Financial Fraud Mitigation With Blockchain Technology

OWASP Indonesia Meetup I 2017

Dimaz Ankaa Wijaya

4 March 2017 | Mozilla Community Space | Jakarta, Indonesia

Indonesia Honeynet Project

Dimaz Ankaa Wijaya, S.Kom., MNS, CSXF

- Education
  - FMIPA UGM – Sarjana Komputer (2007)
  - Faculty of IT, Monash University – Master of Networks and Security (2016)
- Field of Expertise
  - Digital forensic, database, software engineering
  - Network security, software security, cryptocurrency
- Book
  - Mengenal Bitcoin dan Cryptocurrency (2016, Puspantara)
  - Bitcoin Tingkat Lanjut (2016, Puspantara)
- Contact
  - https://kriptologi.com
  - dimaz@kriptologi.com

Today's Menu

- Introduction to Bitcoin
- Financial Fraud
- Blockchain
- Summary

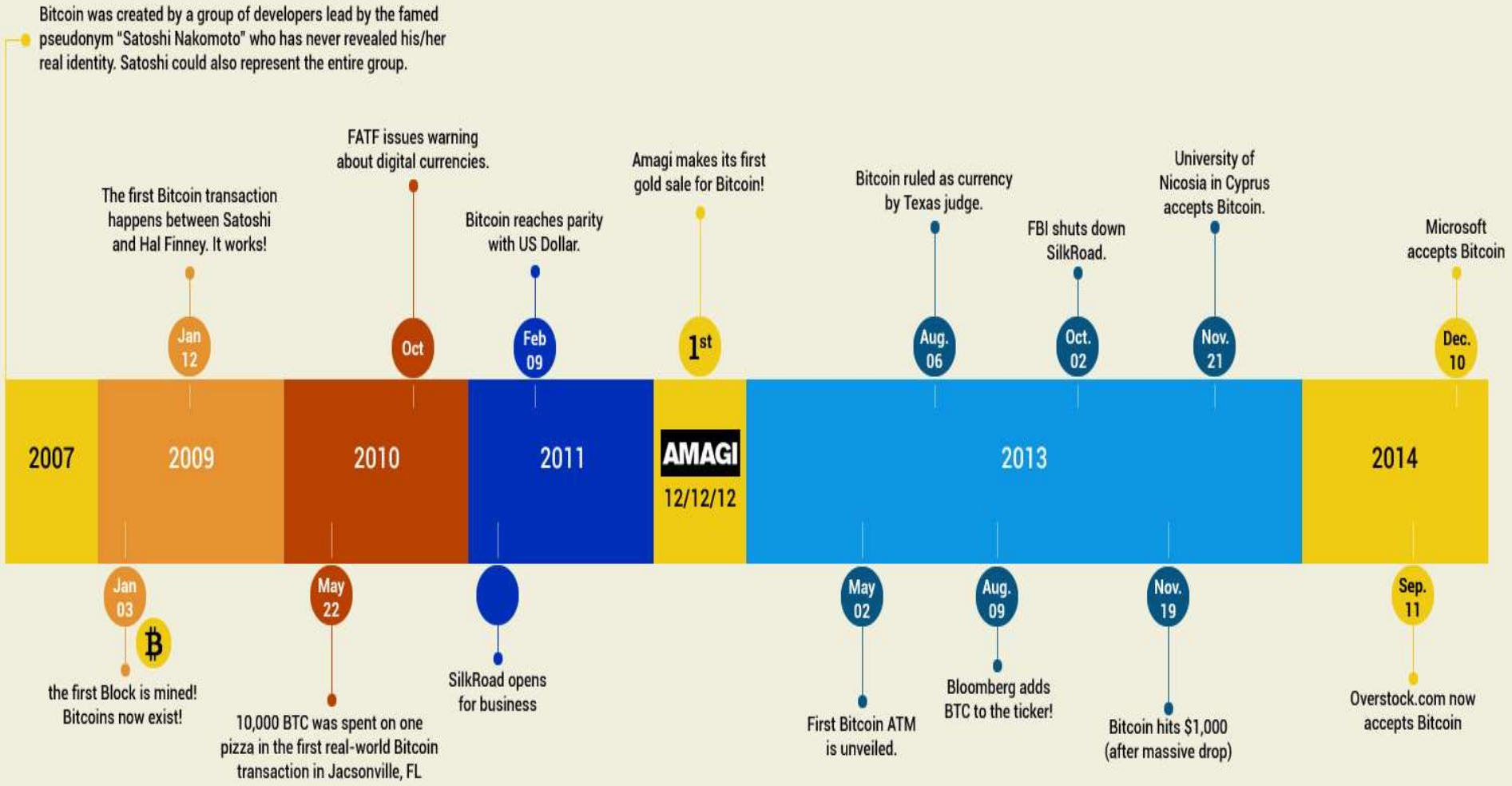
Bitcoin

Bitcoin is not currency; it's the internet of money!

