

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://criptologi.com>
 - dimaz@criptologi.com



Today's Menu

- Introduction to Bitcoin
- Financial Fraud
- Blockchain
- Summary



THE HONEYNET PROJECT

Bitcoin



THE HONEYNODE PROJECT



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

— *Andreas Antonopoulos* —

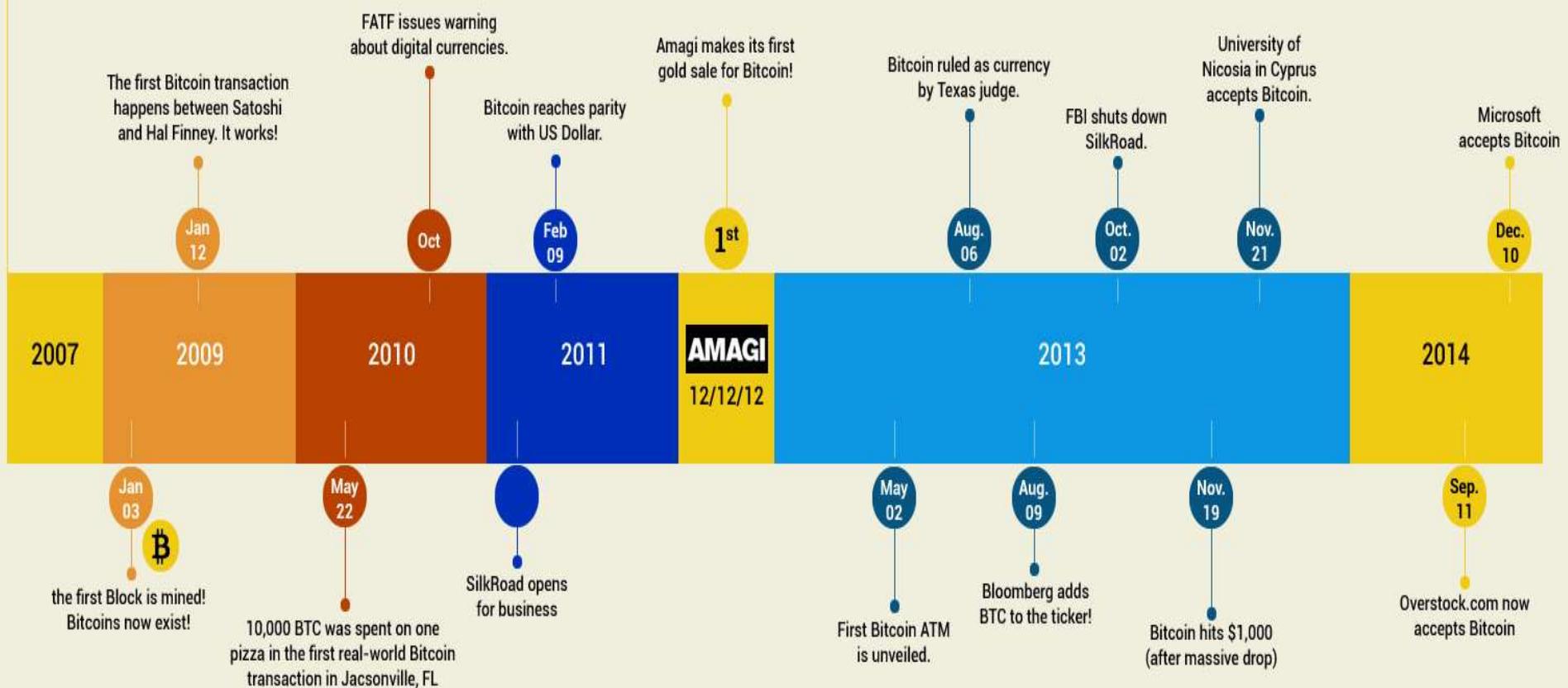
AZ QUOTES



THE HONEYNET PROJECT

History of Bitcoin

Bitcoin was created by a group of developers lead by the famed pseudonym "Satoshi Nakomoto" who has never revealed his/her real identity. Satoshi could also represent the entire group.

