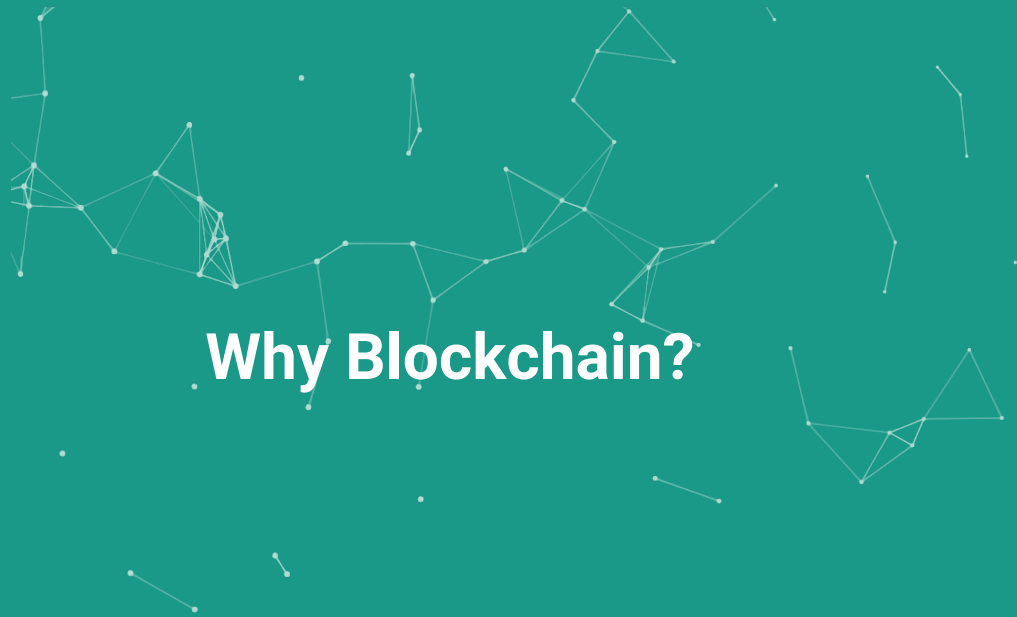
Let’s Learn Blockchain

Blockchain 101

April 11, 2018

Today’s Session

- Blockchain 101 will provide a broad overview of the principles of decentralization and the current state of blockchain technology.
- The participants will gain insight about the various protocols and key concepts such as mining, cyber security, hashing, proof of work/ proof of stake, scalability, privacy, smart contracts and private vs public blockchain.
- Participants will also understand the new financing opportunities and underlying crypto economics that underpin token launch mechanism and the various ways tokens trade.



Why Blockchain?

Blockchain Today

Why it's important

1. Innovation
2. Security
3. Policy

Examples

Government adoption

- Smart Dubai + Estonia
- Venezuela's PetroCoin

Global Crackdown

- Banning of cryptocurrencies
- SEC regulation of Initial Coin Offerings (ICOs)

Blockchain 101

A Brief History of Ledgers

Our world is dependent upon keeping record - of actions, of money, of interactions. These records began in what we commonly refer to **ledgers**.

Satoshi Nakamoto

2008 Global Financial Crisis

Rapidly growing wealth gap

Rise of professional ledger keepers

Evolution of the “ledger”

Ancient Sumeria

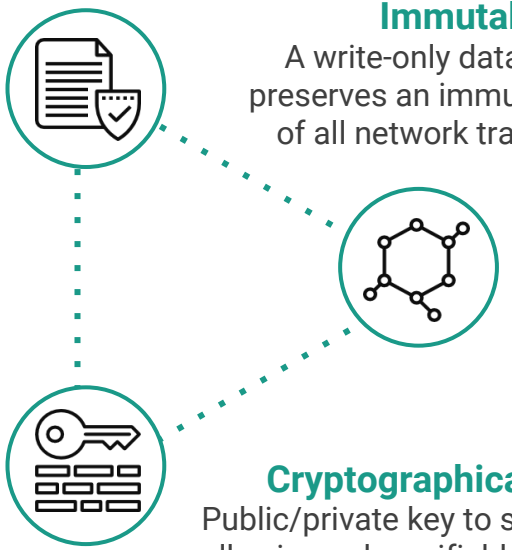
What is blockchain?

Blockchain is a distributed **database**, inherently resistant to attacks and fraud.

Value Proposition

Reduces cost	• Removes the costs of intermediaries • Reduces processing, re-work, and manual errors
Increases revenue	• Creates new products and services • Captures value lost in transit
Reduces risk	• No single point of failure • No unauthorized alterations • Resistant to collusion
Increases speed and transparency	• Verifies provenance • Allows T+0 settlement • Preserves complete audit trail

Key Components



Immutable

A write-only database that preserves an immutable record of all network transactions.

Decentralized

A peer-to-peer platform distributing the same replica of data.

Cryptographically Secure

Public/private key to secure identity, allowing only verifiable transactions.

Why decentralization matters

Through its distributed nature, blockchain enables better, trustless coordination.

Inclusive
More creation and collaboration occurs in a global network that each and every one can join.

Robust
A power outage, natural disaster, or a malfunction cannot bring it down, nor can an attack from malicious actors.

Uncensorable
No government or corporation controls your data. Your privacy remains your own.

Egalitarian
The network is that of the masses. No economic, political, geographic discrimination, no monopoly.

Read More Buterin, V. (2017, February 6). The Meaning of Decentralization.

