

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



THE HONEYNET PROJECT



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

— *Andreas Antonopoulos* —

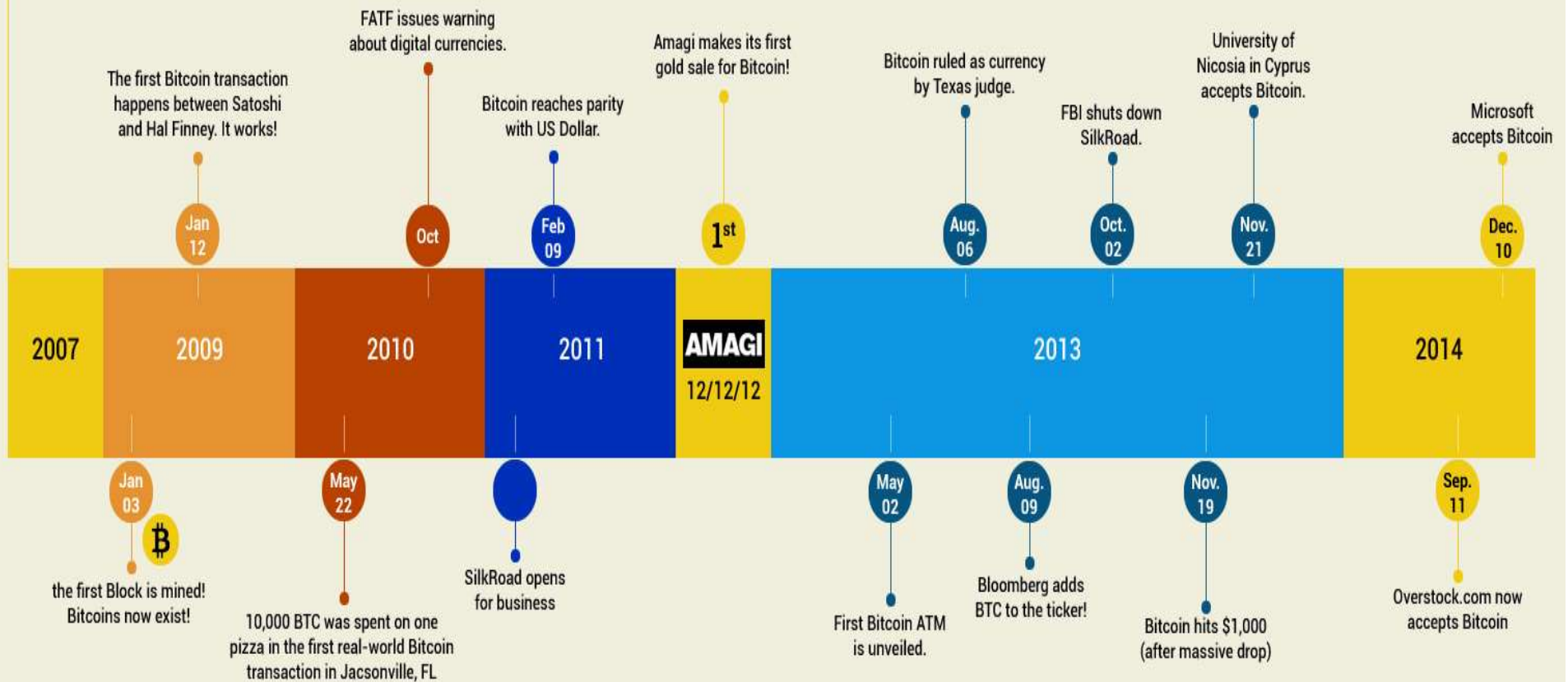
AZ QUOTES



THE HONEYNET PROJECT

History of Bitcoin

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

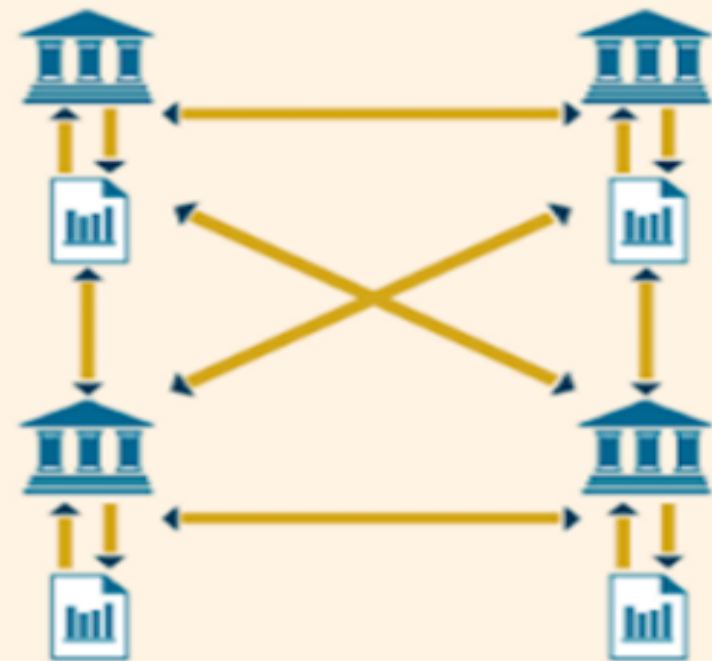


THE HONEYNET PROJECT

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.

WALLETS AND ADDRESSES



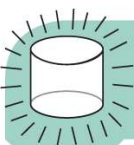
Bob and Alice both have Bitcoin "wallets" on their computers.



Wallets are files that provide access to multiple Bitcoin addresses.



An address is a string of letters and numbers, such as 1HULmWZEPkJEPC438eKJLybLCWfDpN.



Bob creates a new Bitcoin address for Alice to send her payment to.

CREATING A NEW ADDRESS



Each address has its own balance of bitcoins.

SUBMITTING A PAYMENT



Alice tells her Bitcoin client that she'd like to transfer the purchase amount to Bob's address.



Public Key Cryptography 101
When Bob creates a new address, what he's really doing is generating a "cryptographic key pair," composed of a private key and a public key. If you sign a message with a private key (which only you know), it can be verified by using the matching public key (which is known to anyone). Bob's new Bitcoin address represents a unique public key, and the corresponding private key is stored in his wallet. The public key allows anyone to verify that a message signed with the private key is valid.

It's tempting to think of addresses as bank accounts, but they work a bit differently. Bitcoin users can create as many addresses as they wish and in fact are encouraged to create a new one for every new transaction to increase privacy. So long as no one knows which addresses are Alice's, her anonymity is protected.

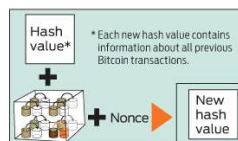
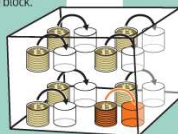


Gary, Garth, and Glenn are Bitcoin miners.