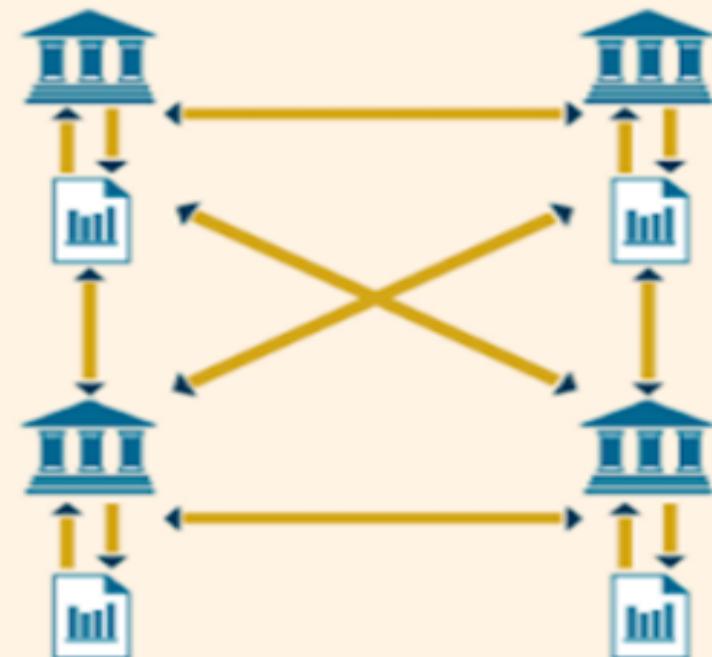


THE HONEYNET PROJECT

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

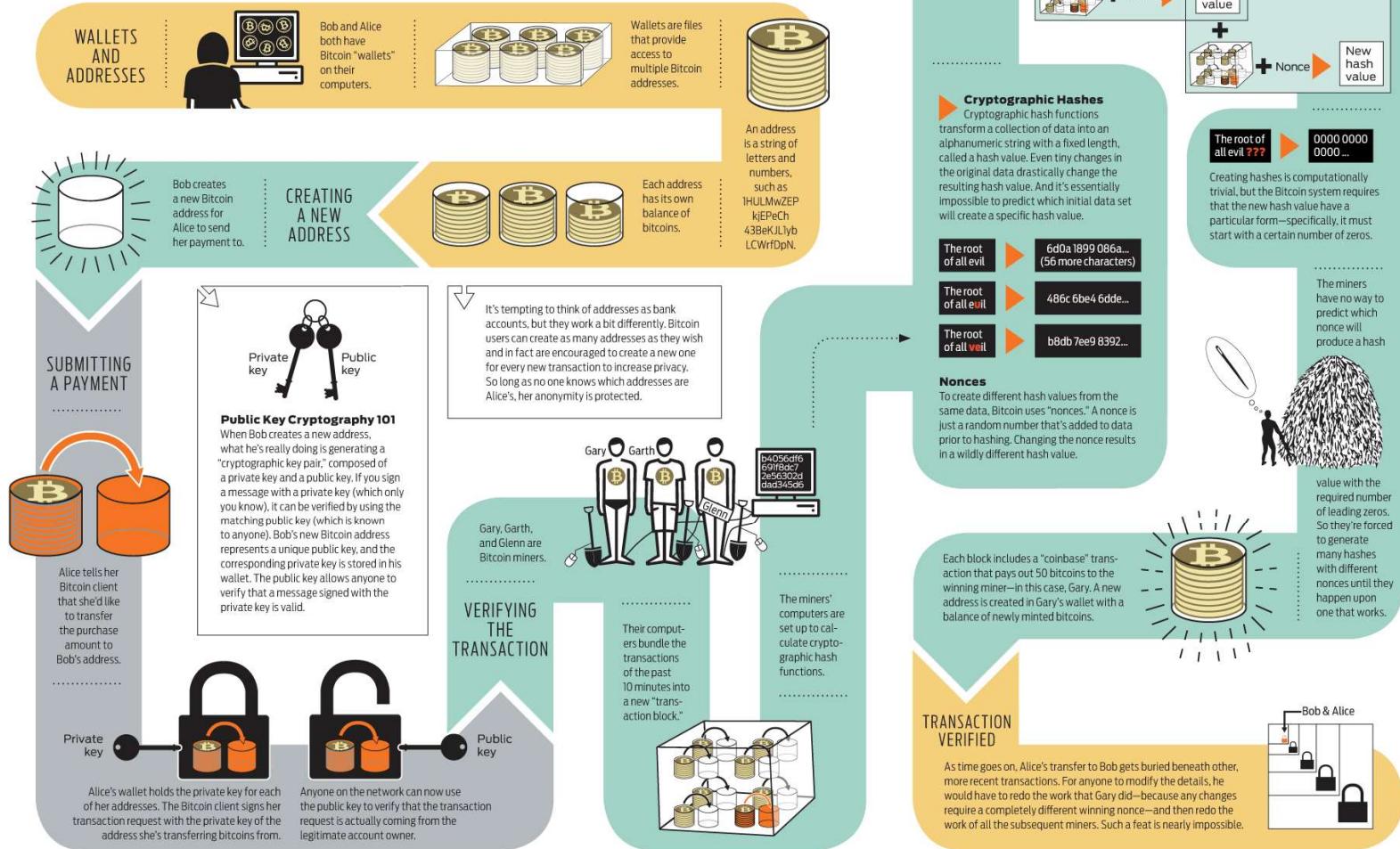
FT



THE HONEYNET PROJECT

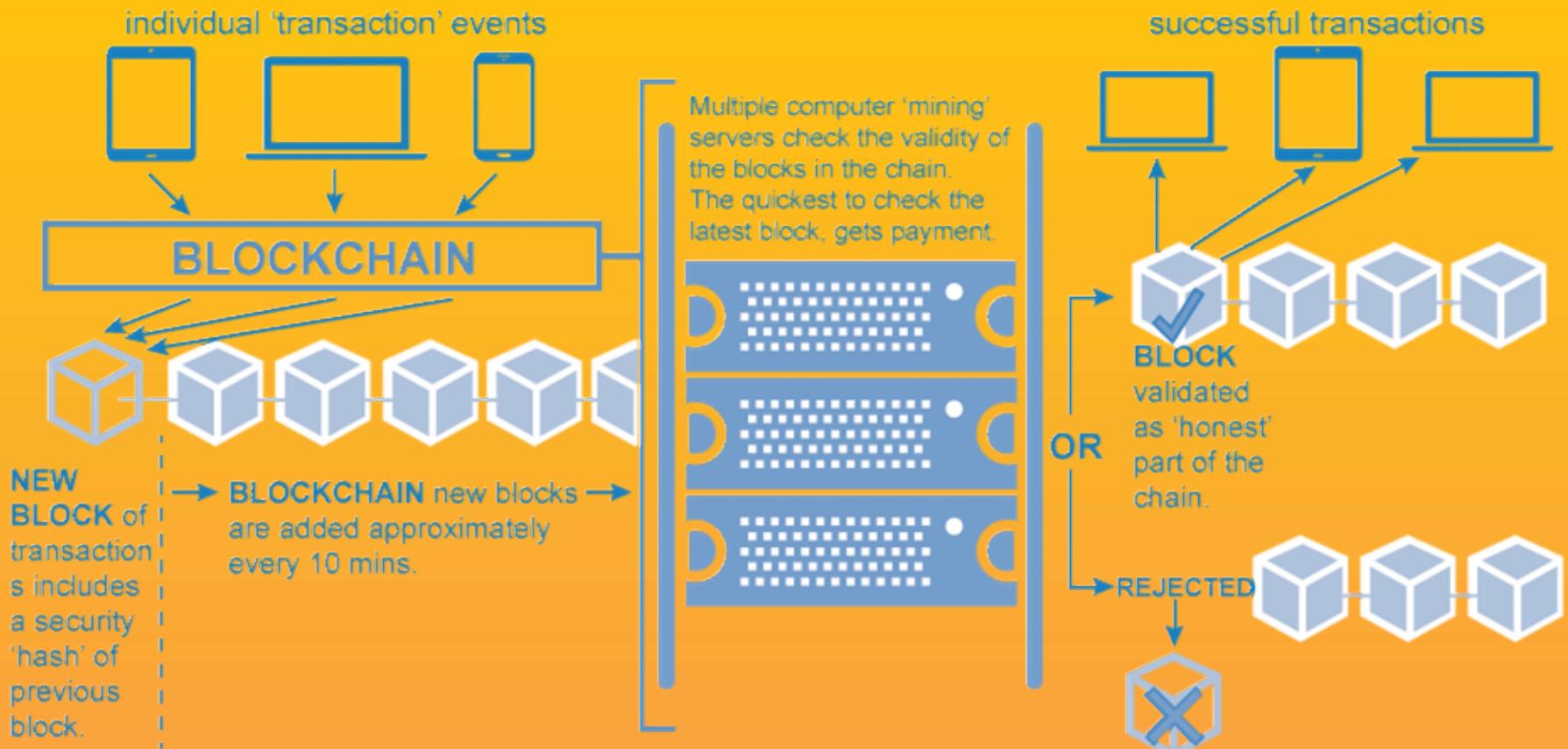
