Introduction to Blockchain

Applications in research, education, and innovation

Think Conference
May 2018

CONSENSYS

Download uPort

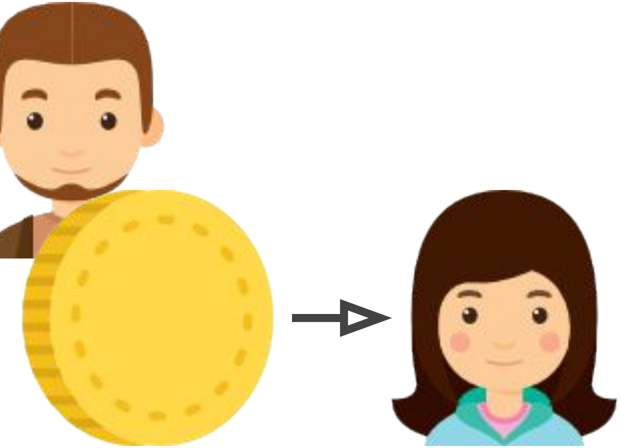
Blockchain 101

Blockchain 101

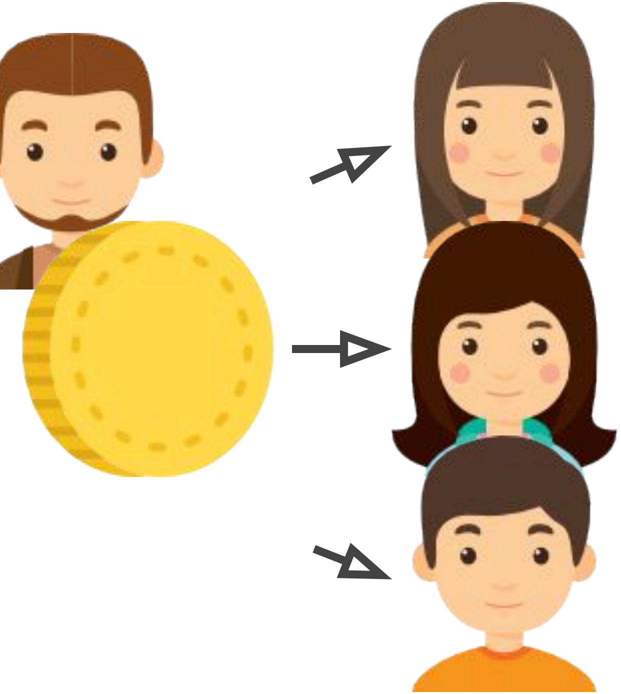
Let’s Create a Blockchain Together

Blockchain 101

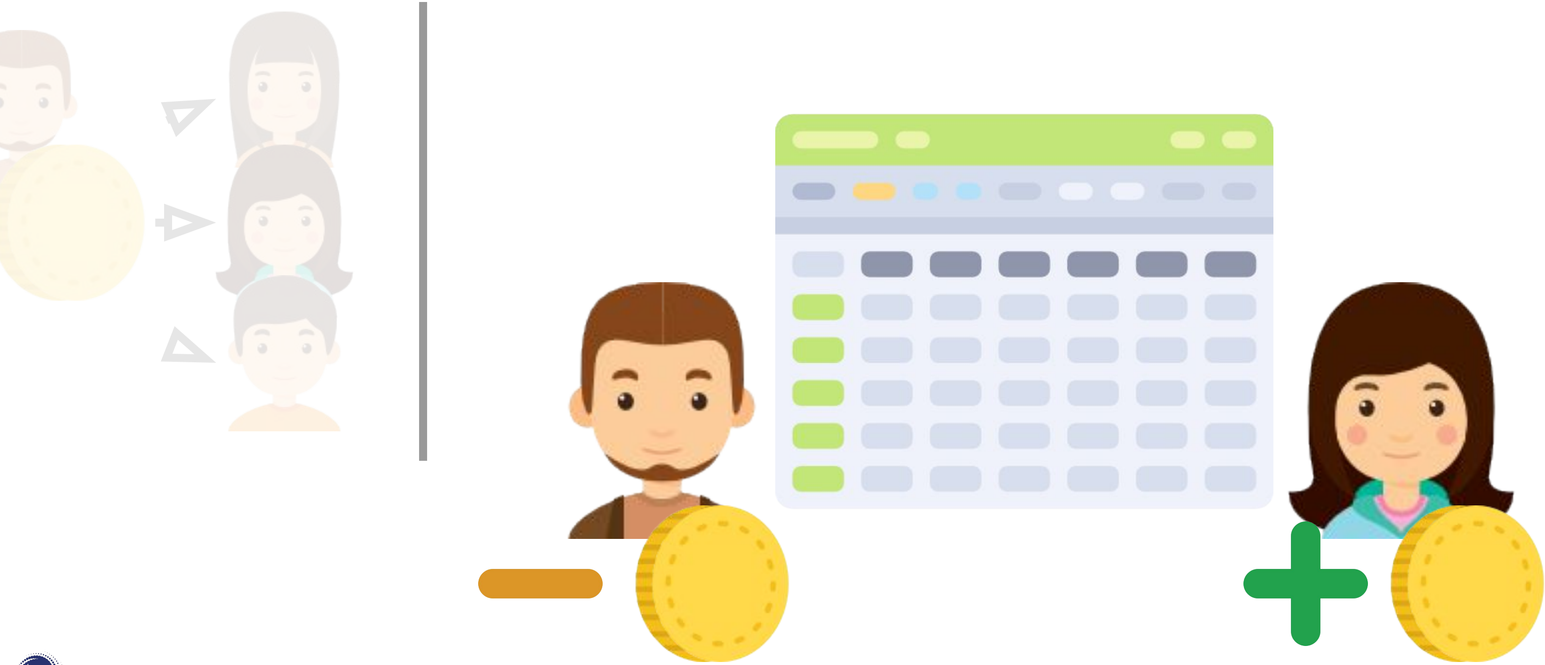
Let’s Create a Blockchain Together



Let’s Create a Blockchain Together



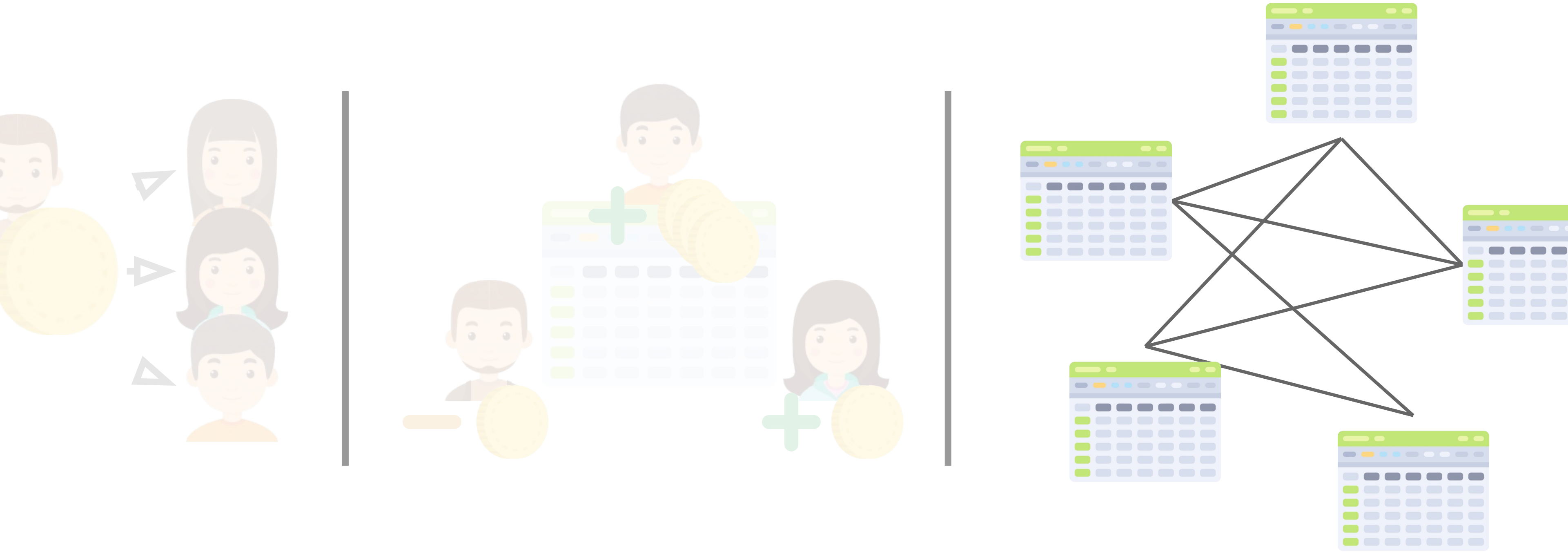
Let’s Create a Blockchain Together



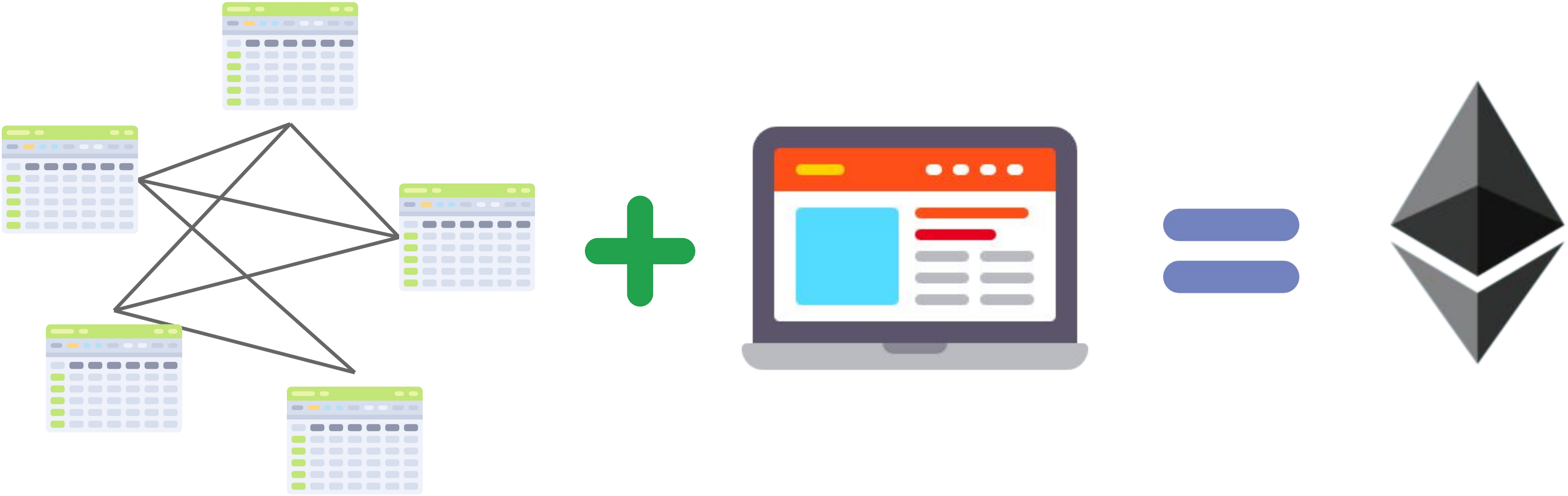
Let’s Create a Blockchain Together

Blockchain 101

Let’s Create a Blockchain Together



Let’s Create a Blockchain Together



Bitcoin, a blockchain minimum viable product

Bitcoin and cryptocurrencies

- Resilient and censorship resistant
- Issued by a decentralized network
- Value determined by supply and demand

Blockchain the technology

- Protocol that enables a network of computers to **store** data, **execute** transactions and **maintain** the integrity of a distributed ledger
