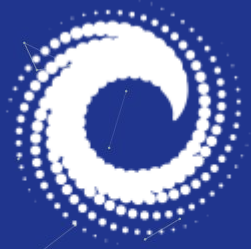
ethereum



CONSENSYS

Blockchain 101

FLOAT Information Session
Jan 23, 2017

Blockchain 101

Jess Marshall

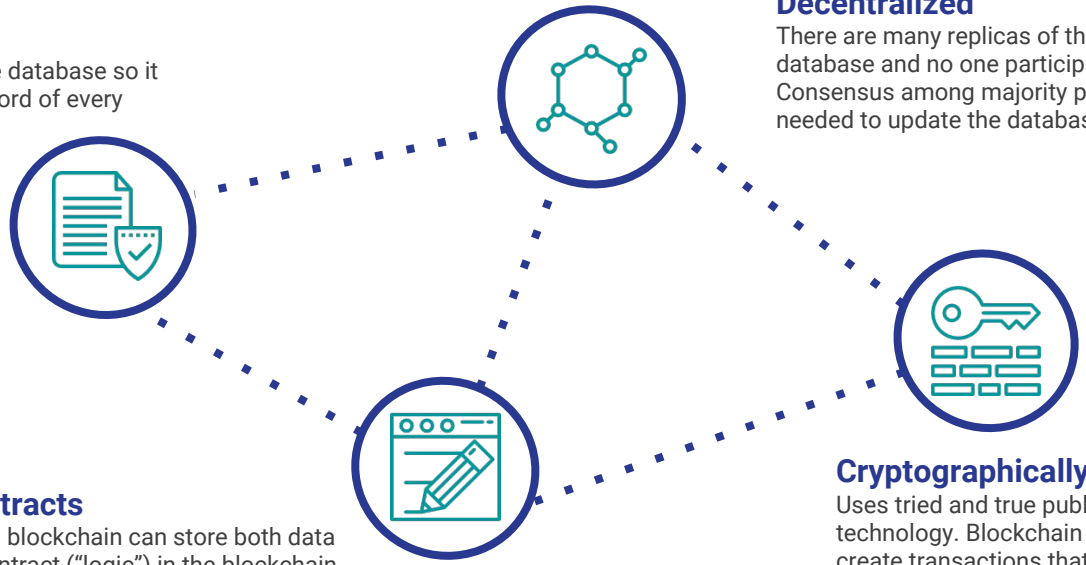
Joseph Bender

What is blockchain

Originally conceived as the underlying protocol of Bitcoin, blockchain technology has since evolved to support a number of applications with the introduction of “smart contracts” in 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

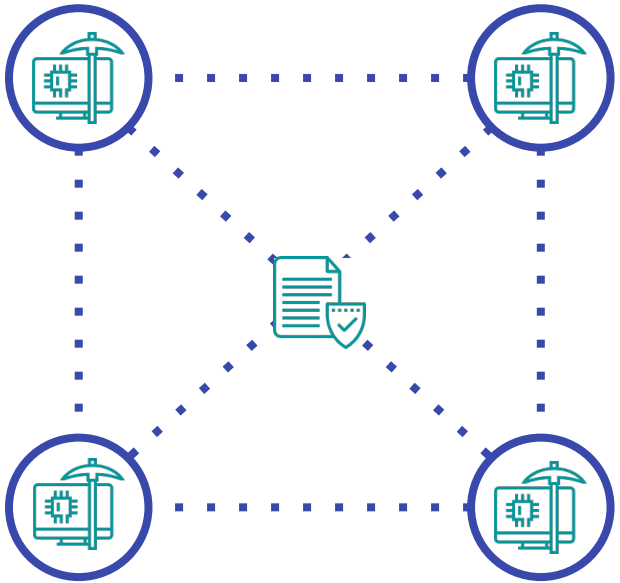
Uses tried and true public/ private signature technology. Blockchain applies this technology to create transactions that are impervious to fraud and establishes a shared truth.