Crypto-currency vs. blockchain technology

Bitcoin was the first use case of blockchain technology solving the challenges of digital cash in a decentralized manner.

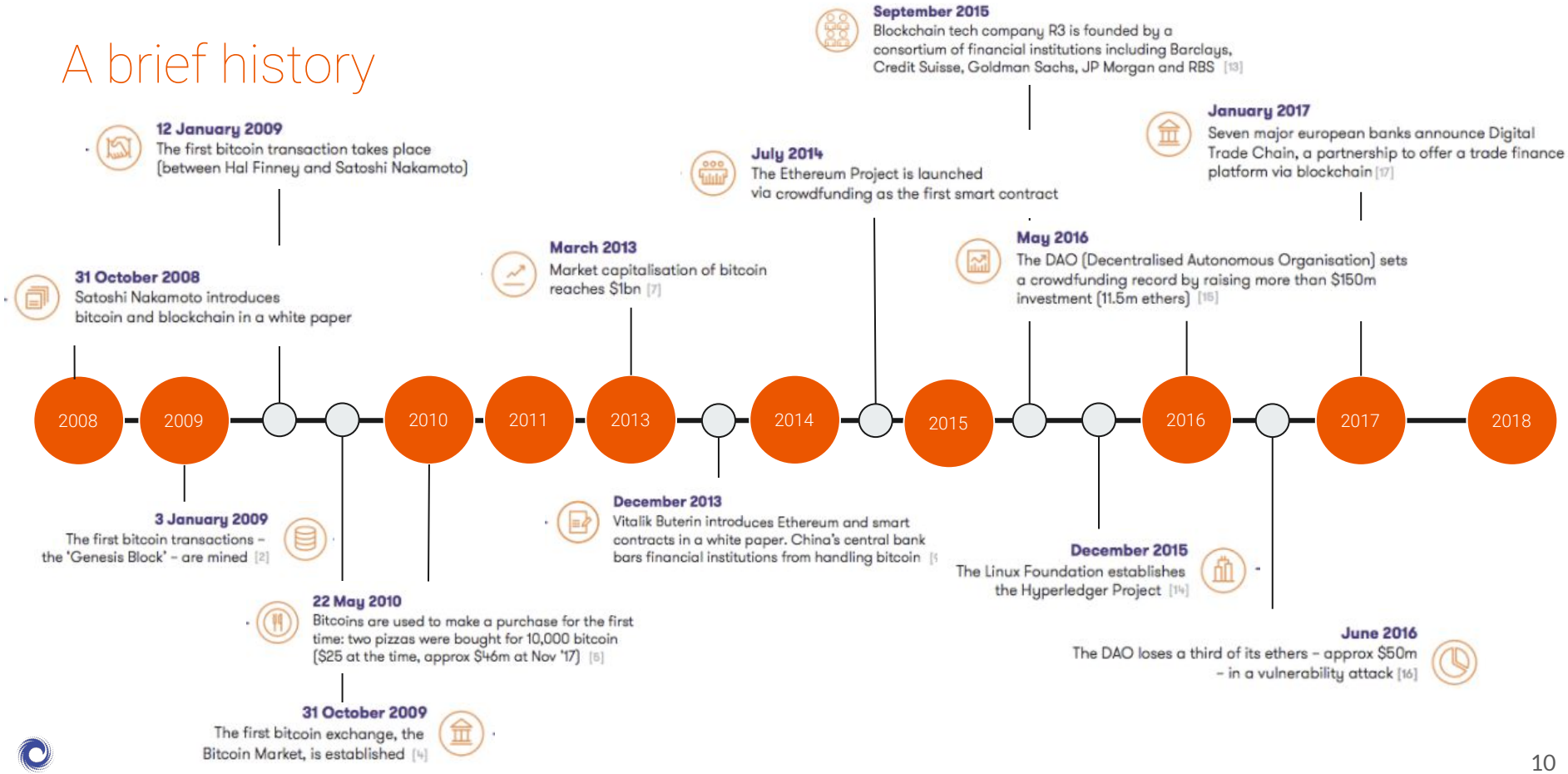
Bitcoin and crypto-currencies

- Electronic money protected through cryptographic mechanisms instead of a central repository
- Issued by a decentralized network/protocol which no one controls and no single point of failure exists
- Intrinsic value dependent on utility
- Eliminates “double spending problem”
- Enables peer to peer transactions w/o inherent need for banks

Blockchain technology

- Technology protocols that group cryptographically signed transactions into blocks, validate blocks and link blocks according to a consensus decision
- All transactions are publicly observable and blocks are replicated across all copies of the ledger within the network
- Allowed the emergence of crypto-currencies by solving the “double spending problem”

A brief history



CONSENSYS

Blockchain & Distributed Ledger Technology

Definition:
Distributed ledgers (DL) use independent computers -- referred to as nodes -- to record, share and synchronize transactions in their respective electronic ledgers, instead of keeping data centralized as in a traditional ledger (World Bank, 2017).

It is important to note that **not all DLT's are considered blockchains** - what makes a blockchain unique is the sequential formation and securing of data in "blocks".

Notable Initiatives

- Hyperledger - open-source network
- Quorum - permissioned blockchain
- R3 - consortium
- Ethereum - public blockchain with private interoperability

CONSENSYS

World Bank, "FinTech Note No.1- Distributed Ledger Technology (DLT) and Blockchain" 2017.

