Vijay Madisetti

Georgia Tech

vkm@madisetti.com

Blockchains & Web 3.0 Perspectives

(PORTIONS OF THIS TALK MAY CONTAIN INTELLECTUAL PROPERTY OF THE PRESENTER OR OTHER ORGANIZATIONS. SOME OF THE IMAGES OBTAINED FROM YOUTUBE AND OTHER ONLINE SOURCES AND MAY BE COPYRIGHTED.)

The Four Industrial Revolutions

Navigating the next industrial revolution

WORLD ECONOMIC FORUM
COMMITTED TO IMPROVING THE STATE OF THE WORLD

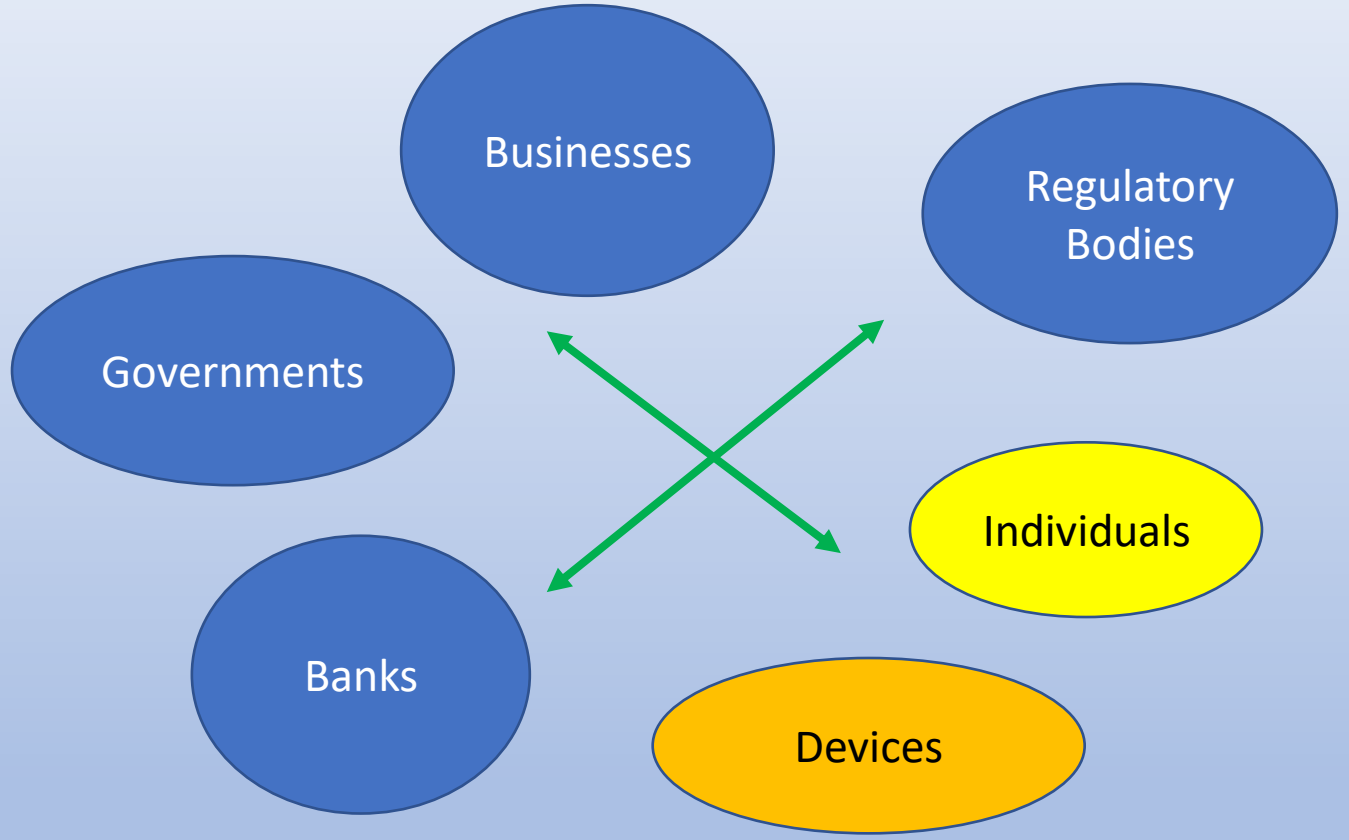
Revolution	Year	Information
1	1784	Steam, water, mechanical production equipment
2	1870	Division of labour, electricity, mass production
3	1969	Electronics, IT, automated production
4	?	Cyber-physical systems

Internet of Things (IoT) Blockchain, Analytics will Play a Central Role in Cyber-Physical Systems

www.weforum.org

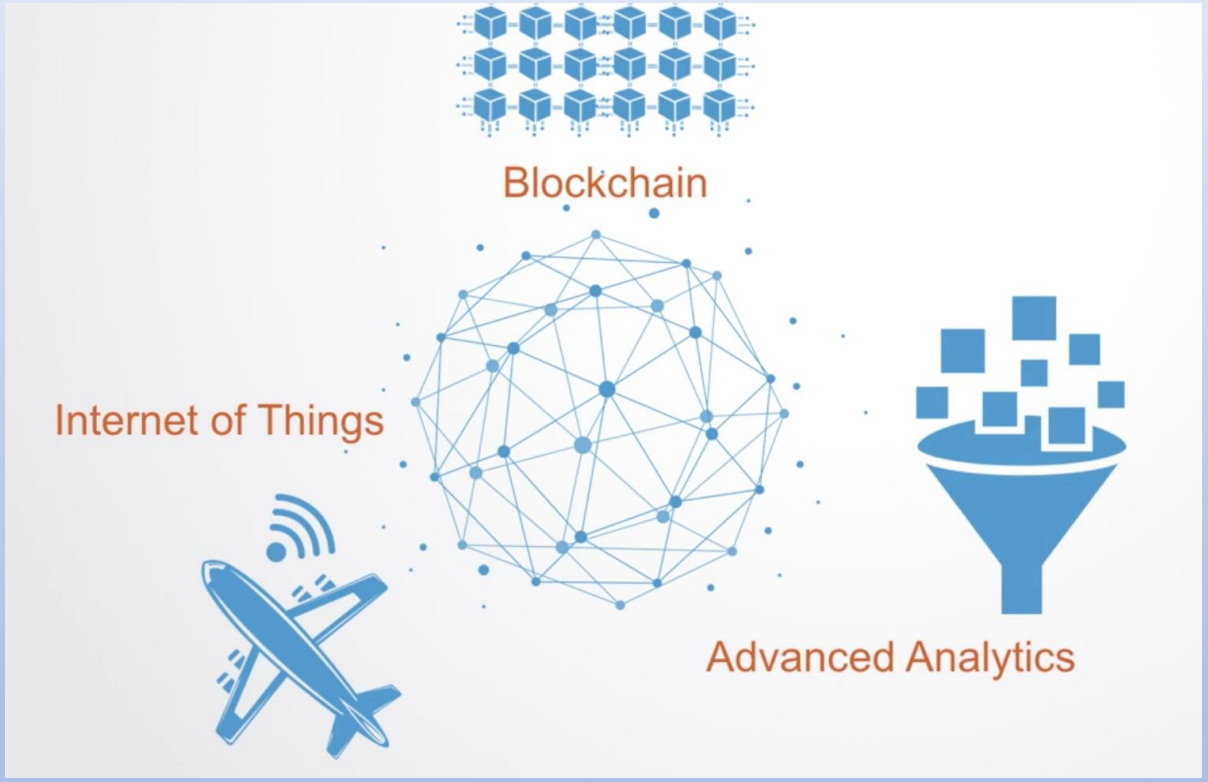
The new world – Web 3.0

Goal: Secure, transparent & efficient business and financial transactions between a large number of diverse and untrusting entities

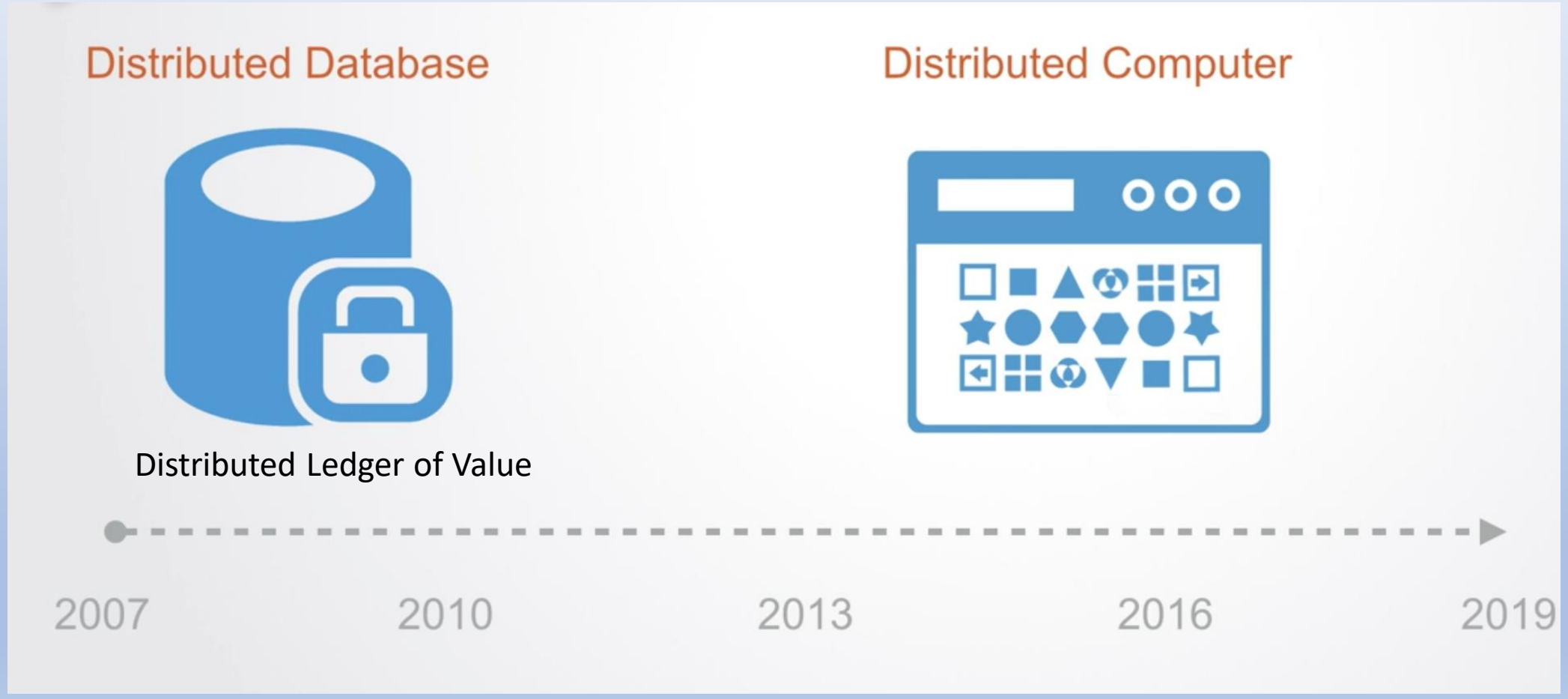


Vijay Madisetti, vkm@madisetti.com - Not for Public Distribution

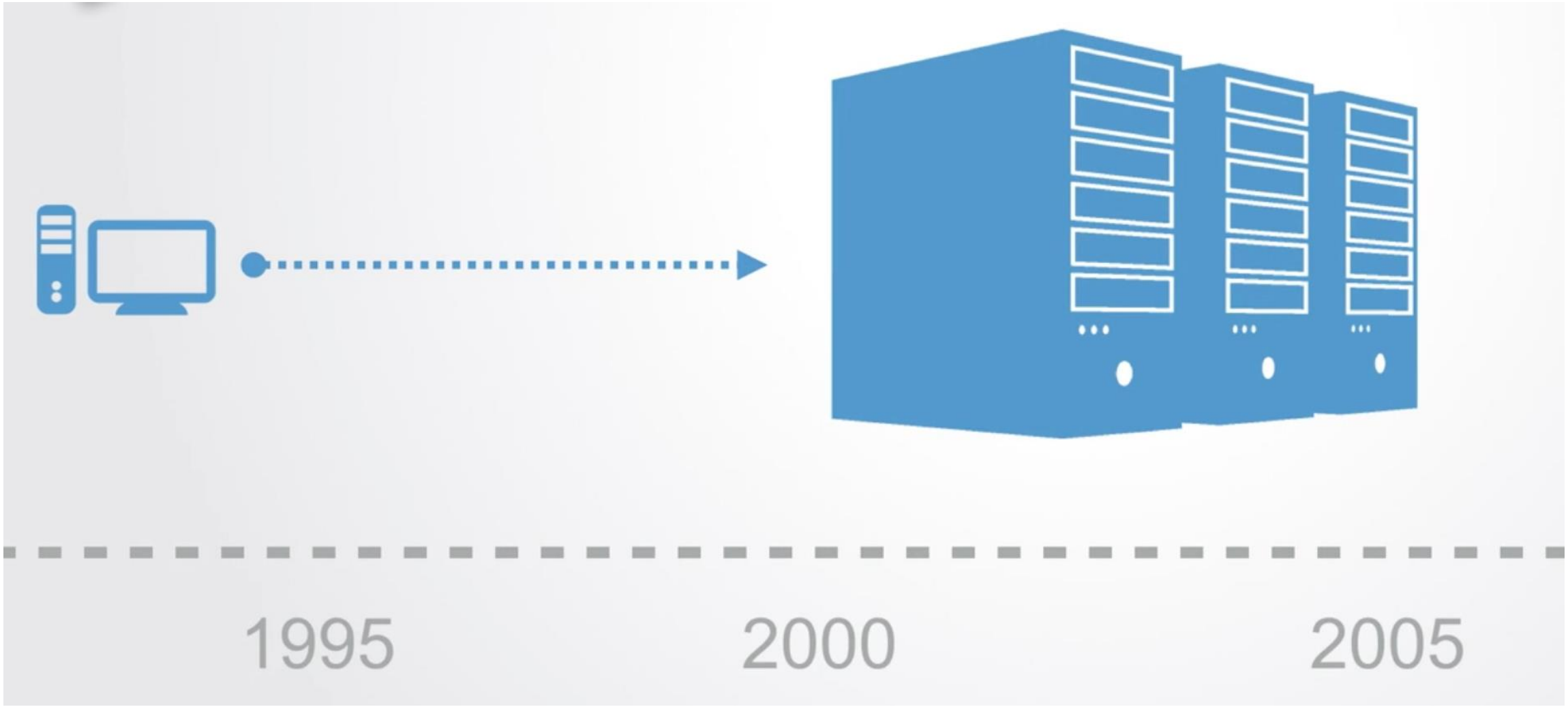
What are the building blocks of Web 3.0 ?