- Replaces trust in central authorities
- Decentralized consensus mechanism among untrusted network participants
- Solves “Double Spending Problem”

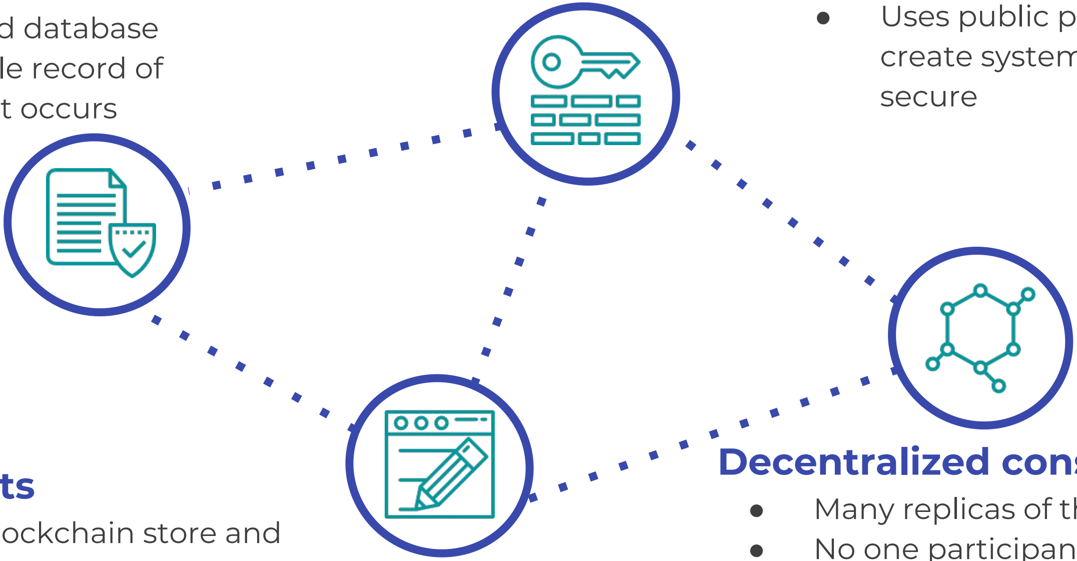
What is a blockchain?

Immutable ledger

- Write-only distributed database registering immutable record of every transaction that occurs

Cryptography

- Uses public private key infrastructure to create system that is tamper-proof and secure



Smart contracts

- Ethereum blockchain store and execute programs on the blockchain

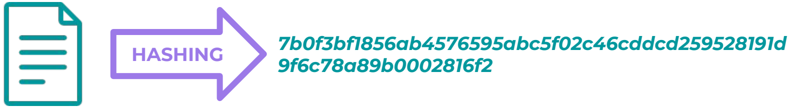
Decentralized consensus

- Many replicas of the blockchain database
- No one participant can tamper it
- Consensus among majority of participants is needed to update database.

Immutability and cryptography

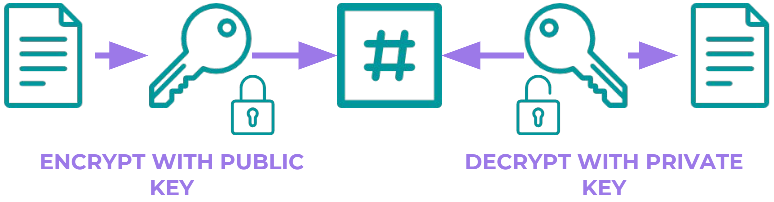
Hashing functions

One way transform of data into unique, fixed length digest that cannot be reversed to produce the original input