The advent of Ethereum

Ethereum was built to extend the blockchain concepts of cryptographic security, decentralization and immutability with the ability to run trustless business logic. As a Turing-complete virtual machine, it can run any conceivable programs using smart contracts.

Censorship-free vendor-neutral computing platform

Formally-specified **security** and **smart contract** capabilities

Multi-billion dollars of **value protected** on the public network

The dominant platform for the **'token ecosystem'**

> *Think of Ethereum as a world computer. What Bitcoin does for payments, Ethereum does for anything that can be programmed.*

Vitalik Buterin, founder of Ethereum

Supports **private permissioning** while maintaining **interoperability with the public chain**

Under **active development** by the Ethereum Foundation

Rapidly growing community with 30,000+ developers

Continues to grow in terms of Enterprise adoption, scalability and functionality

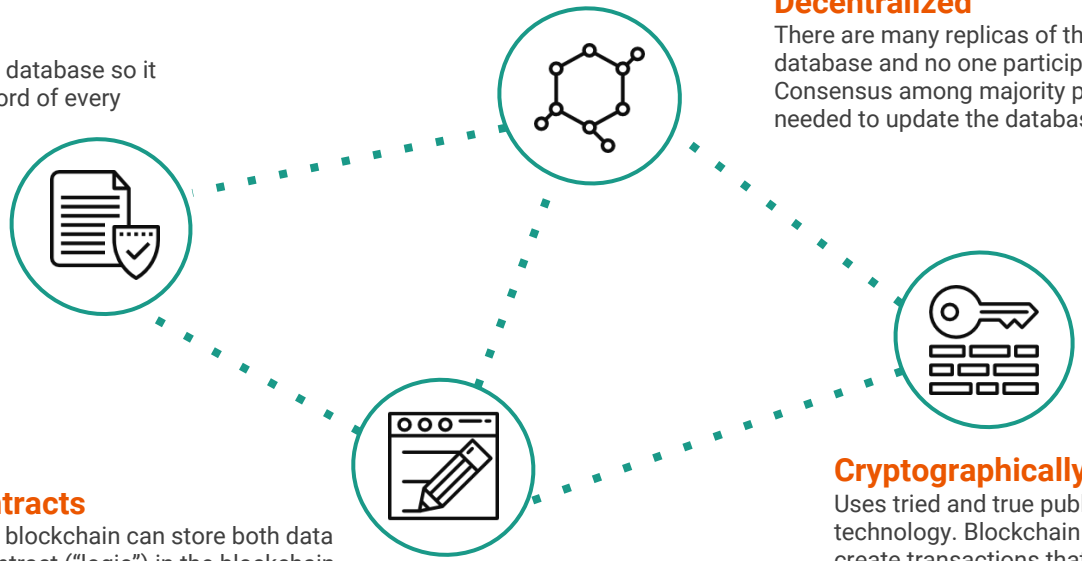
What is Ethereum?

Immutable ledger

Blockchain is a write-once database so it records an immutable record of every transaction that occurs.

Decentralized

There are many replicas of the blockchain database and no one participant can tamper it. Consensus among majority participants is needed to update the database.



Smart Contracts

The Ethereum blockchain can store both data and Smart Contract (“logic”) in the blockchain

Cryptographically Secure

Uses tried and true public/ private signature technology. Blockchain applies this technology to create transactions that are impervious to fraud and establishes a shared truth.

Evolution of blockchain protocols

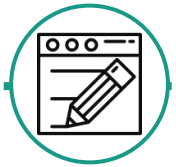
From digital cash to smart contract, blockchain technology has evolved to support a wide range of industry applications.

Bitcoin

Store and transact value (money)

Crypto-assets

Represent and transact other assets (physical or digital)



Smart contract

Describe and execute complex business logic

Different blockchain infrastructures

Depending on the use-case, the blockchain infrastructure may be configured as public, consortium, or private.

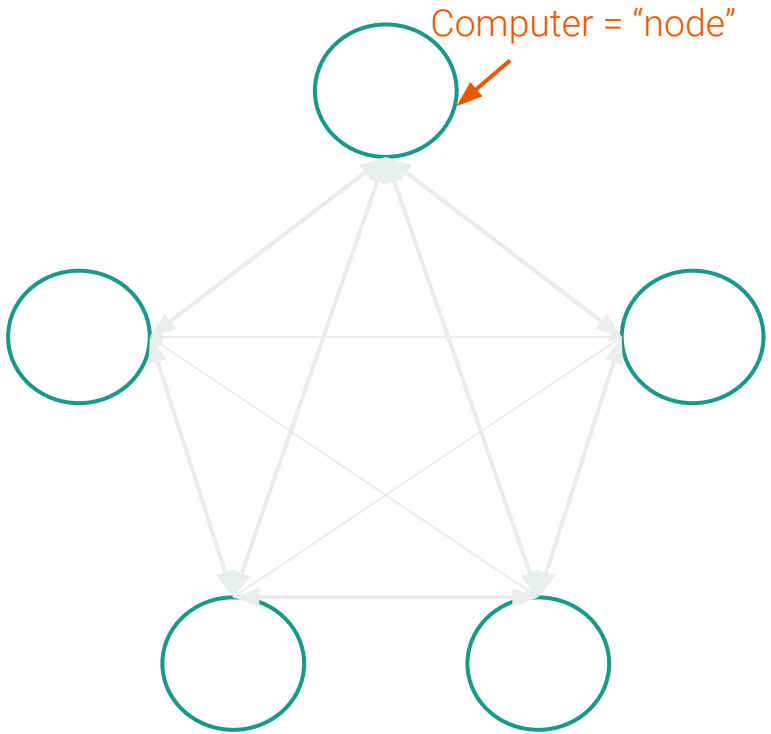
PUBLIC	• Allows anyone to join as a trust-less participant • Transaction processors must invest financially to prevent fraud and spam (e.g. proof-of-work, proof-of-stake) • Costs “crypto fuel” to process transactions and smart contracts (e.g. ether, bitcoin) • Examples include the public Ethereum and Bitcoin networks
CONSORTIUM	• Consortium blockchains are also known as shared permissioned blockchains • Only verified participants are allowed to participate • Can reduce costs and achieve higher transaction throughput compared to public networks
PRIVATE	• Private blockchains are also known as permissioned blockchains or sandboxes • Designed for rapid application development, instant deployment, and single-enterprise deployment solutions • Best suited for prototyping and development needs for learning