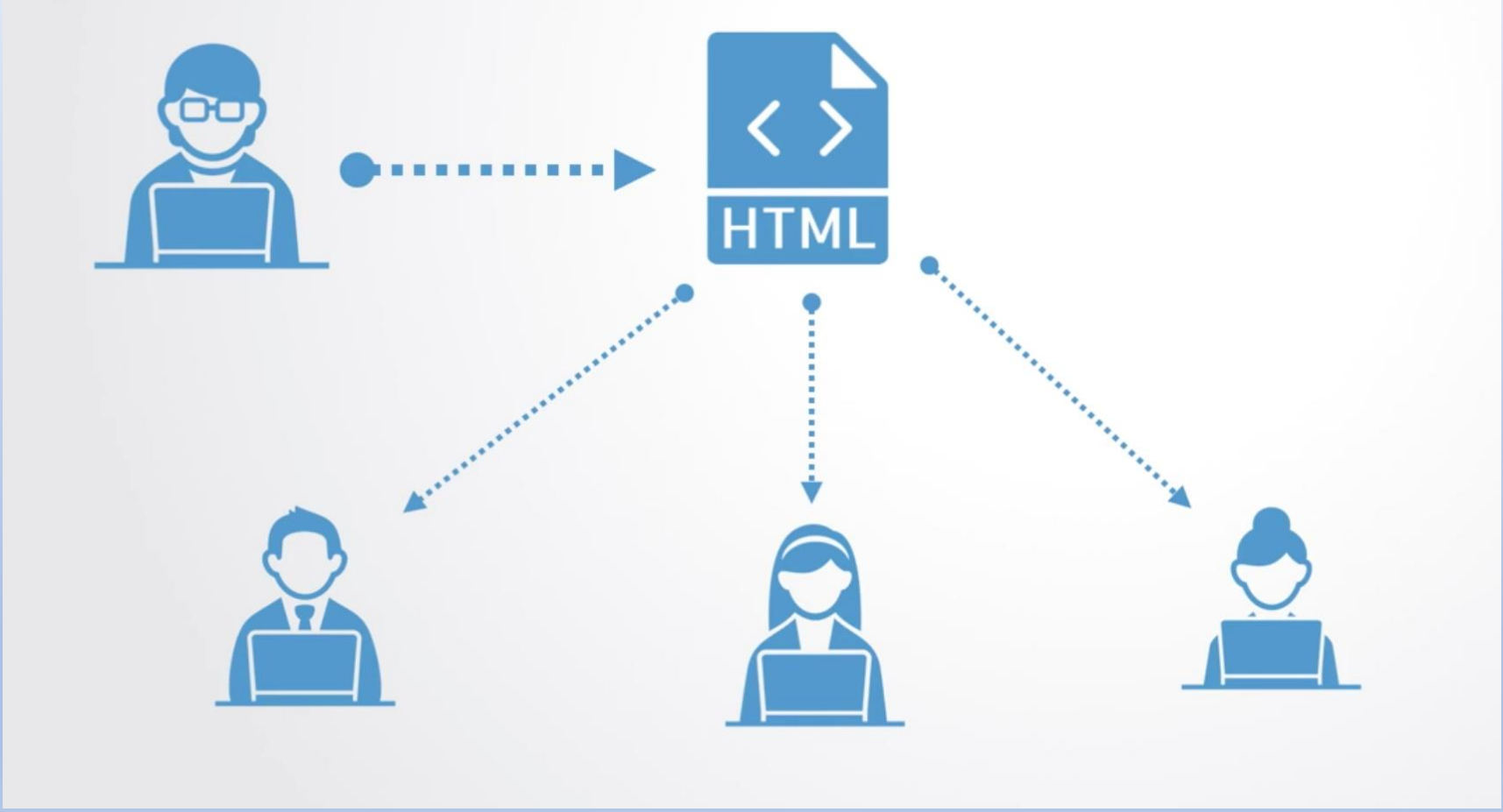
Evolution of Blockchain – Fast Forward



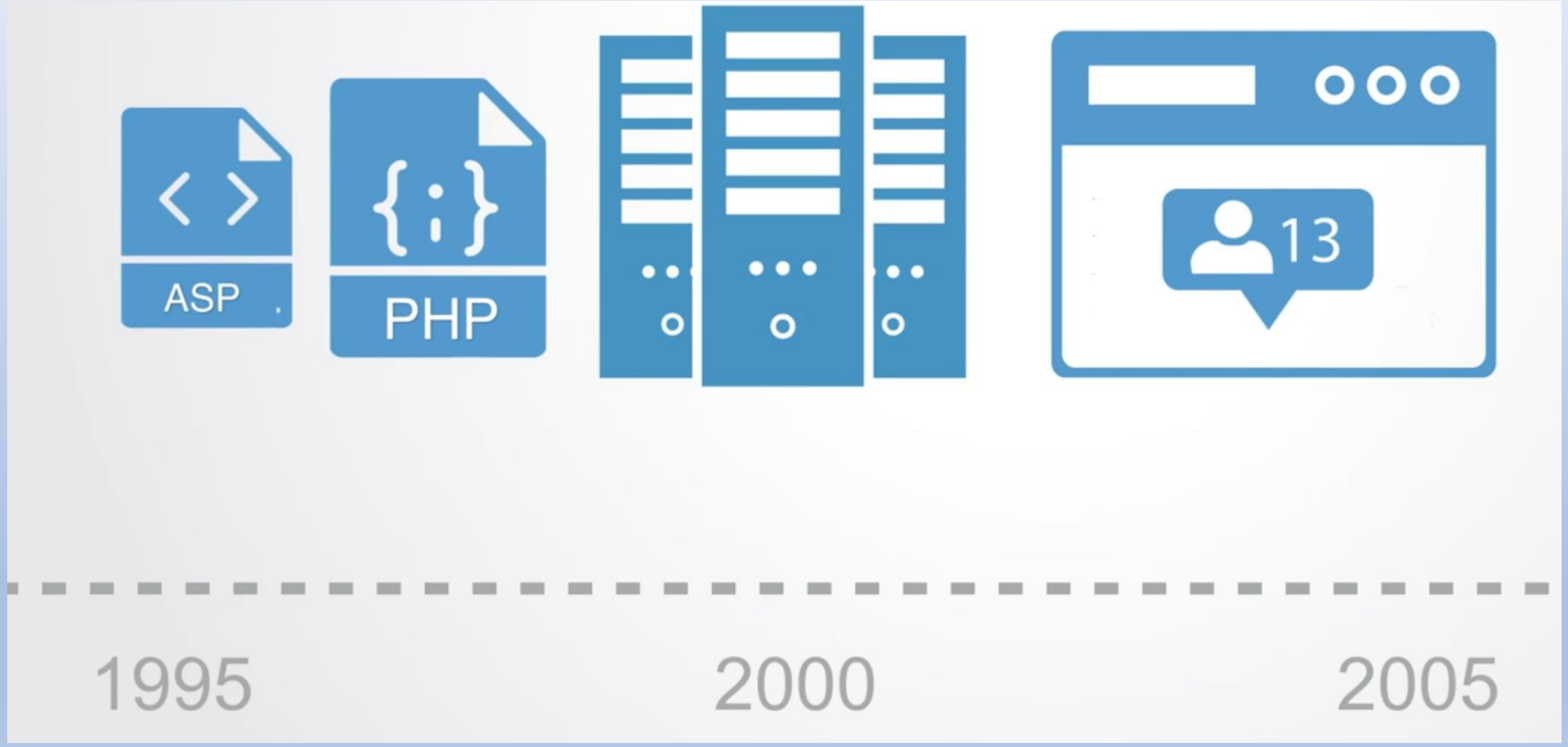
Evolution of the Internet & Web Technologies



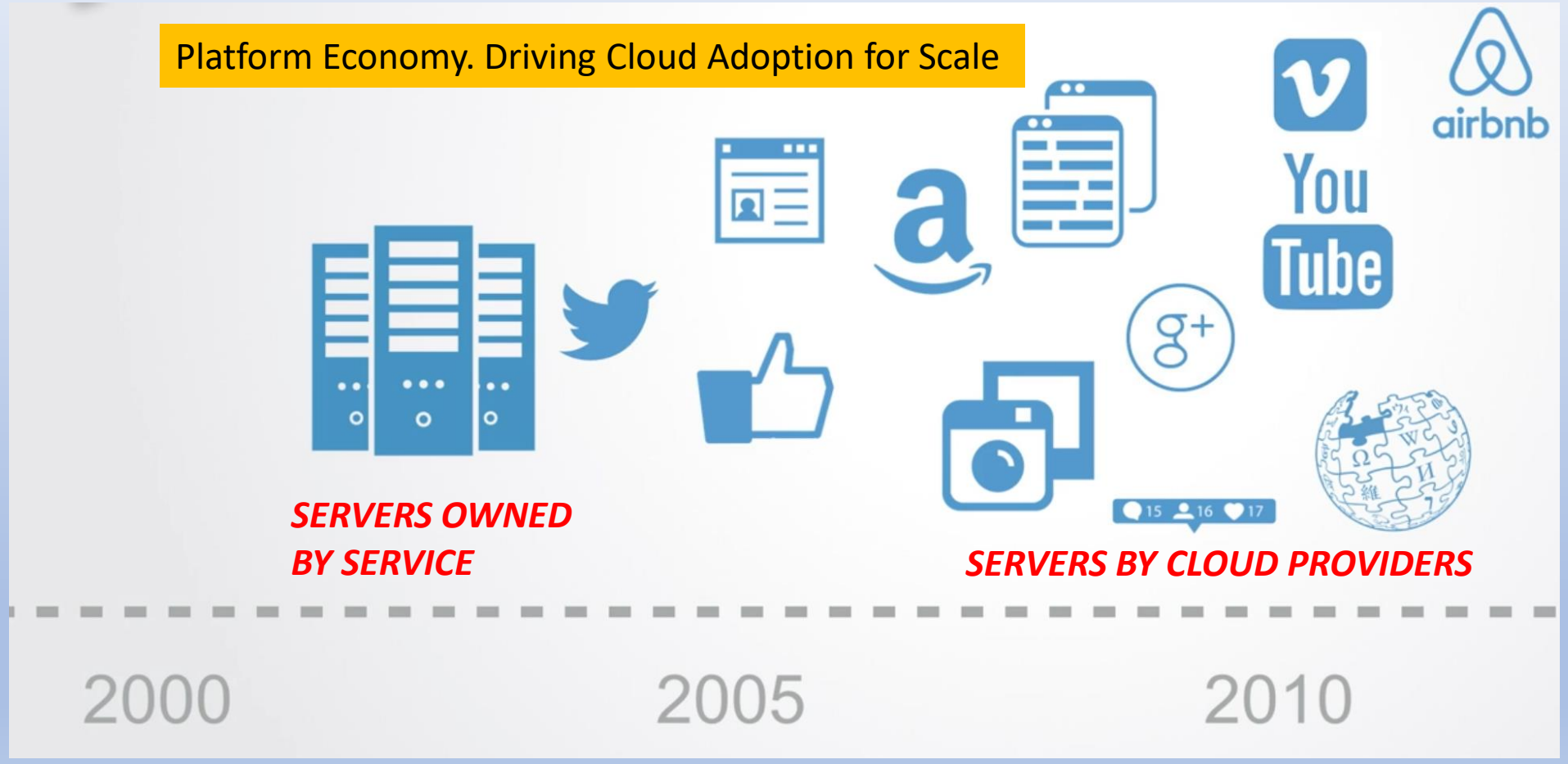
Early Web Simply Distributed Data to Clients



Evolution of the Internet & Web Technologies – Web 2.0

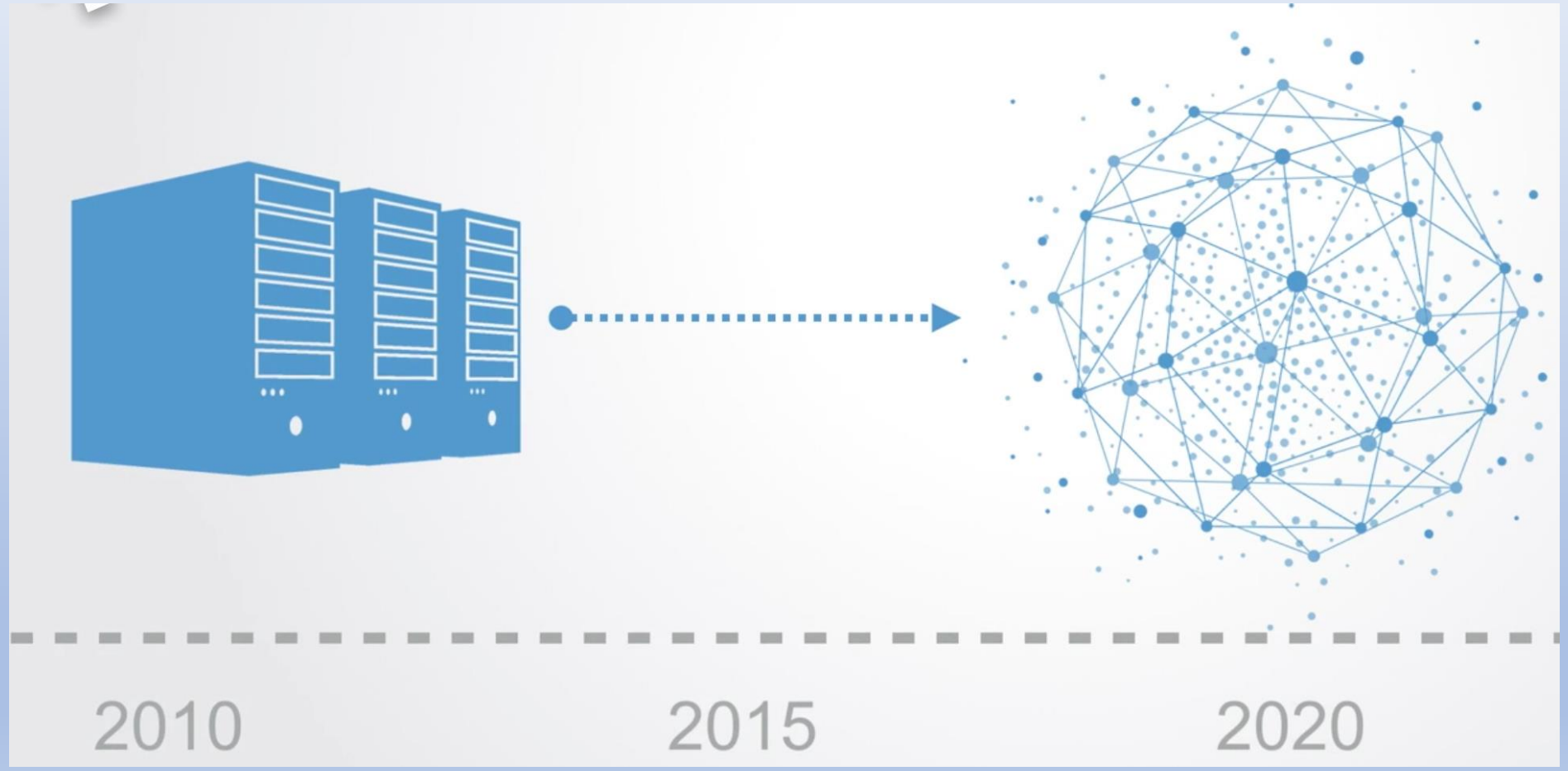


Large Servers & Cloud Platforms & Scalable Applications = Web 2.0

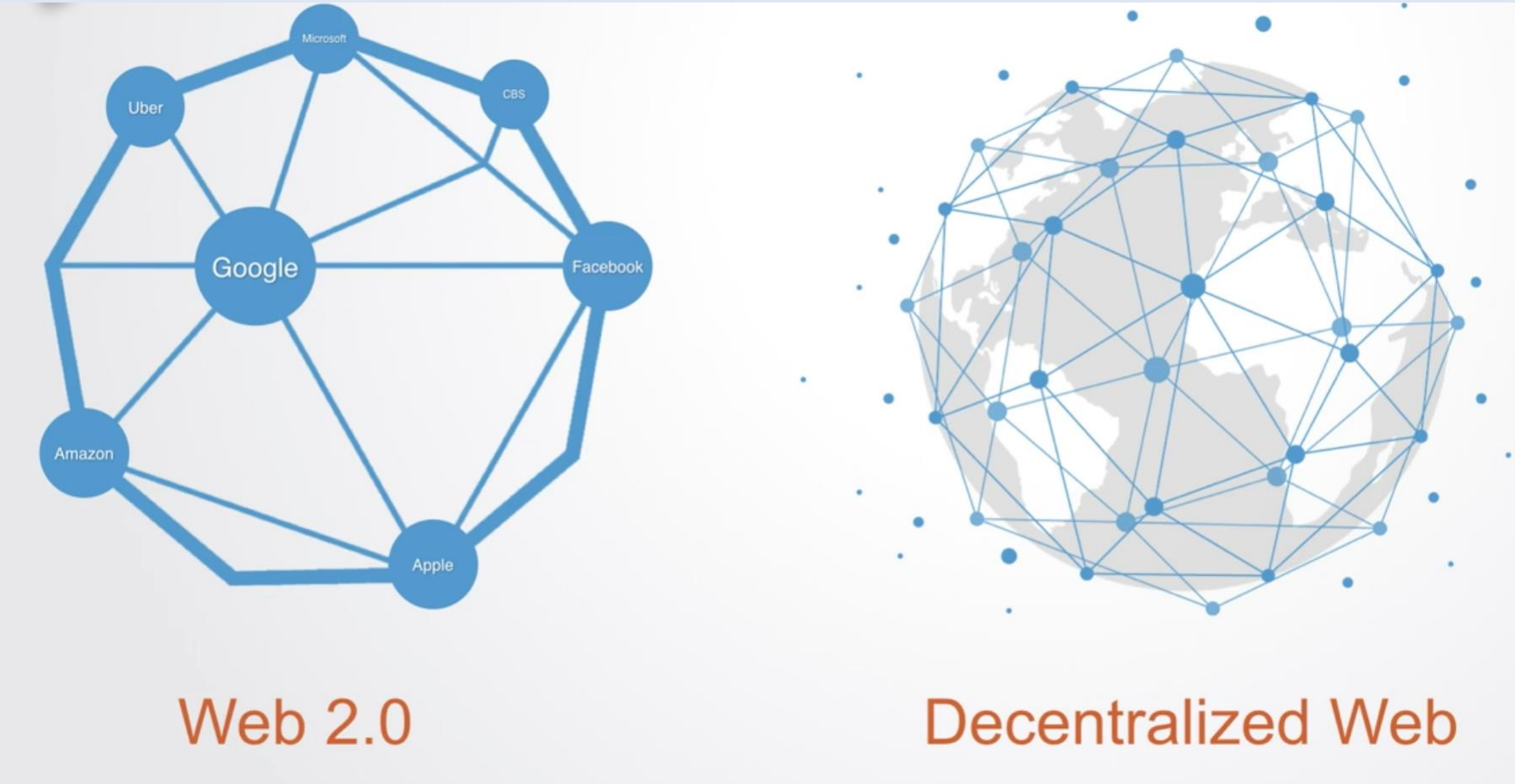


Behemoth Servers and Cloud Platforms Serving Apps - Cloud Computing

What next from Web 2.0 ? A: Web. 3.0 !