— Andreas Antonopoulos —

AZ QUOTES

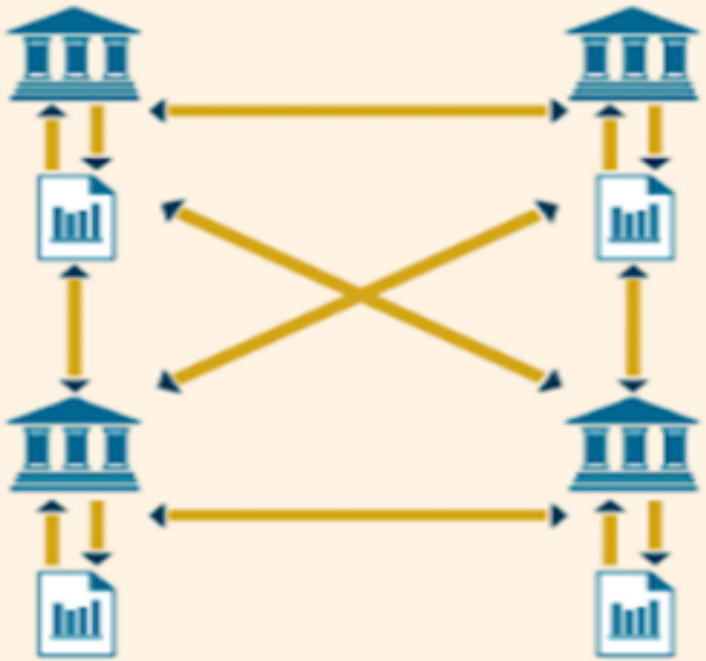
History of Bitcoin



THE HONEYNET PROJECT

Centralized vs Decentralized

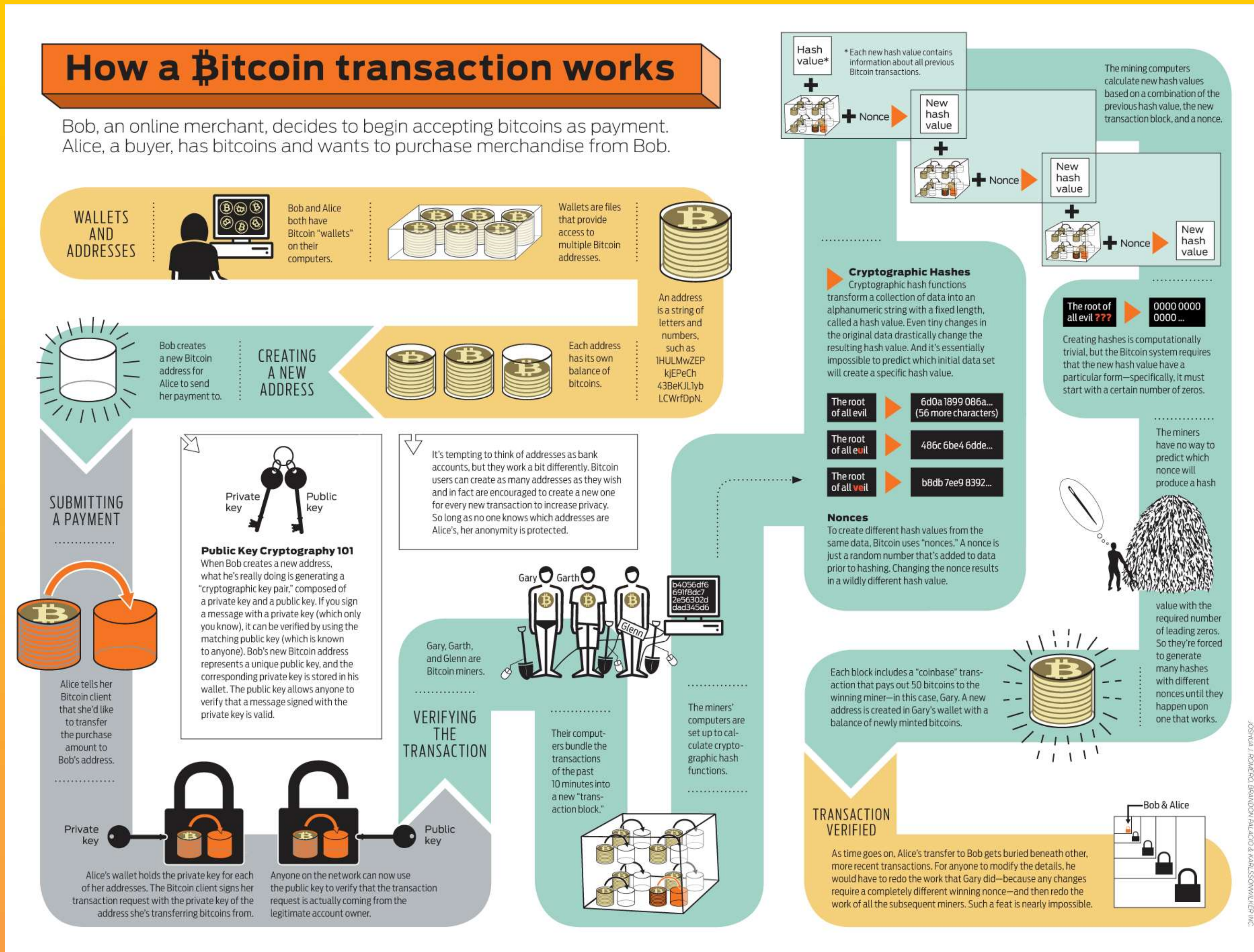
A centralised ledger tracks asset movements within the financial system between institutions



A distributed ledger eliminates the need for central authorities to certify asset ownership. Instead it is held and verified by many institutions, to cut down on fraud and manipulation