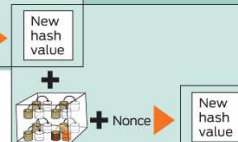
VERIFYING THE TRANSACTION

Their computers bundle the transactions of the past 10 minutes into a new "transaction block."

The miners' computers are set up to calculate cryptographic hash functions.



* Each new hash value contains information about all previous Bitcoin transactions.



The mining computers calculate new hash values based on a combination of the previous hash value, the new transaction block, and a nonce.

Cryptographic Hashes

Cryptographic hash functions transform a collection of data into an alphanumeric string with a fixed length, called a hash value. Even tiny changes in the original data drastically change the resulting hash value. And it's essentially impossible to predict which initial data set will create a specific hash value.

The root of all evil	6d0a 1899 086a... (56 more characters)
The root of all evil	486c 6be4 6dde...
The root of all evil	b8db 7ee9 8392...

Nonces

To create different hash values from the same data, Bitcoin uses "nonces." A nonce is just a random number that's added to data prior to hashing. Changing the nonce results in a wildly different hash value.

The root of all evil ???

Creating hashes is computationally trivial, but the Bitcoin system requires that the new hash value have a particular form—specifically, it must start with a certain number of zeros.



The miners have no way to predict which nonce will produce a hash

value with the required number of leading zeros. So they're forced to generate many hashes with different nonces until they happen upon one that works.



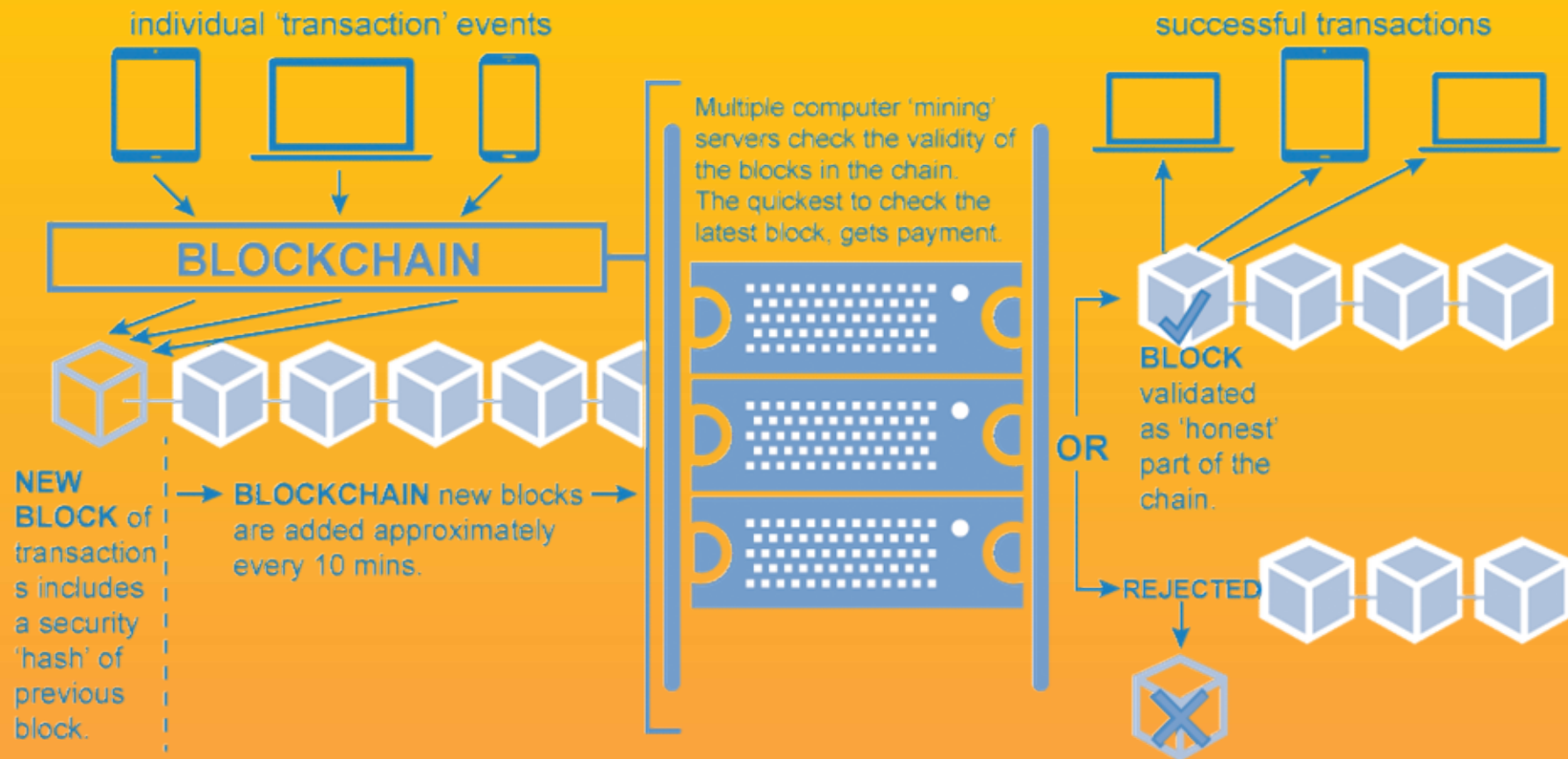
Each block includes a "coinbase" transaction that pays out 50 bitcoins to the winning miner—in this case, Gary. A new address is created in Gary's wallet with a balance of newly minted bitcoins.