How does it work?

Core components

You need a lot of computers talking to each other

1. Transactions can be submitted to any node.
2. The nodes send any transactions they receive to all the nodes they are connected to.
3. Those nodes send the transactions on to the nodes they are connected to.
4. Eventually all the nodes get a copy of the transaction
5. At this stage the transaction is not yet processed.
6. The transactions get put into a batch for processing (generally called a “block” of transactions).
7. Each node processes the same transactions in the same block (that’s called consensus).

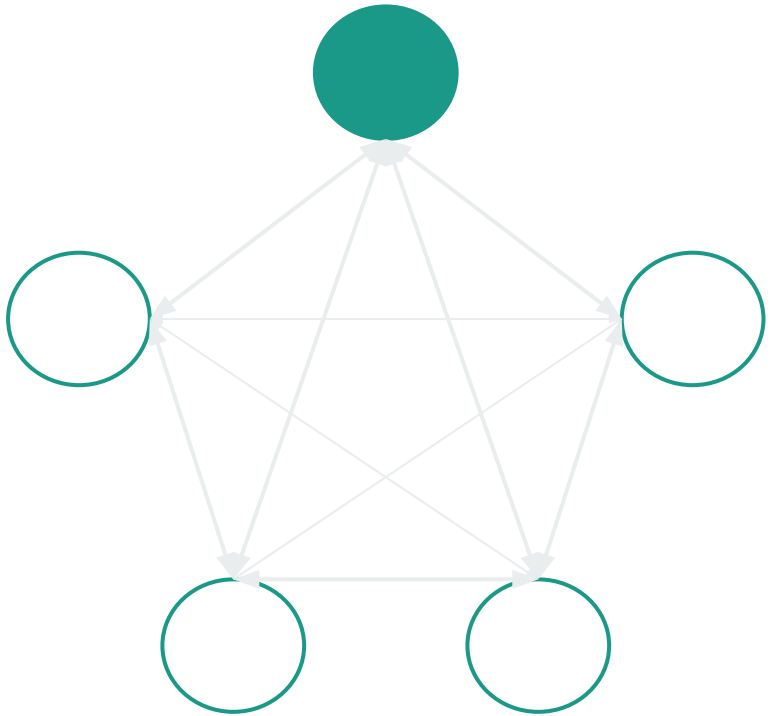


How to reach consensus

Core components

Reaching consensus

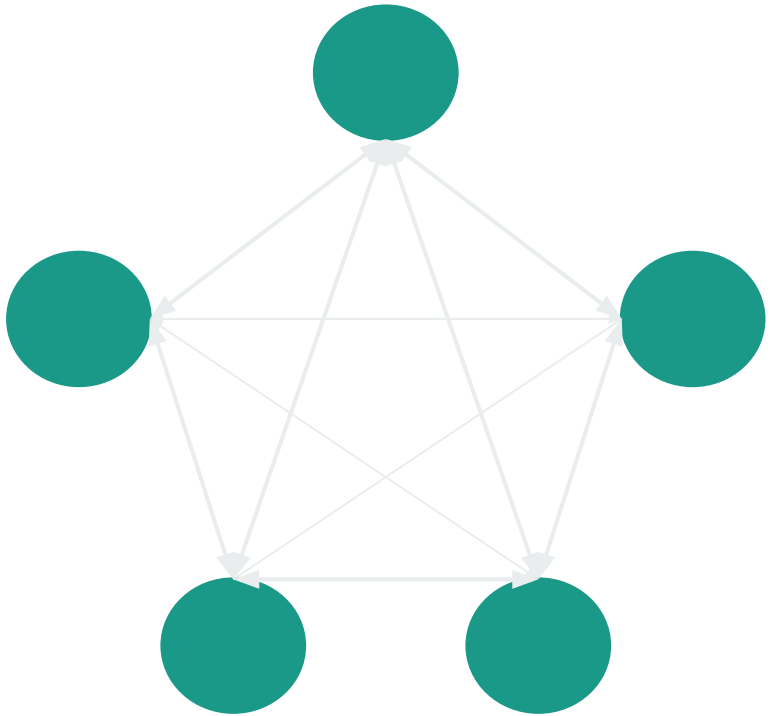
- One of the nodes has to be the leader. The leader's job is to create the next batch of transactions (block) and let every other node on the network know “these are the transactions we are processing”.
- Consensus mechanism can vary depending on type of blockchain



Core components

Transaction log

- Because every node processes the same transactions, each node has the same history as every other node.
- If any node goes down or a new node connects to the network, they just have to load of the history of all the transactions (in their blocks) and they can start participating.