Decentralized consensus

Blockchain adds a way of achieving decentralized consensus to cryptographic security

“Proof of Work” consensus algorithm

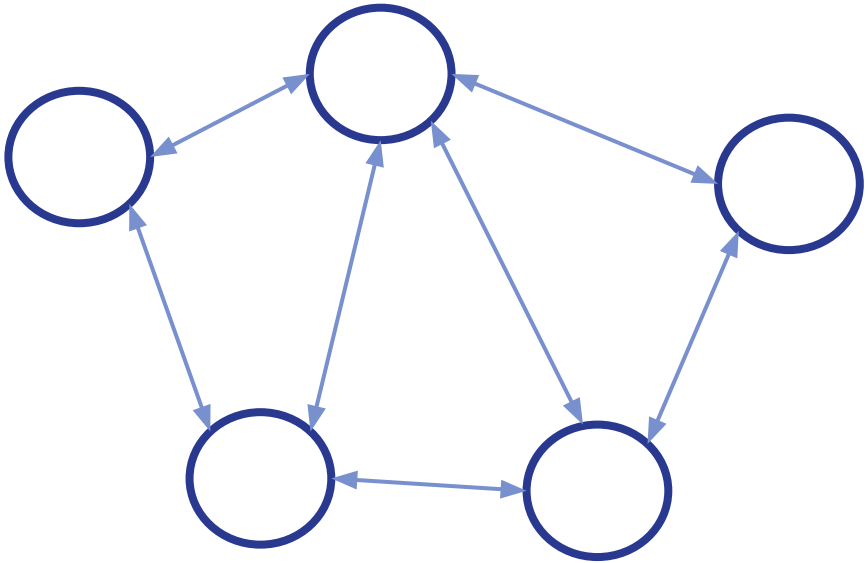
- In 2008 an individual or a group of individuals calling themselves Satoshi Nakamoto published the Bitcoin Whitepaper which described an innovative mechanism known as Proof of Work
- Proof of Work is a computationally complex, energy and hardware intensive, puzzle with an easily verifiable proof used 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.
- Proof of Work enables consensus on the state of the network to be achieved without a central, controlling authority and without trust between the network participants



How does it work

You need a lot of computers talking to each other

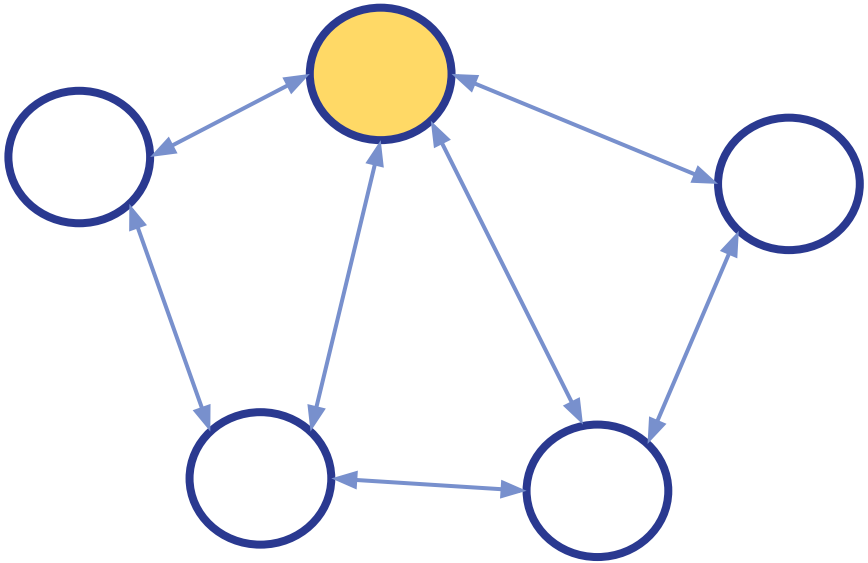
- The are called nodes on the network
- Transactions can be submitted to any node
- The nodes send any transactions they receive to all the nodes they are connected to
- Those node send the transactions on to the nodes they are connected to
- Eventually all the nodes get a copy of the transaction
- At this stage the transaction is not yet processed
- The transactions get put into a batch for processing (generally called a block of transactions)
- Each node processes the same transactions in the same block (that's called consensus)
- How we reach consensus is covered in the next slide