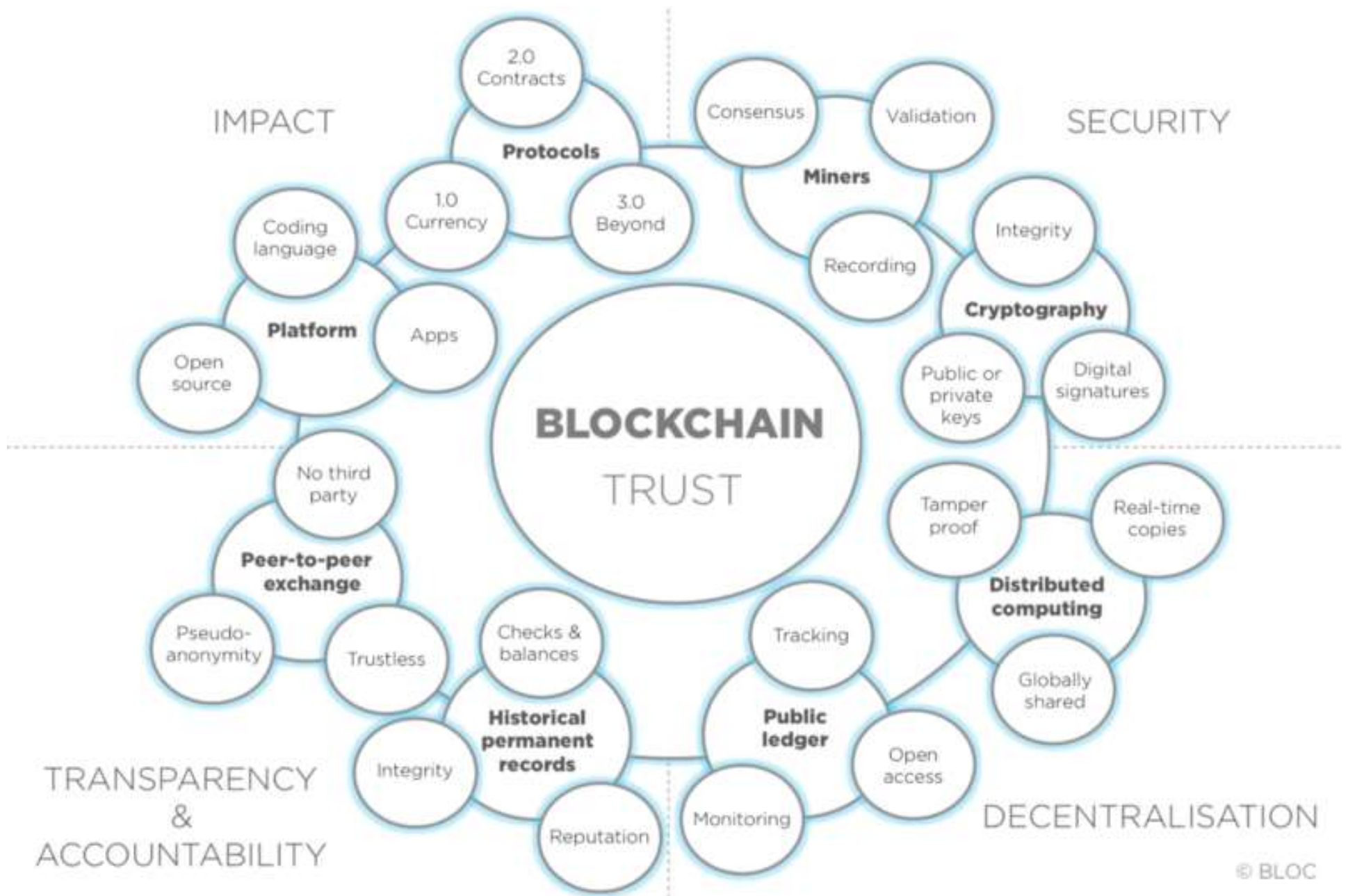
TRANSACTION VERIFIED

As time goes on, Alice's transfer to Bob gets buried beneath other, more recent transactions. For anyone to modify the details, he would have to redo the work that Gary did—because any changes require a completely different winning nonce—and then redo the work of all the subsequent miners. Such a feat is nearly impossible.