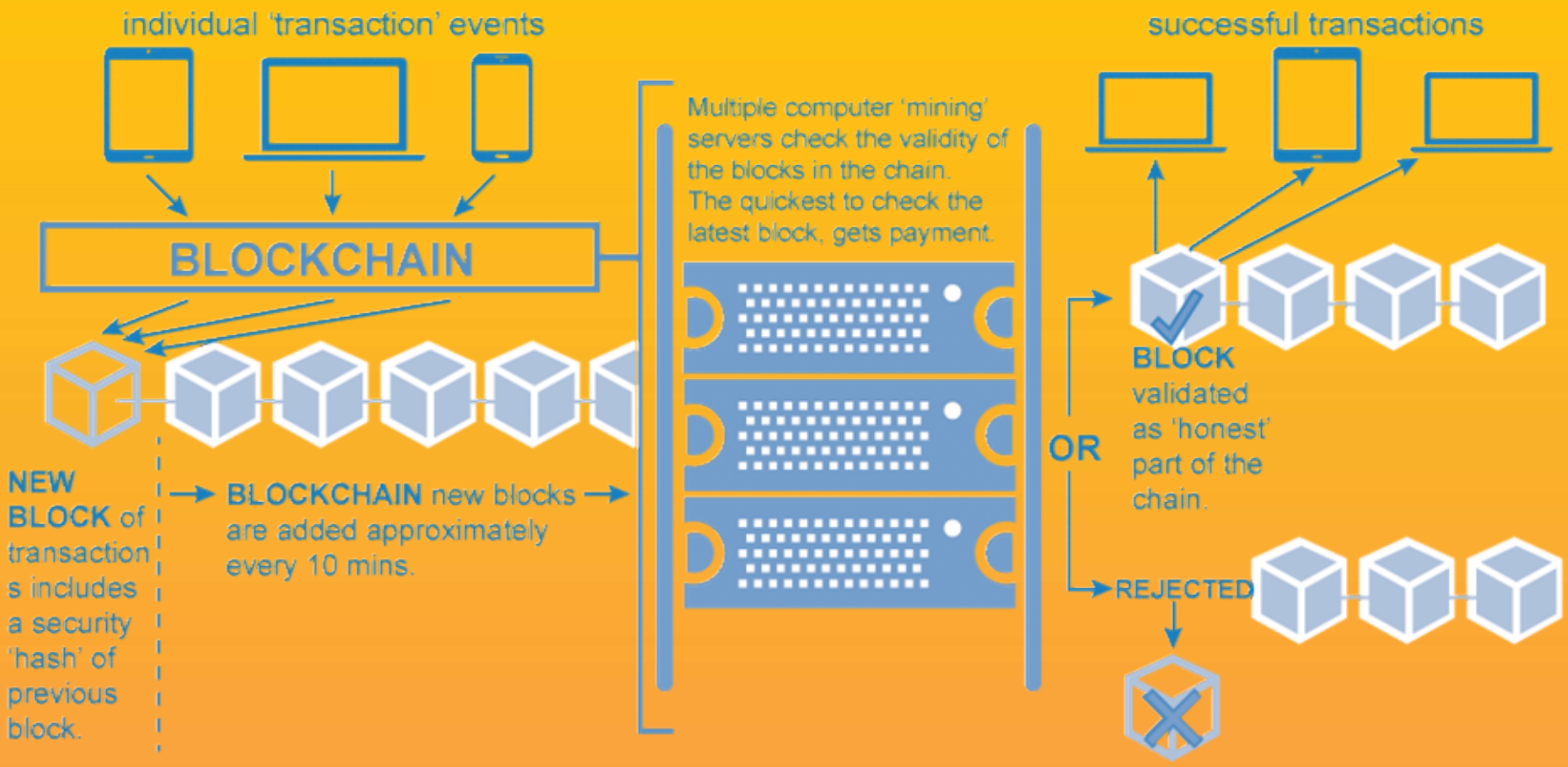
Source: FT research

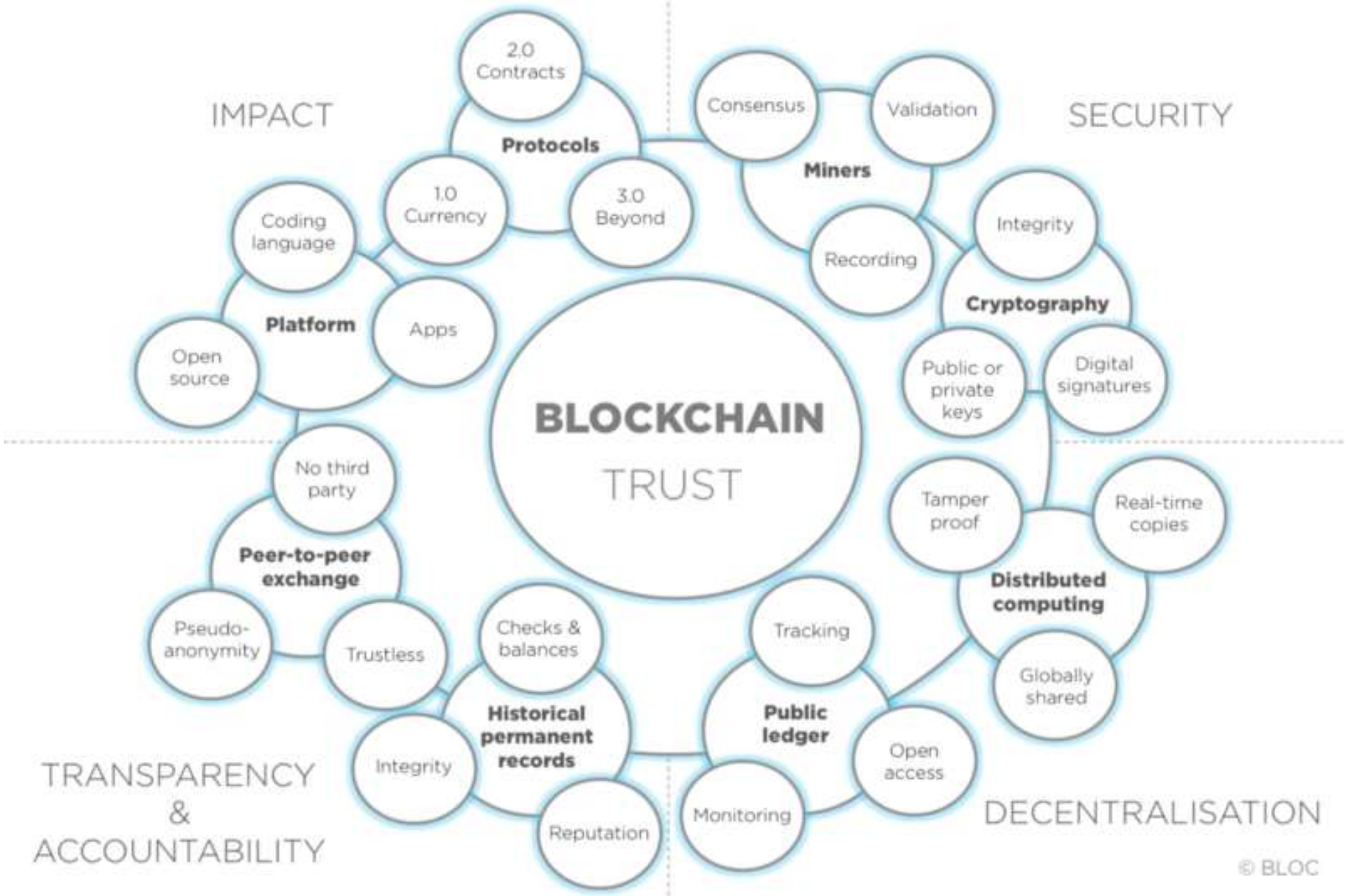
FT



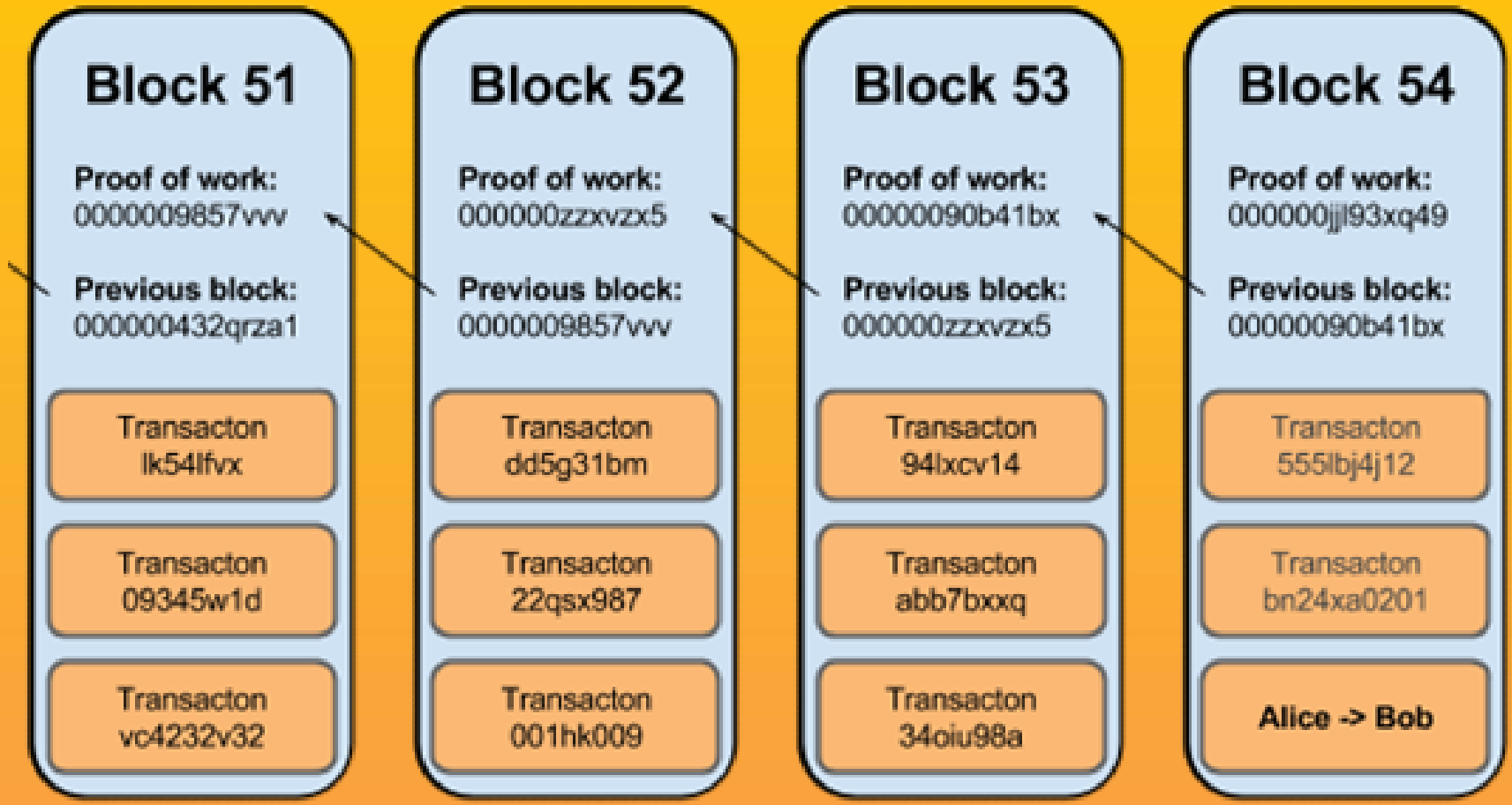
THE HONEYNET PROJECT

Blockchain Overview

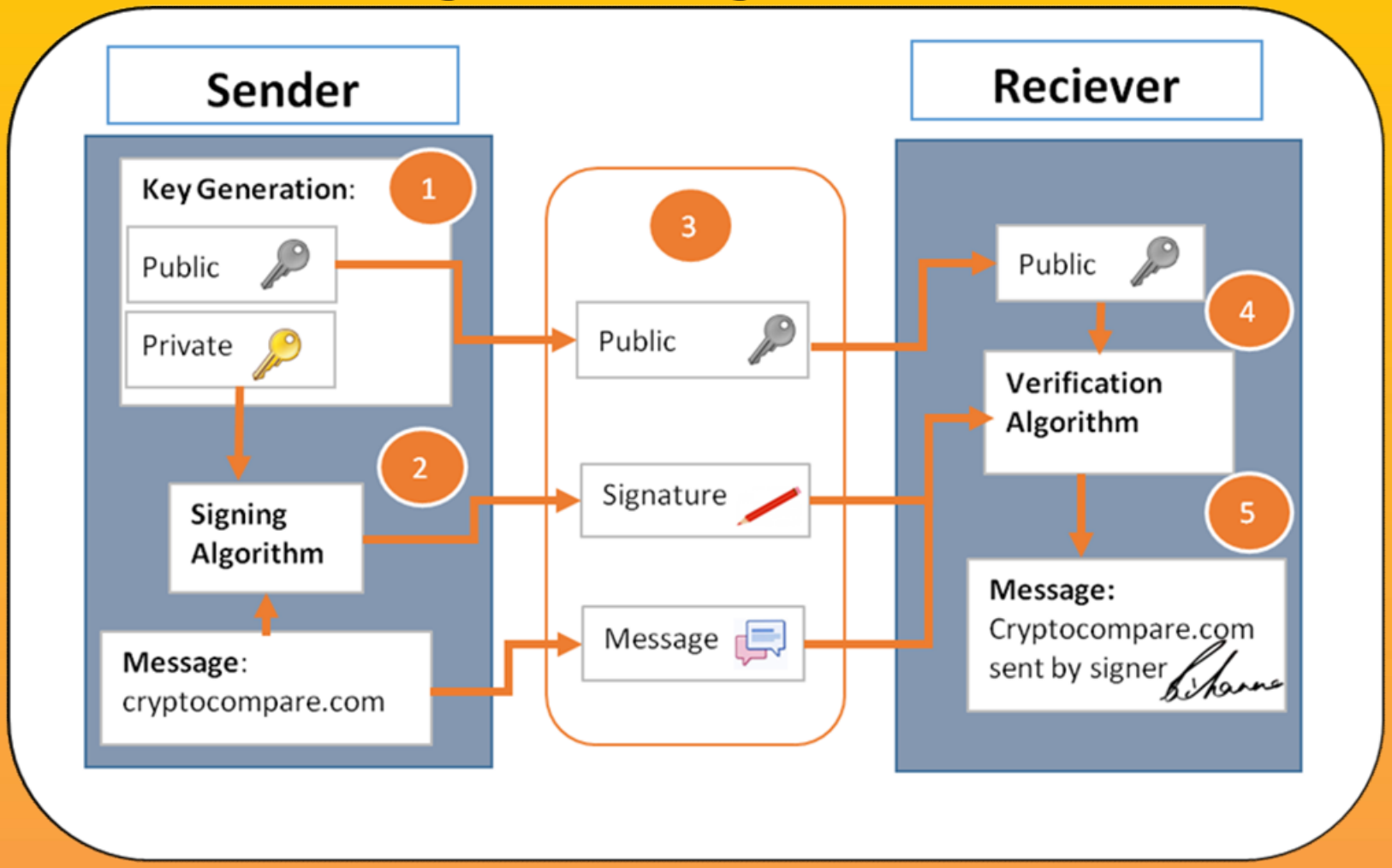



IMPACT
SECURITY
TRANSPARENCY & ACCOUNTABILITY
DECENTRALISATION
BLOCKCHAIN
TRUST
Protocols
2.0 Contracts
1.0 Currency
3.0 Beyond
Platform
Coding language
Apps
Open source
Miners
Consensus
Validation
Recording
Cryptography
Integrity
Public or private keys
Digital signatures
Peer-to-peer exchange
No third party
Pseudo-anonymity
Trustless
Historical permanent records
Checks & balances
Integrity
Reputation
Public ledger
Tracking
Monitoring
Open access
Distributed computing
Tamper proof
Real-time copies
Globally shared
© BLOC

