a distributed ledger?

Important to think about the details of what is being done and how it is being done.

Don't be blinded by buzzwords.

Questions?





Alexander F. L. Sand

Associate

alexandersand@eversheds-sutherland.com

+1 212 287 7019

1114 Avenue of the Americas

New York, NY 10036-7703

212.389.5000

eversheds-sutherland.com

© 2018 Eversheds Sutherland (US) LLP

All rights reserved.

This communication cannot be used for the purpose of avoiding any penalties that may be imposed under federal, state or local tax law.