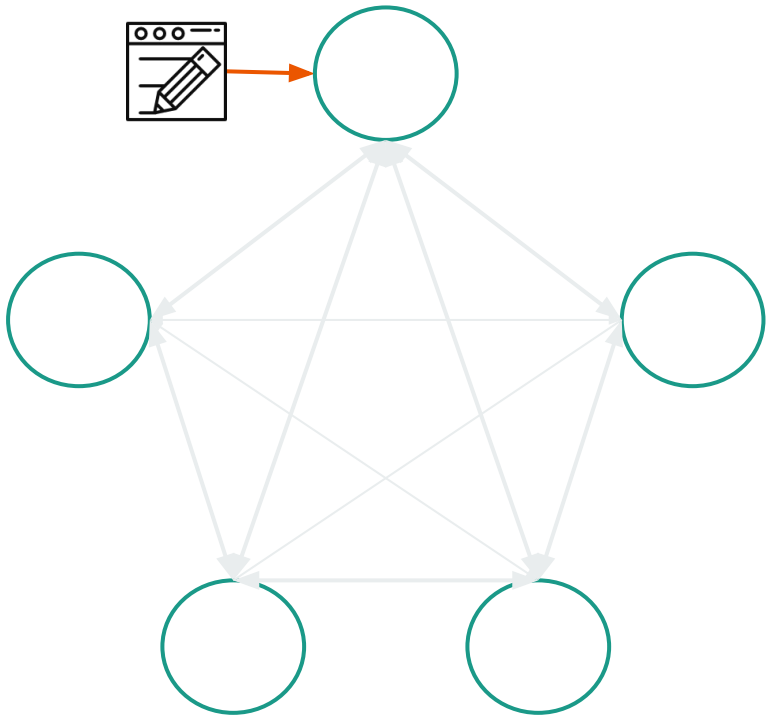


Core components

Smart Contracts

- The smart contracts in ethereum are deployed using a transaction.
- Essentially functions as an automated agreement.

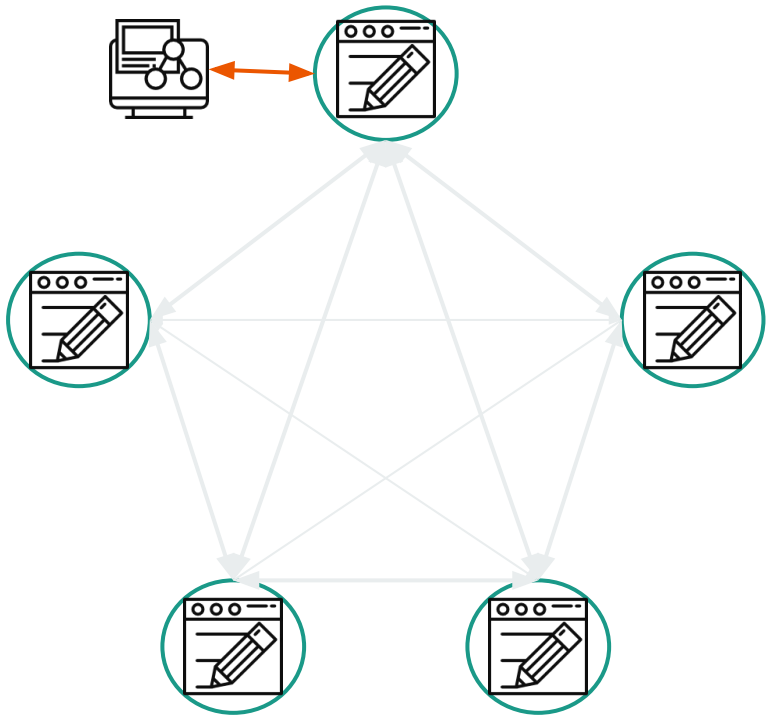
→ **“If this, then that”**



Core components

Distributed Applications (Dapps)

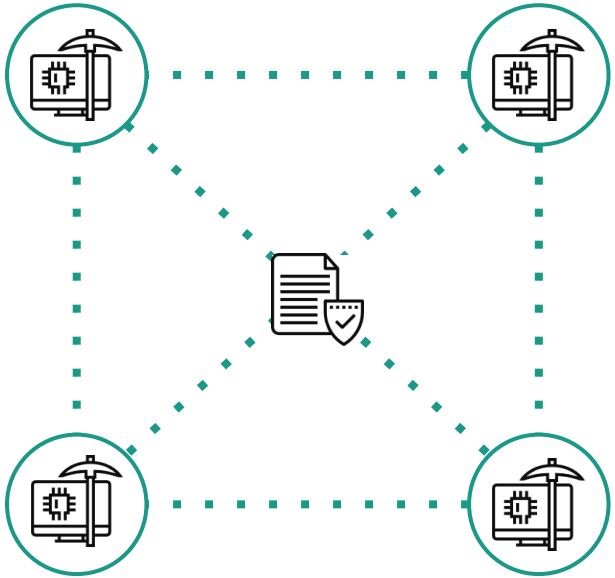
- Now that we have a smart contract deployed to all the nodes, we need to interact with it in some way. We build a Distributed application (Dapp). **Think of this as the front end a user engagees with.**
- It's just a program that can:
  - Send transactions to the node (which gets sent to the whole network)
  - Call methods on the smart contracts
  - Receive events that are raised in the smart contracts



Decentralized consensus

“Proof of Work” consensus algorithm enables consensus on the state of the network to be achieved in a network with unknown and untrusted participants.