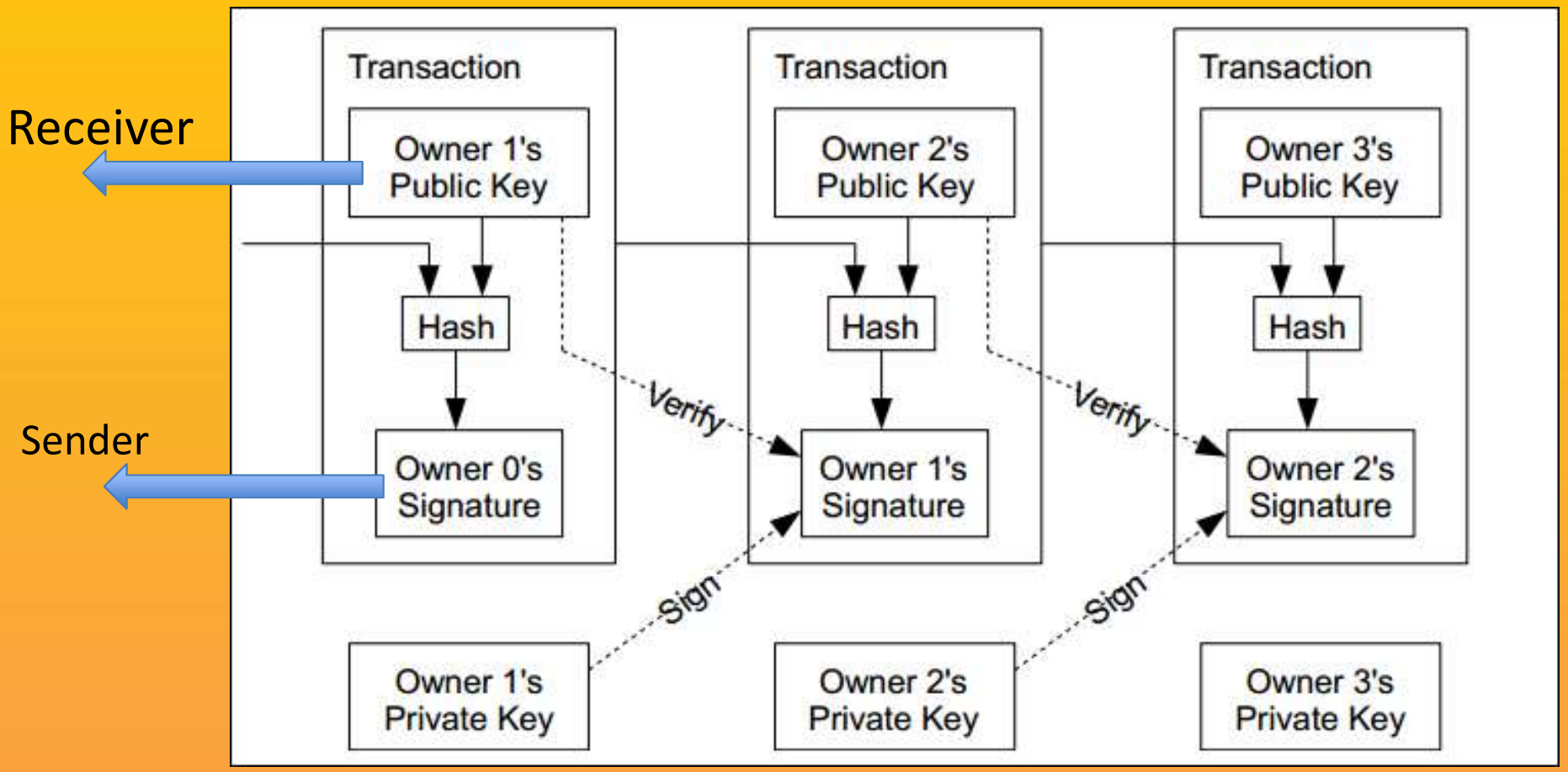
Chain of Blocks



Digital Signature



Bitcoin Transaction

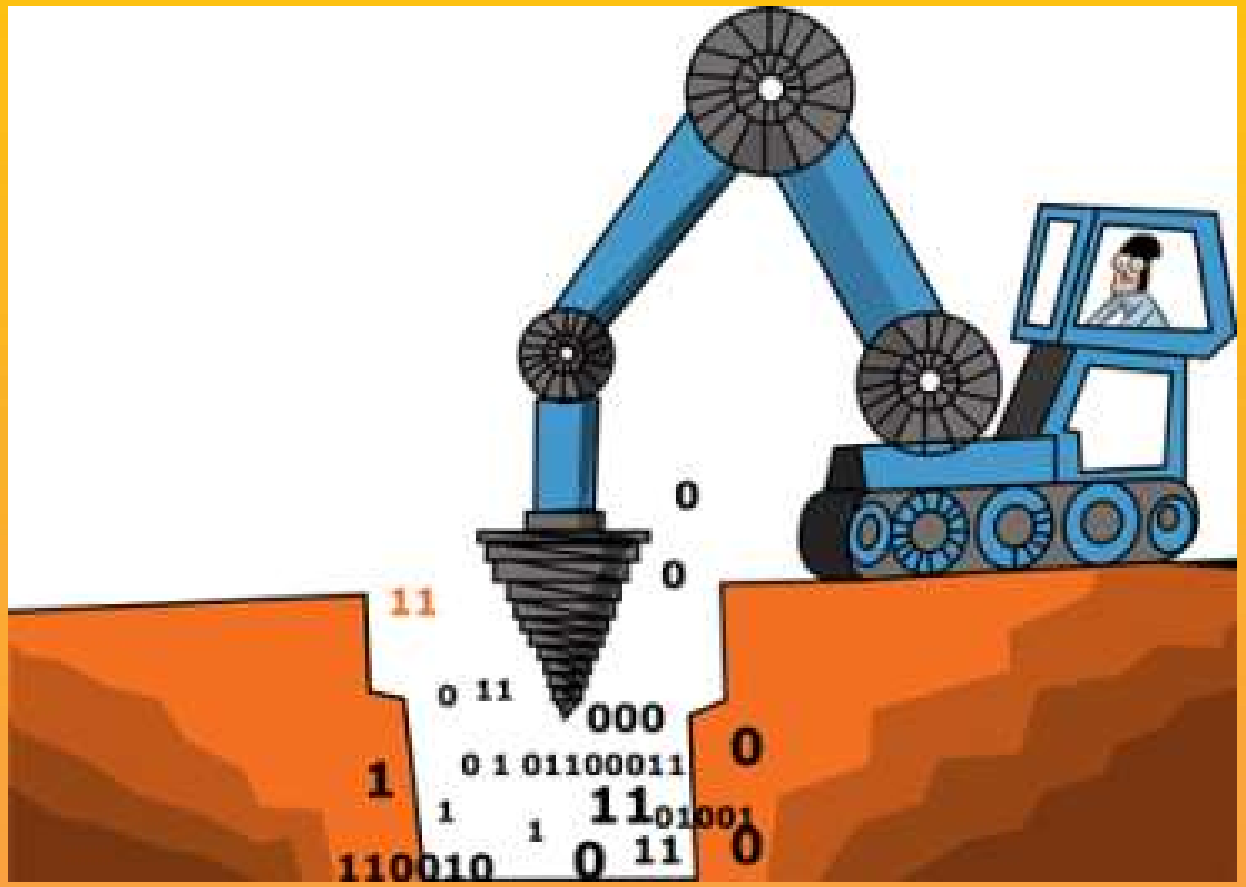


Mining

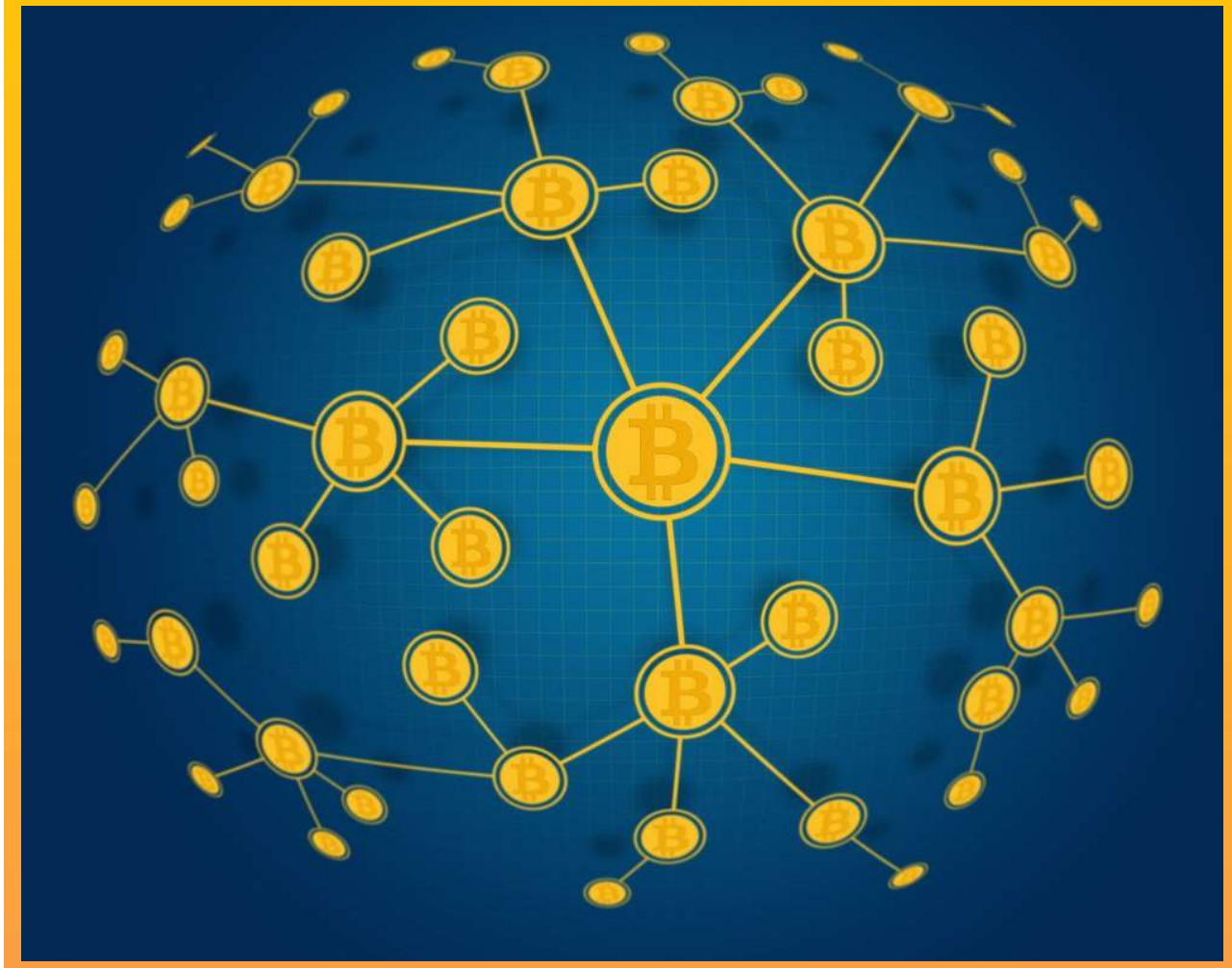
Proof of Work (PoW)

Miners calculate values that match the requirement to create new blocks.

PoW protects the blocks from tampering.



P2P Network



Each server has a complete copy of the blockchain.

They communicate through P2P protocol.