How a Bitcoin transaction works

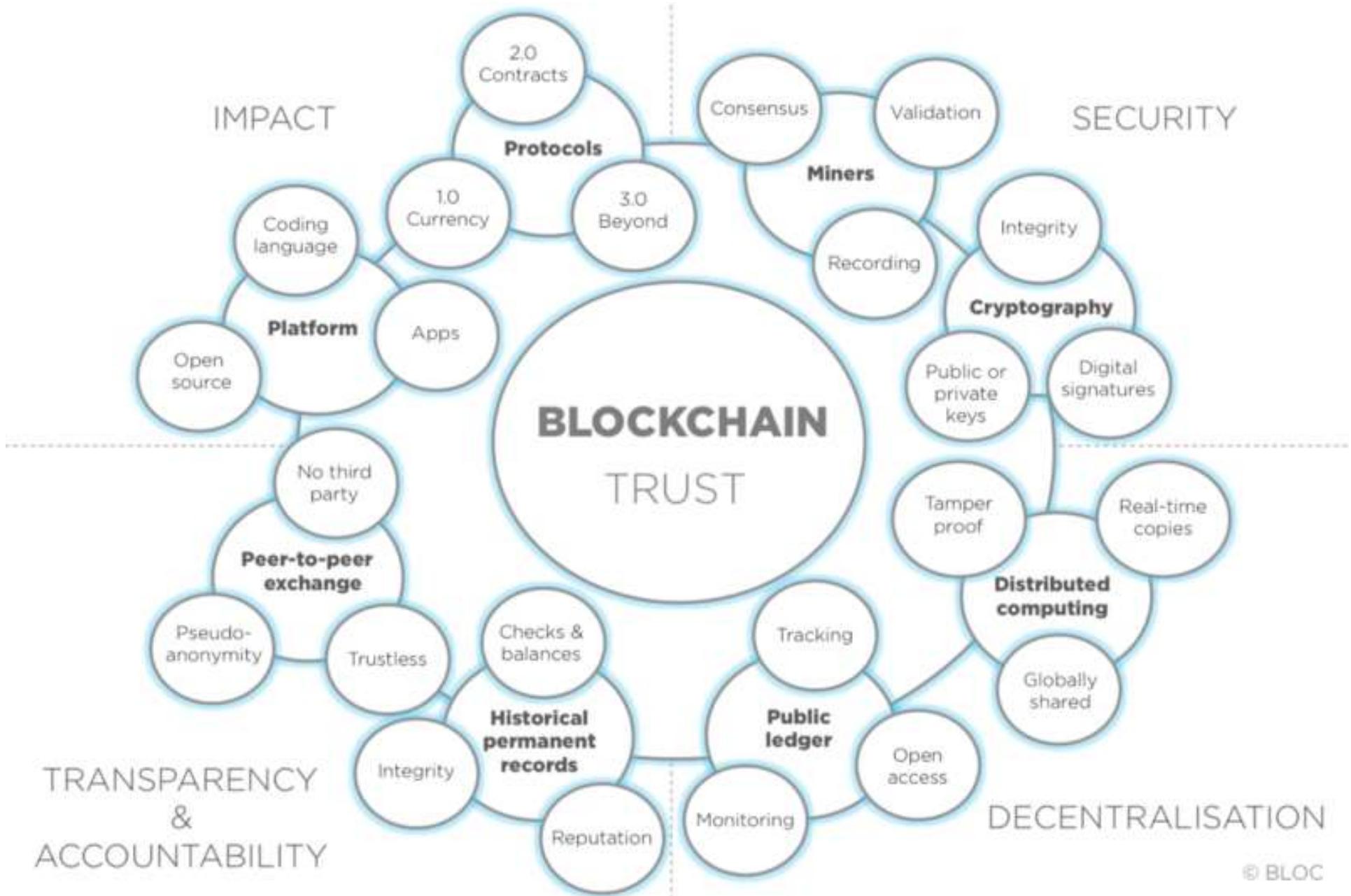
Bob, an online merchant, decides to begin accepting bitcoins as payment. Alice, a buyer, has bitcoins and wants to purchase merchandise from Bob.