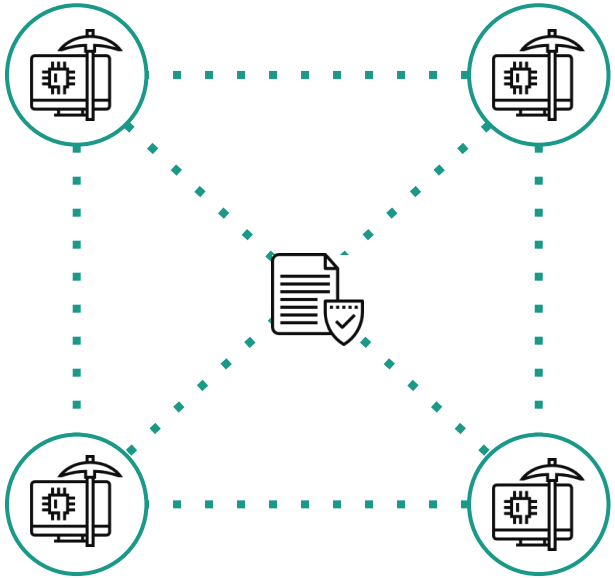
- In 2008 an individual or a group of individuals calling themselves Satoshi Nakamoto published the Bitcoin Whitepaper which described an innovative mechanism known as Proof of Work.
- Proof of Work is a computationally complex, energy and hardware intensive, puzzle with an easily verifiable proof used to verify transactions and determine an update to the distributed ledger.
- The first network participant (i.e. miner) to solve the puzzle receives a reward. Other network participants can easily verify the winner’s puzzle solution. If they agree, they then start solving the next puzzle which includes the next set of transactions.



Decentralized consensus

“Proof of Stake” consensus algorithm offers a less resource-intensive model for validating transactions.

- Introduced with Peercoin in 2012, Proof of Stake offers an alternative to Proof of Work. Stakeholders validate new blocks by utilizing their share of coins on the network, with some controls to prevent monopoly power.
- Various weighting mechanisms are used to determine an update to the distributed ledger.
    - Eg - A user would need to own more than 51% of the coins to attack the network of transactions.



CONSENSYS

Security

Immutability and security

Blockchain technology relies upon well established cryptography primitives such as hashing, digital signatures, and public/private keys.

Hashing functions

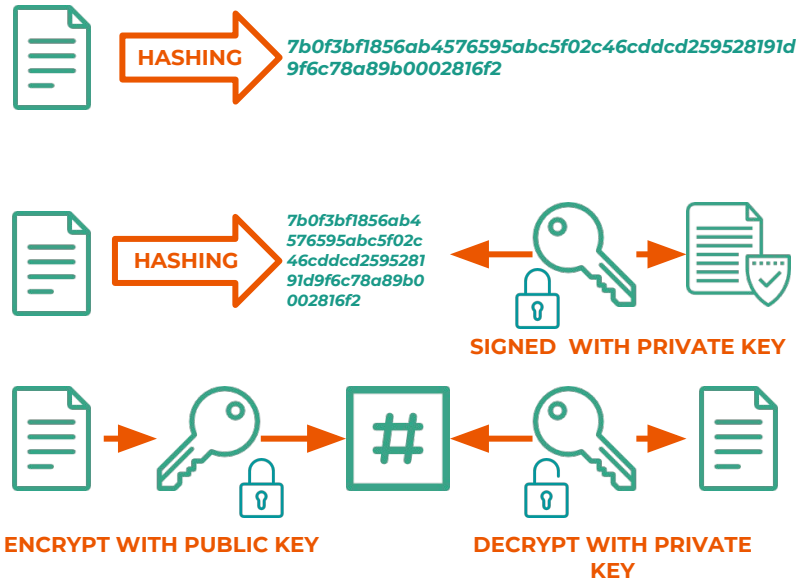
A one way transform of data into a unique, fixed length digest that cannot be reversed to produce inputs

Digital signatures

A mathematical technique used to validate the authenticity, integrity and originator of a message

Public-key cryptography

Enables encryption with a public key that can only be decrypted with a secret, private key and vice versa



Tokens & Cryptoeconomics

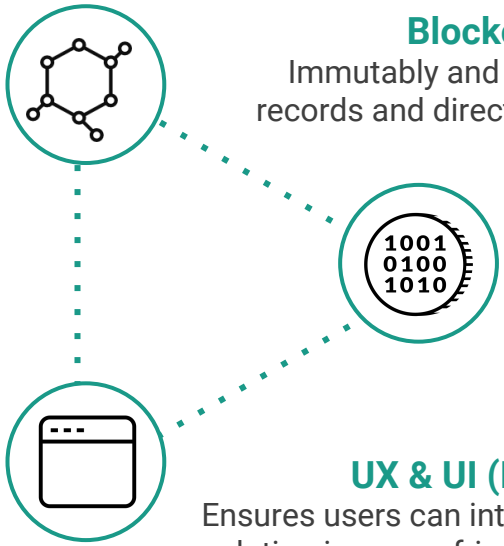
Utility tokens only

Don’t force a token into the system. Focus on solving the problem at hand.