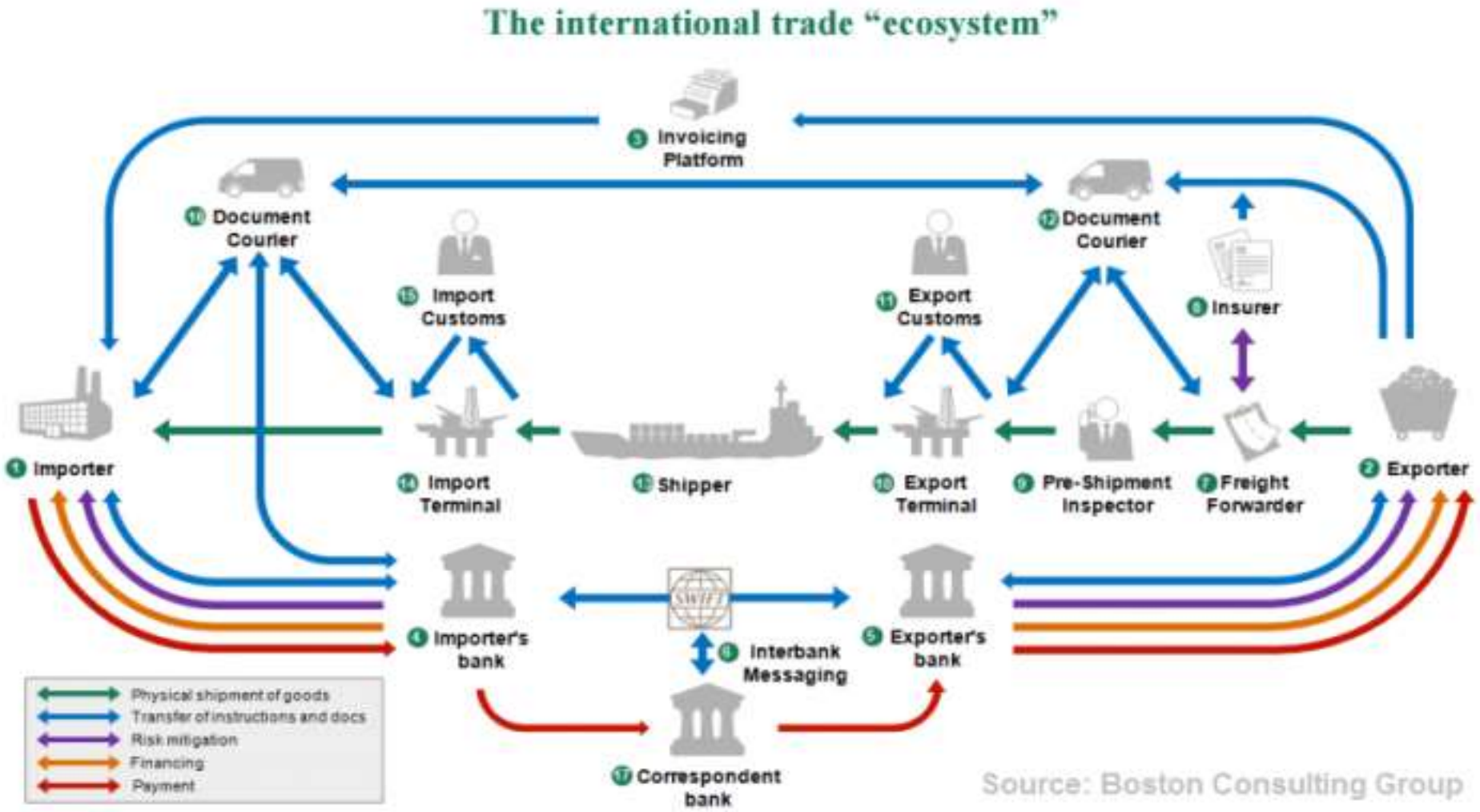
Financial Fraud

- ID Theft
- Cyber Security
- Credit Card Fraud

Financial Fraud (2)

- Falsifying data
  - Enron
  - WorldCom
- Fake document

Financial Scheme

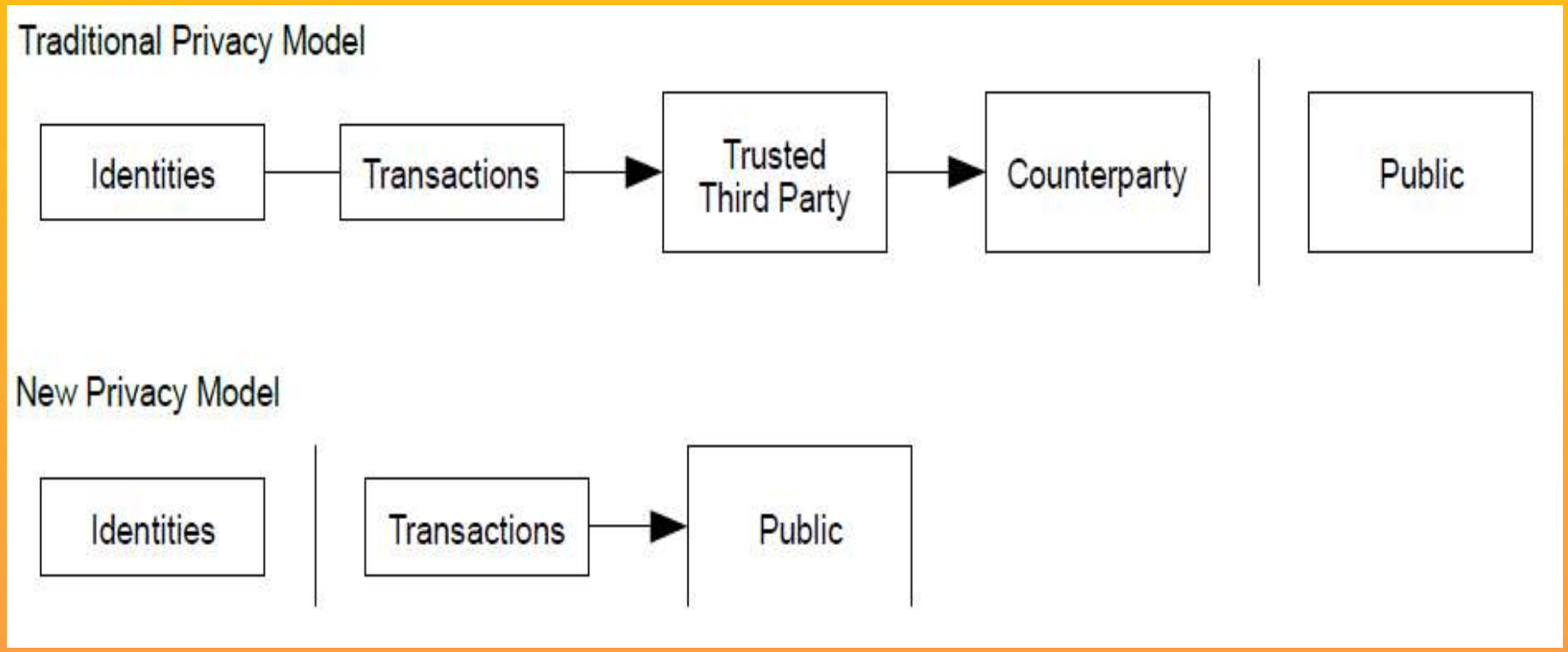


Employing Blockchain in Finance Industry

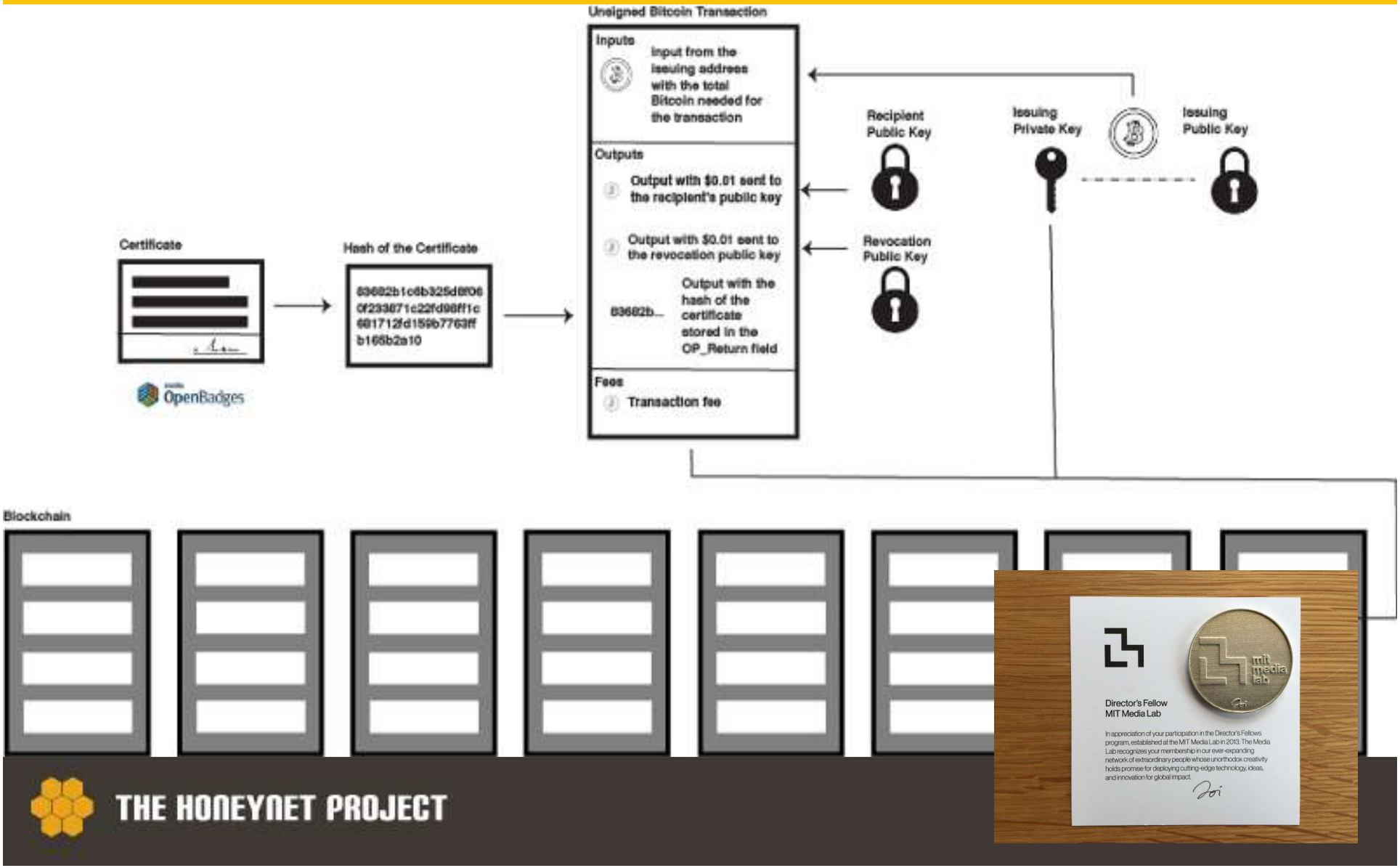
- Transparent – visible ledger
- Trustless – no central authority needed
- Cryptography – digital signature
- Permanent – blockchain