How does it work

Reaching consensus

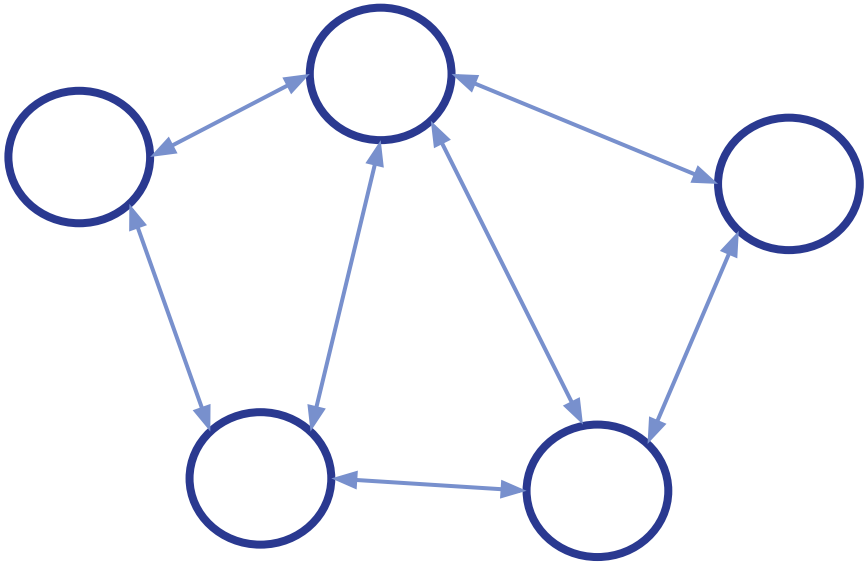
- One of the nodes has to be the leader
- The leader's job is to create the next batch of transactions (block) and let every other node on the network know “These are the transactions we are processing”
- How is the leader chosen? - It depends
- Many public blockchains use Proof of Work (Meritocracy). You have the right to be leader because you have worked hard. It’s a good system. So for every block everyone works hard for the right to lead that round.
- Proof of Stake (Capitalism). You have the right to be leader because you have invested a lot of money into the network
- RAFT (Democracy). Each leader is elected by the other nodes and has a term of office. His leadership terminates when his term is over or he dies. Then the next leader is elected
- Round Robin (Oprah Winfrey leadership). Everyone gets a turn to be leader
- Proof of Authority (Monarchy)
- Single leader for life (Dictatorship)



How does it work

Transaction log

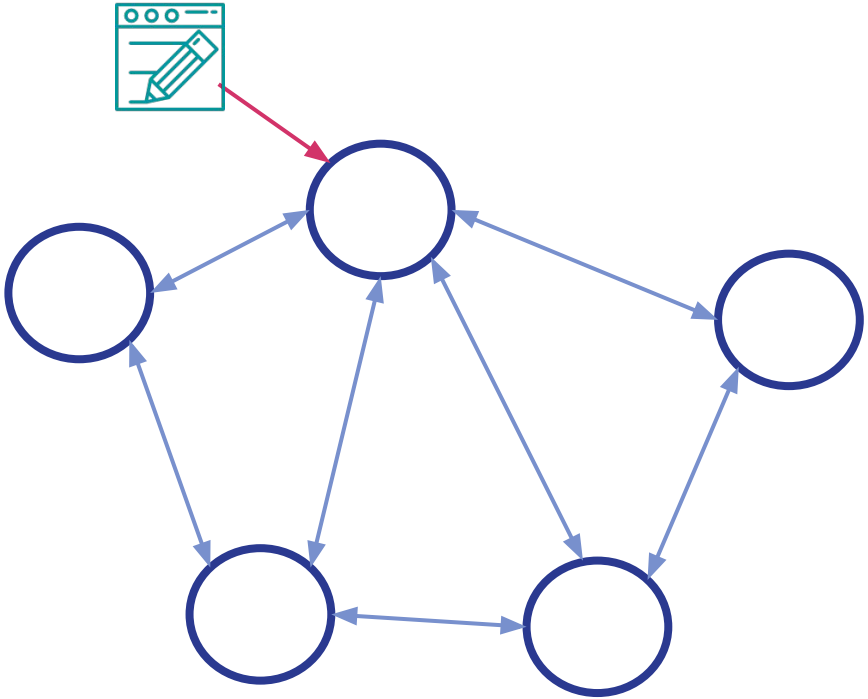
- Because every node processes the same transactions, each node has the same history as every other node
- We can therefore treat the entire network as a single computer
- If any node goes down or a new node connects to the network, they just have to load of the history of all the transactions (in their blocks) and they can start participating
- In the ethereum blockchain, we call this the Ethereum Virtual Machine (EVM)