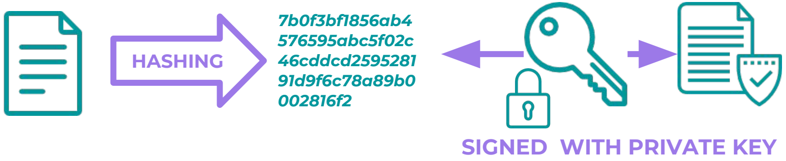
Asymmetric key cryptography

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



Digital signatures

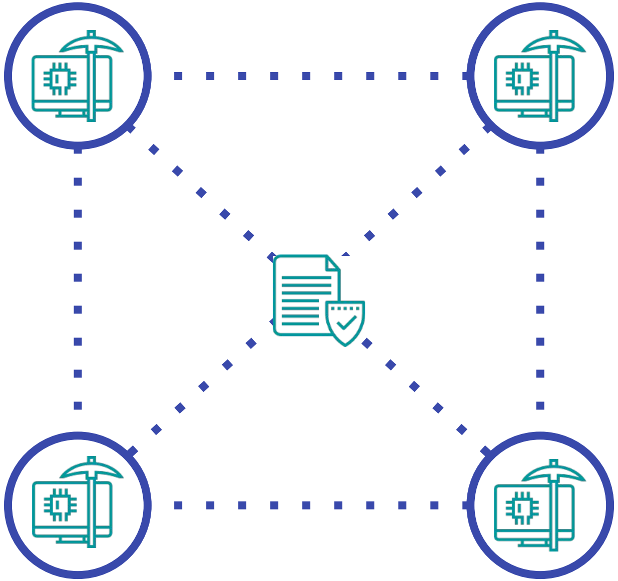
Mathematical technique used to validate authenticity, integrity and originator of message



Decentralized consensus

“Proof of Work” consensus algorithm

- In 2008 Satoshi Nakamoto published Bitcoin whitepaper describing Proof of Work
- Proof of Work enables consensus on state of network achieved without central authority and without trust between participants
- Proof of Work is computationally complex, hardware intensive puzzle used to verify transactions and determine update to ledger
- Other participants can easily verify winner’s puzzle solution
- If agreed, they then start solving next puzzle which includes next set of transactions
- First miner to solve puzzle receives reward

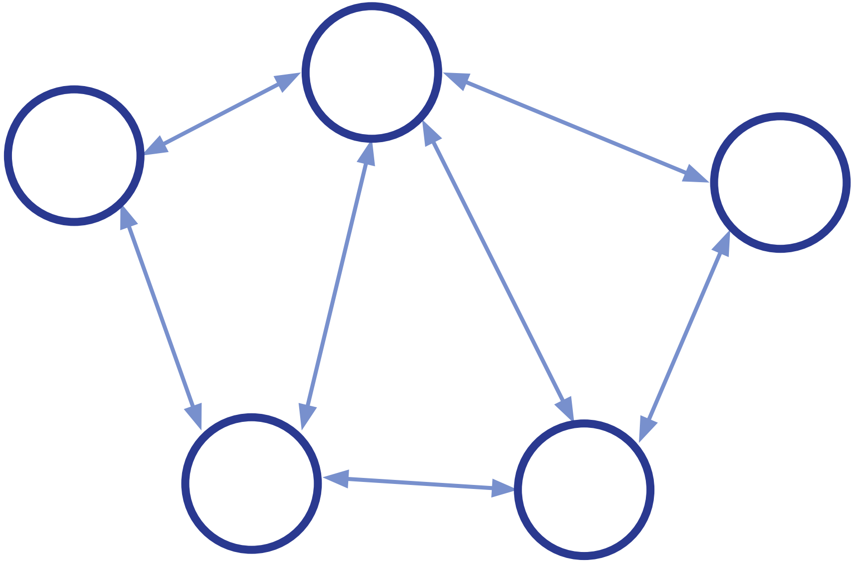


Introduction to blockchain

How does it work

You need a lot of computers talking to each other

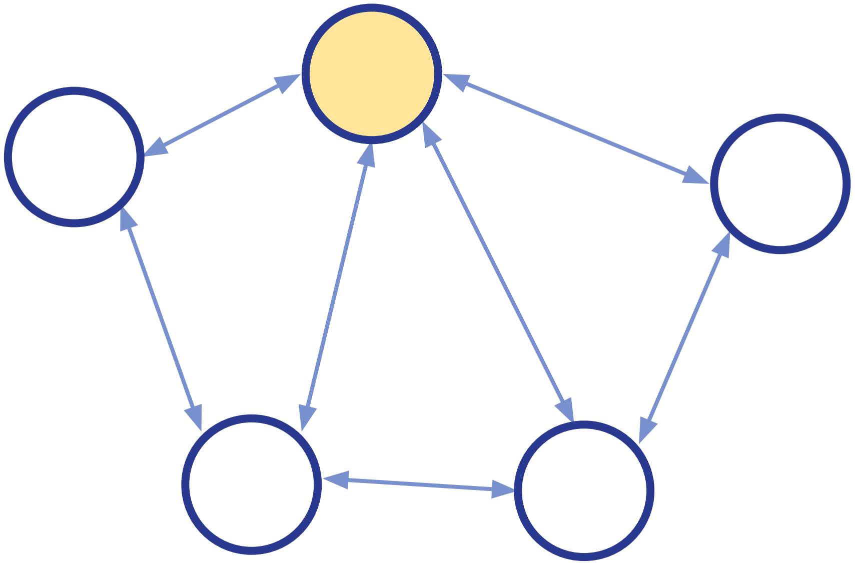
- The are called nodes on the network
- Transactions can be submitted to any node
- The nodes send any transactions they receive to all the nodes they are connected to
- Those node send the transactions on to the nodes they are connected to
- Eventually all the nodes get a copy of the transaction
- At 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

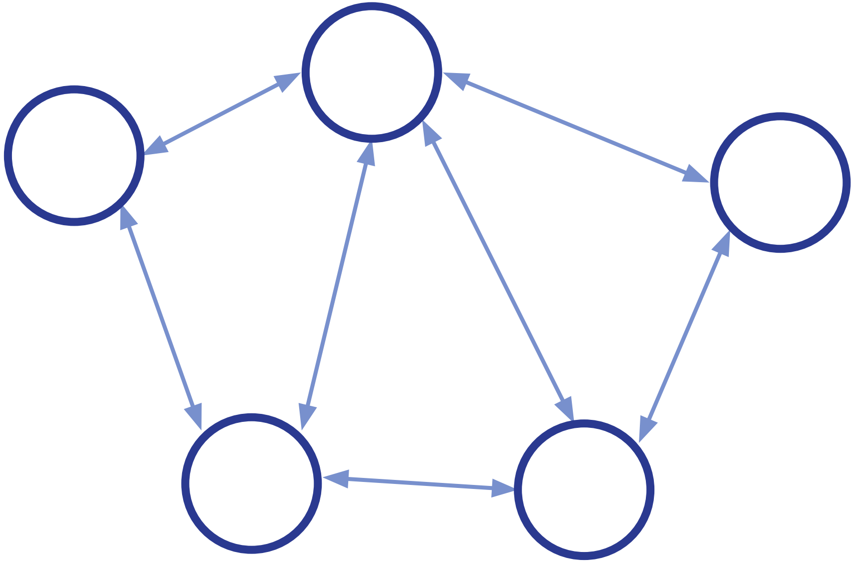
- One of the nodes has to be the leader
- The leader's job is to create the next batch of transactions (block) and let every other node on the network know “These are the transactions we are processing”
- How is the leader chosen? - It depends
- Many public blockchains use Proof of Work (Meritocracy). 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. They work hard to solve a cryptographic puzzle.
- 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 the history and they can start participating



Introduction to blockchain

Why does this work

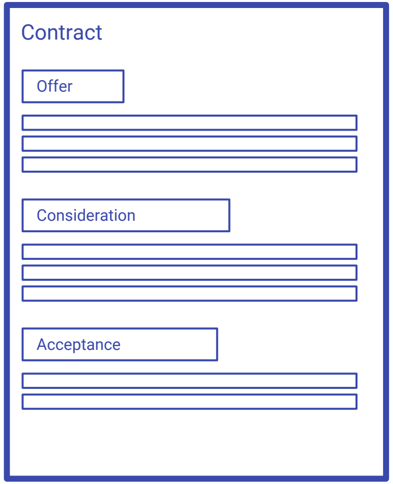
- Everyone has the same copy of the ledger (like a spreadsheet)
- To make a change to the ledger, 51% or more of the computers in the network have to agree on what to enter
- 51% computing power is equivalent to $7B+ in hardware resources for 10 mins of control
- Even if they did take control, the transactions can be traced and the value of the coins will drop if there ever was a 51% attack.
- Strong encryption embedded into every piece of the blockchain