Privacy Model

- Disconnecting Identities and Transactions

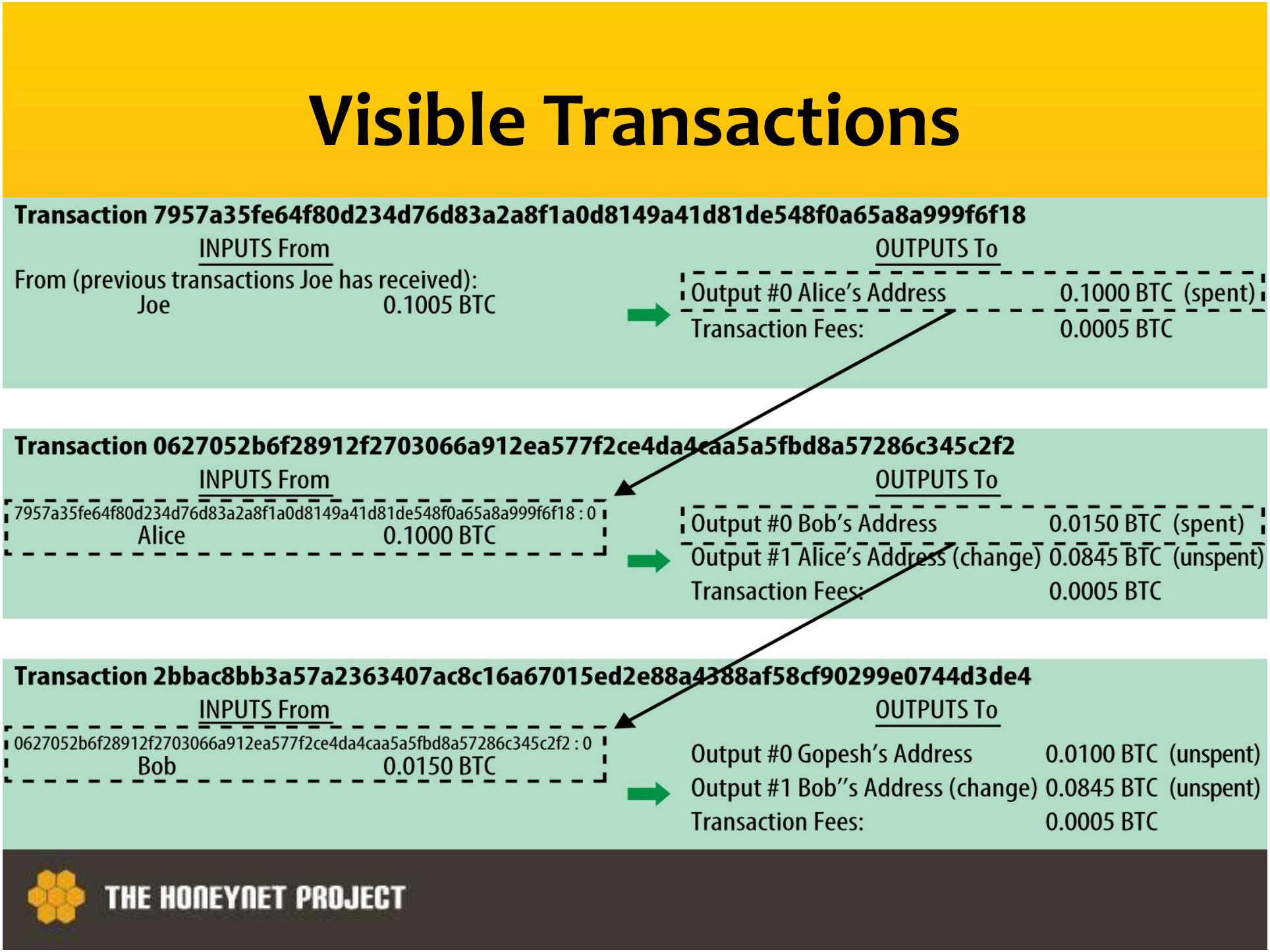


Blockchain-based Digital Certificate



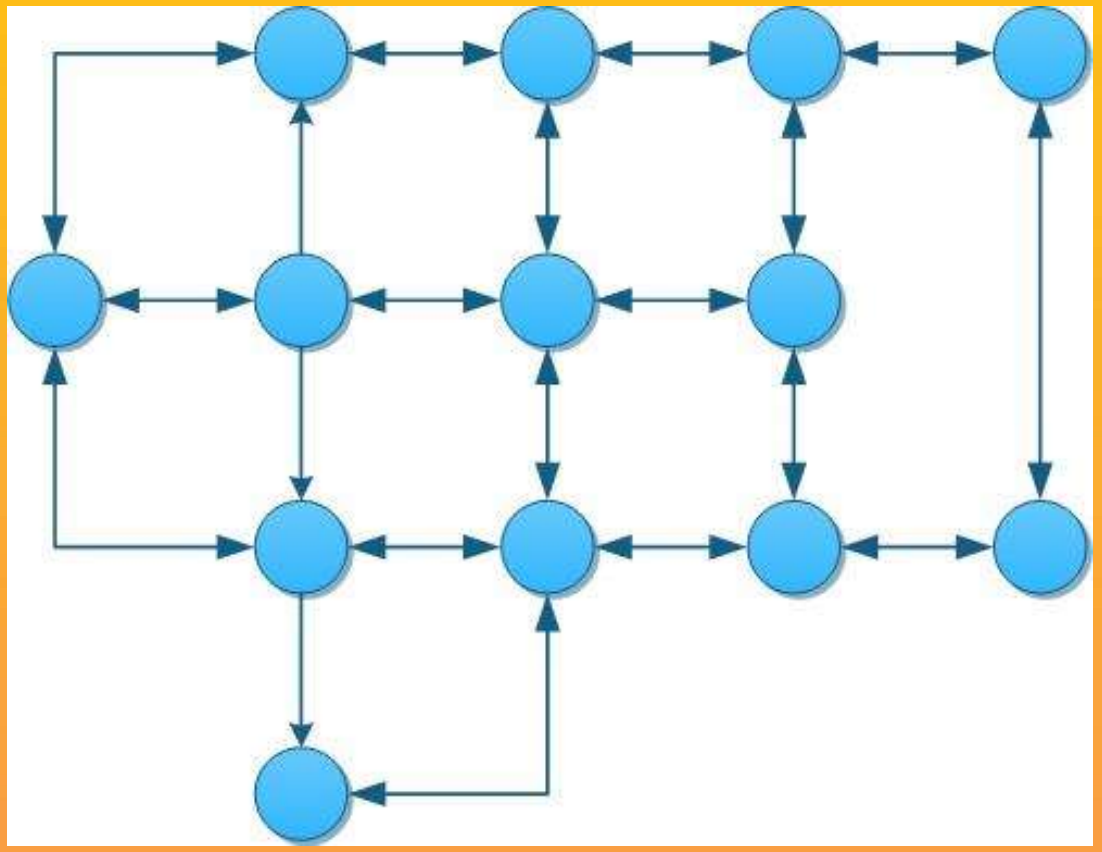
Multisignature

Visible Transactions



No Single Point of Failure

- Peer-to-Peer Network
- Multiple nodes
- Synchronization



Eliminating Middleman

- Reducing fees and risks

Customized Transactions

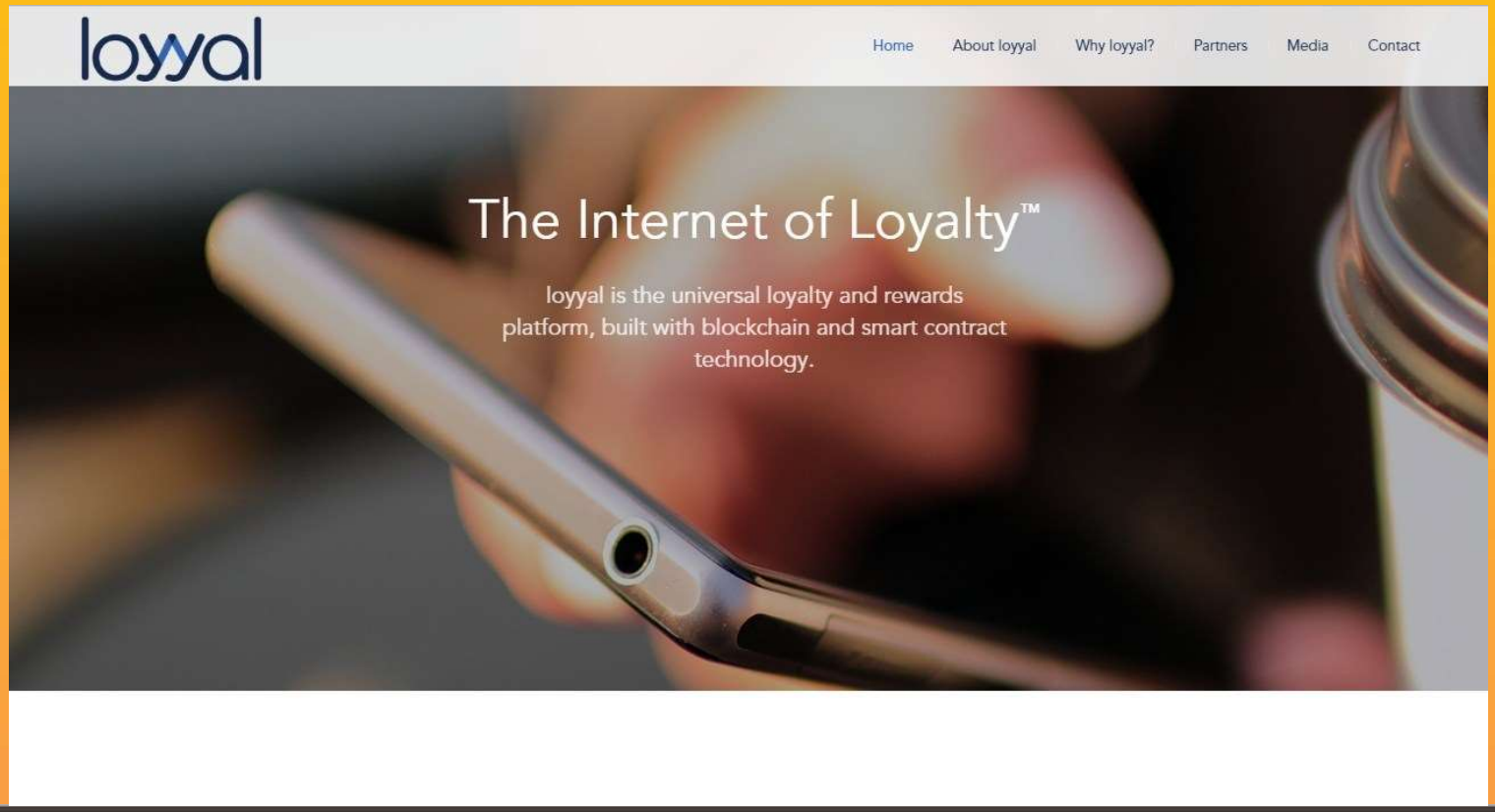
- Escrow transaction
- Hash-locked transaction
- Time-locked transaction

…And Many More!

- Ring Signature (Monero)
- Smart Contract (Ethereum)