How does it work

Smart Contracts

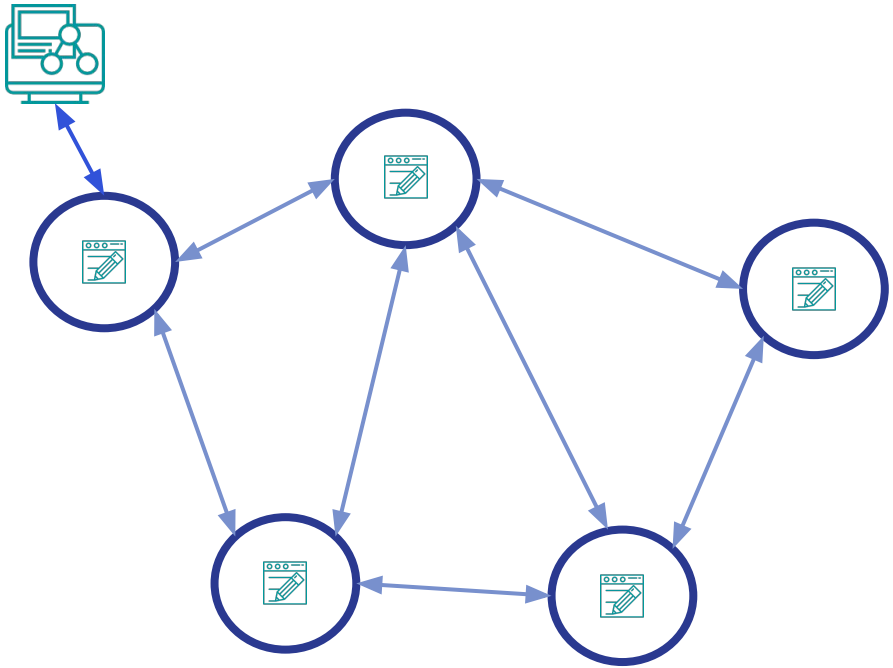
- The smart contracts in ethereum are deployed using a transaction.
- Someone writes the smart contract code, tests it and then wants to deploy it. They put it into a special contract that says “deploy this smart contract”. All the nodes run that transaction and the contract code is deployed onto all the nodes
- Anyone who has permission to can now use that contract in a subsequent transaction



How does it work

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).
- The Dapp can run on any node
- 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
- It could be a website, a mobile application, an integration component into a banking system etc, etc
- Every transaction it sends gets propagated to the whole network, so all the nodes stay in synch
- In ethereum is uses a library called web3 to communicate to the node
- Java: web3j
- Javascript: web3js
- C#: Nethereum



Immutability and security

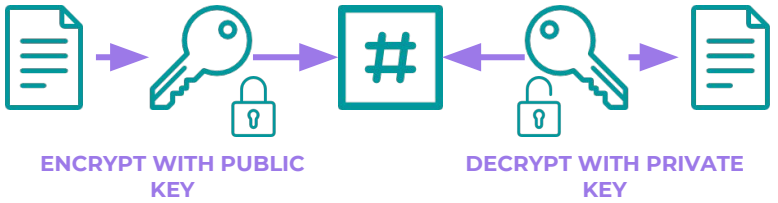
Blockchain technology relies upon well established cryptography

Hashing functions

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

Public-key cryptography

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



Digital signatures

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

Bitcoin, a blockchain MVP (Minimum Viable Product)

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

Bitcoin and crypto-currencies

- Resilient and censorship resistant digital currency based on blockchain protocols
- Issued by a decentralized network/protocol, not a central authority
- No intrinsic value but determined by adoption and acceptance in the “real” economy

Blockchain the technology

- Technology protocol that allows a network of computers to store data, execute transactions and maintain a distributed ledger of all the transactions
- Replaces trust in central authorities with a decentralized consensus mechanism among untrusted network participants that resolves “Double Spending Problem”

Evolution of blockchain protocols

From crypto-currencies to sophisticated business logics enabled by “smart contracts”

Bitcoin

Store and transact value (money)

Crypto-assets

Represent and transact other assets (physical or digital)