Smart contracts

Ethereum is the first blockchain to introduce smart contracts on blockchain

Smart contracts, Dapps and DAOs

- Smart contracts are code stored on blockchain
- Applications run on Turing-complete Ethereum Virtual Machine (EVM)
- Dapp is collection of integrated smart contracts and traditional web technologies
- Decentralized autonomous organizations (DAOs)

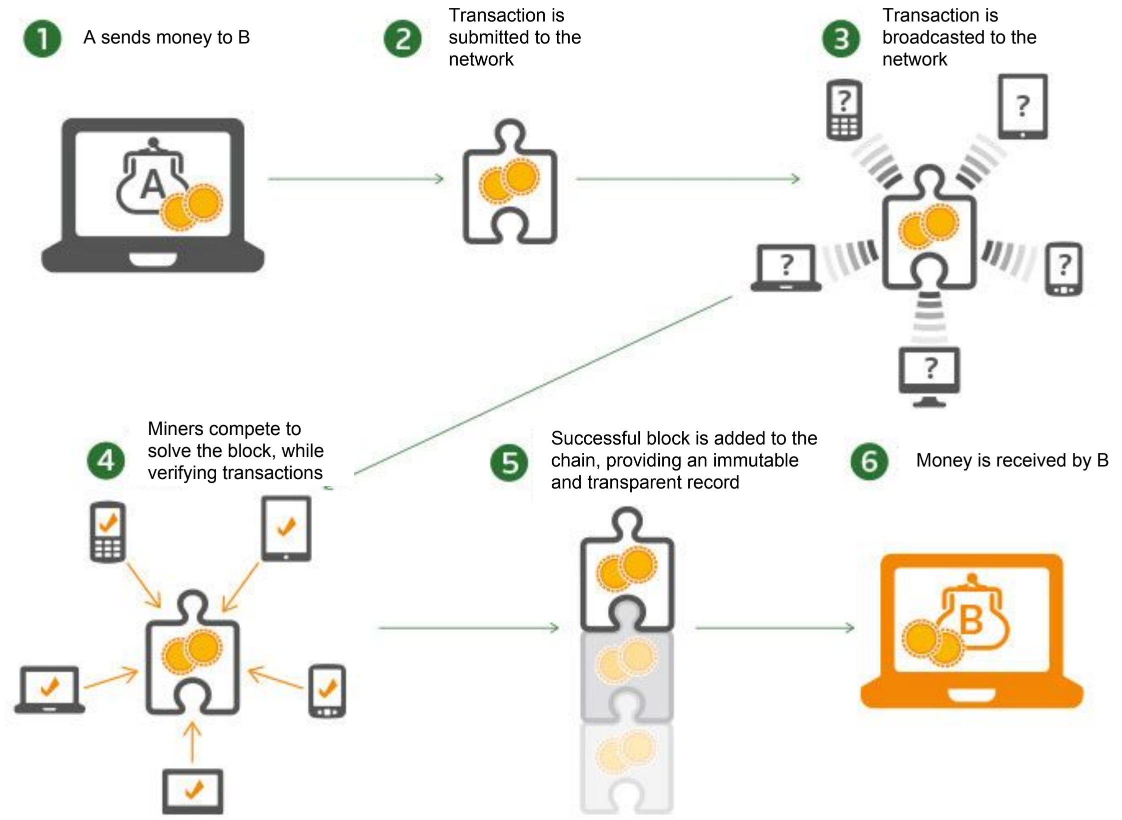


```
<smart contract>


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 {
</smart contract>
                    acceptance_rate = rate;
          }
```

Putting it all together



1 A sends money to B

2 Transaction is submitted to the network

3 Transaction is broadcasted to the network

4 Miners compete to solve the block, while verifying transactions

5 Successful block is added to the chain, providing an immutable and transparent record

6 Money is received by B

Ethereum

> *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

Smart contract capabilities

Vendor-neutral

Public – private blockchains compatibility

Private, permissioned blockchains for enterprise use cases

Rapidly growing community encompassing 30,000+ developers

Multi-billion dollars of value protected on the public network

Enterprise Ethereum Alliance is the largest consortia

The dominant platform for the 'token ecosystem’

Technical and operational challenges

With any emerging technology, limitations of the technology exists but the technical community is actively working to overcome these obstacles

Scalability

Proof of Work is not sustainable for higher volume of transactions

Latency

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

Privacy

Pseudonymity does not satisfy privacy requirements for many use cases

Integration

Limited interoperability and integration between different protocols and legacy systems

Operating Model

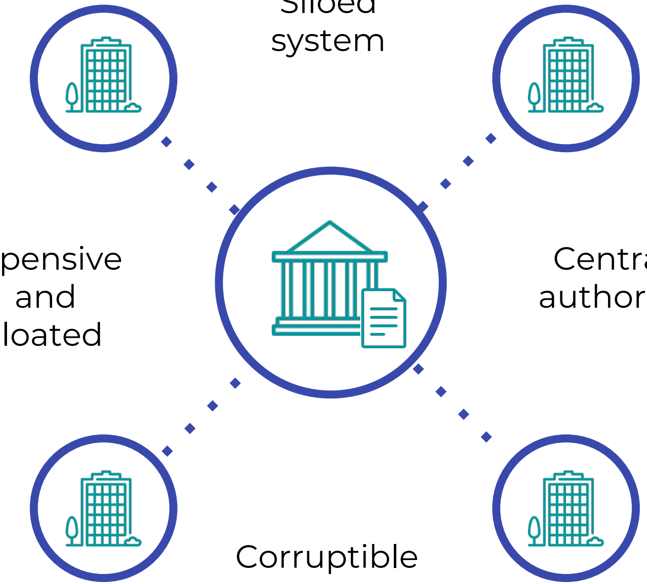
Operation of new blockchain utilities and consortia requires new governance models

Regulations

Regulatory framework is still uncertain, limiting institutional adoption

Distributed and disintermediated models

Centralized Systems



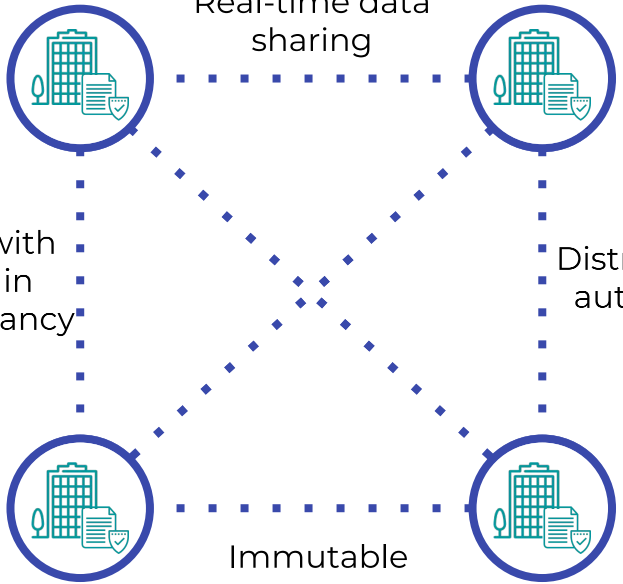
Siloed system

Expensive and bloated

Central authority

Corruptible

Distributed Systems



Real-time data sharing

Lean with built in redundancy

Distributed authority

Immutable

Blockchain 101

Why blockchain?