THE HONEYNET PROJECT

Blockchain Overview

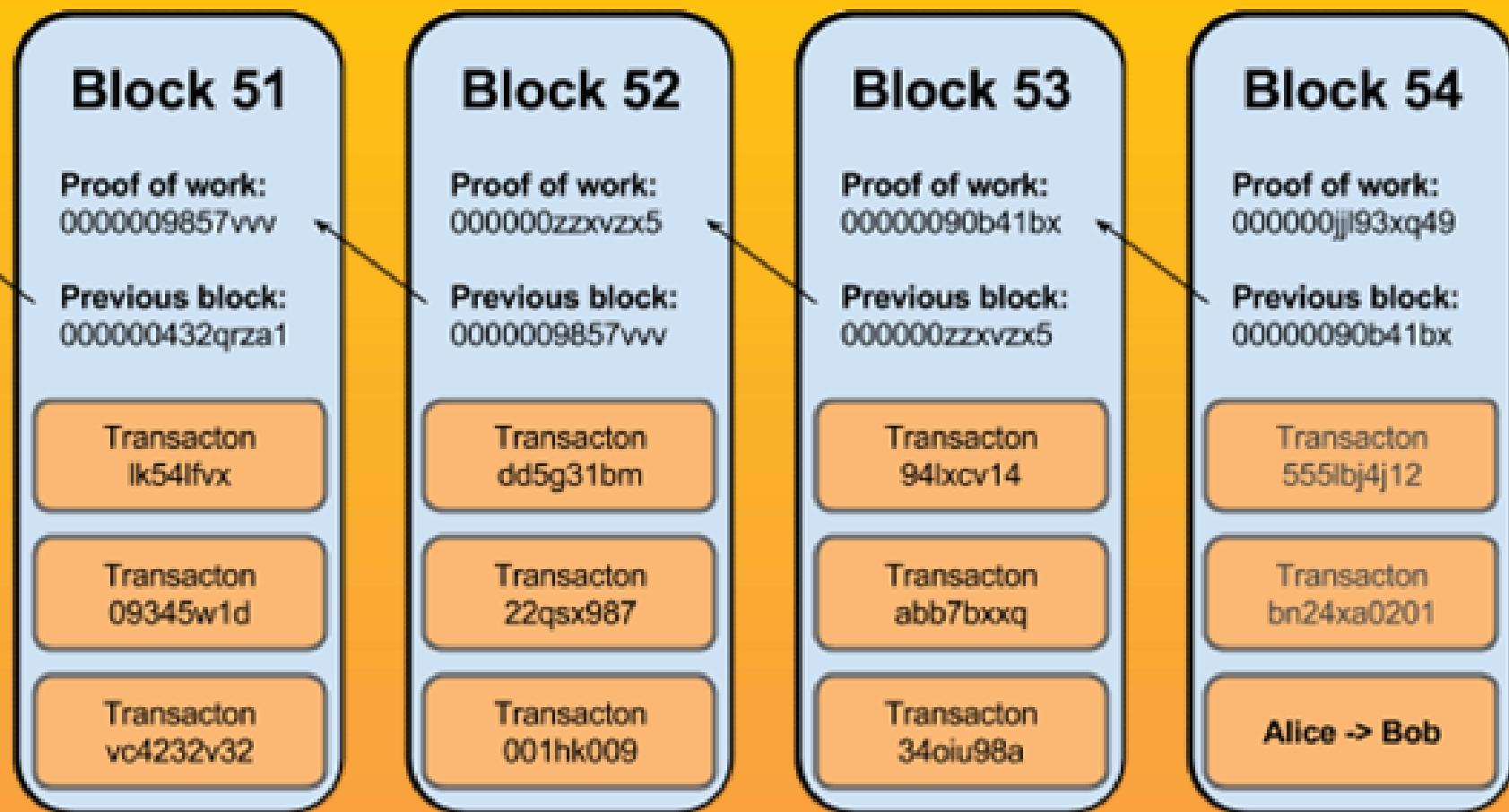




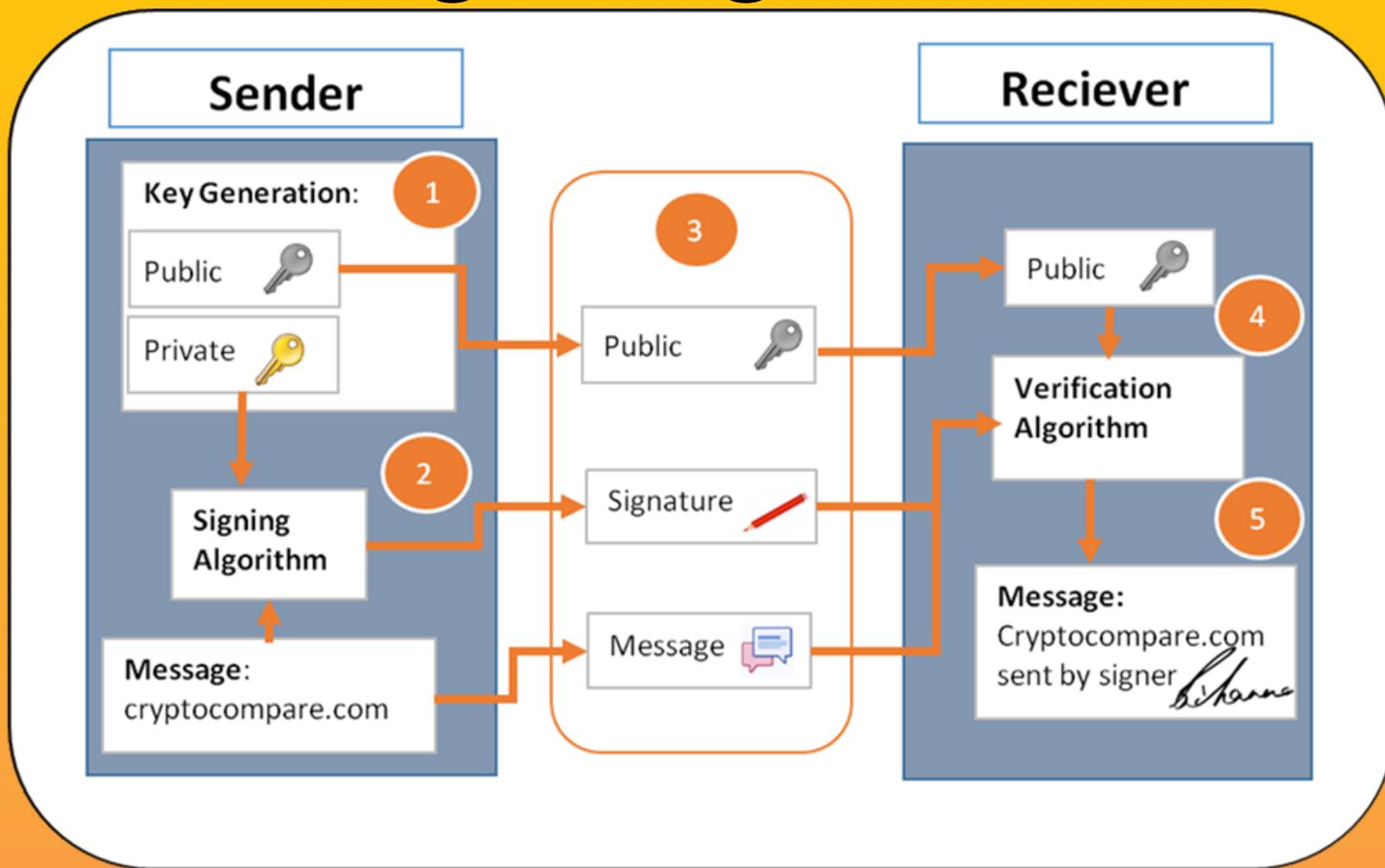
THE HONEYNET PROJECT

© BLOC

Chain of Blocks

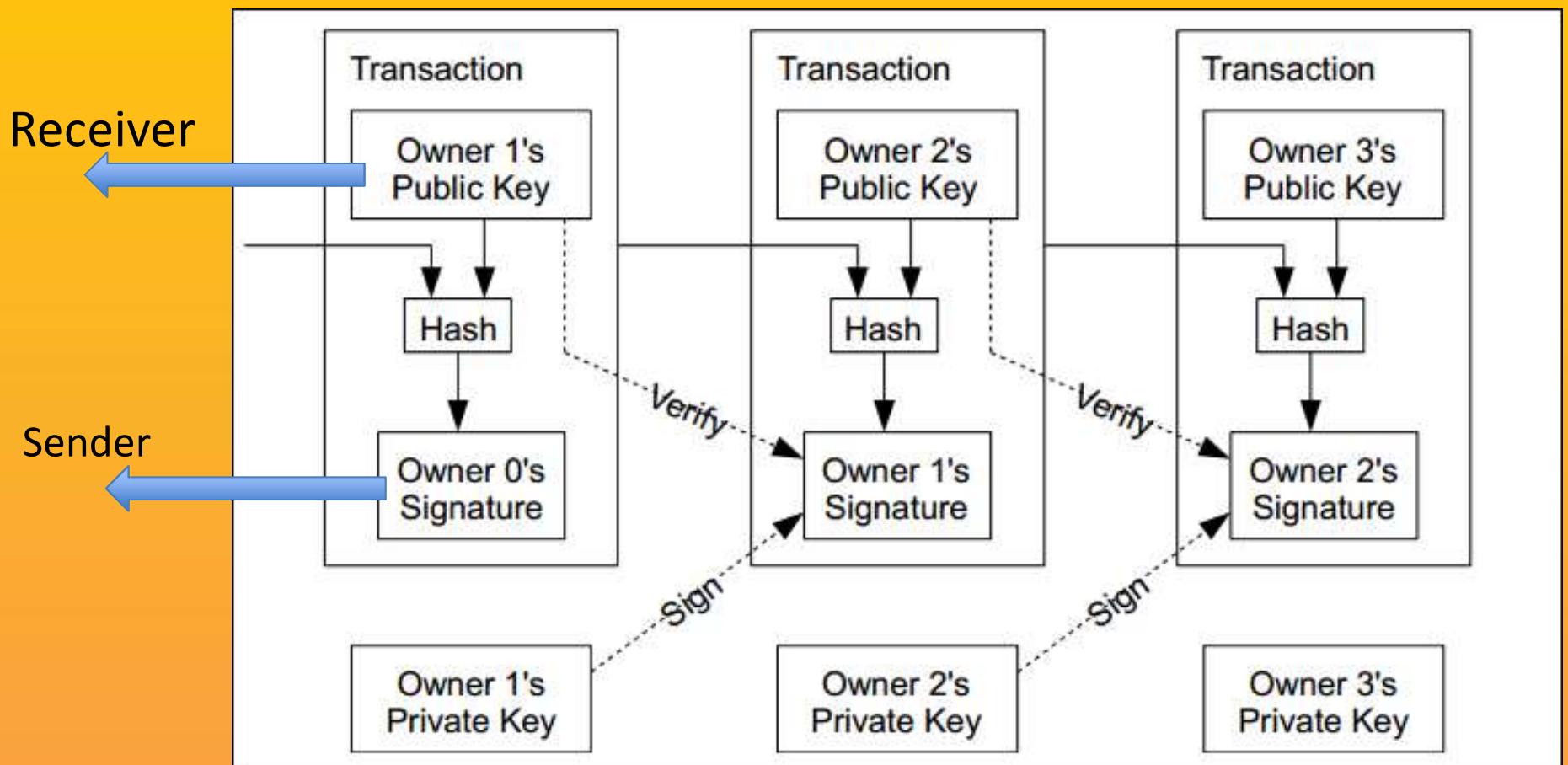


Digital Signature