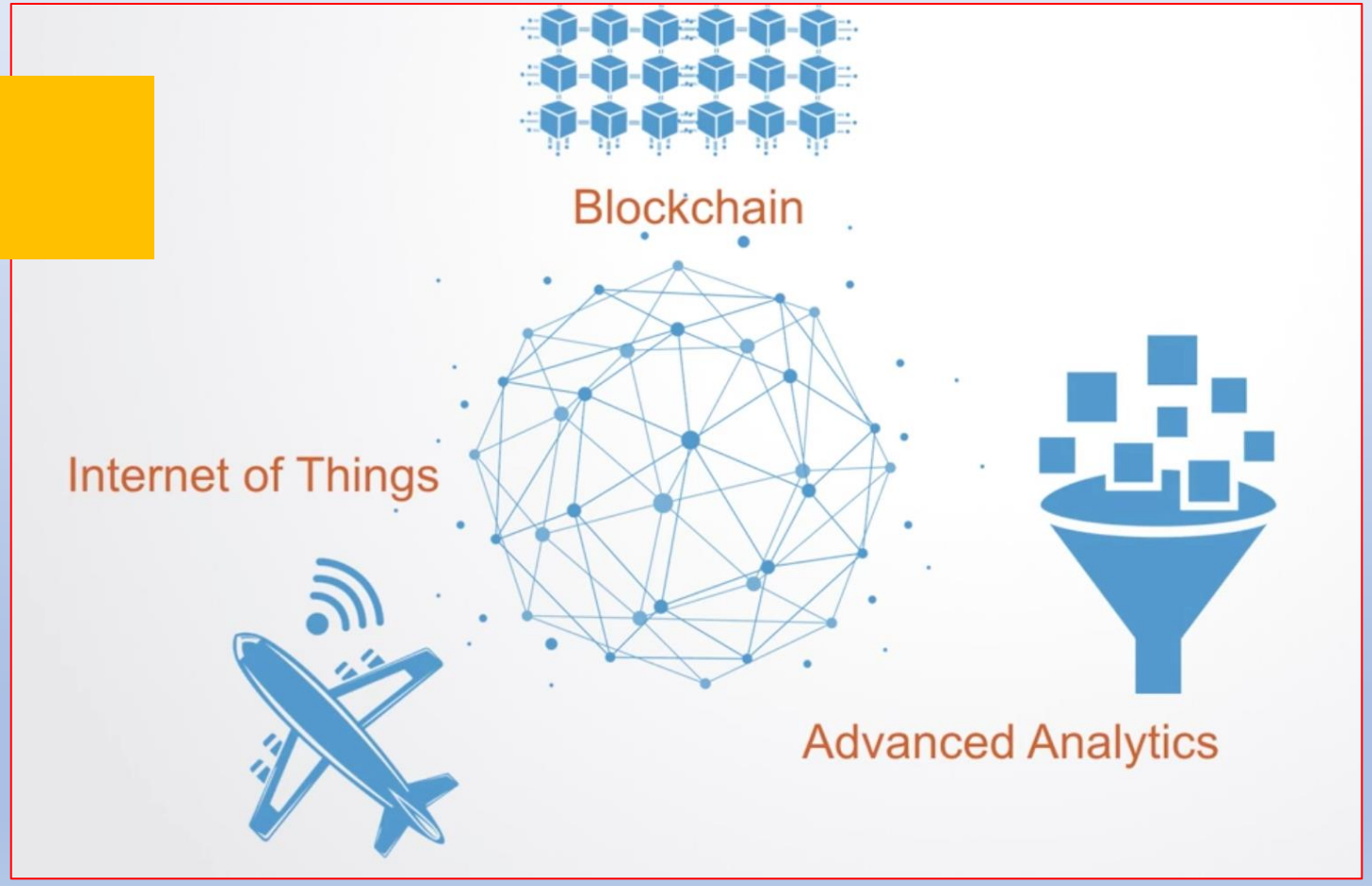
Big Centralized Servers to Fully Decentralized Nodes



What are the building blocks of Web 3.0 ?

Token Economy

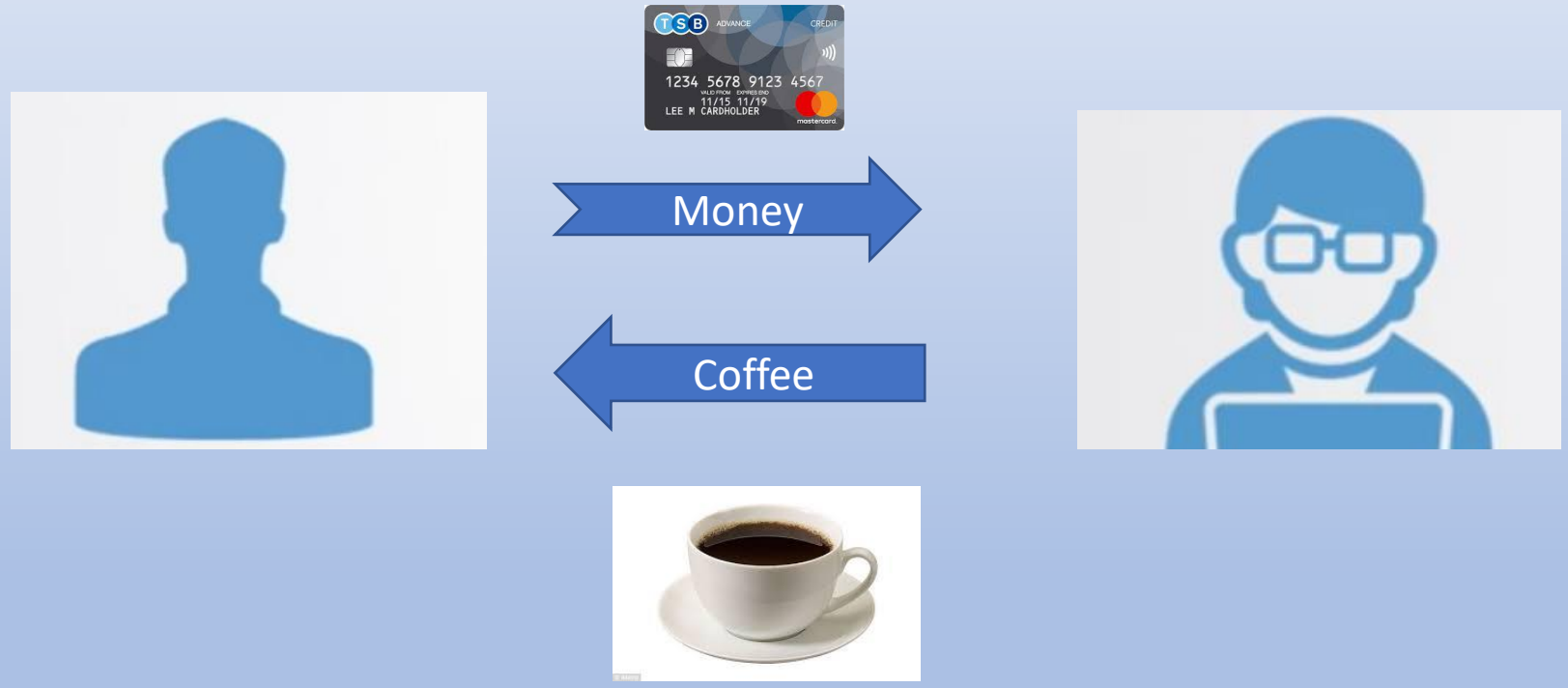
Token Networks



What are all these new business models and payment protocols ?

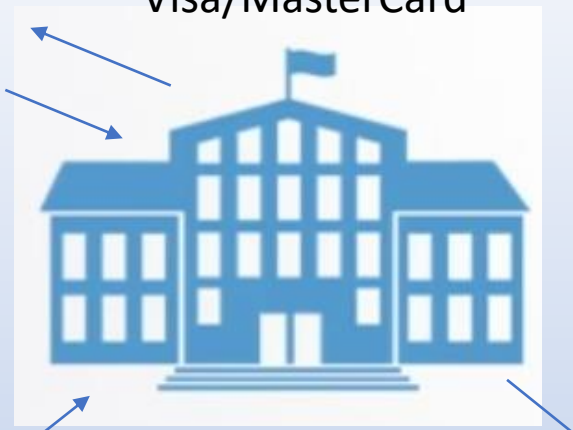
(Why) Is blockchain going to change the world ?

A very common transaction ……. (today)

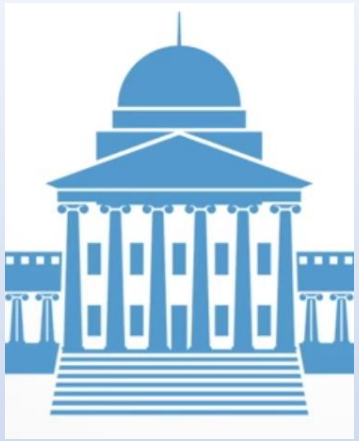


Bank

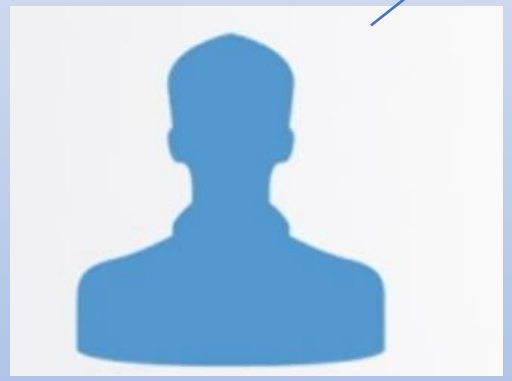
Visa/MasterCard

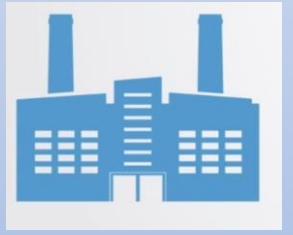


Bank



Tax



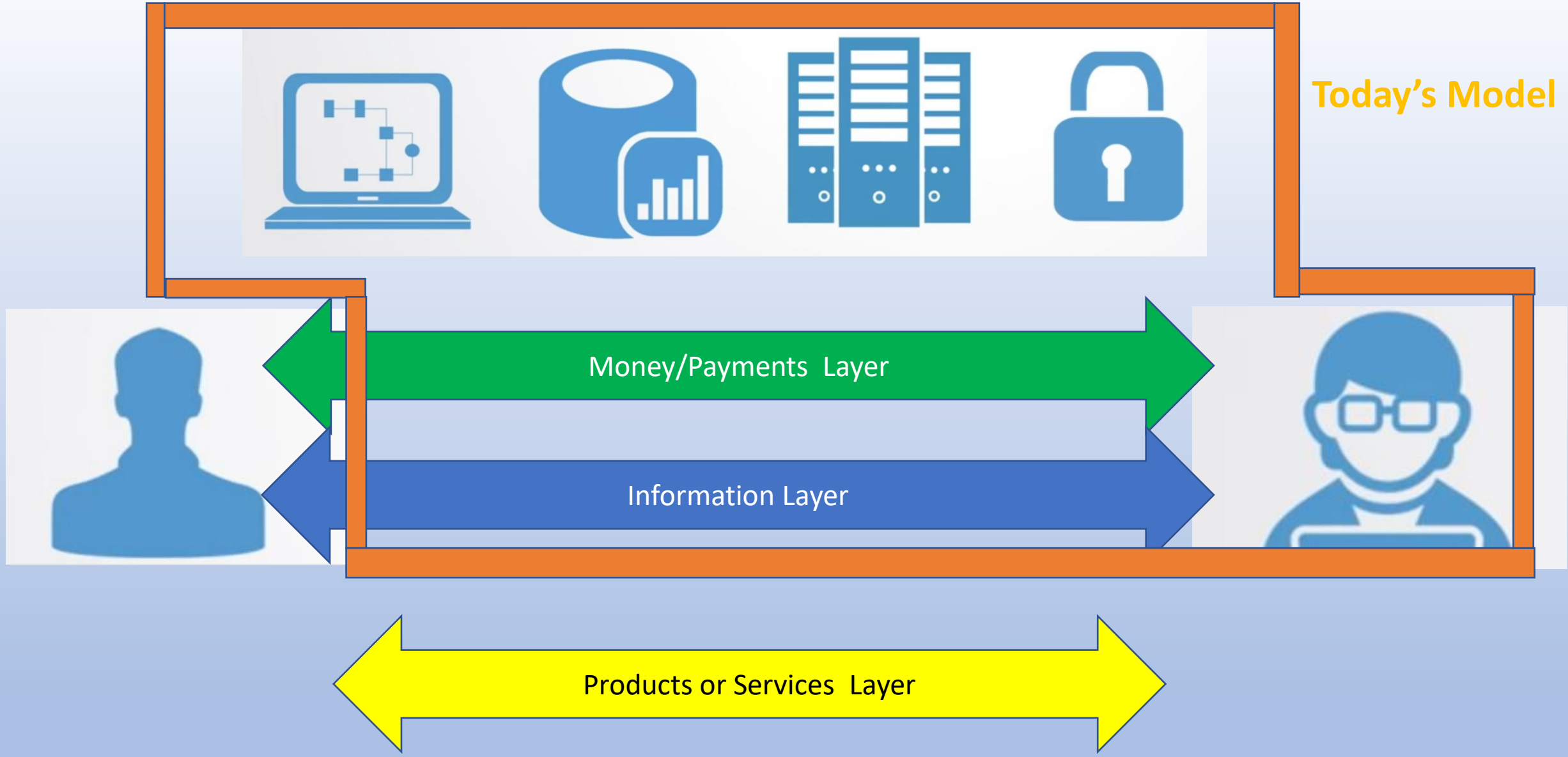


Suppliers

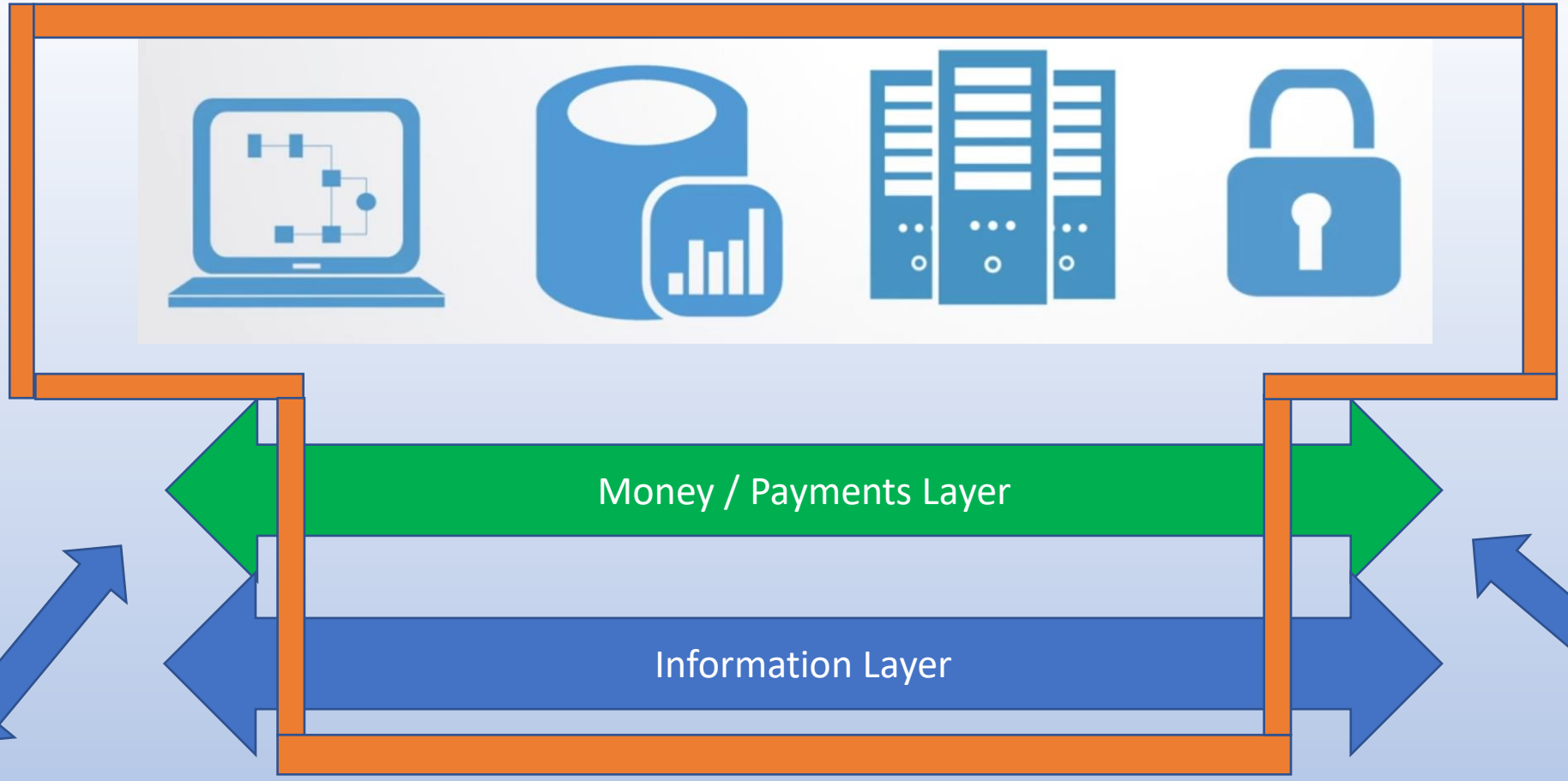
Product

What is going on behind the scenes ?