Reduce costs

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

Reduce risk

- No single point of failure or attack
- Non-repudiability reduces fraud risk
- Immutable audit trail and provenance

Increase revenues

- Creation of new products and services
- Capture value from demonstrating provable provenance

Improve speed and experience

- Simplify value chain by removing intermediaries
- Allow T+0 settlement

Art of The Possible

Art of the Possible

Blockchain enablers (1/2)

	Description
Asset tokenization	Tokenization of physical and digital assets for trading and settlement with multiple parties
Custody & escrow	Trustless transaction with assets in escrow managed by smart contract
Provenance tracking	Single source of truth that conveys information about asset across its journey from one custodian to another
Accounting & reconciliations	New accounting paradigm where every debit and credit is recorded with immutable entry on blockchain

Art of the Possible

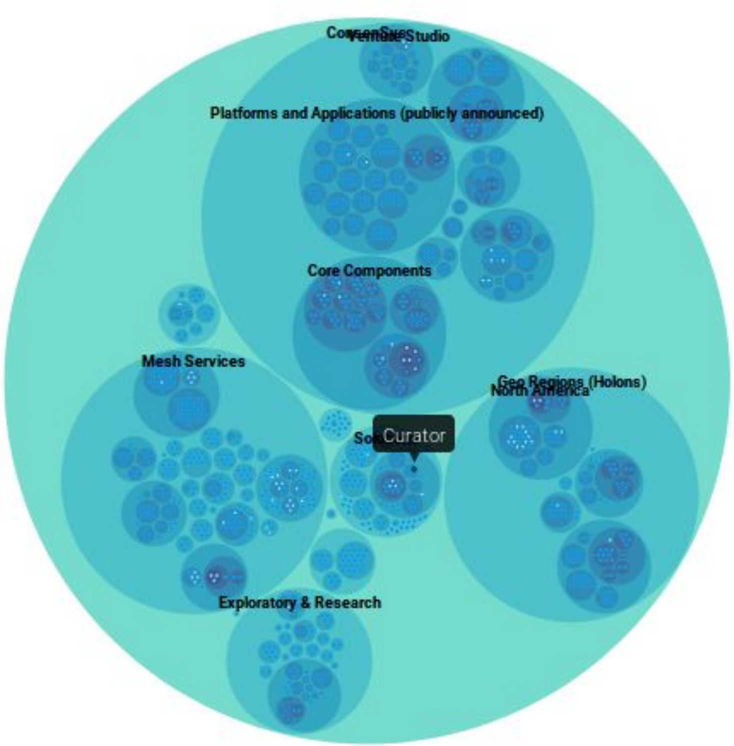
Blockchain enablers (2/2)

	Description
Digital identity	Consolidation and management of ID with attributes stored and verified on blockchain
Real-time transactions	Atomic transactions ensure trade is settlement, removing lag time
Micro payments & funding	Transactions of minimum value enable P2P payments, M2M payments and capital raising
Automated execution	Full automation of contract lifecycle from issuance, transfers, revisions and execution

Relevant Use Cases

Traditional Management Nullification Tool

https://consensys-mesh.ga/home



Relevant Use Cases

Global Interest & Adoption

European Commission

Launched in 2018 the Blockchain Observatory and Forum to highlight key developments and promote European actors

United States SEC

Actively pursuing assessment and definition of new regulatory frameworks for cryptocurrencies and tokens

Singapore MAS

Since 2017 has been driving the development of pilot projects using blockchain for invoice tracking and settlements

Smart Dubai Office

In 2017 kicked-off an integrated blockchain strategy comprising PoCs, BaaS platform, industry and talent development

Relevant Use Cases

Key Strategic Drivers

Government efficiency

Achieve efficiency and improve services by using blockchain across applicable services

Industry and job creation

Create an active and enabling blockchain ecosystem for startups, businesses and talent

International leadership

Lead the thinking to attract cross-border applications and investments

Key IT Drivers

Data orchestration and processing

Distributed access to data, automated rule driven processing, no single point of failure

Service enablement and automation

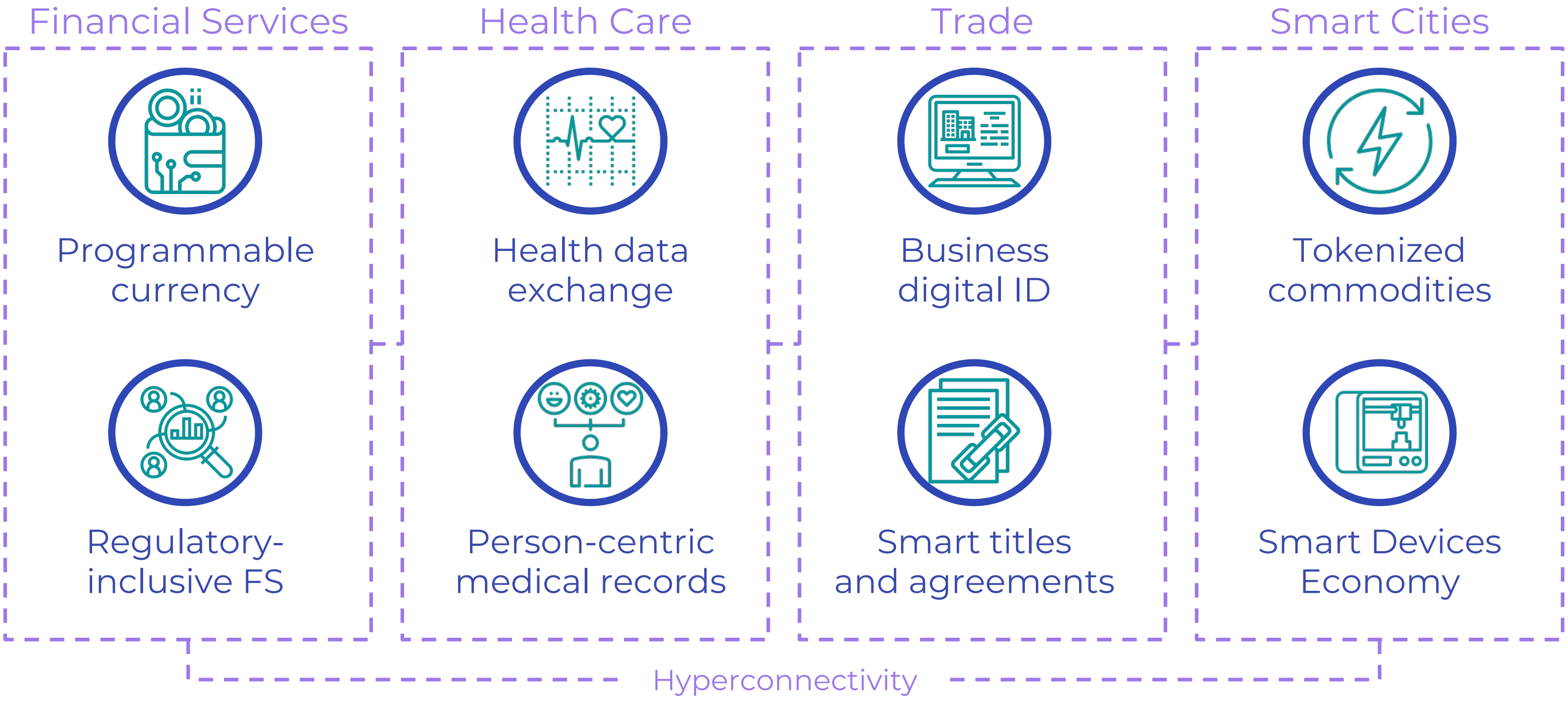
Verifiable business logic execution, integrated workflows, decentralized ID, micropayments

Security and auditability

Digital signatures, non repudiation of events, tamper proof log of transactions and events

Relevant Use Cases

Emerging Use Cases



Financial Services

- Programmable currency
- Regulatory-inclusive FS

Health Care

- Health data exchange
- Person-centric medical records

Trade

- Business digital ID
- Smart titles and agreements

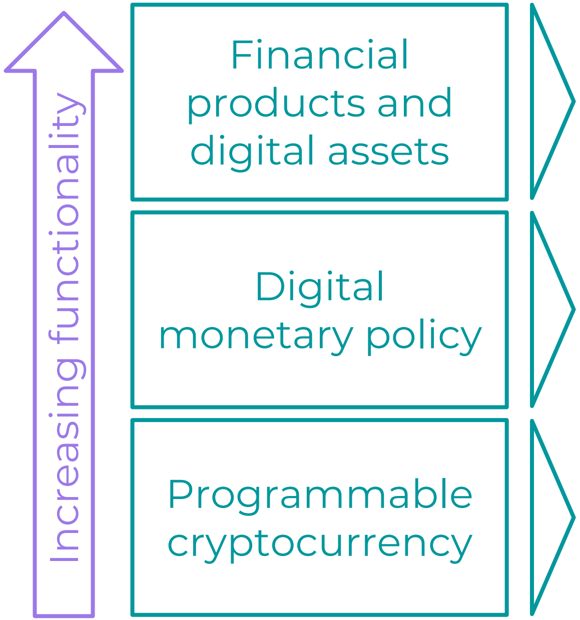
Smart Cities

- Tokenized commodities
- Smart Devices Economy

Hyperconnectivity

Relevant Use Cases

Programmable Currency



Increasing functionality

Financial products and digital assets

Financial products and digital assets abide by the Central Bank’s rules and regulations by default and automate reporting and tax collection