Blockchain Overview



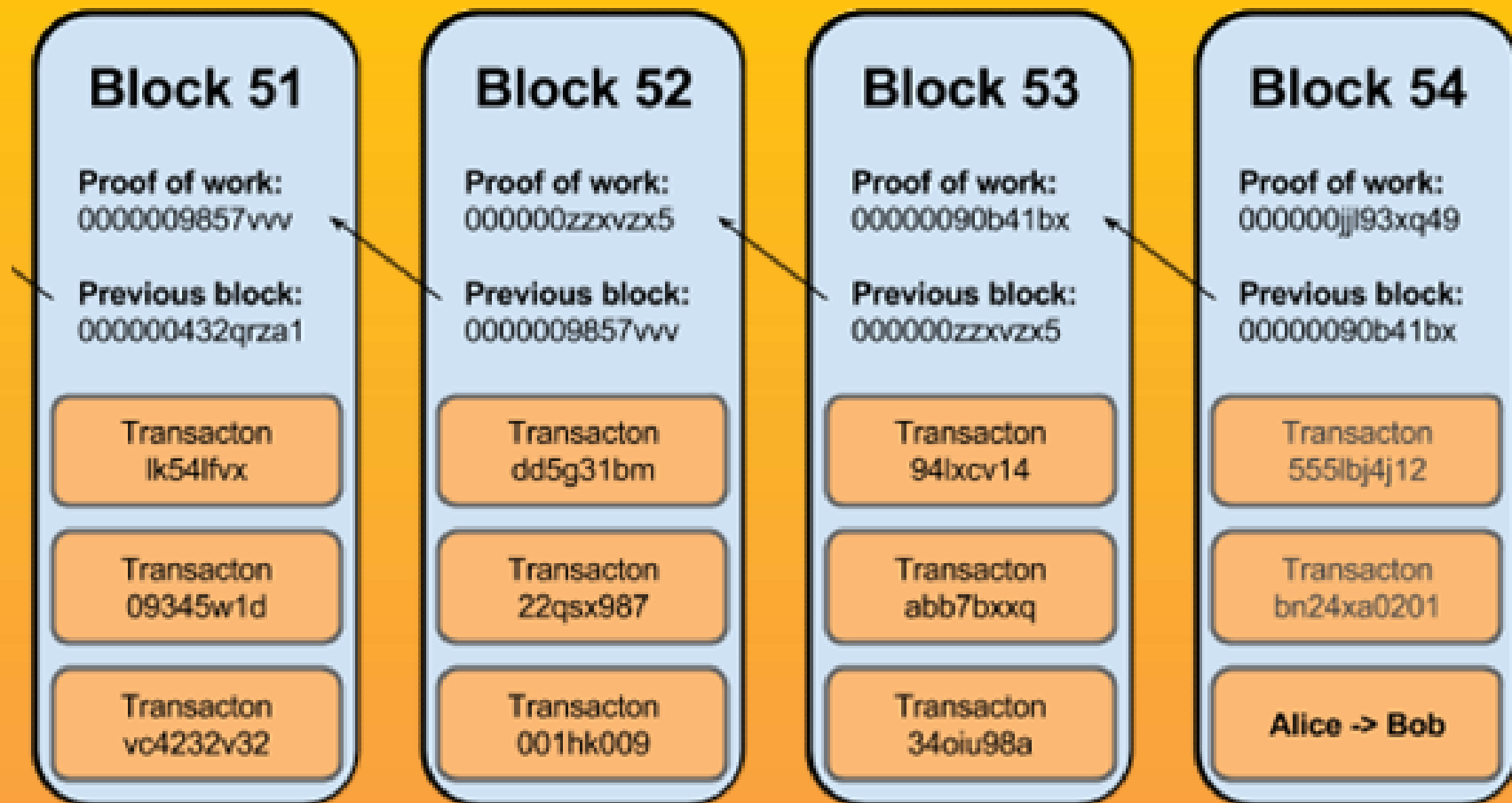


© BLOC

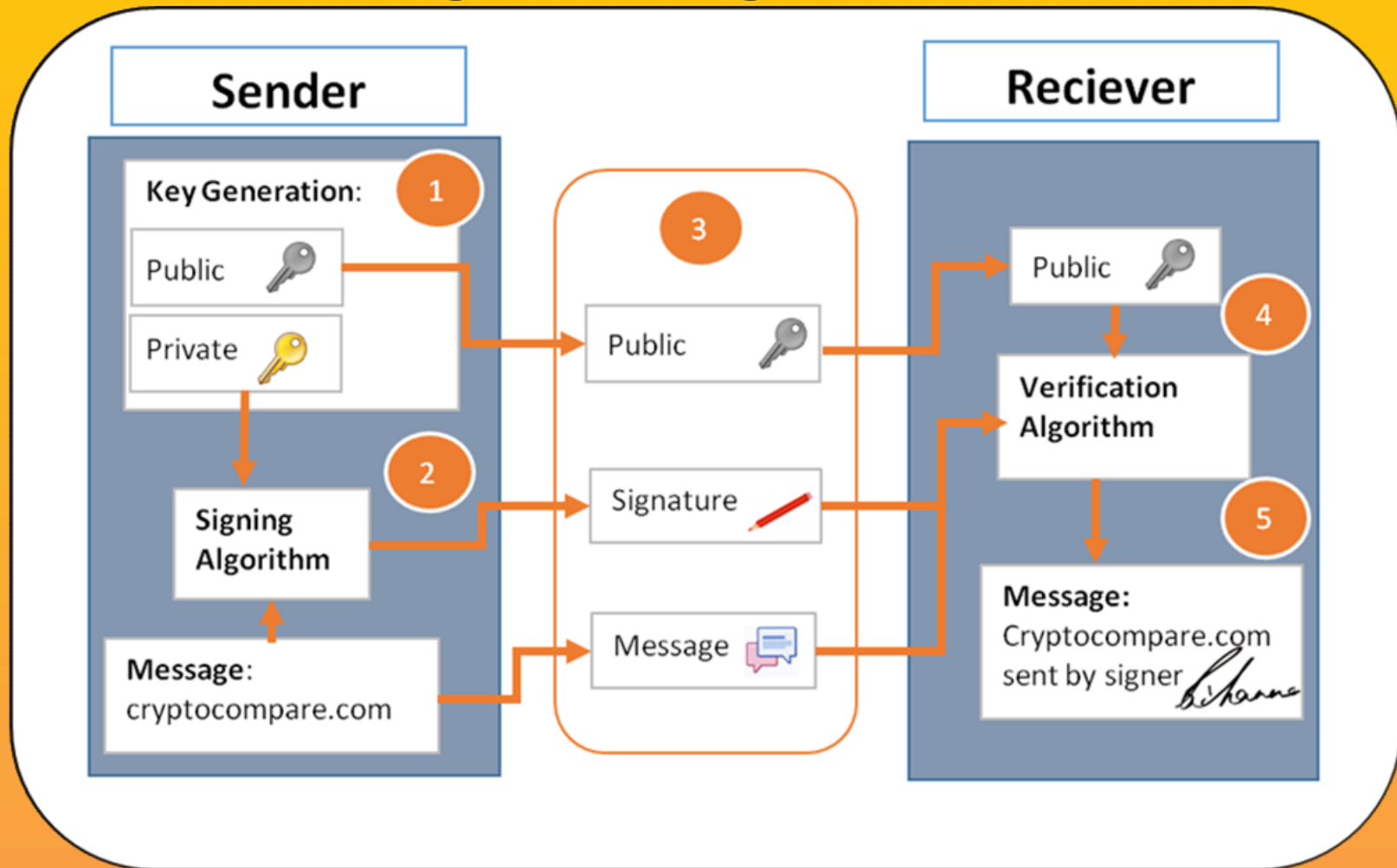


THE HONEYNET PROJECT

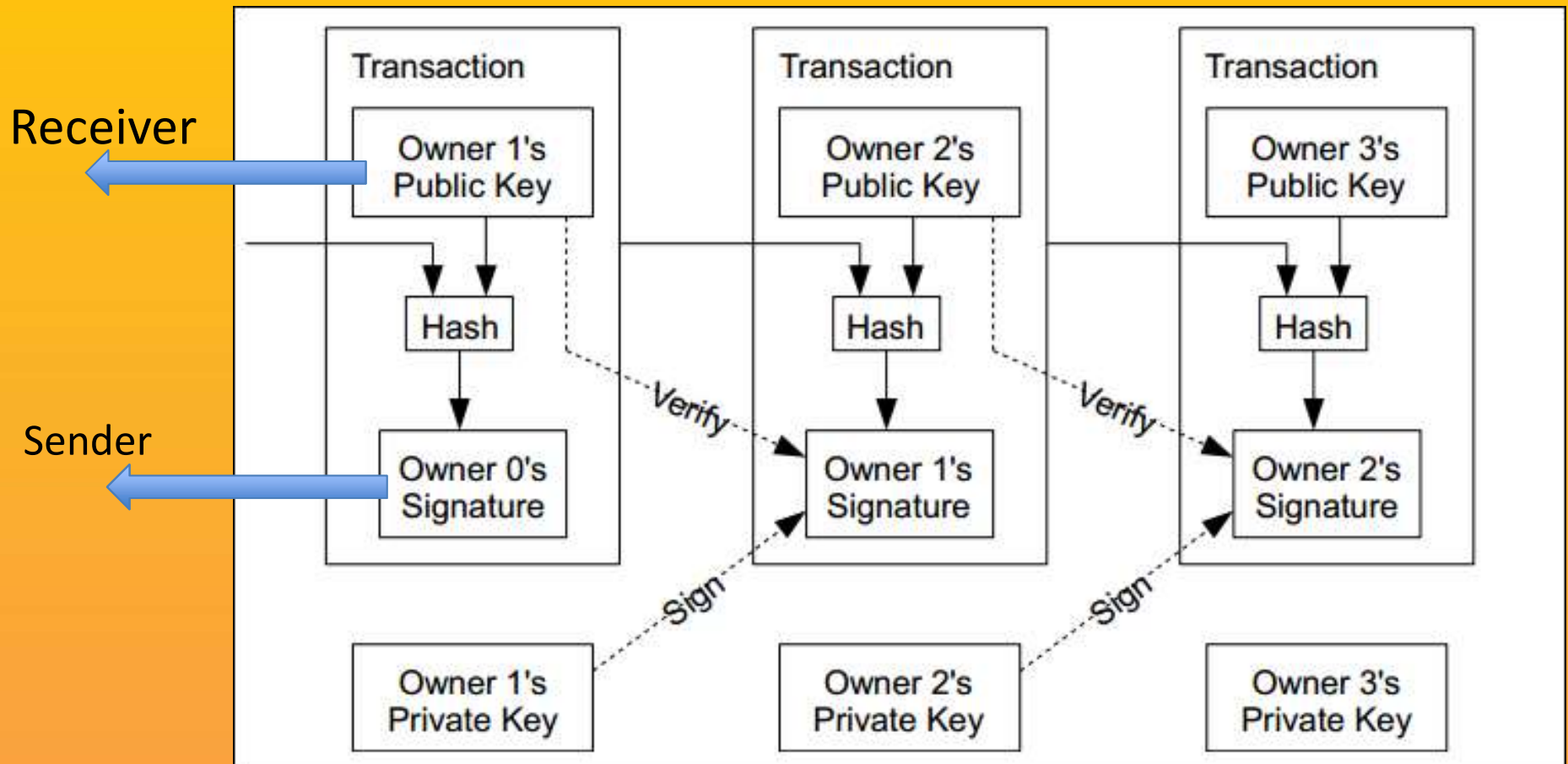
Chain of Blocks



Digital Signature



Bitcoin Transaction