Today's Model

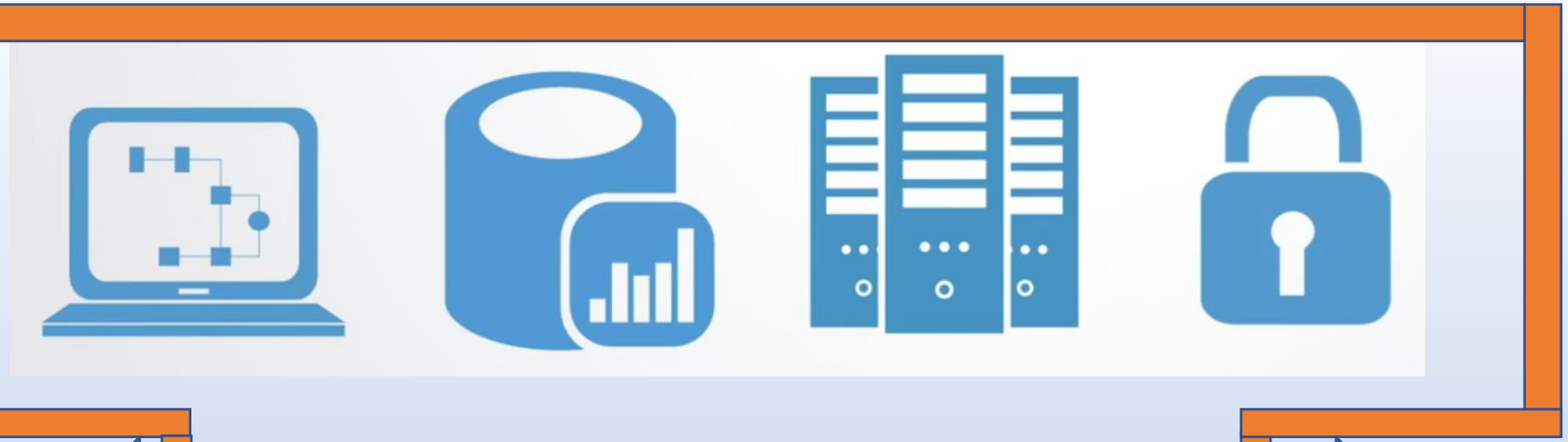


Less Old Model



Products or Services Layer

Less Old Model



Payments/Money Layer

Information Layer

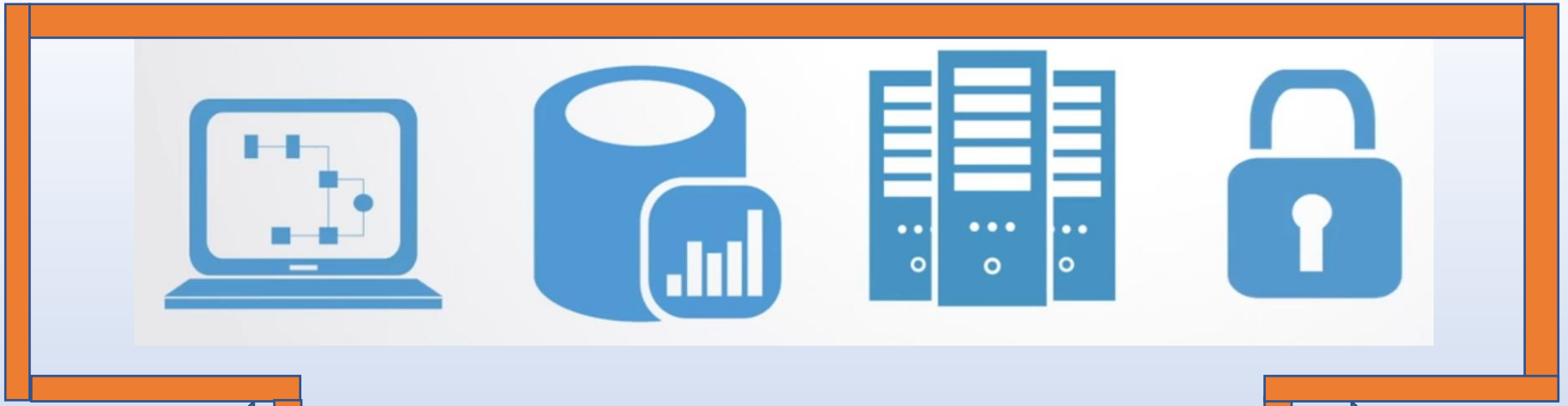
Products or Services Layer

Rents Private Car for 2 days for $25.00

Car Owner – Spends $50k

High Price

Newer Model



Money/Payments Layer

Information Layer

Products or Services Layer

Use for 2 hours for
$1.50 twice a month

Jane – Frequent Use

$150 tool set – Lower Price

Tom


Lending
(483 Companies)
LendingClub
Kabbage
PROSPER
lighter capital
OnDeck
Funding Circle
earnest
affirm
borro
Personal Finance
(238 Companies)
Credit Karma
payoff
mint
OnTrees
CoverHound
BILL GUARD
HelloWallet
smartasset
planwise
credit sesame
Payments
(492 Companies)
Square
stripe
Paydiant
proteân
Be In The Loop
WEPAY
venmo
iZettle
Braintree
Equity Financing
(140 Companies)
CircleUp
LOYAL3
SHARESPOST
EquityNet
seedinvest
gust
crowdfunder
exitround
International Transfer
(76 Companies)
WorldRemit
XOOM
azimo
CurrencyFair
kantox
Ebury
The Currency Cloud
ayannah
Payoneer
REMITLY
Retail Investing
(166 Companies)
ROBINHOOD
motif
eToro
Betterment
BUX
KAPITALL
wealthfront
FutureAdvisor
SigFig
FINANCIAL
TECHNOLOGY
VENTURE SCANNER
The Venture Scanner research platform currently tracks 2,285 financial tech startups with $80B in funding
Institutional Investing
(181 Companies)
ADDEPAR
KENSHO
finalta
Quovo
Hedge SPA
StockTwits
SumZero
CONTIX
Security
(113 Companies)
riskified
Centrify
SIGNIFYD
sift science
EyeVerify
dashlane
feedzai
NORSECORP
Accertify
Infrastructure
(150 Companies)
DemystData
plaid
CUneXus
MAMBU
STANDARD TREASURY
eWise
Ebury
Business Tools
(233 Companies)
xero
GUSTO
zenpayroll
fraktek
@Scred
Crowdfunding
(79 Companies)
KICKSTARTER
INDIEGOGO
FUNDLY
hubbub
tilt
Digital Banking
(75 Companies)
SIMPLE
GOBank
Atom
Cardlike
vudubu
Moven
Research & Data
(83 Companies)
COSEER
xignite
heckyl
STOCK TAGON
source venture scanner via @mikequindazzi
The graphic above shows a random sampling of companies in each category, data cumulative as of December 2017
5

What is the ”New” Token Model ?

Get rid of the middle guys – decentralization !

Peer

Value or Token Layer

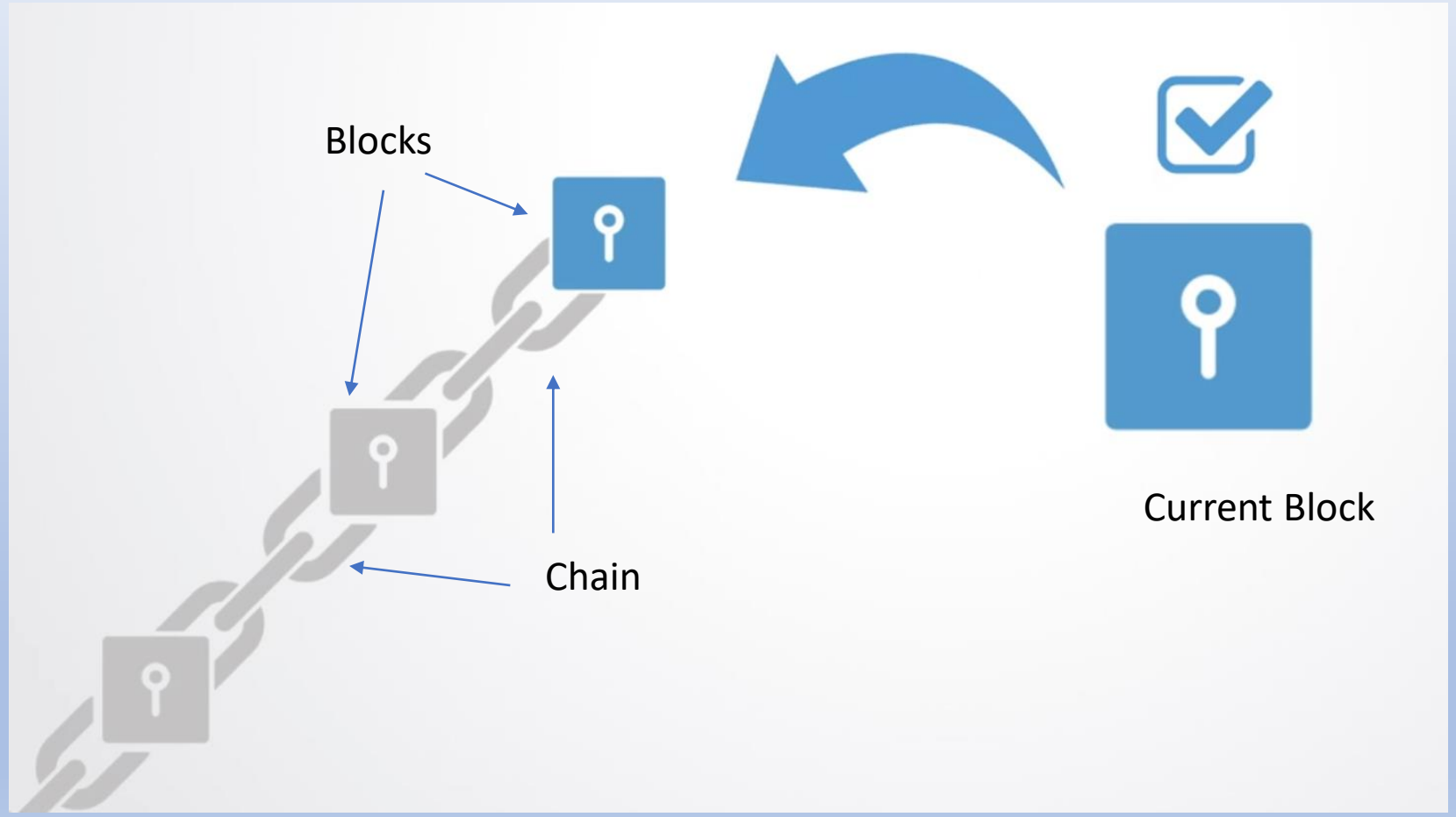
Information Layer

Products or Service Layer

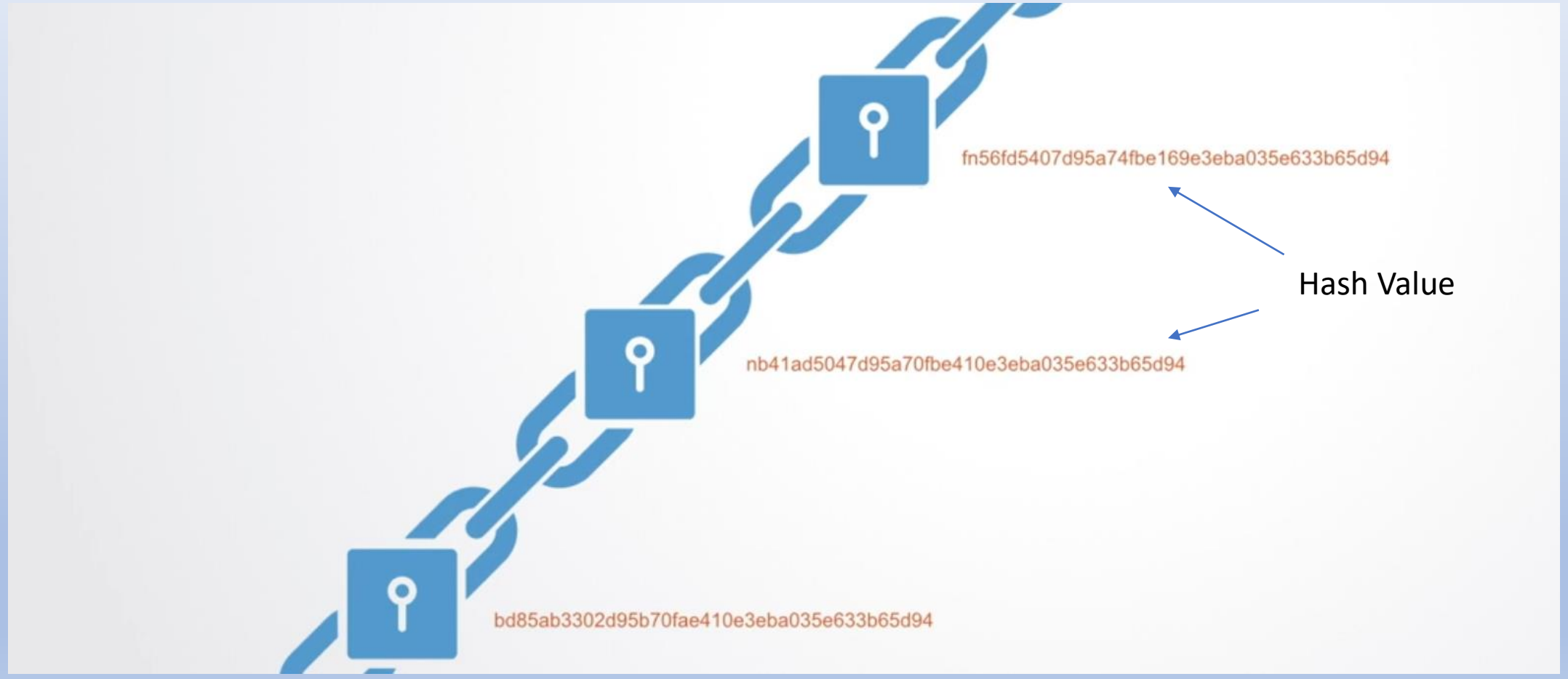
This is what Blockchain and Web 3.0 seek to accomplish !

What is Blockchain ?

Basics of Blockchain



Blockchain Built Up



SHA-256 hash calculator

Hash is a one-way function that generates hash of constant length irrespective of input text size.

SHA-256 produces a 256-bit (32-byte) hash value.

Data

This is a test of the blockchain banking system as we do not know it.

SHA-256 hash

e8257987147f8f818f0085713eb7a51c6aeee869cb4734bc469ef1cb3aa55876

Calculate SHA256 hash

SHA-256 hash calculator

SHA-256 produces a 256-bit (32-byte) hash value.

Data

We built this feature, and it's very useful. There were a lot of people using it up until we shut it down today," Chief Executive Mark Zuckerberg said in a call with reporters Wednesday.

Facebook said in a blog post Wednesday, "Given the scale and sophistication of the activity we've seen, we believe most people on Facebook could have had their public profile scraped."

Hackers also abused Facebook's account recovery function, by pretending to be legitimate users who had forgotten account details. Facebook's recovery system served up names, profile pictures and links to the public profiles themselves. This tool could also be blocked in privacy settings.