THE HONEYNET PROJECT

Bitcoin Transaction



Mining

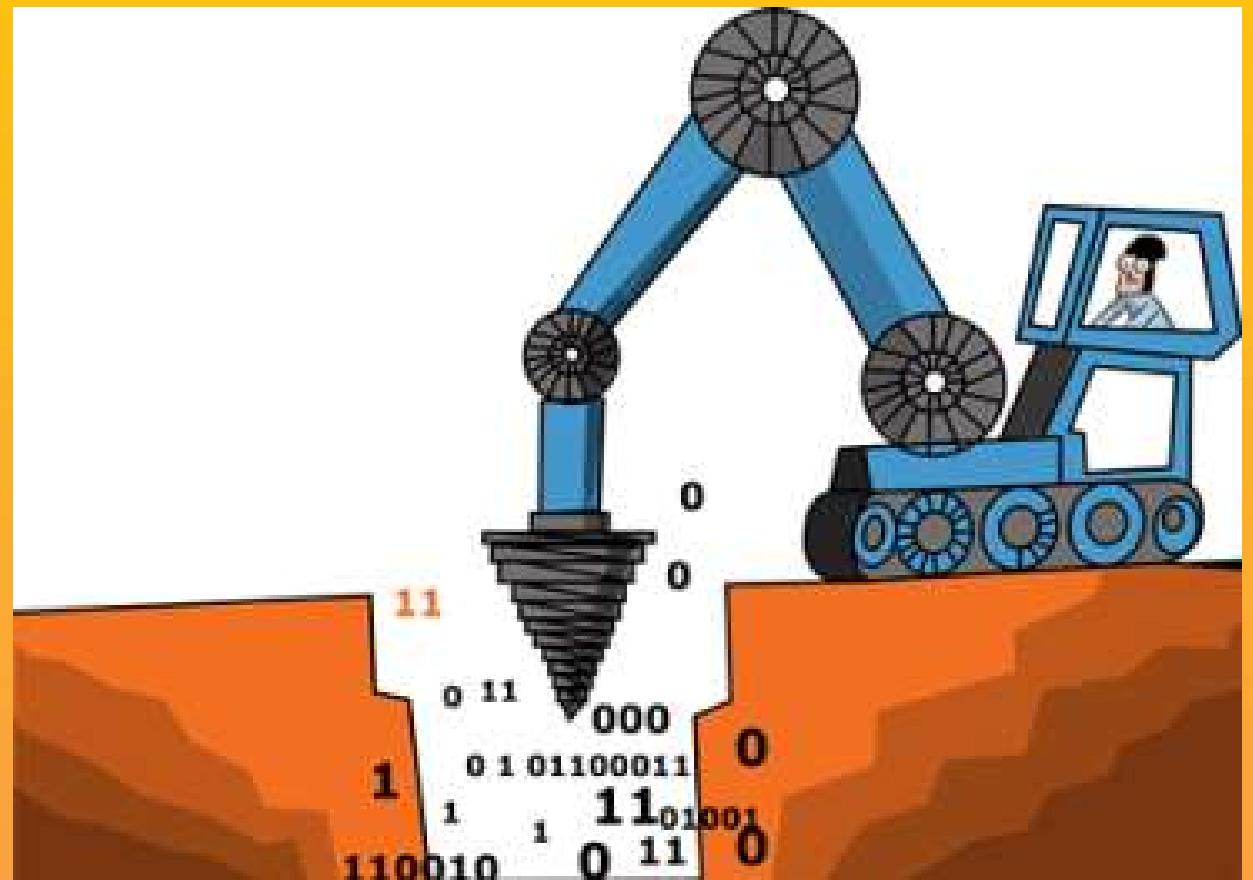


THE HONEYNODE PROJECT

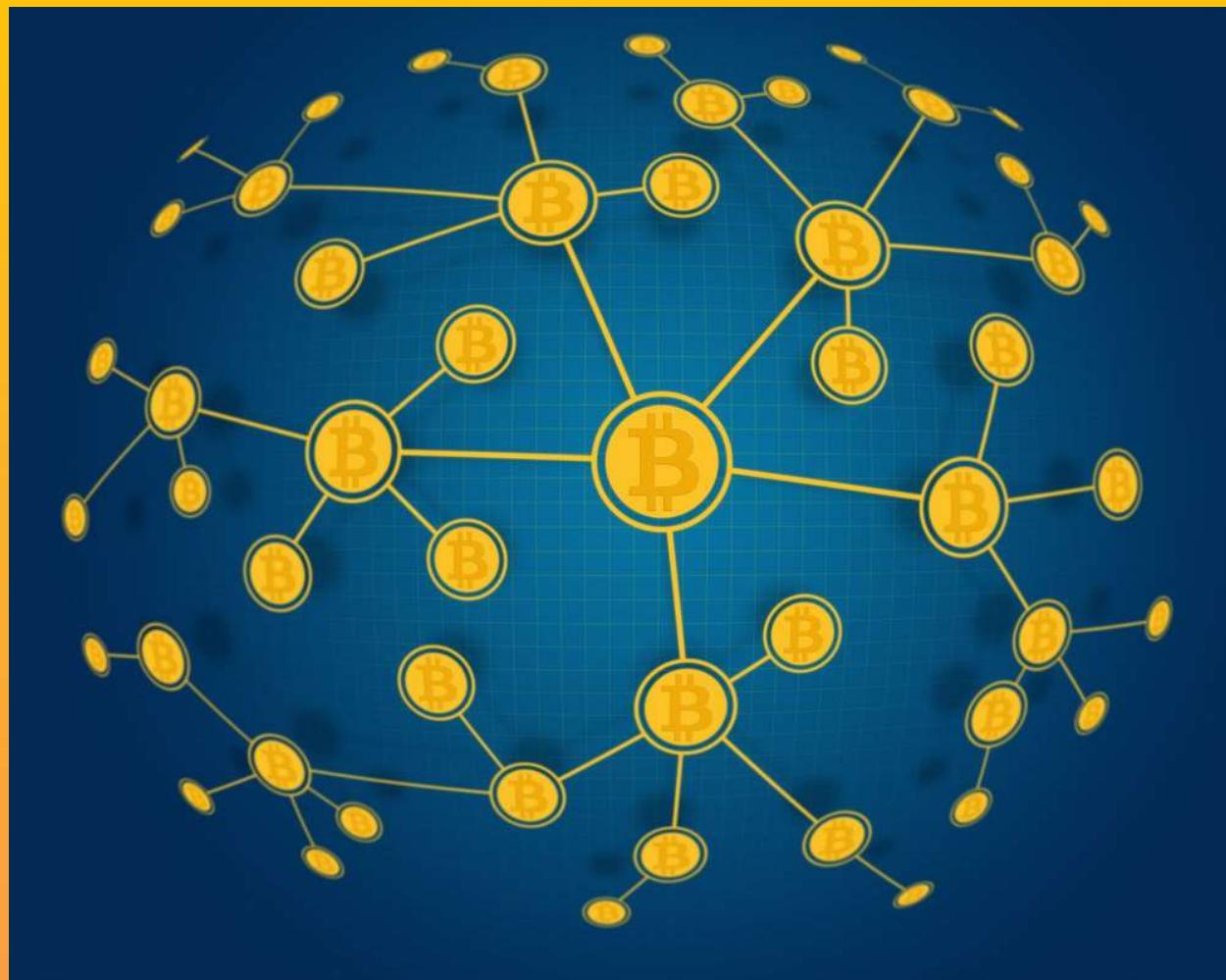
Proof of Work (PoW)

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.