Digital monetary policy

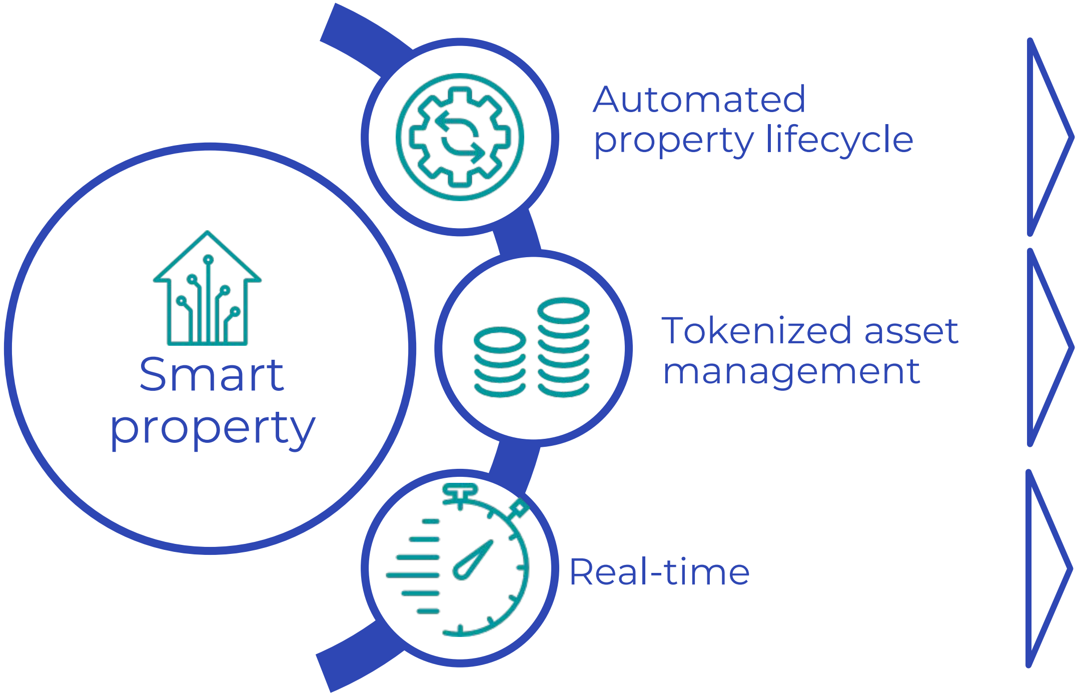
Custom logic, reporting, and analytics capabilities can be built into the system allowing the Central Bank to enact banking, credit, and monetary policy

Programmable cryptocurrency

A core platform allowing the Central Bank to issue programmable cryptocurrency and to authorize agencies, banks, and individuals to send payments

Relevant Use Cases

Smart titles



Smart property

Automated property lifecycle

Government entities can define workflows to facilitate execution of the property lifecycle and automate compliance

Tokenized asset management

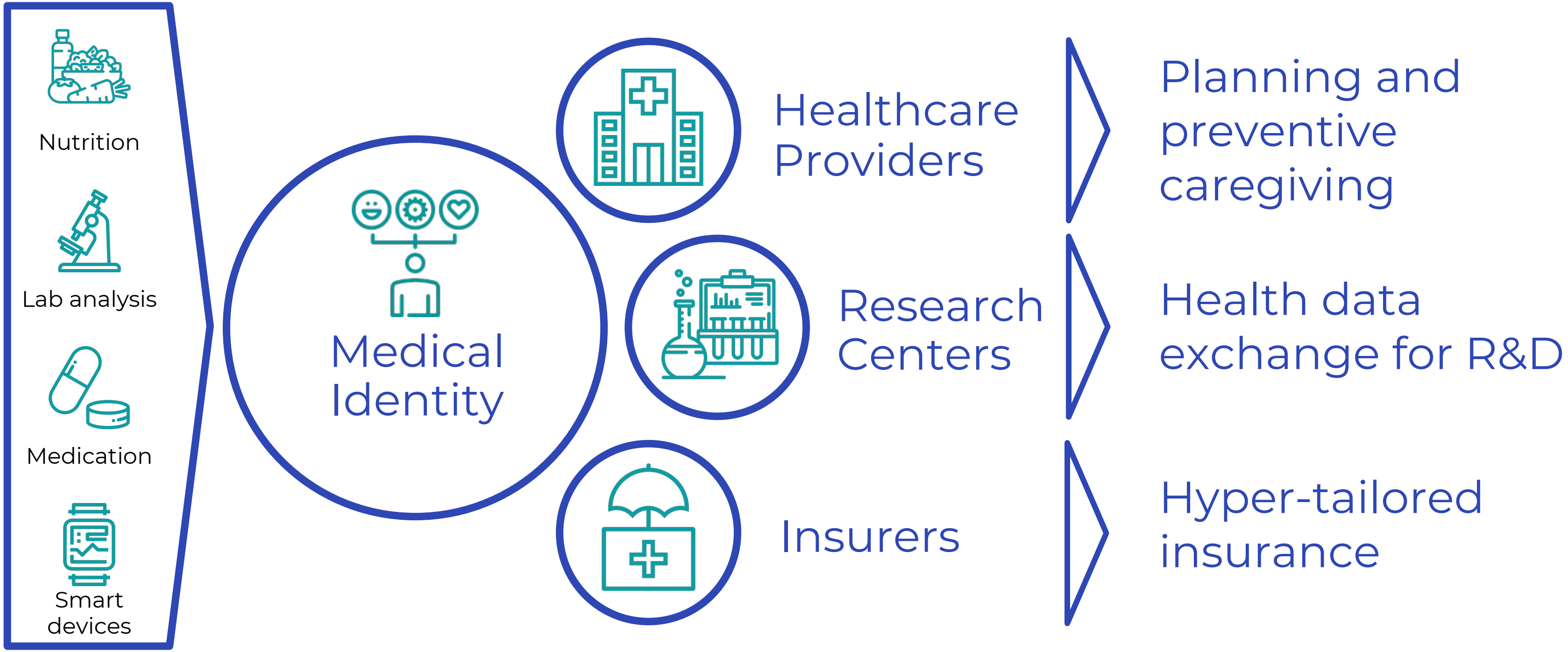
Property ownership becomes fractional and can be traded across borders and remotely

Real-time

Byers and renters can walk into a property, make an offer, get approved, and receive the title or lease, all on-site

Relevant Use Cases

Medical Identity



Nutrition

Lab analysis

Medication

Smart devices

Medical Identity

Healthcare Providers

Planning and preventive caregiving

Research Centers

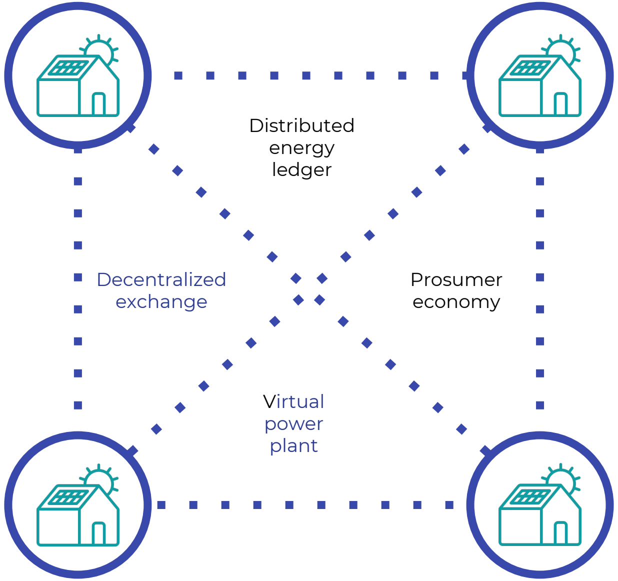
Health data exchange for R&D

Insurers

Hyper-tailored insurance

Relevant Use Cases

Tokenized Energy Trading



The producer / consumers (prosumers) can be net providers or consumers based on their production capacity and energy needs