Mining

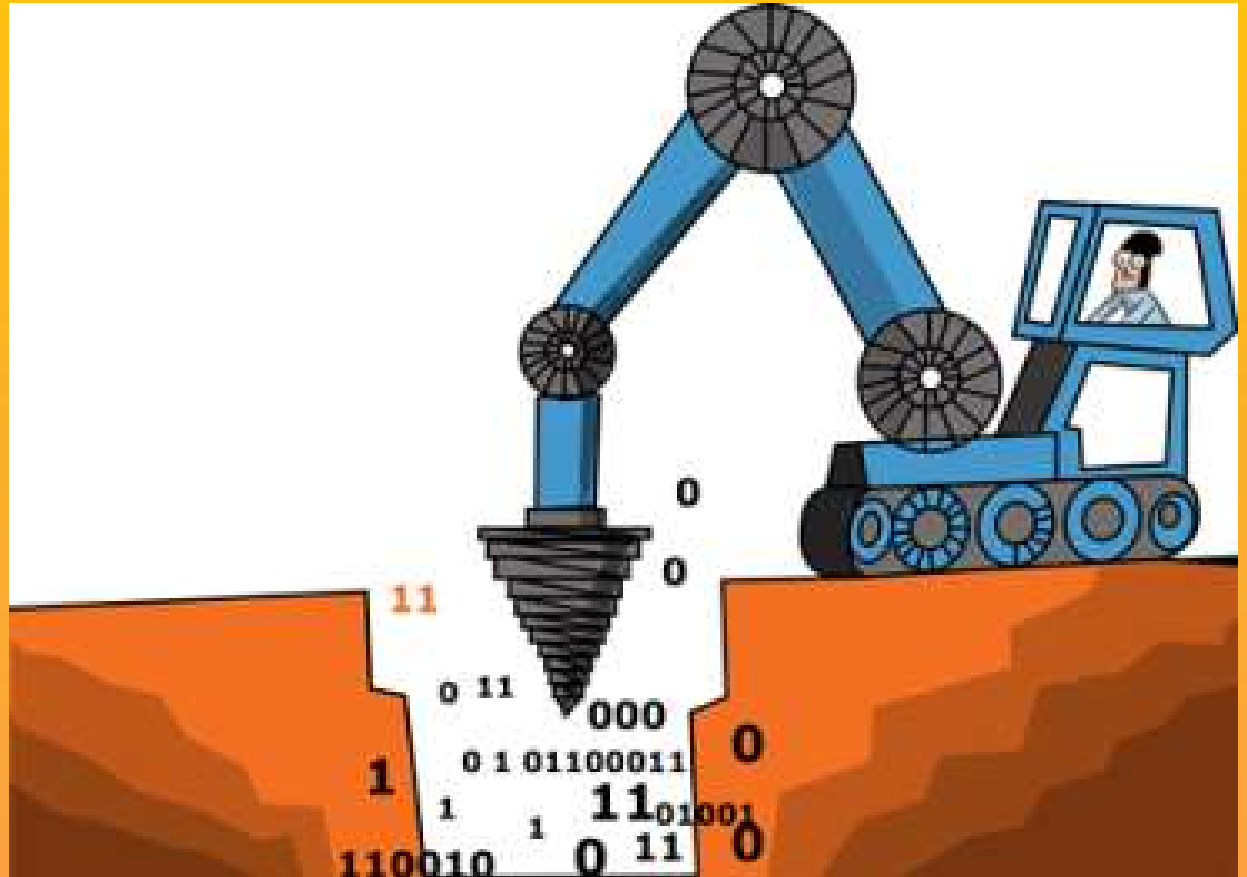


THE HONEYNET PROJECT

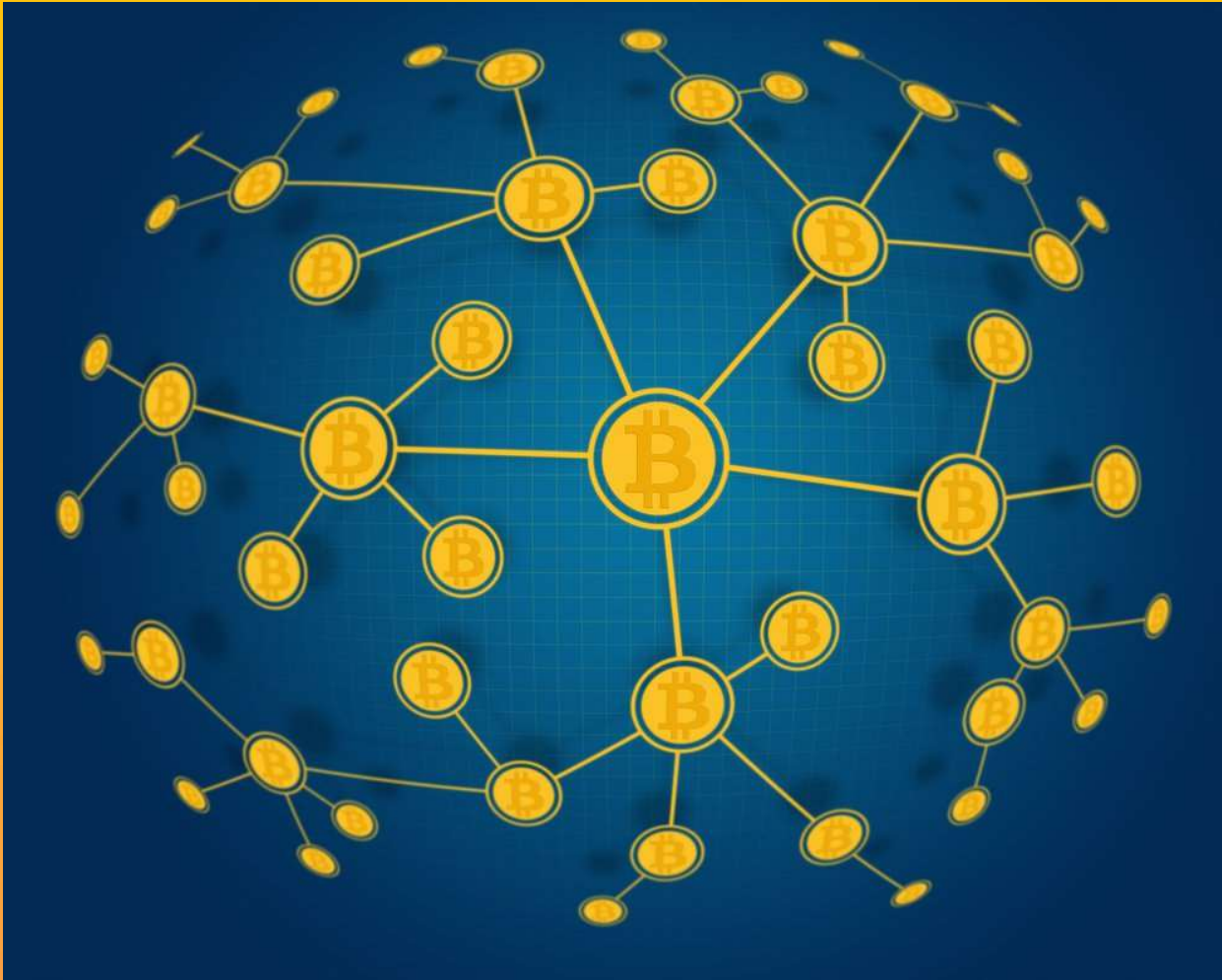
Proof of Work (PoW)

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.



Financial Fraud

- ID Theft