THE HONEYNET PROJECT

Financial Fraud

- ID Theft
- Cyber Security
- Credit Card Fraud



THE HONEYNET PROJECT

Financial Fraud (2)

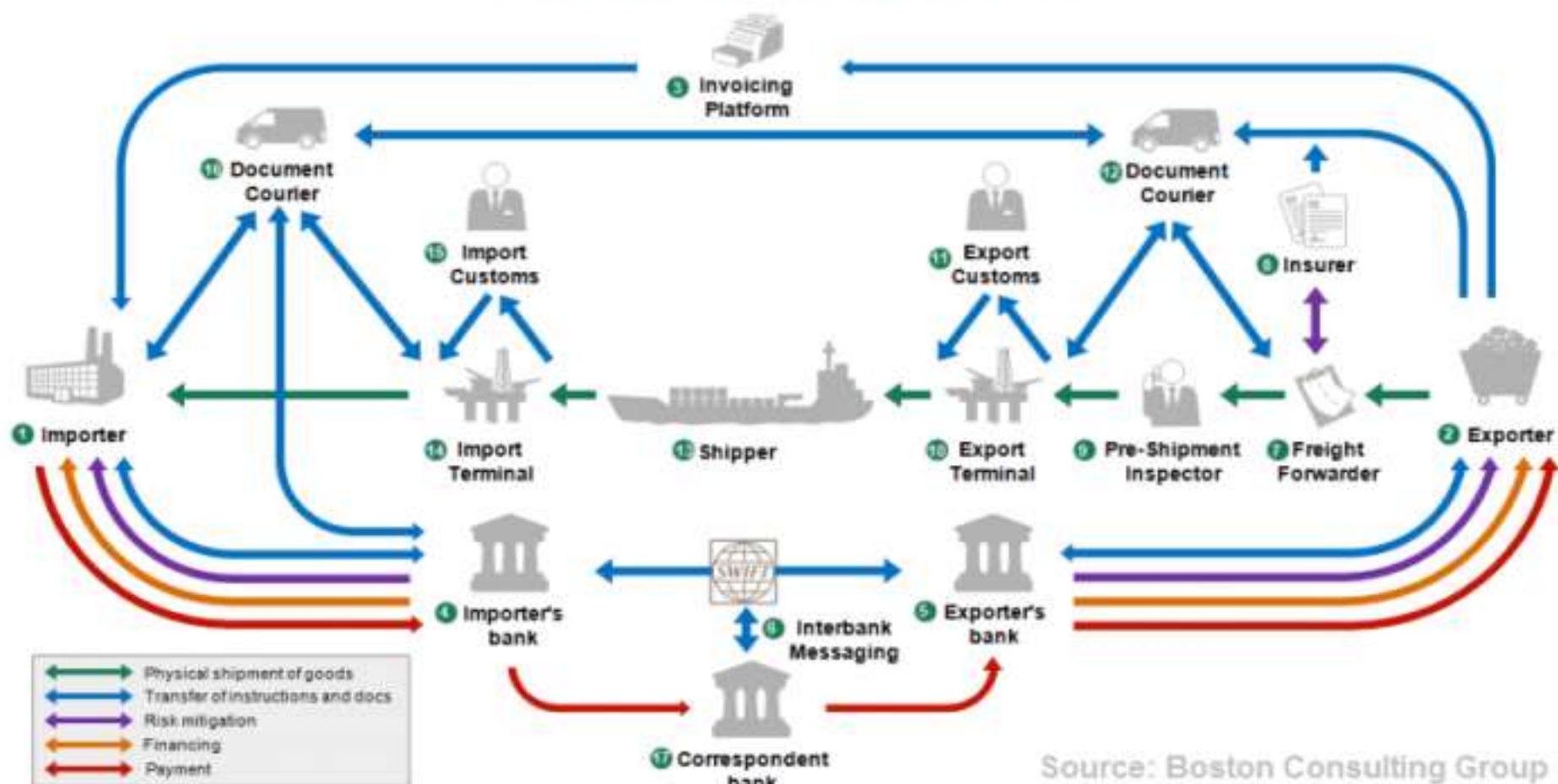
- Falsifying data
 - Enron
 - WorldCom
- Fake document



THE HONEYNET PROJECT

Financial Scheme

The international trade “ecosystem”



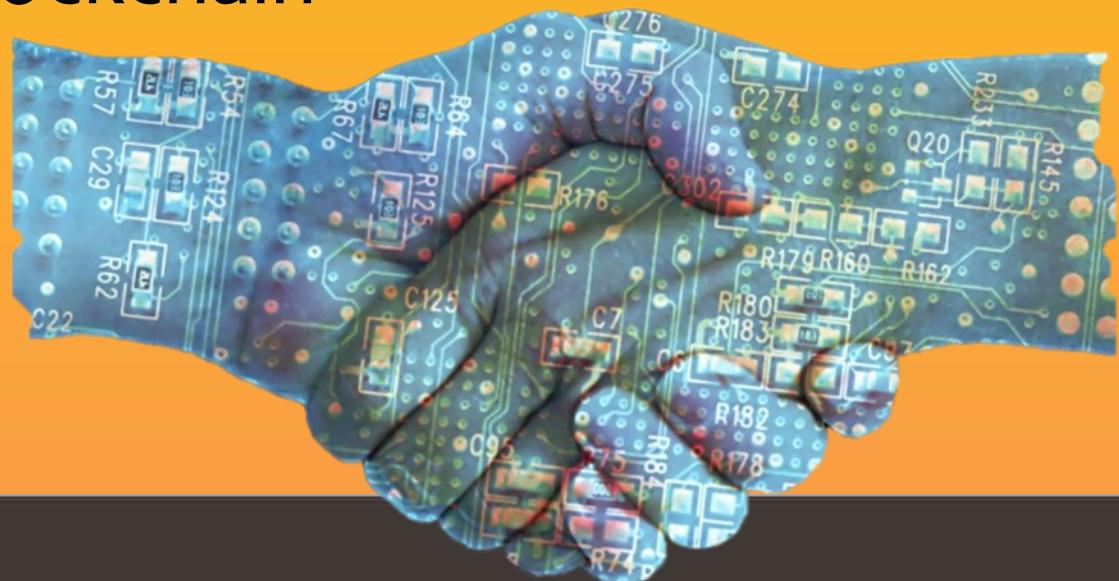
Source: Boston Consulting Group



THE HONEYNET PROJECT

Employing Blockchain in Finance Industry

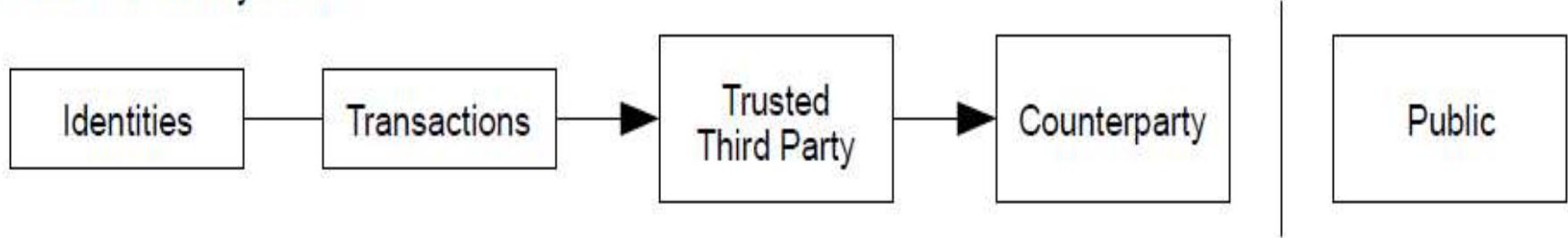
- Transparent – visible ledger
- Trustless – no central authority needed
- Cryptography – digital signature
- Permanent – blockchain