Smart contracts

Describe and execute complex business logics

Smart contracts

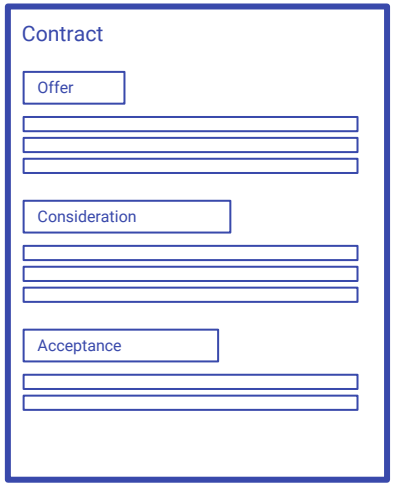
Ethereum was the previous blockchain to introduce the notion of self-executing smart contracts

Smart contracts, Dapps and DAOs

Smart contracts are code that is stored on the blockchain and self-executes using the trust and security of the blockchain network.

They provide an application logic that runs in a distributed fashion on the Ethereum blockchain and operates using the power of the Turing-complete Ethereum Virtual Machine (EVM), allowing for enhanced or completely redesign business processes and services.

Collections of integrated smart contracts and traditional web technologies realize a new breed of decentralized applications (dapps) and a create a vision for decentralized autonomous organizations (DAOs)




```
<smart contract>


contract OfferContract {
        uint public acceptance_rate = 50;
        mapping (address => uint)
tradeAccount;
        mapping (address => uint)
coinAccount;
        address public owner;

        function Consideration() {
                owner = msg.sender;
        }
        modifier onlyOwner {
        if (msg.sender != owner) sign;
        }
        function setAccept(uint rate)
onlyOwner {
                acceptance_rate = rate;
        }
</smart contract>
```

What is Ethereum

Ethereum was built to extend the blockchain concept with the ability to also run veridical business logic (Smart Contracts) using a decentralised network, creating a globally distributed World Computer

Ethereum value proposition

- Builds on the Blockchain concepts of Cryptographic Security, Decentralisation and Immutability
- Adds in the capability to run decentralised Smart Contracts, a Turing complete programming language running in the Ethereum Virtual Machine
- Supports private permissioning and additional privacy features while maintaining interoperability with the public chain
- Under active development by the Ethereum Foundation, the platform continues to grow in terms of both Enterprise adoption and also functionality
- With the establishment of the Enterprise Ethereum Alliance, Ethereum is becoming the de-facto blockchain technology of choice for enterprise projects

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

Vitalik Buterin, Ethereum Inventor

The Ethereum advantage

Ethereum is the only blockchain infrastructure with a built-in Turing-complete virtual machine within the full security of the blockchain protocol

Formally specified security and smart contract capabilities

Vendor-neutral

Public – private blockchains compatibility

Private, permissioned blockchains for enterprise and government use cases

Rapidly growing community encompassing 30,000+ developers

Multi-billion dollars of value protected on the public network

Enterprise Ethereum Alliance (EEA) is growing faster than all other blockchain consortia

The dominant platform for the 'token ecosystem'

Technical and operational challenges

As with any emerging technology, limitations to the adoption of blockchain still exist but a talented and enthusiastic community is actively working to overcome such obstacles

Scalability
Proof of Work is not sustainable for higher volume of transactions

Latency
Current transaction speed and latency represent a limit to adoption for some use cases

Privacy
Pseudonymity doesn't satisfy the privacy requirements for many use cases

Integration
Limited interoperability and integration between different protocols and legacy systems

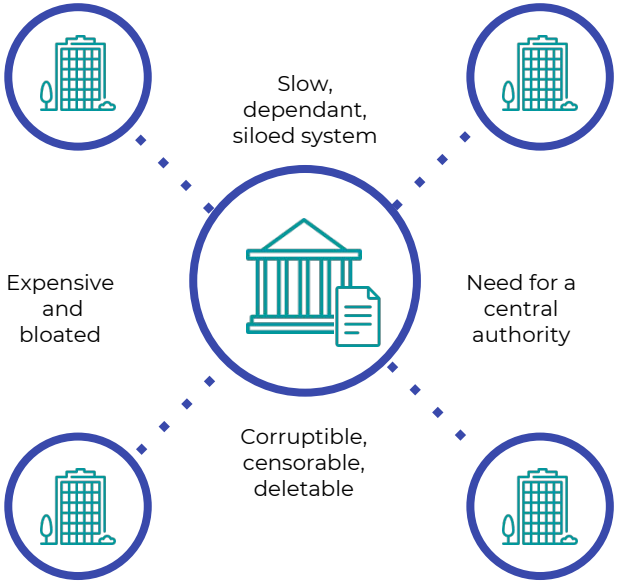
operating Model
Operation of new blockchain utilities and consortia requires new governance models