Defining Features of a Utility Token

Passes the Howey Test	• The use and reason for the token must not fall under the scope of the 1934 Security Exchange Act
Unique	• The token should not be interchangeable with existing ones
Has utility	• Membership and/or stake • Voting rights • Payment • Access to services
Essential to the system	• Any other version of the project would not work without a token

Key System Components



Blockchain
Immutably and autonomously records and directing transactions

Utility token
Provides an incentive to use and maintain governance of the cryptosystem

UX & UI (DApp)
Ensures users can interact with the solution in a user-friendly interface

How can it be used?

How to determine if blockchain is necessary

An exceptional blockchain use case is **always** faster, cheaper, and more reliable

Obscurity
The current process has no transparency and fragmented systems for keeping records

Inefficiency
The current process needs middlemen that increase the overall cost of the services being rendered

Low-trust
The actors transacting between each other rely on *innate trust* or a suspicious third-party

Poor Coordination
The actors' actions are uncoordinated and result in a suboptimal outcome for all

Obscurity: demanding transparent processes

Any use case where a transactional settlement record is needed to provide an immutable proof of the solution's overlying transactions—whether that "transaction" is storing data, sending money, or shipping something.

There must be **a demand for transparency and streamlined processes** so that a blockchain solution is always quicker and more cost-effective than the one used in the current state.

[Example]

The legacy system of healthcare is much fragmented with critical information scattered across multiple systems and facilities, often unavailable when it is most needed, costing money and even lives. Blockchain gives promise to an integrated healthcare system that significantly streamlines processes, cuts down waiting times and costs, while improving patients' care experience.

Inefficiency: getting rid of middlemen

Any use case that **requires middlemen and intermediaries** in the process to provide scalable solutions.

Traditional Model

Blockchain Model

[Example]

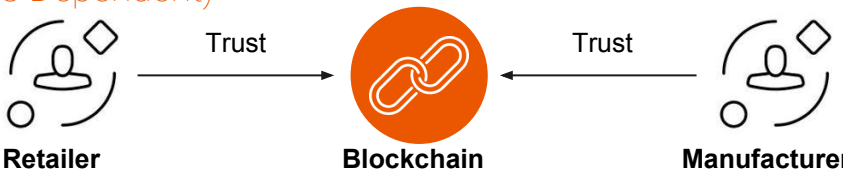
Distributed solar generation will soon become the most cost-effective means of electrical generation. Higher solar and battery penetration, coupled with a system of smart grids and smart “metering” will lead to more efficient markets and a more robust grid infrastructure, fundamentally altering the way we produce and consume energy.

Low-trust: need for a ‘trustless’ environment

Any use case where a **low amount of trust** exist between parties or a **third-party information guardian** is needed to mitigate counterparty risks.

Traditional Model
(Innate Trust Dependent)

Blockchain Model
(Trustless Dependent)

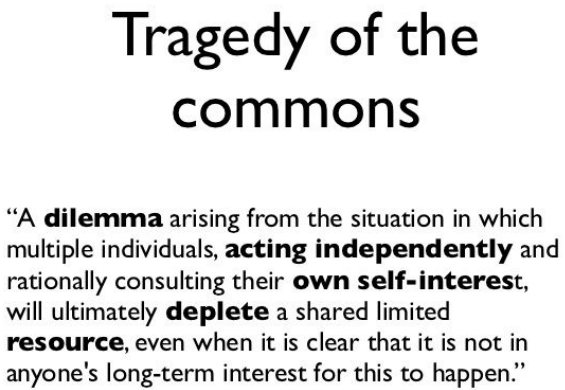


[Example]

Representative democracy has been under fire these days with mounting mistrust between people and the government. Historically impossible to achieve, liquid democracy now emerges as an alternative form of governance where voters can fluidly delegate votes based on each issue being voted, instead of delegating all votes to a single representative. Ethereum is an ideal platform to implement liquid democracy.

Poor coordination: reaching a better state

Any use case that will lead to **a worse outcome for all** if the actions of the involved stakeholders are poorly coordinated.



http://en.wikipedia.org/wiki/Tragedy_of_the_commons

[Example]

Climate change. It takes the coordinated effort of all on this planet to prevent us from reaching the irreversible tipping point of climate change. Various carbon trading, tree-planting, fish-tracking and recycling systems are being built on the blockchain to incentivize individual contributions to reduce carbon footprints.

Blockchain Opportunities

Blockchain enablers

Key patterns enabling blockchain-based disruption

	Description	Area of application	Example
Asset tokenization	Tokenization of physical and digital assets for trading and settlement with multiple parties on the blockchain	Real-world assets that are bound by the rules of traditional trust and distribution mechanisms	Loyalty programs: Unlocks the power of loyalty points by providing secondary markets & instant reconciliation
Custody & escrow	Trustless transaction capability with assets in escrow managed by a smart contract	Transactions involving intermediary agents who provides trust as a service between two or more trading parties	Betting/Gambling: Funds used to stake a bet are held in escrow on the smart contract until winner is decided
Provenance & tracking	Single source of truth that conveys information about the asset across its journey from one custodian to the next	Traditional supply chains that use conventional methods to track the custody of an asset	Supply chain: Asset tracking processes reimagined on blockchain for tracking of tokenized physical assets
Accounting & reconciliations	New accounting paradigm where every debit and credit is recorded with an immutable entry on the blockchain	Traditional double-entry bookkeeping systems with disparate sources and uses of data in need of reconciliation	Trading books: Automated reconciliation of trading positions among financial institutions