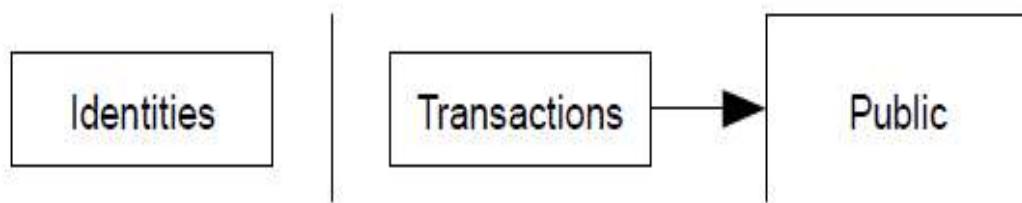
Privacy Model

- Disconnecting Identities and Transactions

Traditional Privacy Model

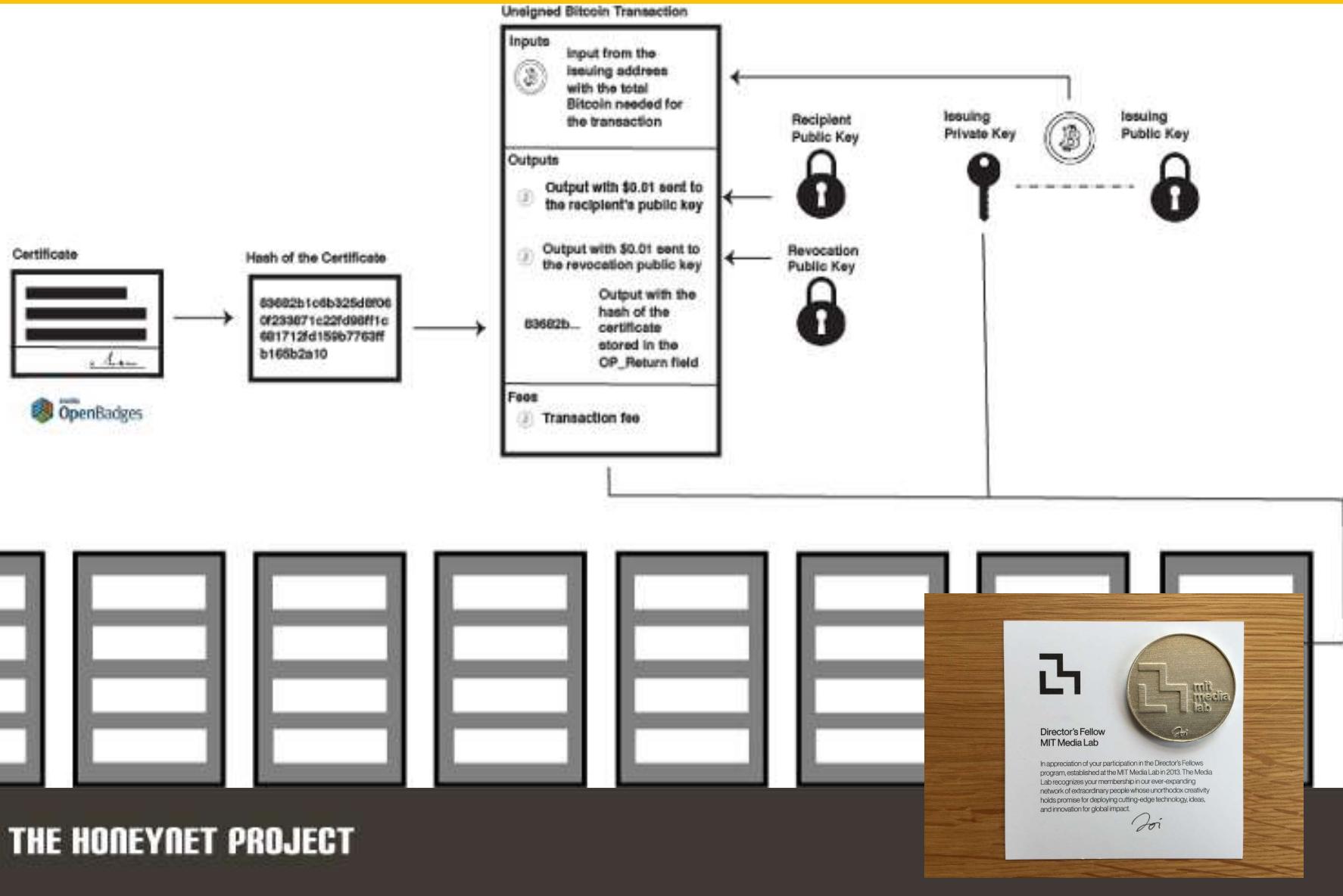


New Privacy Model



THE HONEYNET PROJECT

Blockchain-based Digital Certificate



Multisignature



THE HONEYNET PROJECT

Visible Transactions

Transaction 7957a35fe64f80d234d76d83a2a8f1a0d8149a41d81de548f0a65a8a999f6f18

INPUTS From
From (previous transactions Joe has received):
Joe 0.1005 BTC

OUTPUTS To
Output #0 Alice's Address 0.1000 BTC (spent)
Transaction Fees: 0.0005 BTC

Transaction 0627052b6f28912f2703066a912ea577f2ce4da4caa5a5fb8a57286c345c2f2

INPUTS From
7957a35fe64f80d234d76d83a2a8f1a0d8149a41d81de548f0a65a8a999f6f18 : 0
Alice 0.1000 BTC

OUTPUTS To
Output #0 Bob's Address 0.0150 BTC (spent)
Output #1 Alice's Address (change) 0.0845 BTC (unspent)
Transaction Fees: 0.0005 BTC

Transaction 2bbac8bb3a57a2363407ac8c16a67015ed2e88a4388af58cf90299e0744d3de4

INPUTS From
0627052b6f28912f2703066a912ea577f2ce4da4caa5a5fb8a57286c345c2f2 : 0
Bob 0.0150 BTC