SHA-256 hash

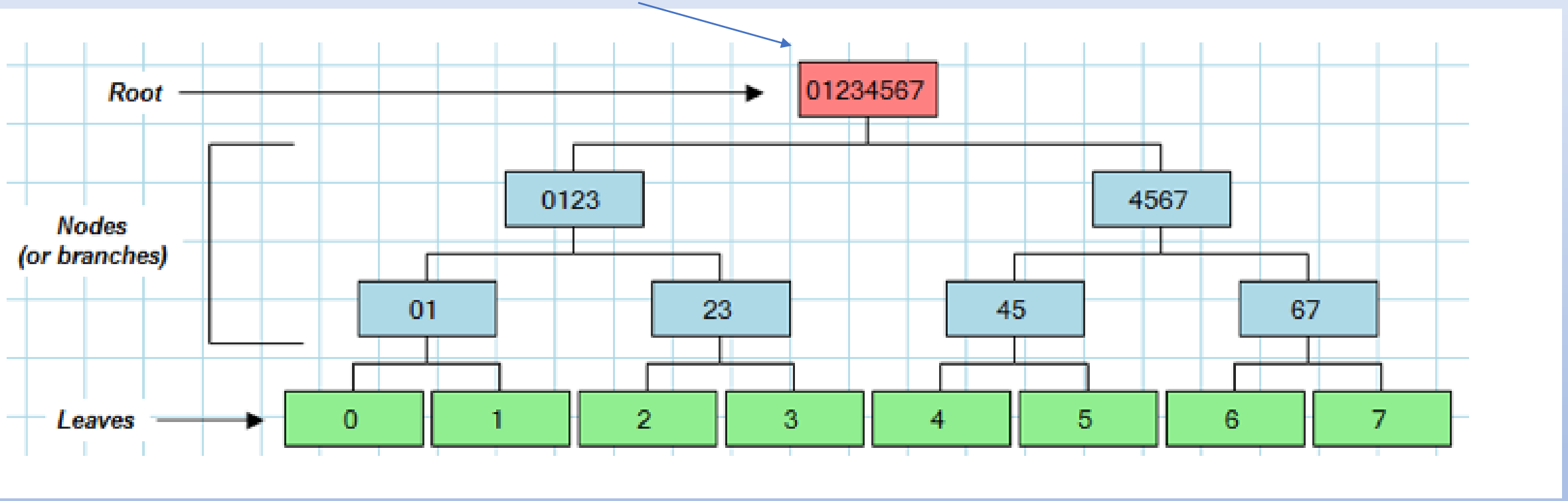
```
e8257987147f8f818f0085713eb7a51c6aeee869cb4734bc469ef1cb3aa55876
```

SHA-256 hash

```
288247b86b5978d73c9184e4f589d6e4bf008de4137fb2aa1b9e64e399c51788
```

Hash Demystified

Root Hash for the Block

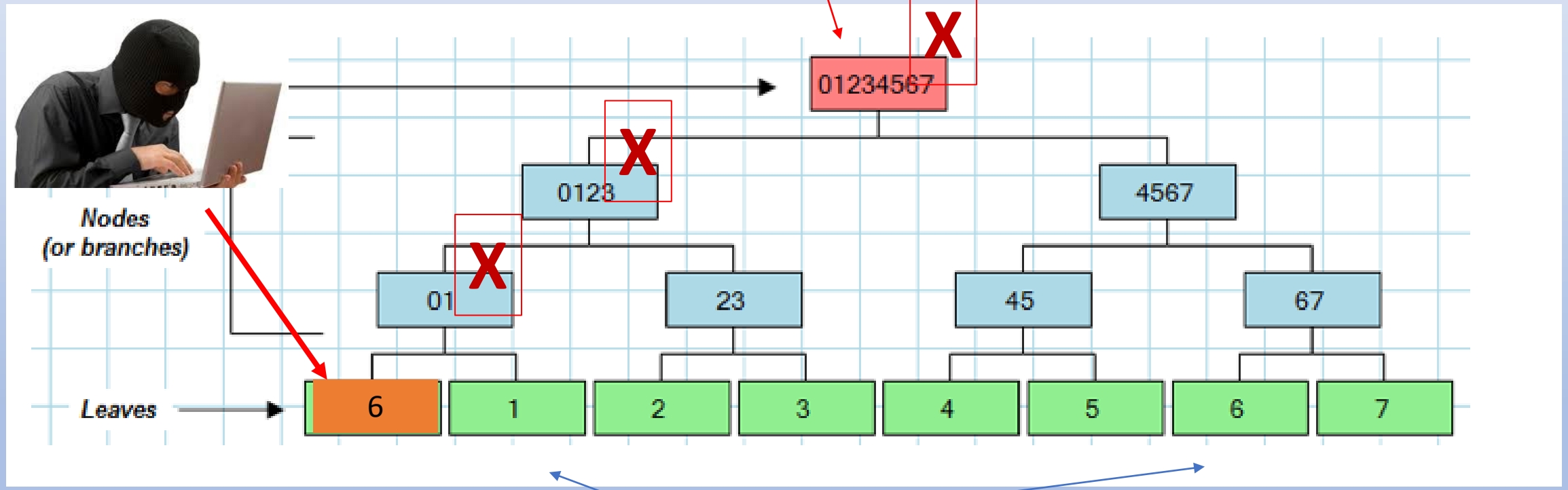


Transaction Hashes Within a Block

How hashes protect integrity of data !

Hash Demystified

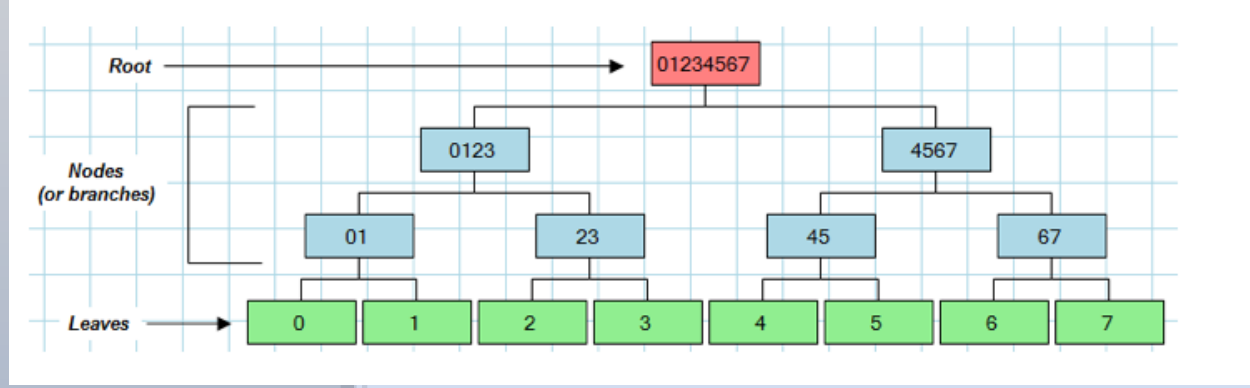
Root Hash for the Block – Merkle root

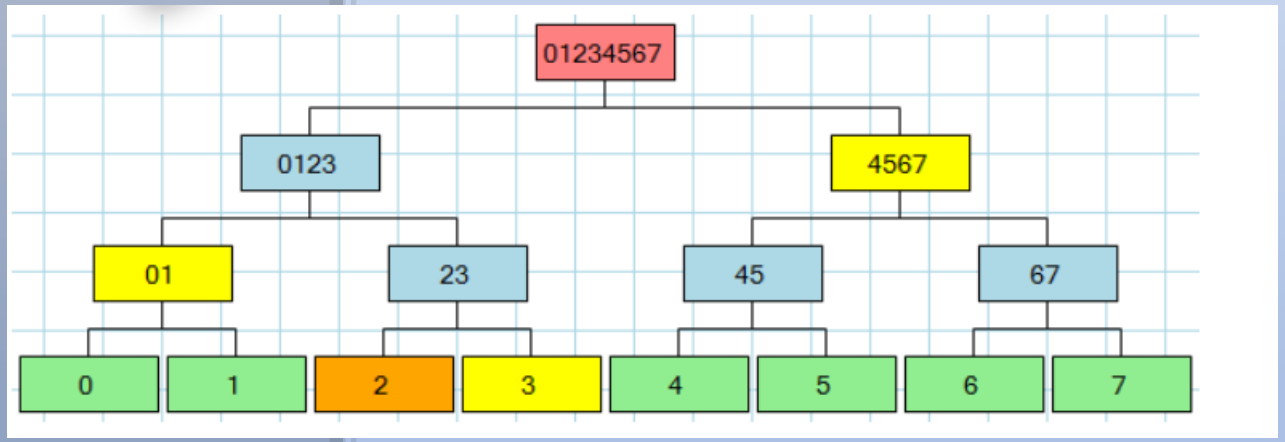


Transaction Hashes Within a Block

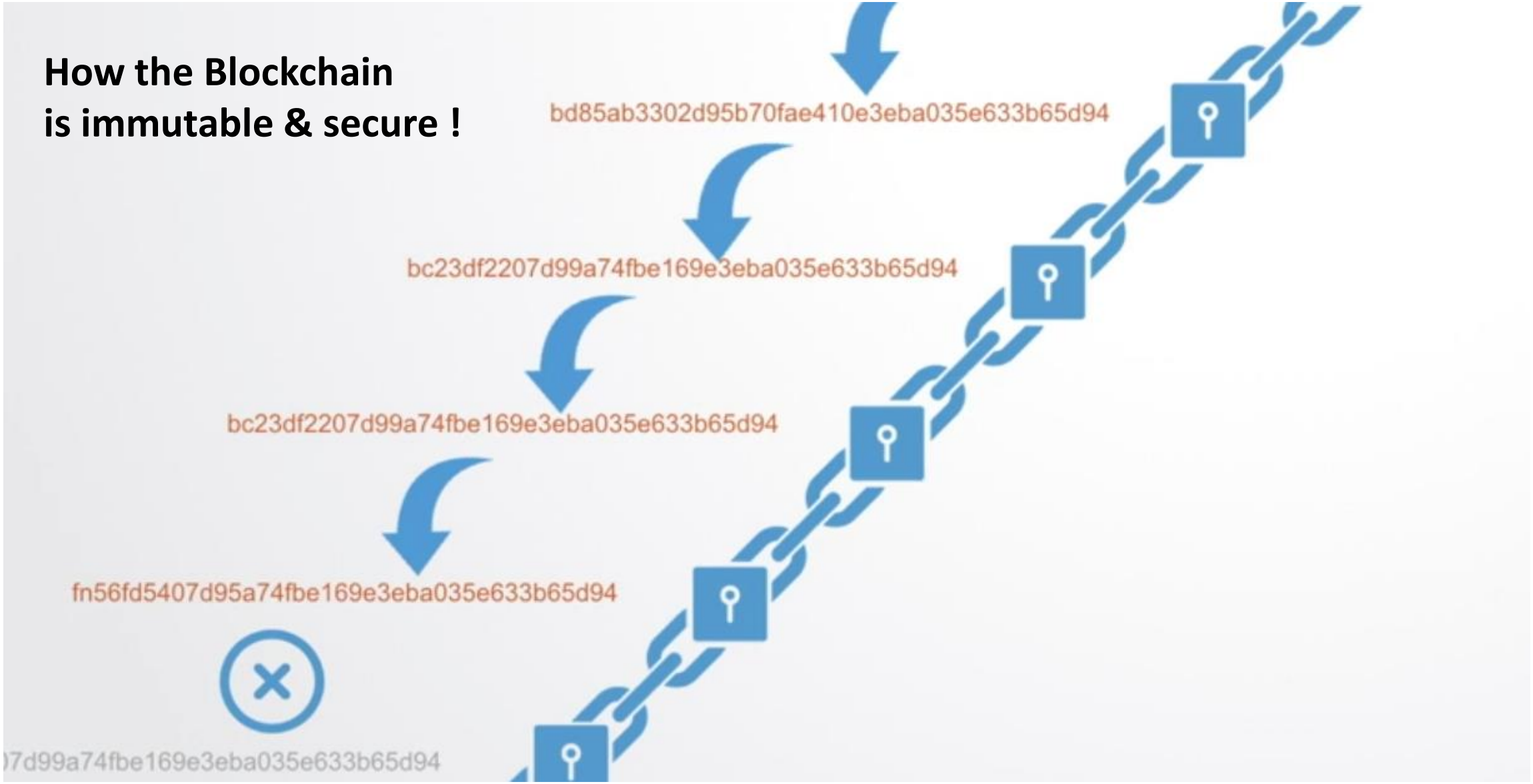
How to Test if a Particular Transaction “2” is Present ?

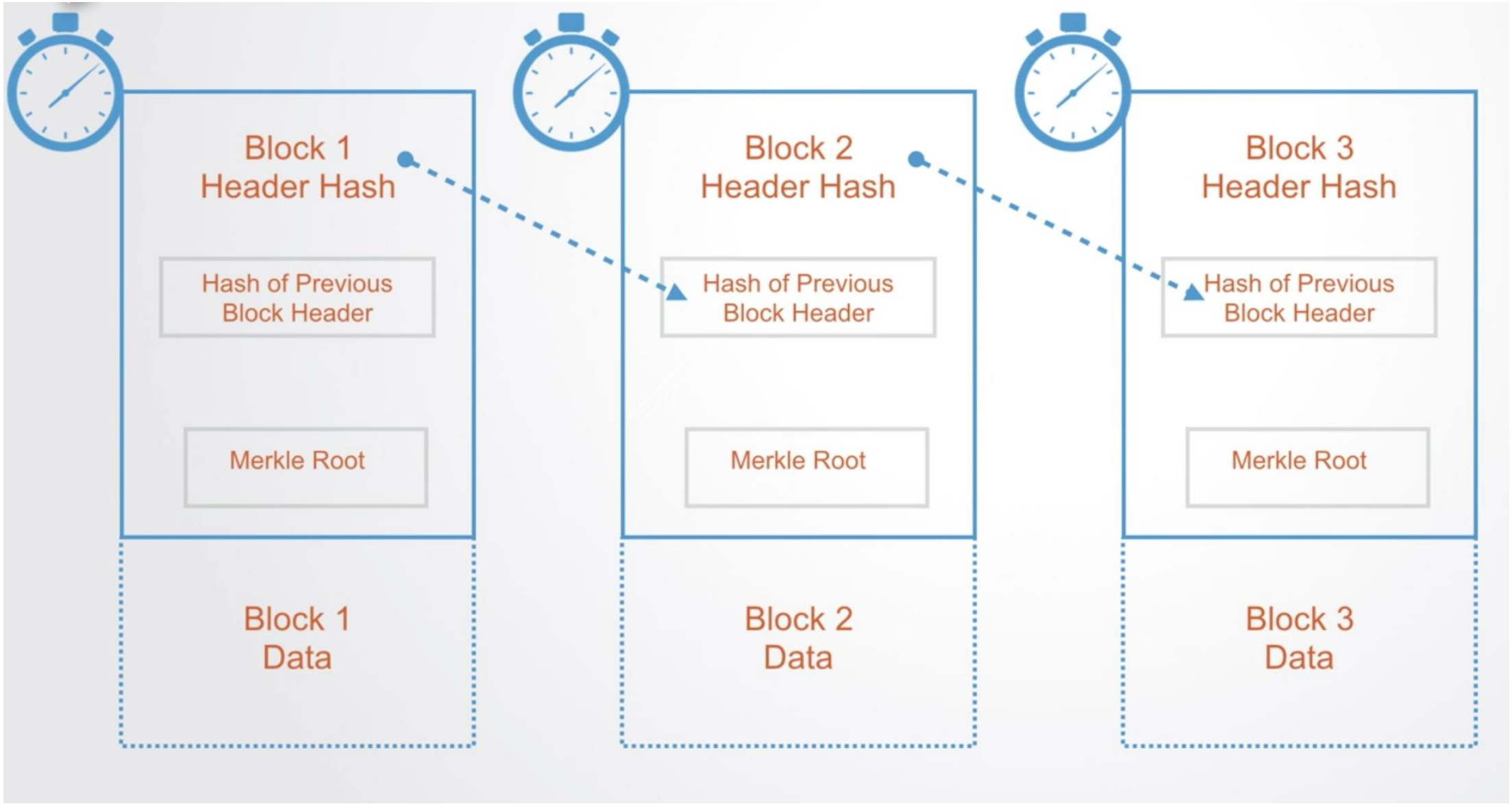
- The Root Hash is Stored in a Trusted Server and Known to the Asker.
- The Server Returns 01, 3, and 4567 and their position.





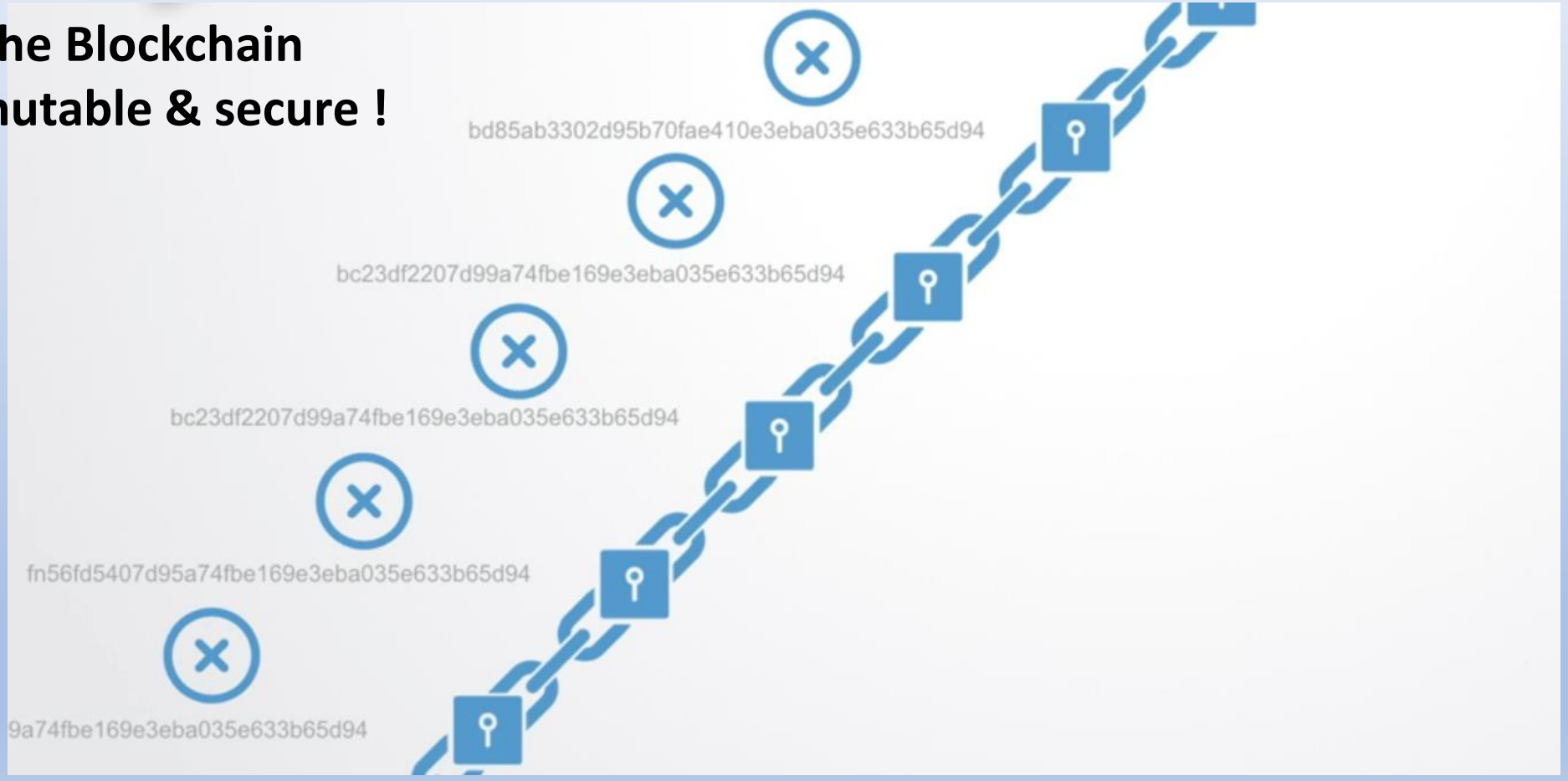
How the Blockchain is immutable & secure !