Tokenized exchanges incentivize individuals to pursue green energy production and sustainable consumption

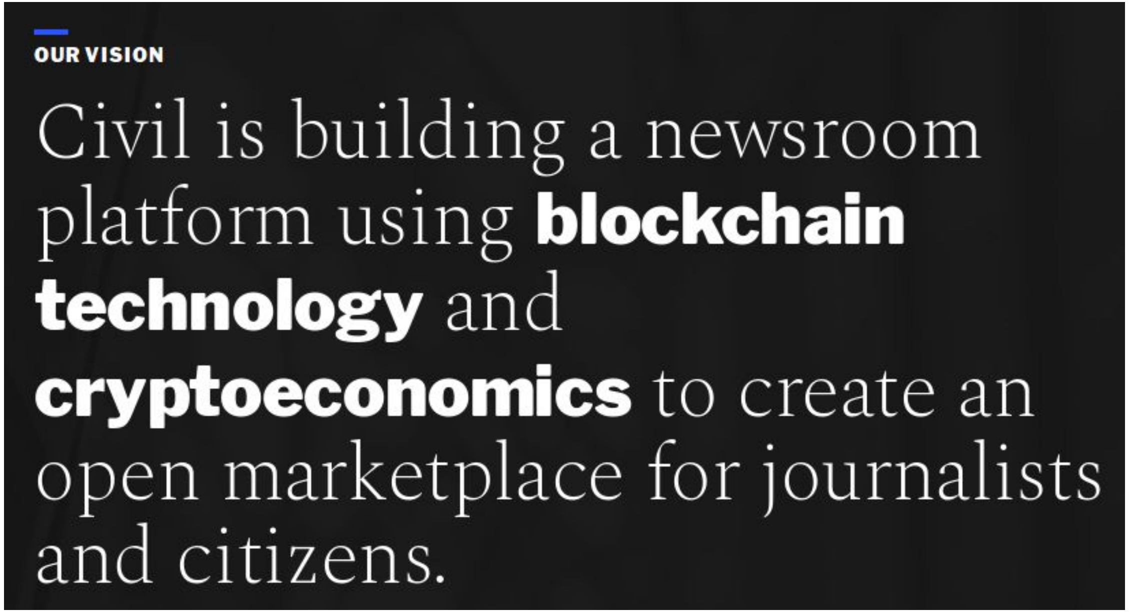
CO2 emissions decrease without Government subsidies

Public Sector use-cases

Civil

https://joincivil.com

A Marketplace for Sustainable Journalism (True News you and facts you can Trust)



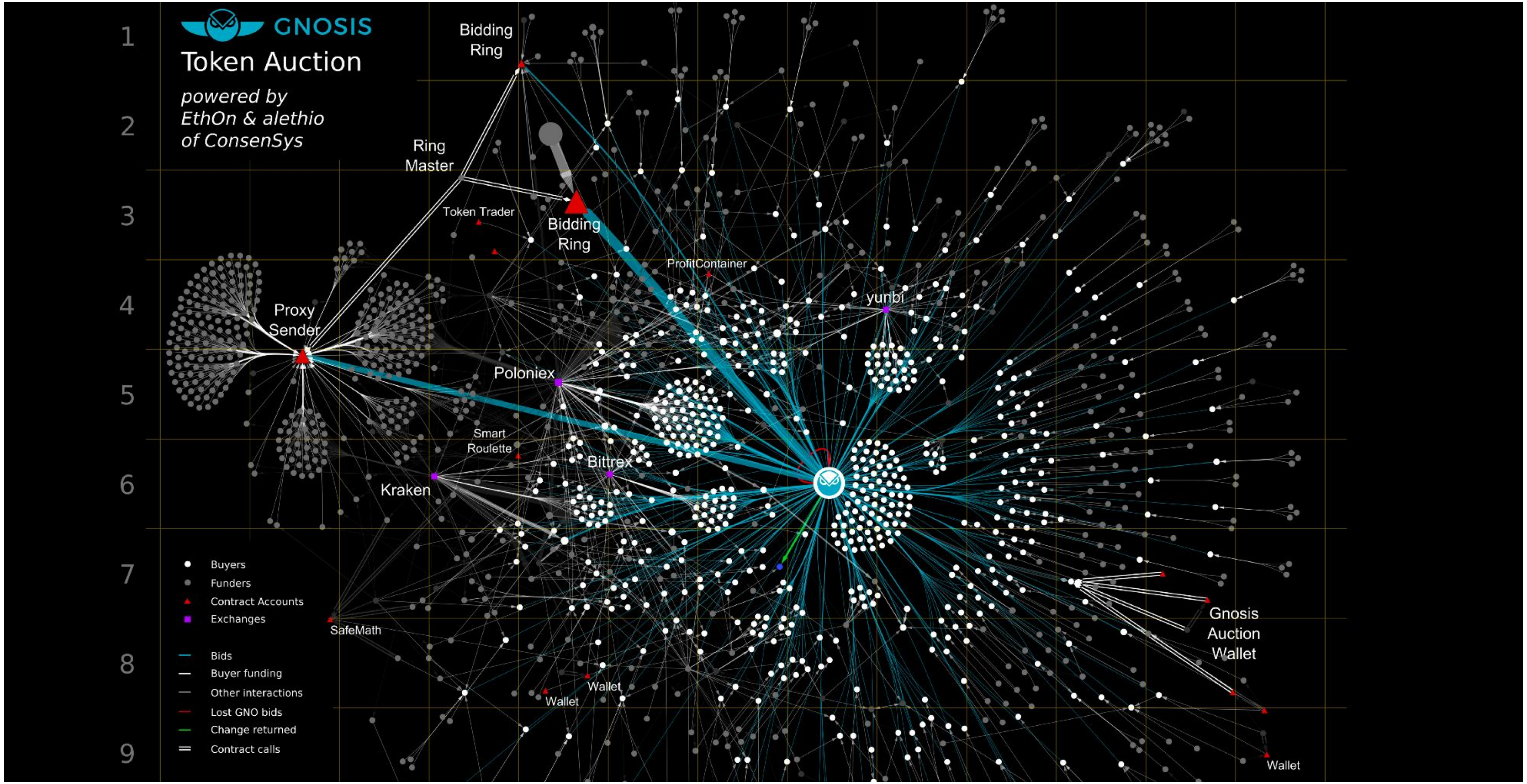
OUR VISION

Civil is building a newsroom platform using **blockchain technology** and **cryptoeconomics** to create an open marketplace for journalists and citizens.