- Cyber Security
- Credit Card Fraud



THE HONEYNET PROJECT

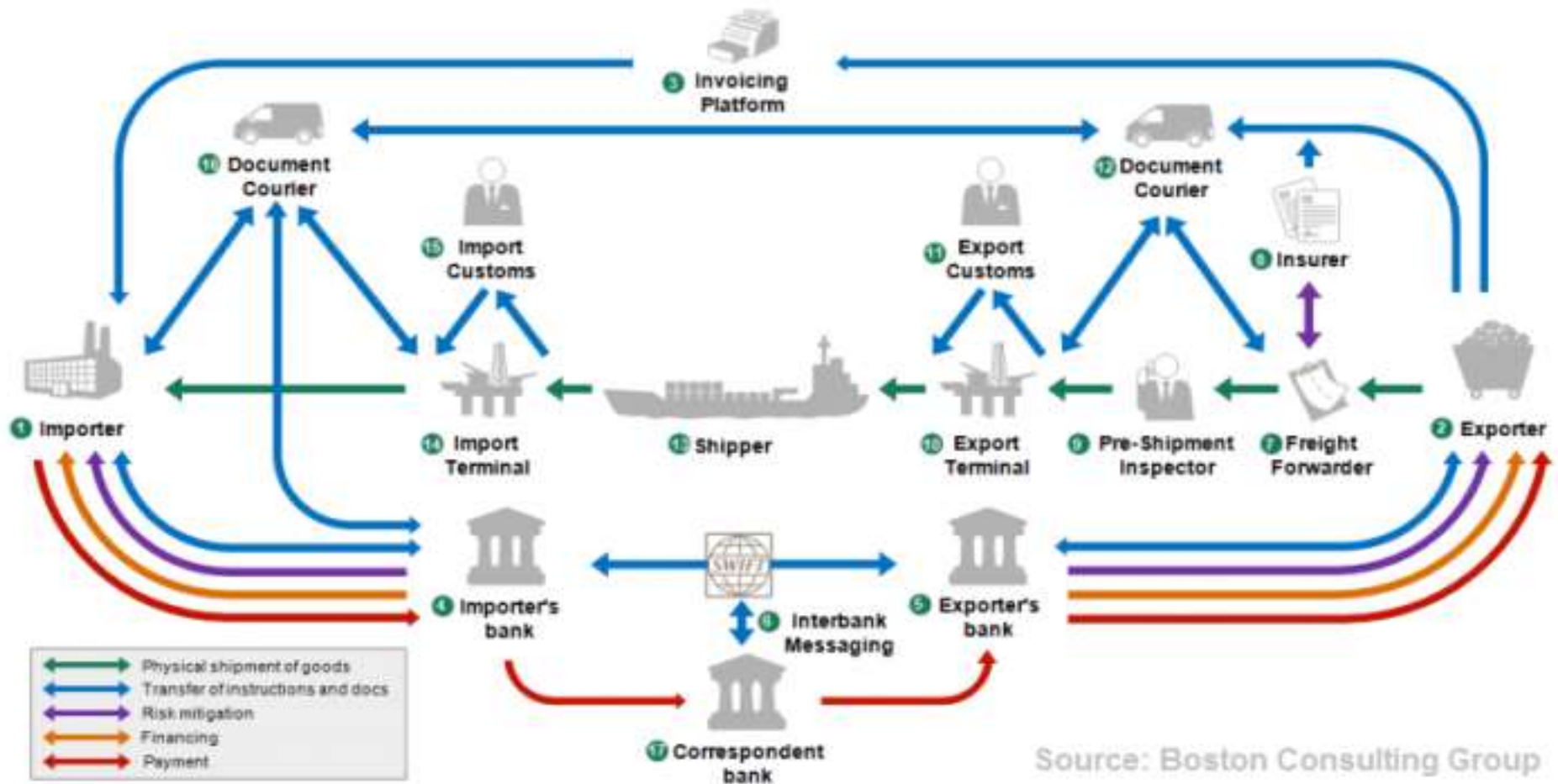
Financial Fraud (2)

- Falsifying data
 - Enron
 - WorldCom
- Fake document



Financial Scheme

The international trade “ecosystem”