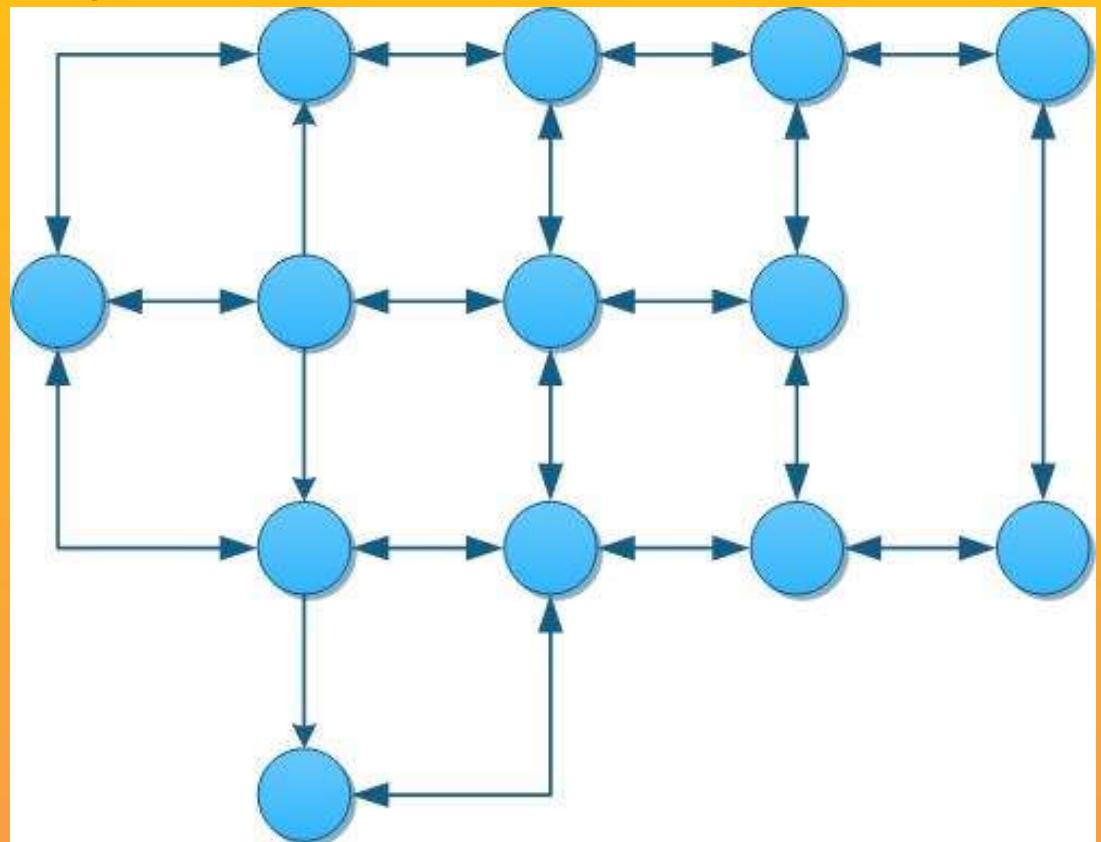
OUTPUTS To
Output #0 Gopesh's Address 0.0100 BTC (unspent)
Output #1 Bob's Address (change) 0.0845 BTC (unspent)
Transaction Fees: 0.0005 BTC



THE HONEYNET PROJECT

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



THE HONEYNET PROJECT

...And Many More!

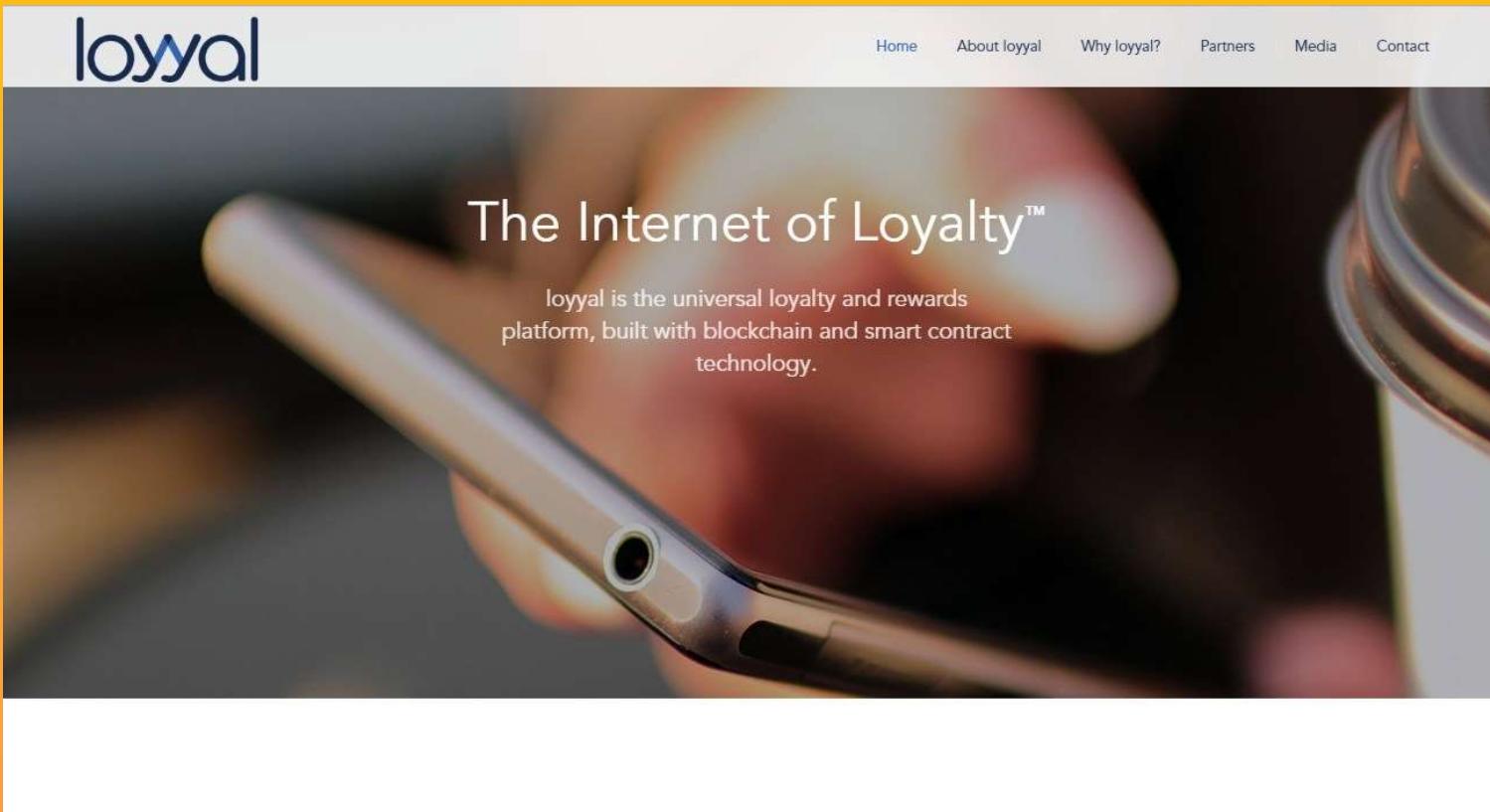
- Ring Signature (Monero)
- Smart Contract (Ethereum)



THE HONEYNET PROJECT

Current Usage

- Loyalty Program



The image shows the homepage of the Loyyal website. The header features the word "loyyal" in a blue, lowercase, sans-serif font. To the right of the logo are navigation links: Home, About loygal, Why loygal?, Partners, Media, and Contact. Below the header is a large, blurred background image of a hand holding a smartphone. Overlaid on this image is the text "The Internet of Loyalty™" in a white, sans-serif font. Underneath this, a smaller text block reads: "loygal is the universal loyalty and rewards platform, built with blockchain and smart contract technology." The bottom portion of the page has a solid black background.



THE HONEYNET PROJECT

Recent Development

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



THE HONEYNET PROJECT



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.





THE HONEYNET PROJECT



Indonesia Honeynet Project