Truth

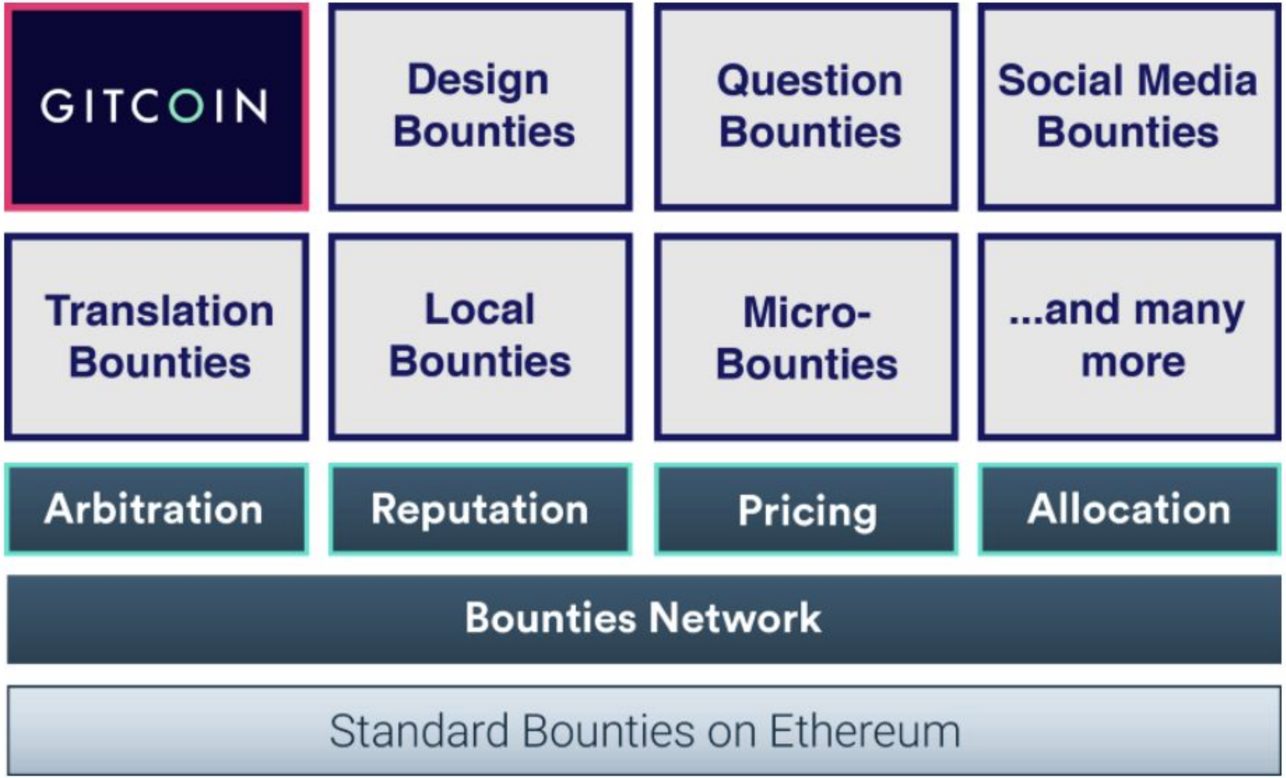
https://aleth.io

Intelligence, Big Data, and Analytics



https://bounties.network

Future of Work

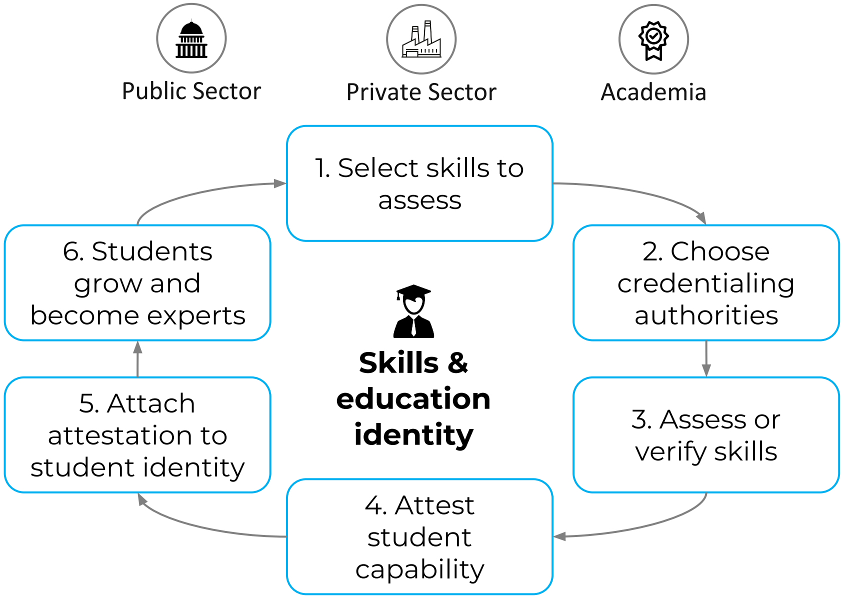


Gitcoin (depth-first) and Bounties Network (breadth-first) have integrated!

Education - Assessment

Decentralized assessment is foundational

Whether to facilitate learning styles or accelerate absorption of new technologies, decentralized assessment is foundational to education of the future


Public Sector
Private Sector
Academia
1. Select skills to assess
2. Choose credentialing authorities
3. Assess or verify skills
4. Attest student capability
5. Attach attestation to student identity
6. Students grow and become experts
Skills & education identity

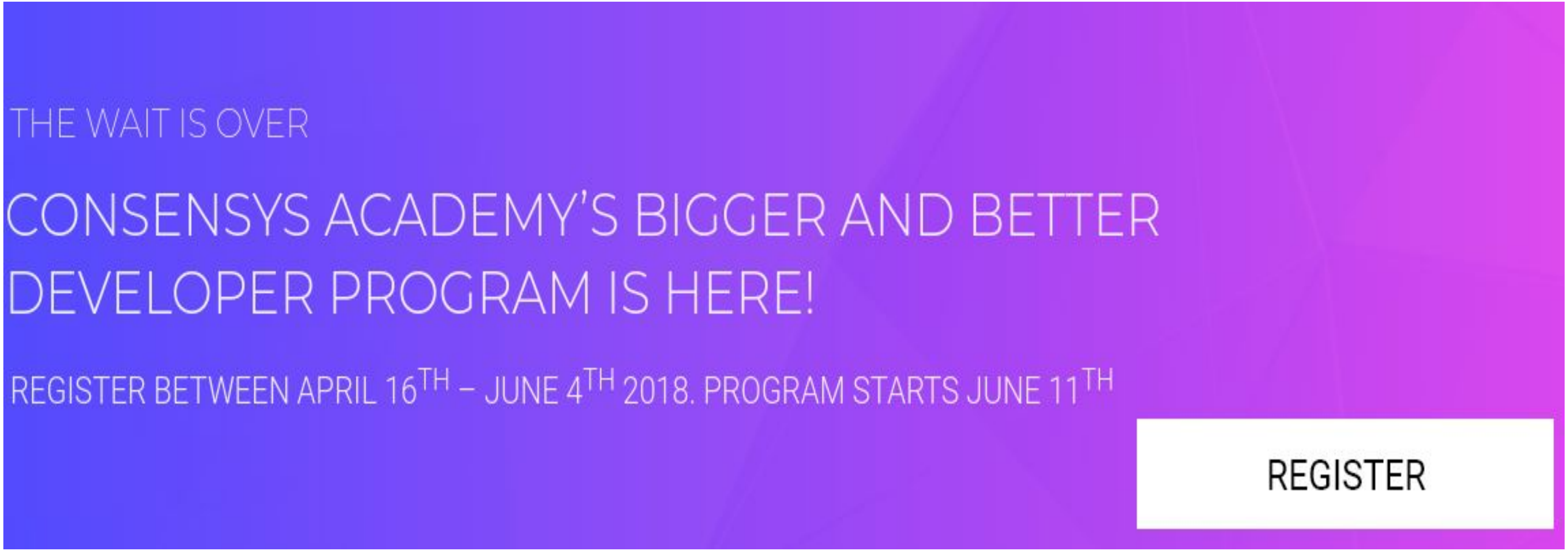
Evidenced qualifications are critical to workforce enablement

Chain of trust provides evidence of claimed skills via attestations and evidence of assessments

Employment requirements can be easily matched to specific skills (vs more generic qualifications)

Can be integrated and supplement existing processes/services, such as immigration, enrolment, and digital identity https://consensys.net/academy/developer/

Upcoming on-line course



THE WAIT IS OVER

CONSENSYS ACADEMY'S BIGGER AND BETTER DEVELOPER PROGRAM IS HERE!

REGISTER BETWEEN APRIL 16TH – JUNE 4TH 2018. PROGRAM STARTS JUNE 11TH https://block2.splashthat.com

Join us for a special meetup on Friday!

Block 2 : Developing on Open Systems

MAY 4TH 7:00PM

RSVP