Regulations
The regulatory framework is still totally uncertain, limiting institutional adoption

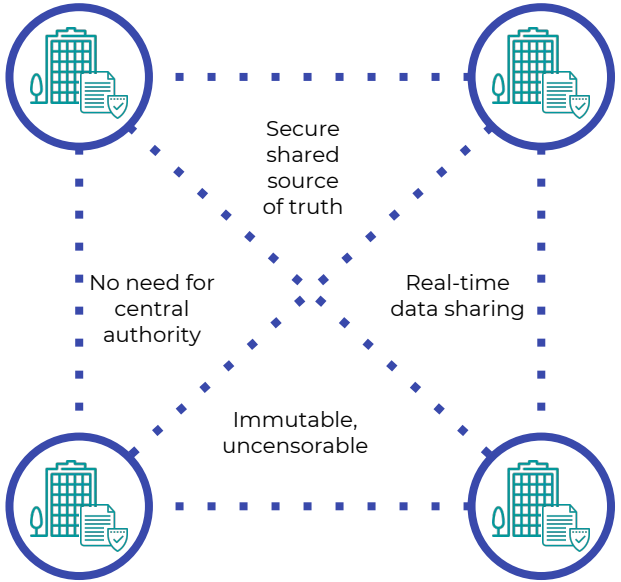
Distributed and disintermediated models

A move toward distribution and disintermediation is a move toward scalability, resilience, efficiency, cost reduction, stability and reliability

Centralized Systems



Distributed Ledger



Why blockchain?

Blockchain offers a number of benefits over traditional and legacy systems

Reduce costs

Removes cost of intermediaries and smart contract automation reduces manual processing, re-work, and processing errors

Reduce risk

No single point of failure or attack and non-repudiability reduces risk of fraud thanks to immutable audit trail and provenance

Increase revenues

Creation of new products and services and value capture from demonstrating provable provenance of commodity products

Improve speed and experience

Simplifies value chain by removing intermediaries and allows T+0 settlement

Social and political implications

Blockchain developments in the private and public sector have far reaching implications on society

Stronger cooperative economy

Disintermediate non value added activities to strengthen the participant's participation in the economy and their ability to capture value.

Social enterprise

The ability to trace transactions and set up organizations and voting mechanisms linked to reputation and identity will provide for the ability to recognize and report corruption. Immutable reputation will also incentivize best behavior.

New governance models

Ability for blockchain to organize and help in the delivery of projects through real time voting, which will have greater consequences when applied to liquid democracies, and prediction markets.

Self-sovereign identity

Individuals will control their identity which will greatly impact ability to gain access to credit, potential fluidity between geographies, and trade.

Accessible financial services

Bringing financial services to the billions of unbanked through near zero transaction fees and east of micropayments.

Art of The Possible

CONSENSYS

High potential use cases

Blockchain applications are emerging across many industries

Supply Chain

Provenance of assets become verifiable and traceable leading to the revolution of supply chains.

Governance

DAOs built on blockchains to maintain transparency and governance.

Self-sovereign identity

People and business own their own identity, with no central control, and build universal reputation.

Medical records

Personal ownership of medical records that can be used universally.

Decentralized storage

Does not require additional backups and disaster recovery. No central point of failure and control.

Creative work

Art ownership and distribution, where creators receive direct compensation for their work.

Fundraising

Initial Coin Offerings (ICOs) emerging as an alternative to venture capital.

IoT

Blockchain used as a means to connect and audit IoT, M2M value transfer.

Commodities trading

Tokenization, tracking and p2p trading of commodities, such as energy.

Art of the Possible

Blockchain enablers (1/2)

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

Art of the Possible

Blockchain enablers (2/2)

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

THANK YOU