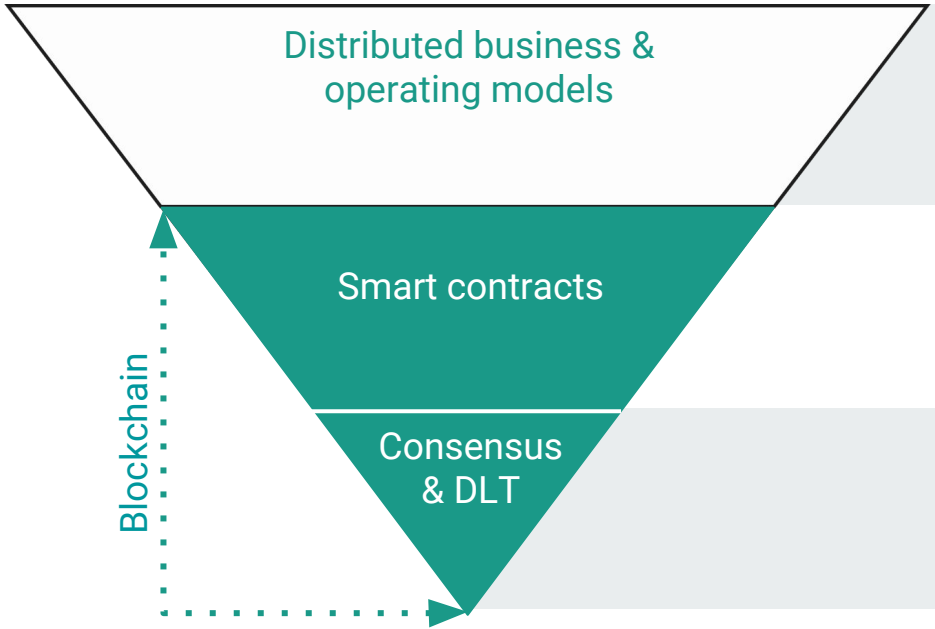
Blockchain enablers

Key patterns enabling blockchain-based disruption

	Description	Area of application	Example
Digital identity	Consolidation and management of individual / entity ID with attributes stored and verified on a blockchain	Multiple sources of identification with disparate data points and potential risk of duplication	Medical records: Holistic records management enables patient profiling and effective treatment
Real-time transactions	Atomic transactions ensure that 'the trade is the settlement' thus bringing the lag time to negligible minimum	Conventional systems where there is significant intermediation and time lag before final settlement	Capital markets: Instant settlement of trades removes reconciliations and improved capital efficiency
Micro payments & funding	Transactions of minimum value that enable P2P payments, M2M payments and capital raising	Traditional commercial transactions where small sale amount are made anti-economical by payment fees	Publishing: Distribution of single pieces of content charging a micro fee rather than subscription
Automated execution	Full automation of contract lifecycle form issuance, transfers, revisions and up to final execution	Conventional contract and security issuance process that depends on multiple intermediaries	Property sale: Title update and execution through property development and sales process

Distributed business and operating models

Blockchain capabilities enable the transition to innovative and more efficient business and operating models that support the creation of green-field products and services



- Full provenance and transparency
- Disintermediation and true P2P
- Real-time transactions
- Inclusion and participation
- Green-field products and services

- Registered on the distributed ledger
- Programmable business logic
- Deterministic and self-executing
- Validated and executed through consensus
- Automatically update the ledger

- Immutable, tamper-resistant and transparent
- Decentralized, distributed and replicated
- Consensus mechanism
- Transaction validation and execution
- P2P networking and messaging

Blockchain & Social Impact

What does it mean for social impact?

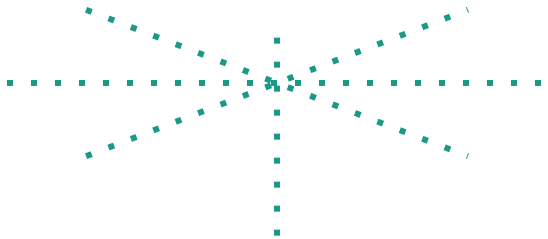
By leapfrogging centralized systems, blockchain can reshuffle the current social and political landscape.

Alternate Source of Funding
Increases donation and crowdfunding for community projects. Incentivizes doing good in gamified cryptosystems.

Self-sovereign Identity
A persistent, private and portable digital identity that accumulates reputation without the need of a centralized authority.

Economy for the Unbanked
Brings commerce and finance to the billions of unbanked in the borderless and frictionless network..

Peer-to-Peer Marketplaces
Enables peer-to-peer trading of energy, carbon, water, wood and many other precious resources.



Transparent Supply Chain
Cuts out middlemen, eases administrative load, and traces the movements of funds, goods and assets.

Decentralized Governance
Inspires new governance models through prediction markets, quadratic voting and liquid democracy.

Tamper-proof records
Stores rights, titles and records safely in a corruption- and fraud-proof database.

Effective Philanthropy
Coordinates efforts of charities and philanthropy organizations to track impact goals, audit funds, and pursue more effective aid.

Impact Areas

- Sex Trafficking Prevention
- International Money Transfers (Remittances, Donations)
- Encrypted Communication
- Uncensored Internet Access
- Law Enforcement Accountability
- Voter Transparency
- Donation Transparency
- Resource Allocation (Homeless, Refugees)
- Self-Sovereign Identity in low-infrastructure areas
- Self-Sovereign finance
- Public Health
  - Sexual Assault/Rape Kits
  - Electronic Health Records
  - Monitoring & Evaluation

Contact Us
socialimpact@consensys.net

For More Information
www. blockchainforsocialimpact.com

@ethereum4impact