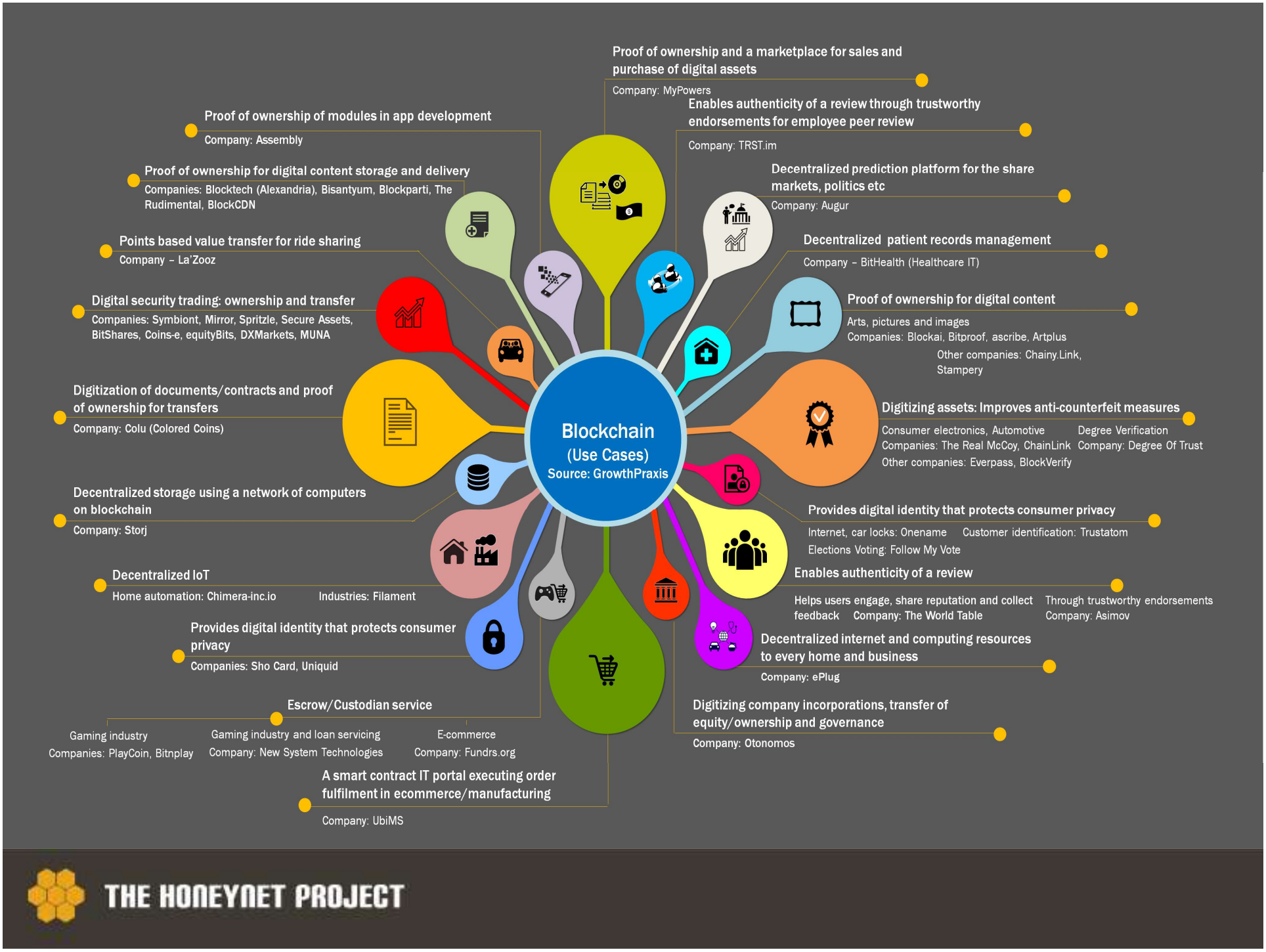
Current Usage

- Loyalty Program



Recent Development

- R3CEV
- Hyperledger
- Blockchain of things
- Ms. Azure's BaaS



THE HONEYNET PROJECT

Summary

- Blockchain supports transparency in financial industry by using public ledger.
- Blockchain protects the data from unauthorized modification.
- Blockchain supports authentication and non-repudiation in financial transaction by utilizing cryptographic functions.
- These characteristics minimize the risk in financial fraud.


Backspace
Thank You
Page Up
Home
Page Down
Insert
Shift