Block 1
Header Hash
Hash of Previous
Block Header
Merkle Root
Block 1
Data
Block 2
Header Hash
Hash of Previous
Block Header
Merkle Root
Block 2
Data
Block 3
Header Hash
Hash of Previous
Block Header
Merkle Root
Block 3
Data

Hash Roots are linked in a chain !

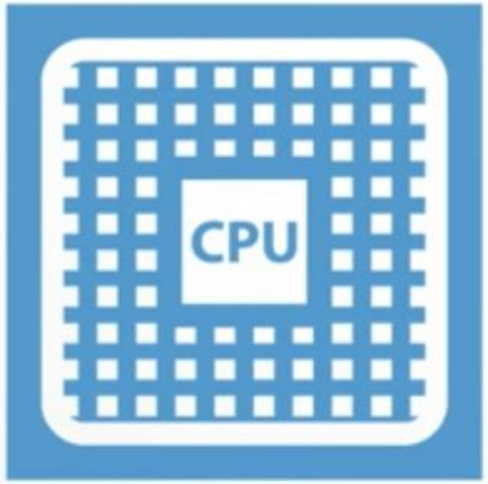
How the Blockchain is immutable & secure !



Encryption & Hashing

01100
10110
11110

Proof of Work



Network Consensus

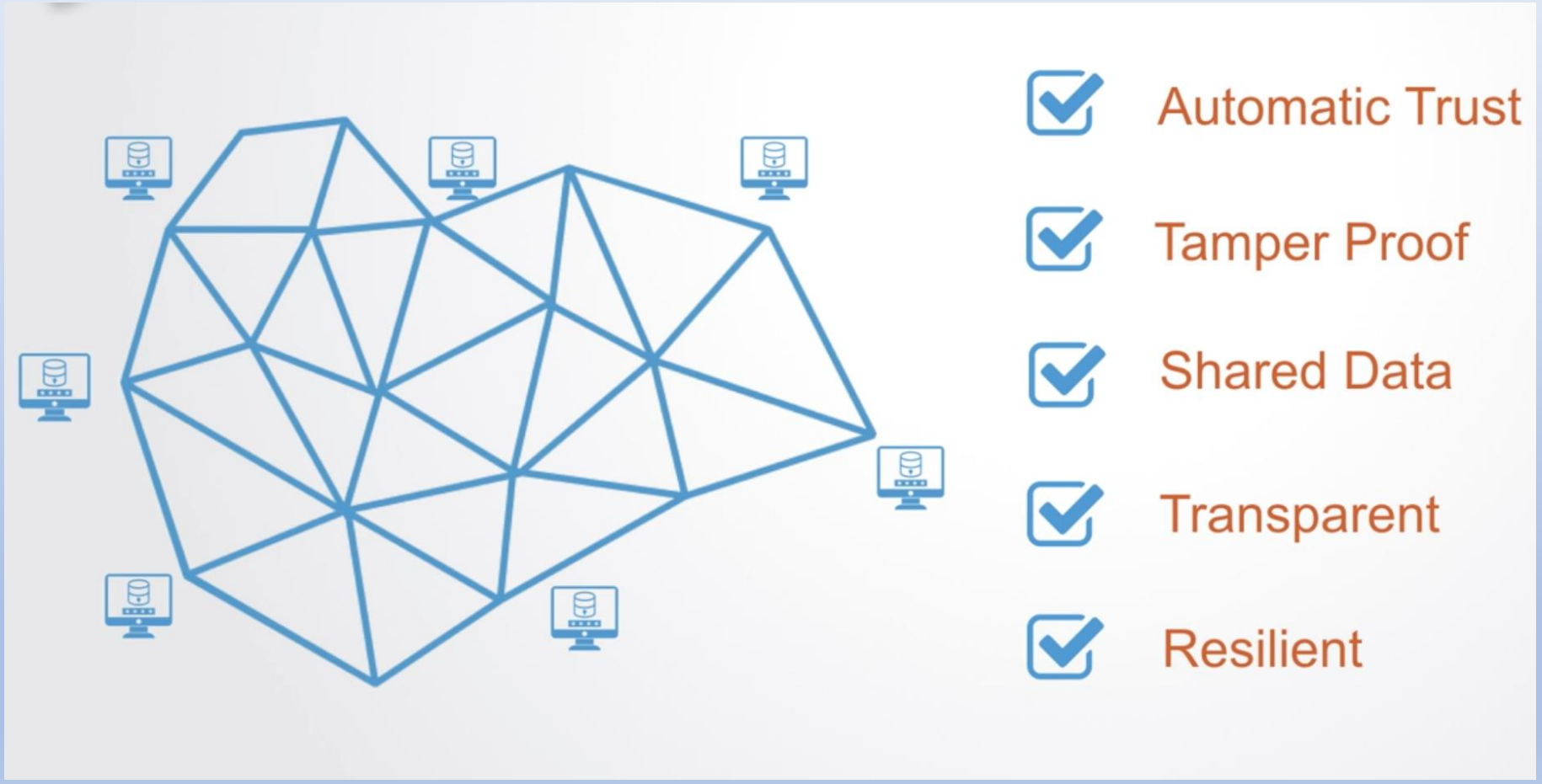
Blockchain Consensus Algorithms

- **Proof-of-work (PoW)**
  - PoW is a transaction validation and consensus mechanism used in blockchain platforms.
  - Miners on the blockchain network create their own blocks by collecting the new transactions and then compute a proof-of-work for their blocks.
  - Proof-of-work (PoW) is a cryptographically secure nonce that proves that a certain amount of work was done to find the nonce input to the PoW algorithm.
- **Proof-of-Stake (PoS)**
  - PoS is an alternative to PoW for providing consensus and preventing double-spend on a blockchain platform.
  - Unlike PoW, in PoS, there is no mining involved. Instead, PoS involves validating the blocks and the peers who perform block validation are called validators.
  - Each validator owns a ‘stake’ in the network in the form of a bond or security-deposit.
  - PoS algorithm randomly selects a validator and assigns it the right to create the next block
- **Proof of Authority (PoA)**
  - Proof of Authority (PoA) is a modified form of Proof of Stake (PoS) where instead of stake with the monetary value, a validator's identity performs the role of stake.
  - Staking identity means voluntarily disclosing who you are in exchange for the right to validate the blocks.
  - Transactions and blocks are validated by approved accounts, known as validators.

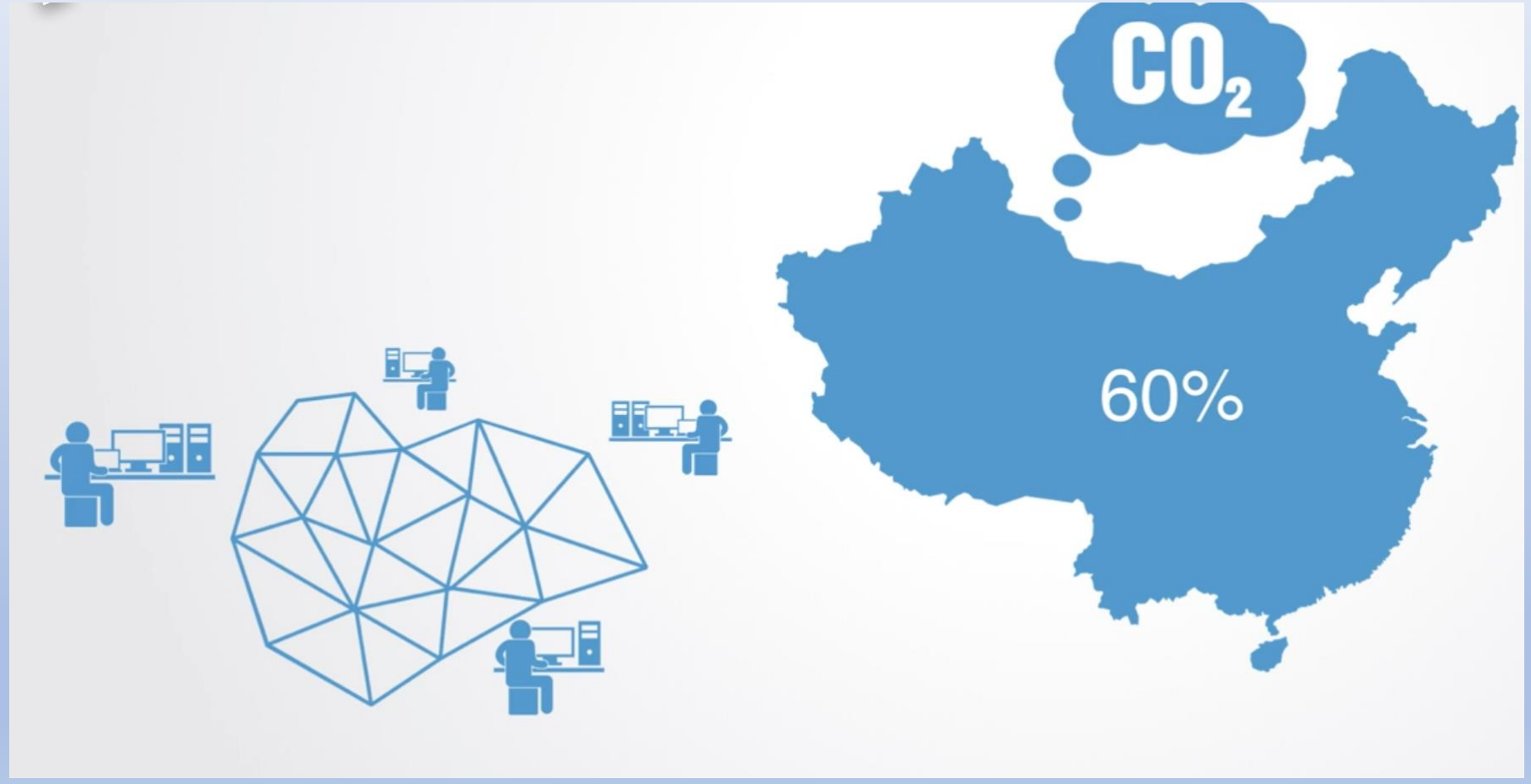
Consensus Algorithms Used by Blockchains

Blockchain Network	Consensus
Bitcoin	Proof of Work
Ethereum	Proof of Work (Ethash)
Ethereum Kovan Testnet	Proof of Authority
Neo	Proof of Stake
Lisk	Delegated Proof of Stake
EOS	Delegated Proof of Stake
Hyperledger	Practical Byzantine Fault Tolerance (PBFT)
Ripple	Ripple Protocol consensus algorithm (RPCA)

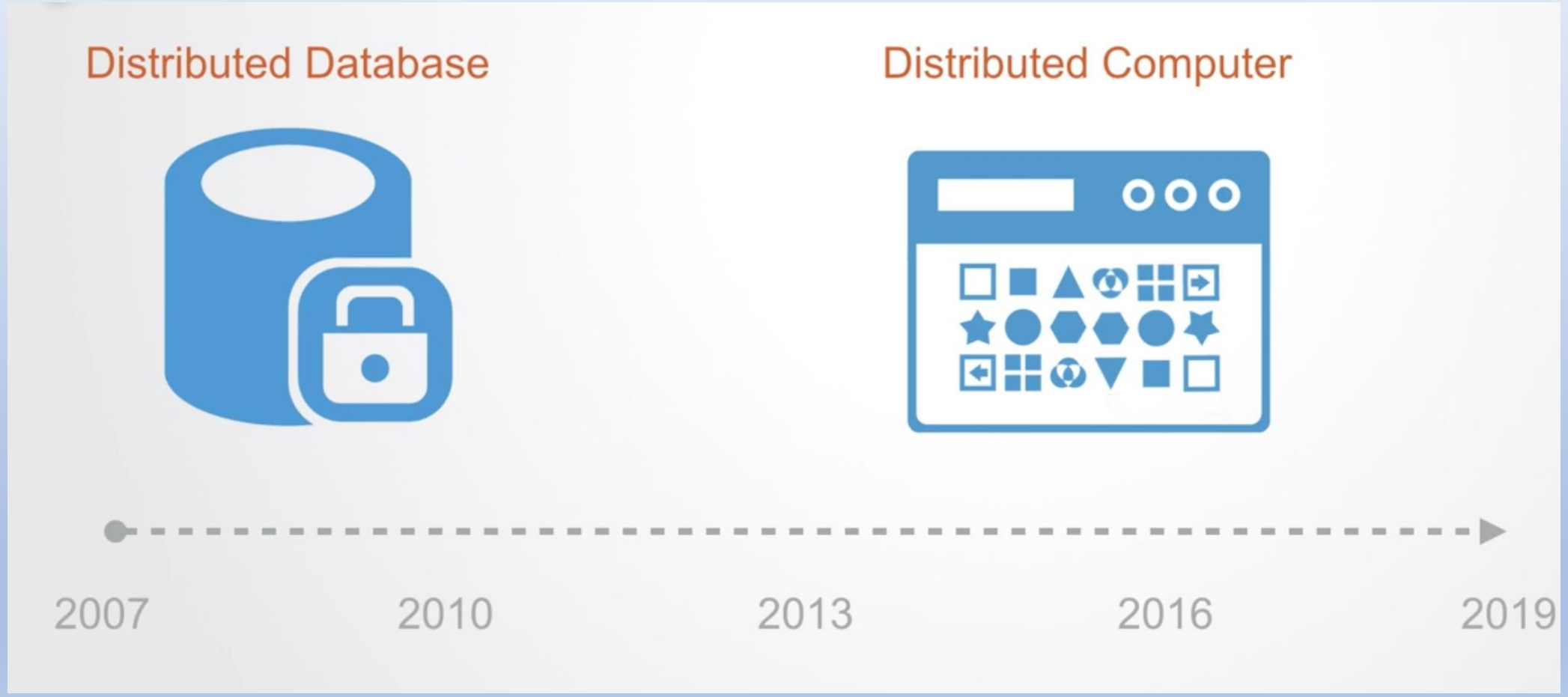
Blockchain Replicates Processing on Nodes