Employing Blockchain in Finance Industry

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



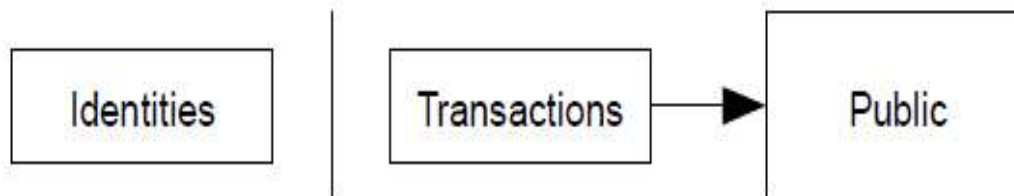
Privacy Model

- Disconnecting Identities and Transactions

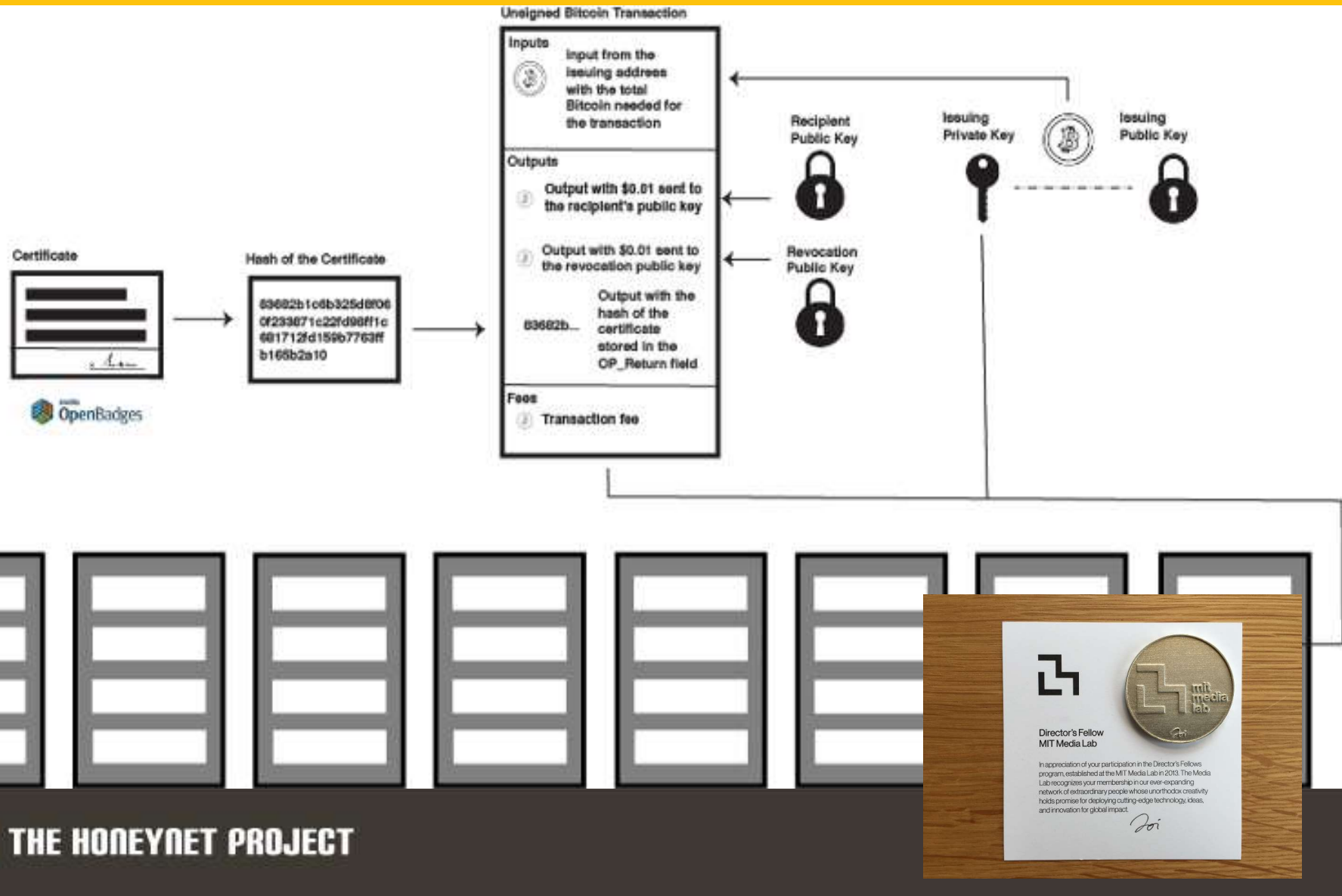
Traditional Privacy Model



New Privacy Model



Blockchain-based Digital Certificate



Multisignature



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 0627052b6f28912f2703066a912ea577f2ce4da4caa5a5fbd8a57286c345c2f2

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

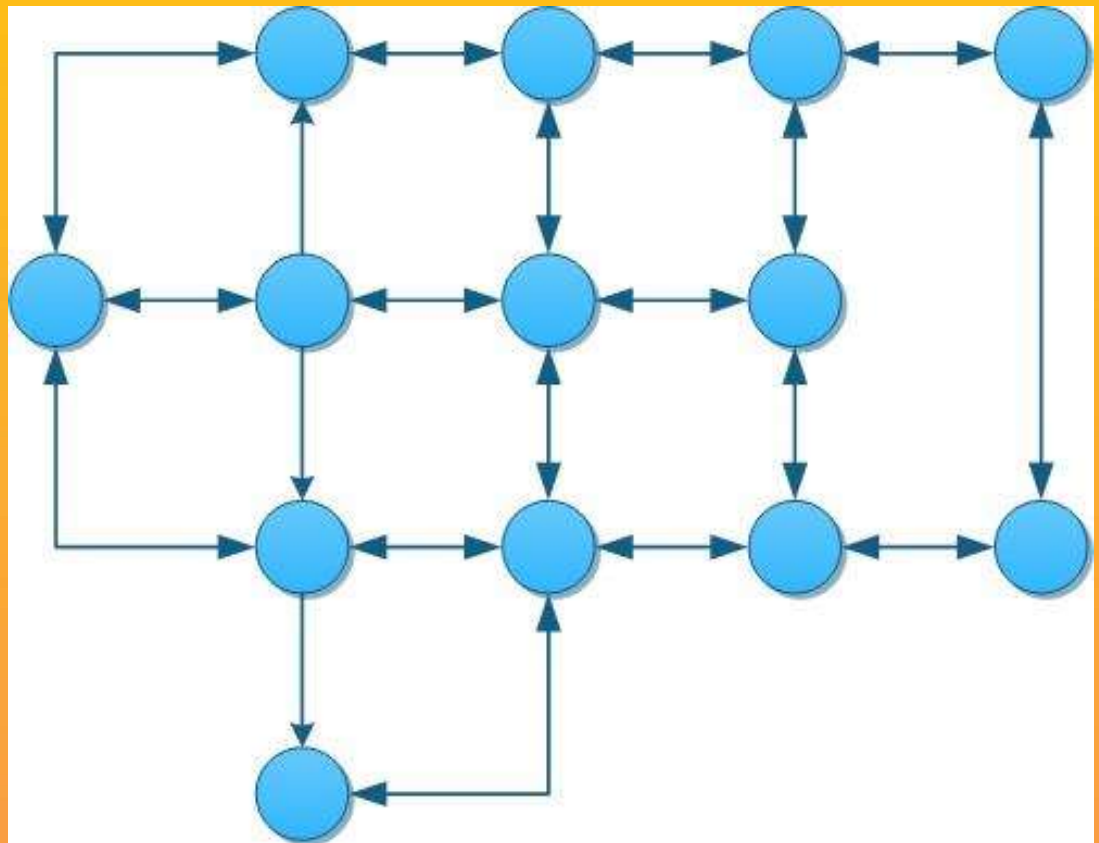
INPUTS From
0627052b6f28912f2703066a912ea577f2ce4da4caa5a5fbd8a57286c345c2f2 : 0
Bob 0.0150 BTC