Blockchains Consume a Lot of Energy

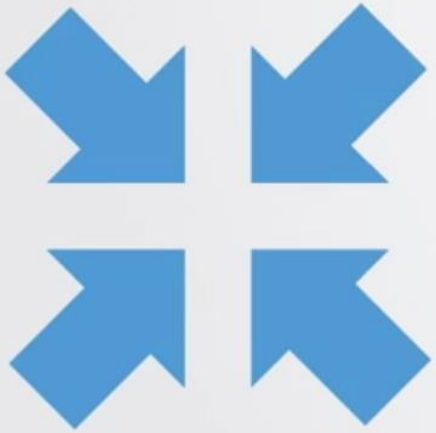


Blockchain is at least a secure distributed databaseo – Fast Forward

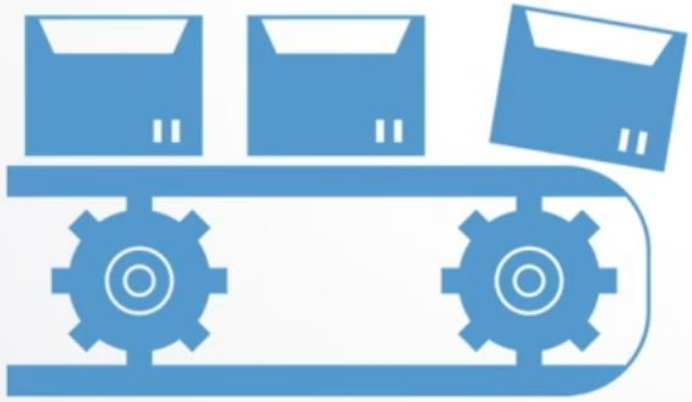


Industrial & Information Revolution

Centralization



Mass Production

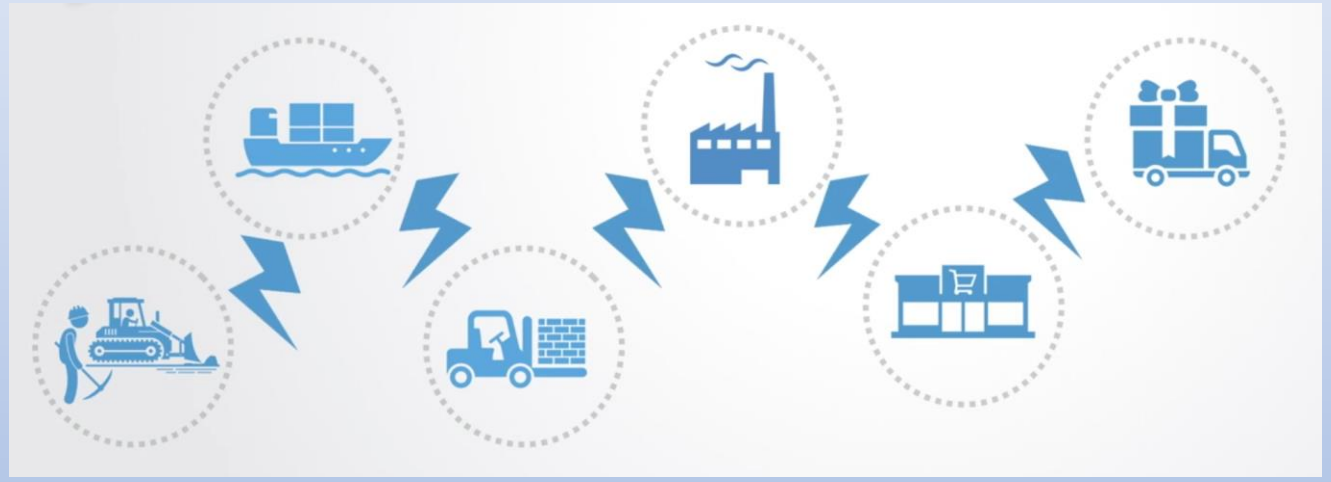


Economies of Scale

Organizations not designed to work with or trust other organizations

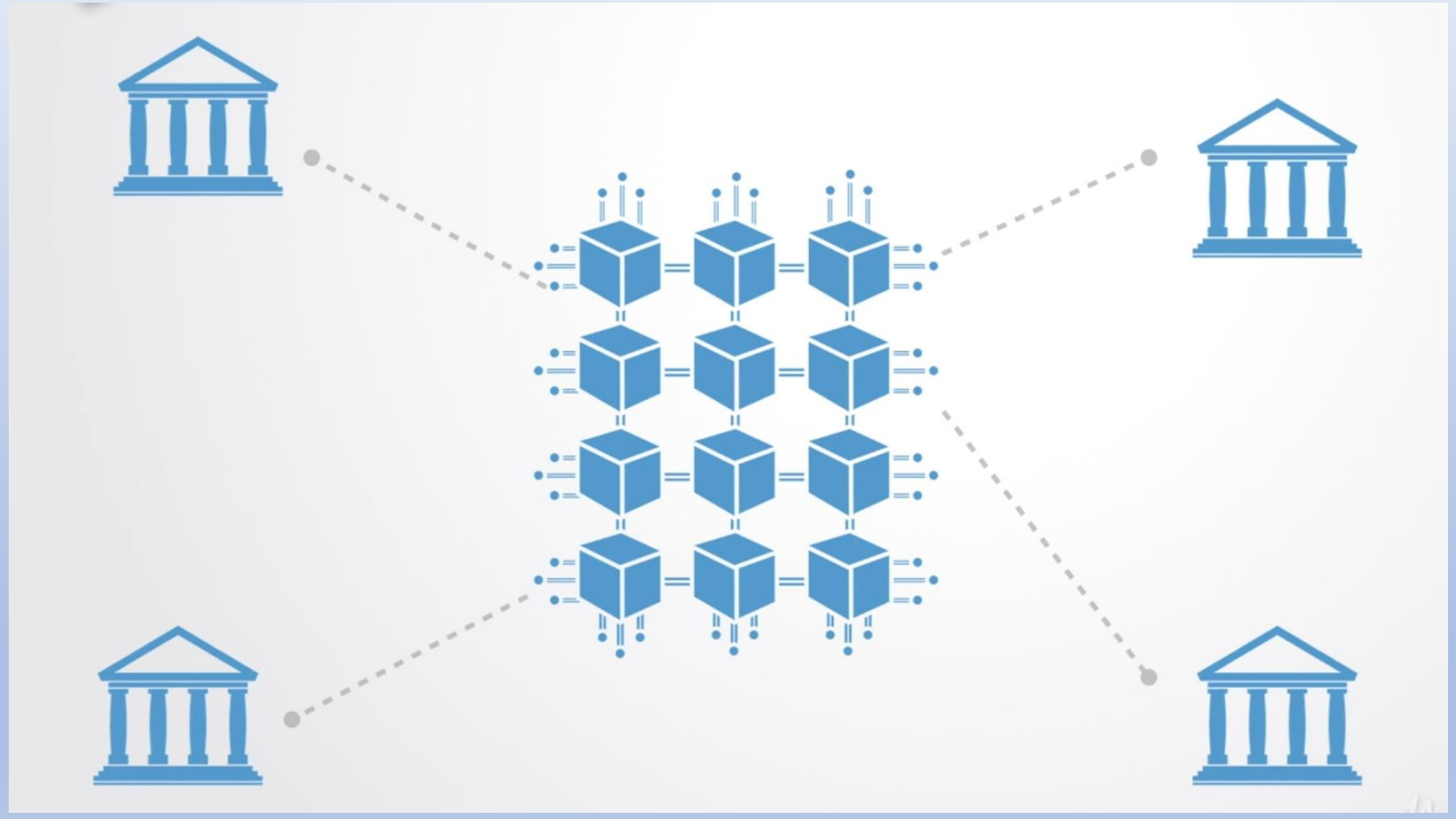
- Results

- Inefficiency
- Competition with cooperation



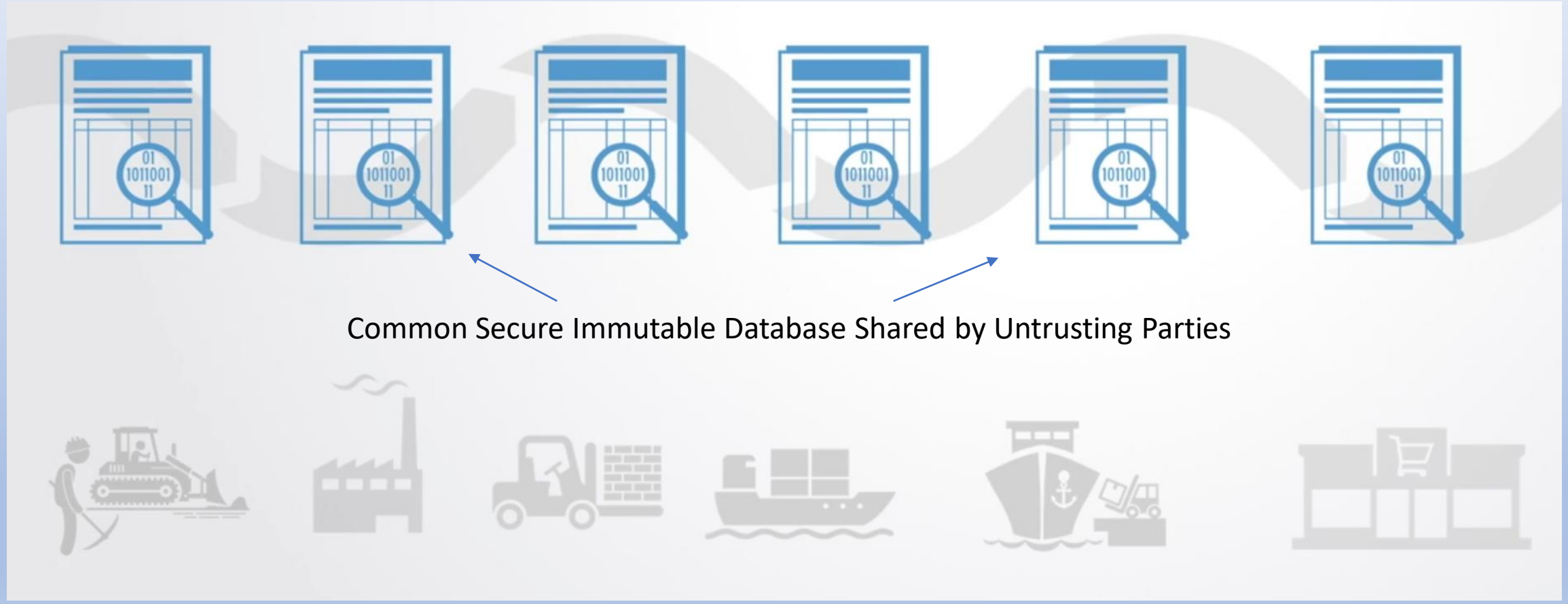
Current Disorganized Centralized Organizations

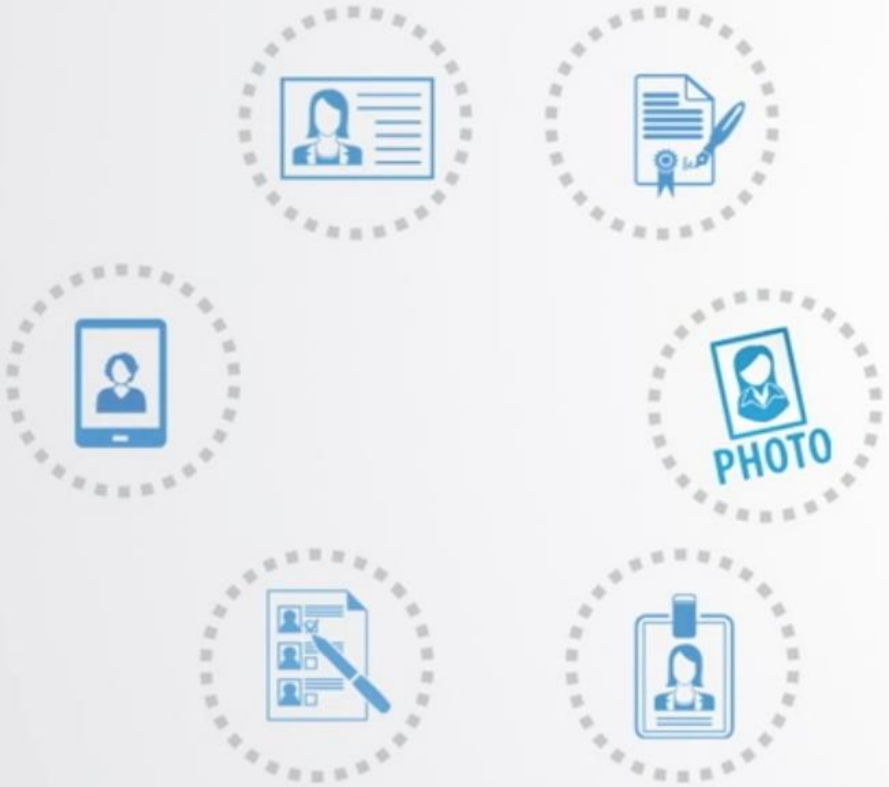
Blockchain Forces a Common Secure Database



Each organization has its own data & formats

Blockchain Allows Frictionless Processes between Organization





Interference

1 - 1 = 0

Synergies

1 + 1 = 3

What is the ”New” Token Model ?

Get rid of the middle guys – decentralization !

Peer

Value or Token Layer

Information Layer

Products or Service Layer

This is what Blockchain and Web 3.0 seek to accomplish !