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



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



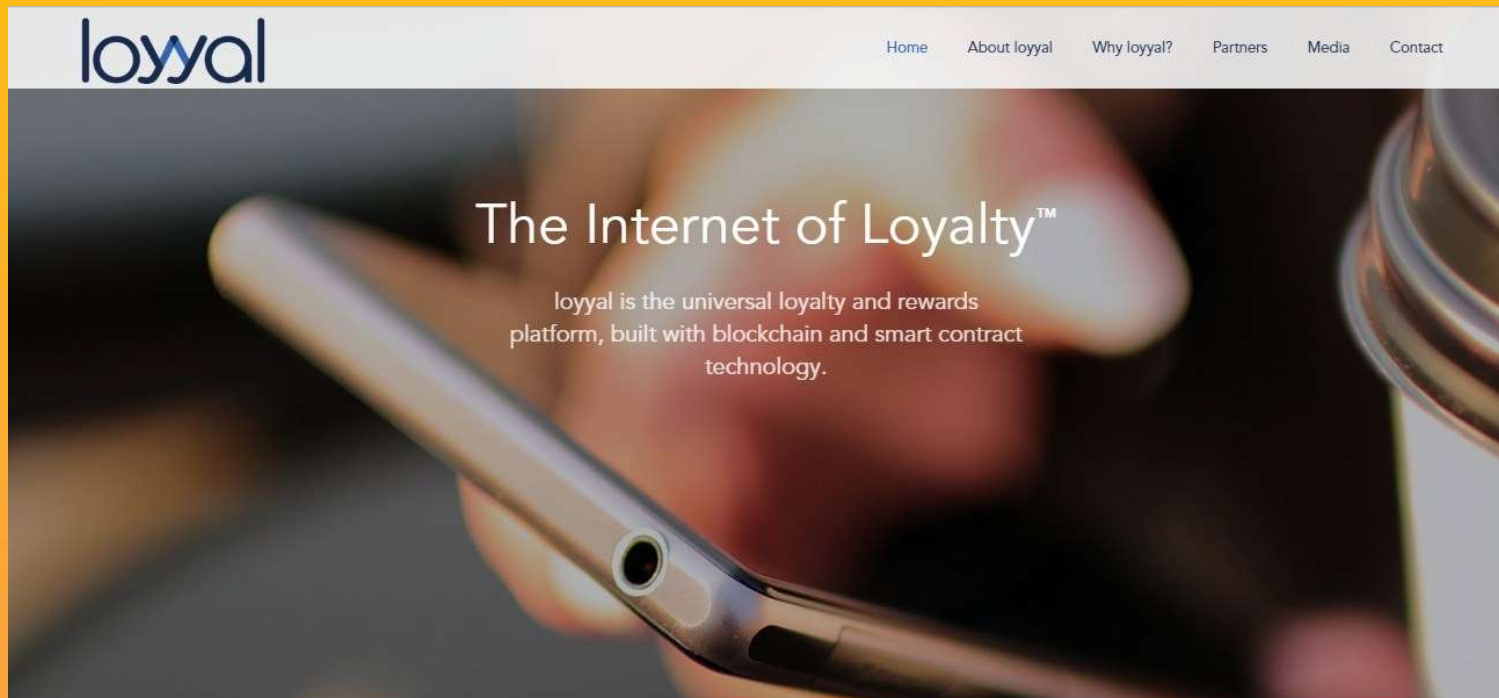
...And Many More!

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



Current Usage

- Loyalty Program



THE HONEYNET PROJECT

Recent Development

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



Blockchain (Use Cases)

Source: GrowthPraxis

Proof of ownership and a marketplace for sales and purchase of digital assets

Company: MyPowers

Enables authenticity of a review through trustworthy endorsements for employee peer review

Company: TRST.im

Decentralized prediction platform for the share markets, politics etc

Company: Augur

Decentralized patient records management

Company - BitHealth (Healthcare IT)

Proof of ownership for digital content

Arts, pictures and images

Companies: Blockai, Bitproof, ascribe, Artplus

Other companies: Chainy.Link, Stampery

Digitizing assets: Improves anti-counterfeit measures

Consumer electronics, Automotive

Degree Verification

Companies: The Real McCoy, ChainLink

Company: Degree Of Trust

Other companies: Everpass, BlockVerify

Provides digital identity that protects consumer privacy

Internet, car locks: Oname

Customer identification: Trustatom

Elections Voting: Follow My Vote

Enables authenticity of a review

Helps users engage, share reputation and collect feedback

Company: The World Table

Through trustworthy endorsements

Company: Asimov

Decentralized internet and computing resources to every home and business

Company: ePlug

Digitizing company incorporations, transfer of equity/ownership and governance

Company: Otonomos

A smart contract IT portal executing order fulfilment in ecommerce/manufacturing

Company: UbiMS

Escrow/Custodian service

E-commerce

Company: Funds.org

Gaming industry and loan servicing

Company: New System Technologies

Gaming industry

Companies: PlayCoin, Bitnplay

Proof of ownership of modules in app development

Company: Assembly

Proof of ownership for digital content storage and delivery

Companies: Blocktech (Alexandria), Bisantyum, Blockparti, The Rudimental, BlockCDN

Points based value transfer for ride sharing

Company - La'Zooz

Digital security trading: ownership and transfer

Companies: Symbiont, Mirror, Spritzle, Secure Assets, BitShares, Coins-e, equityBits, DXMarkets, MUNA

Digitization of documents/contracts and proof of ownership for transfers

Company: Colu (Colored Coins)

Decentralized storage using a network of computers on blockchain

Company: Storj

Decentralized IoT

Home automation: Chimera-inc.io

Industries: Filament

Provides digital identity that protects consumer privacy

Companies: Sho Card, Uniquid



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