Token is a programmable unit of value

Blood Diamonds

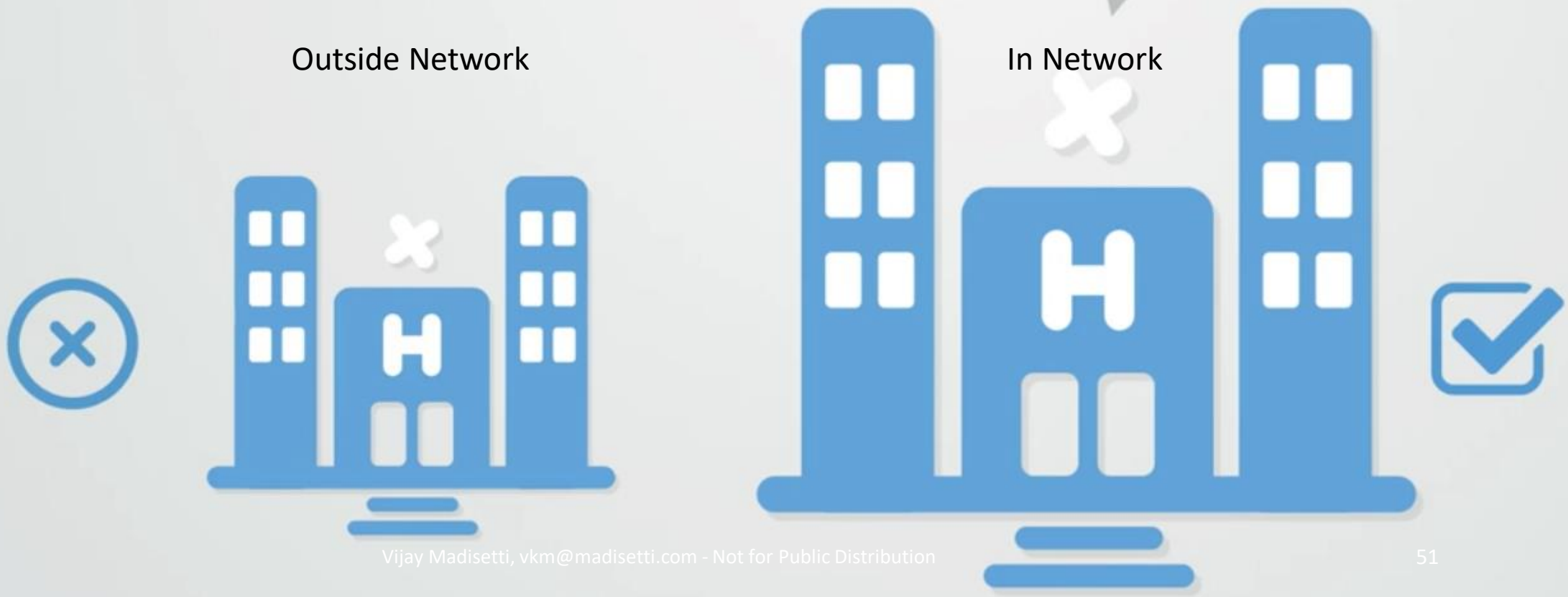
Legal Diamonds

Token is a programmable unit of value

Health Care Networks

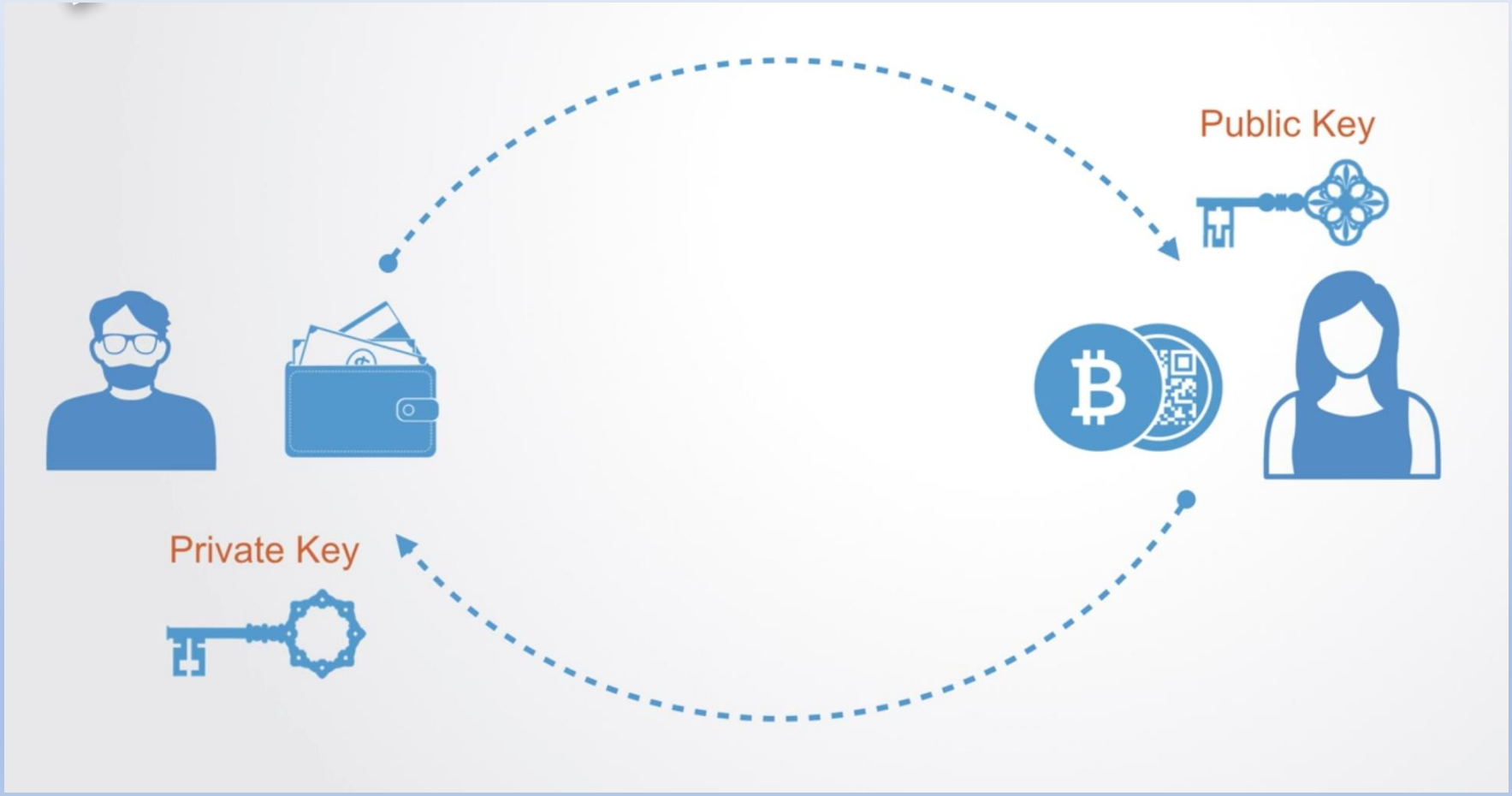
Outside Network

In Network

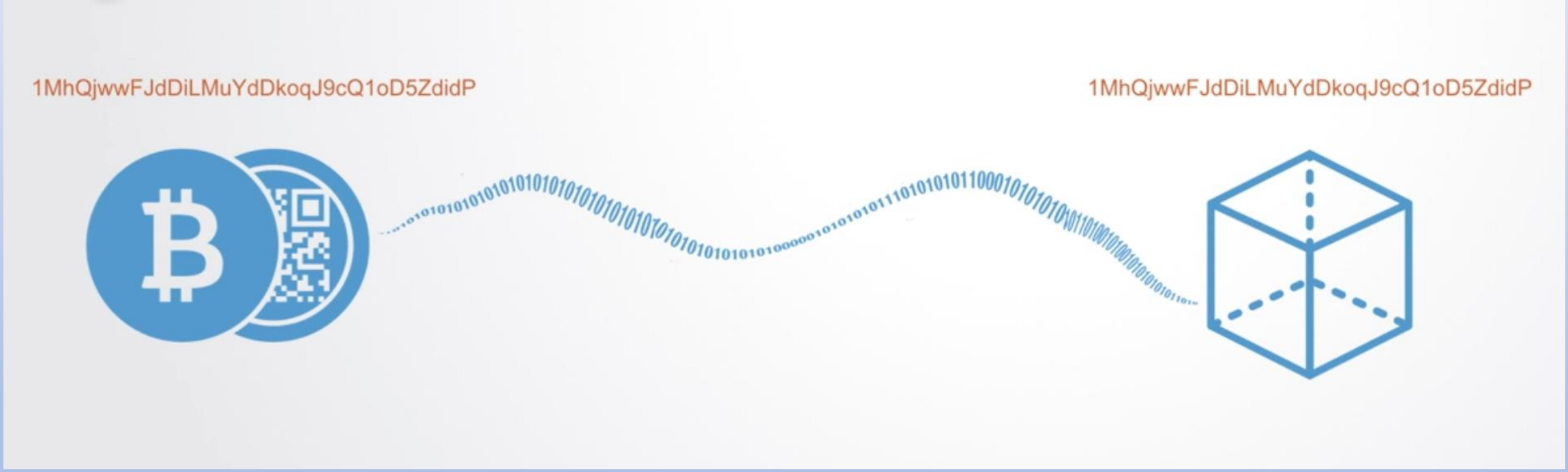


Encryption and Privacy

How a Peer to Peer Transaction Works ?



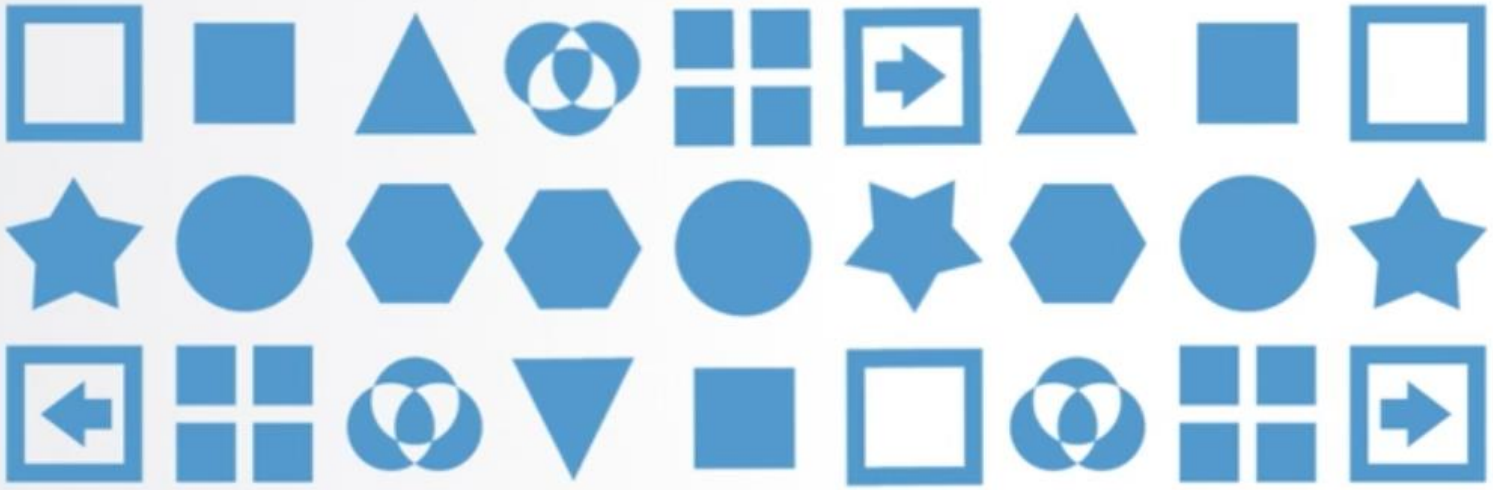
The Transaction is Recorded in a Block



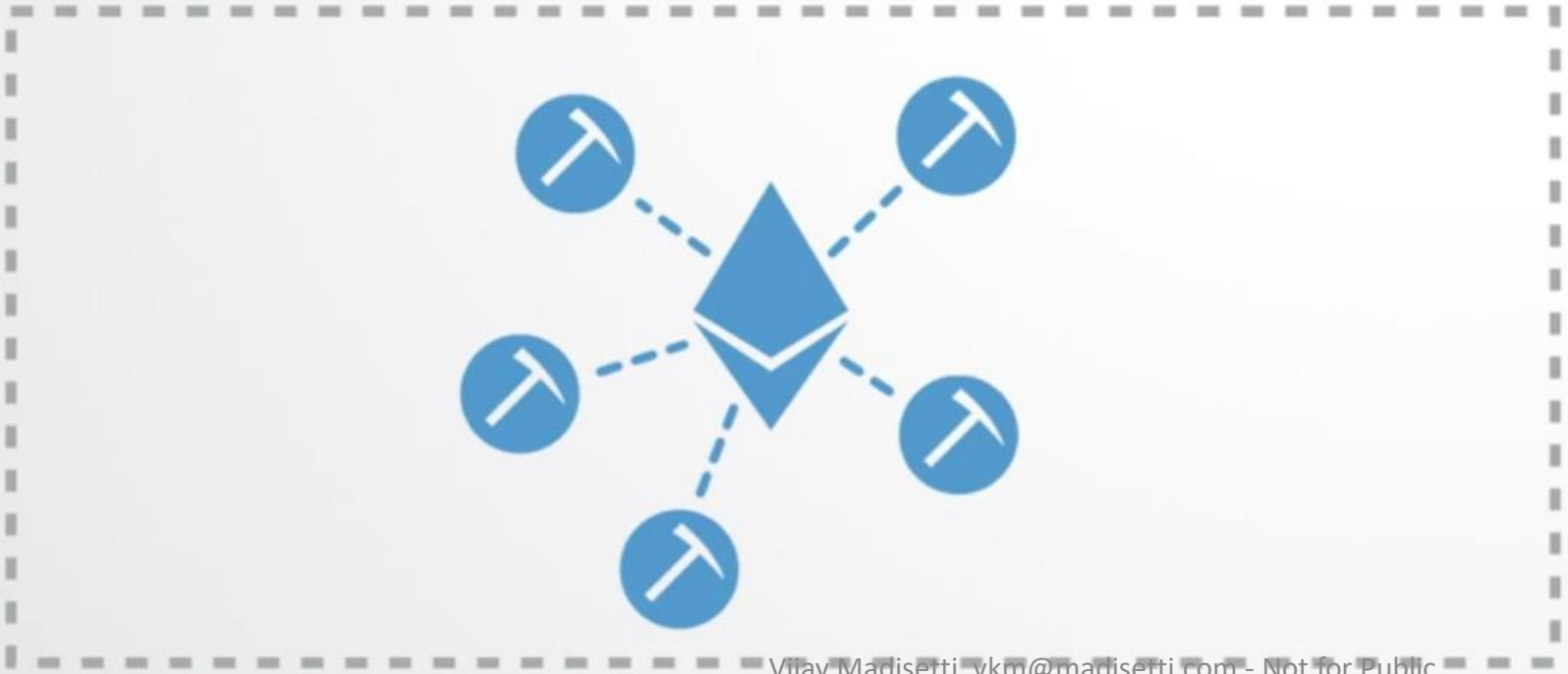
Distributed Database

Distributed Cloud Computer

2007 2010 2013 2016 2019

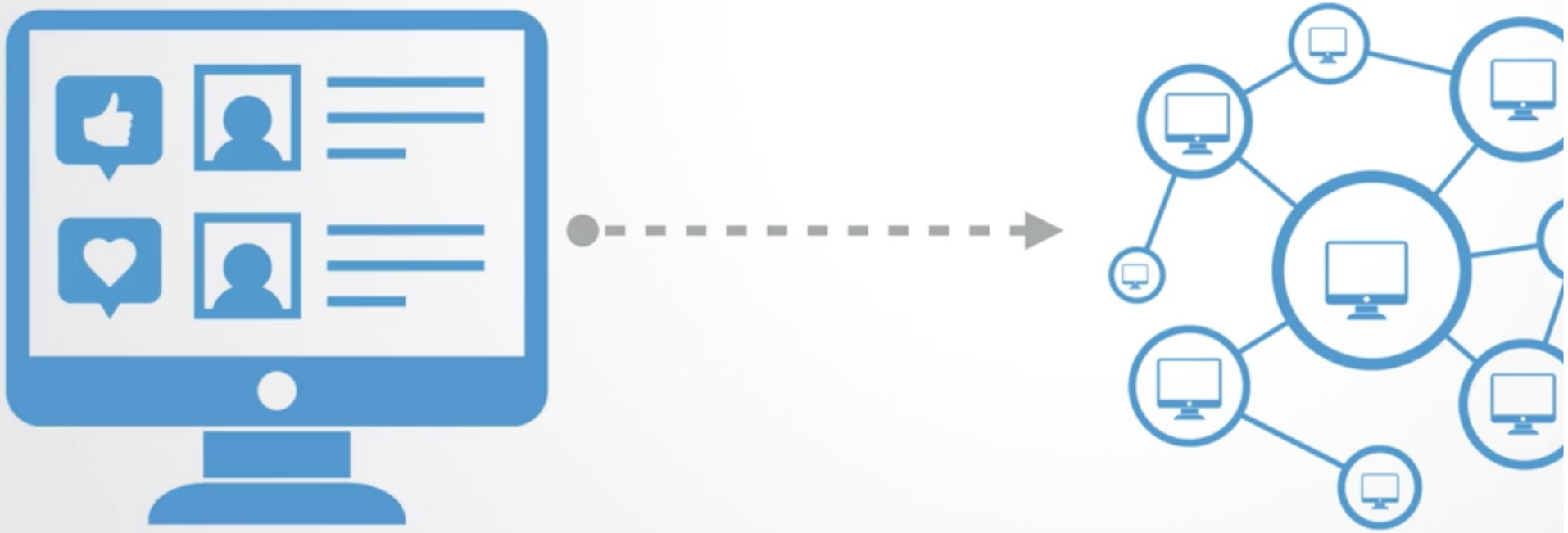


Dapps



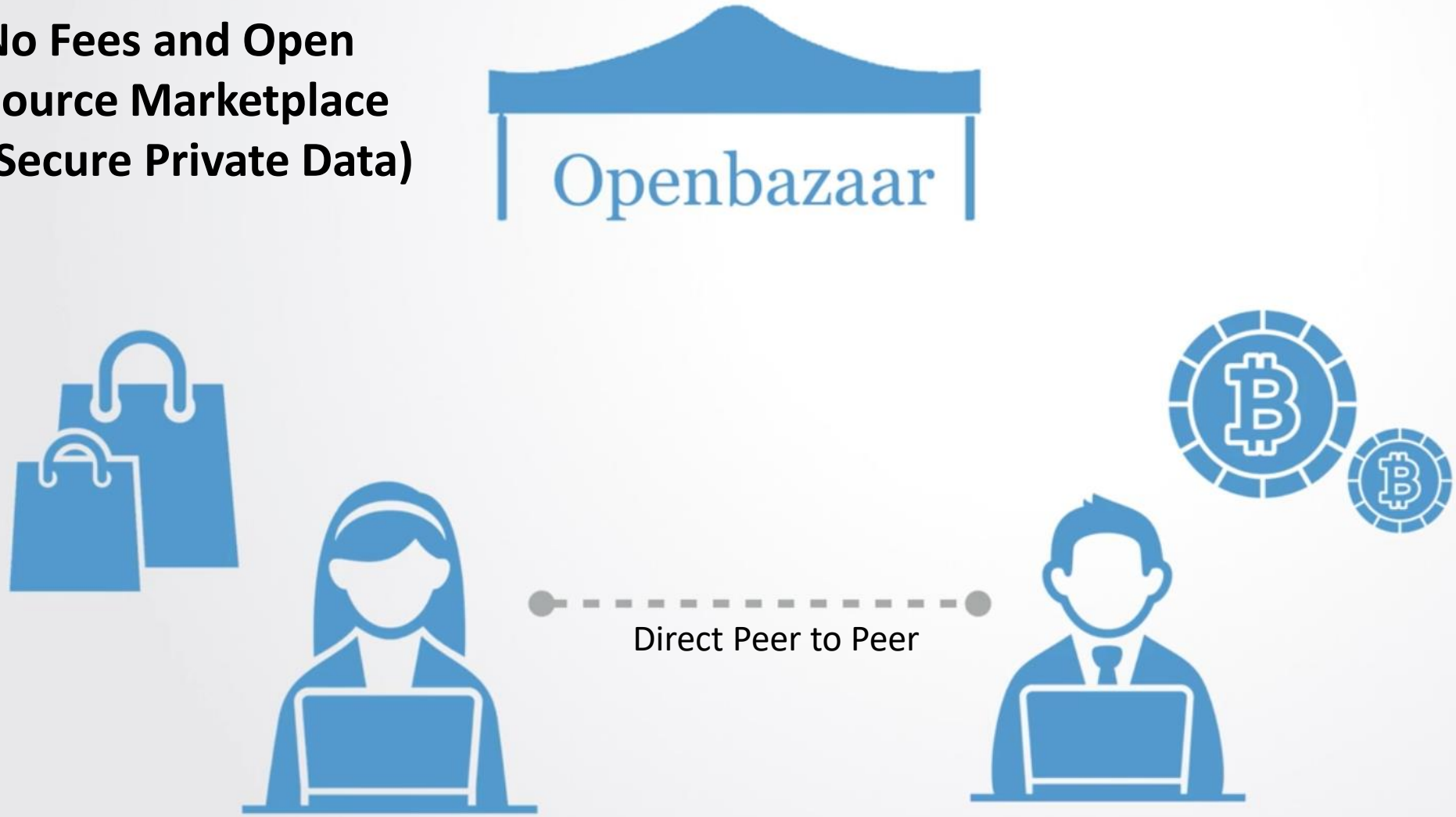
Ethereum

Daaps – Decentralized Applications



Not just financial applications

No Fees and Open Source Marketplace (Secure Private Data)



Secure

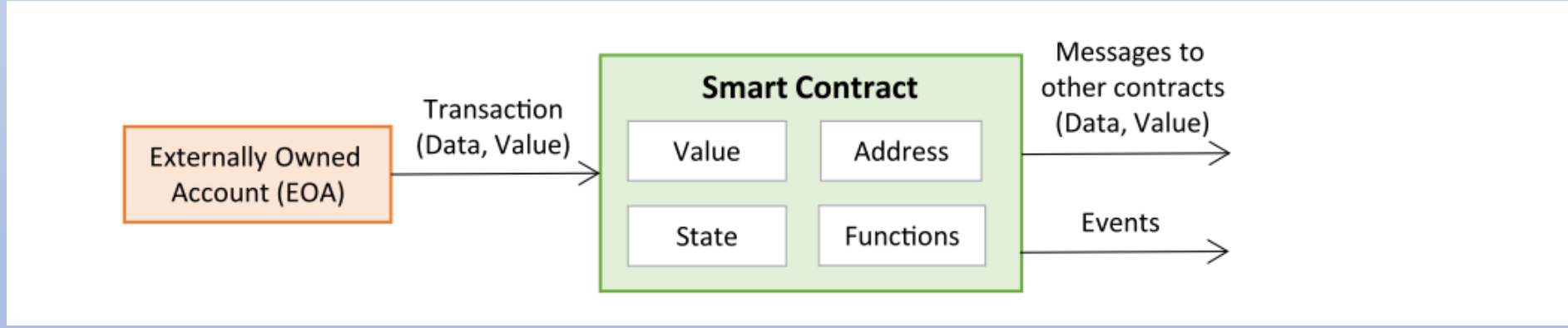
Decentralized

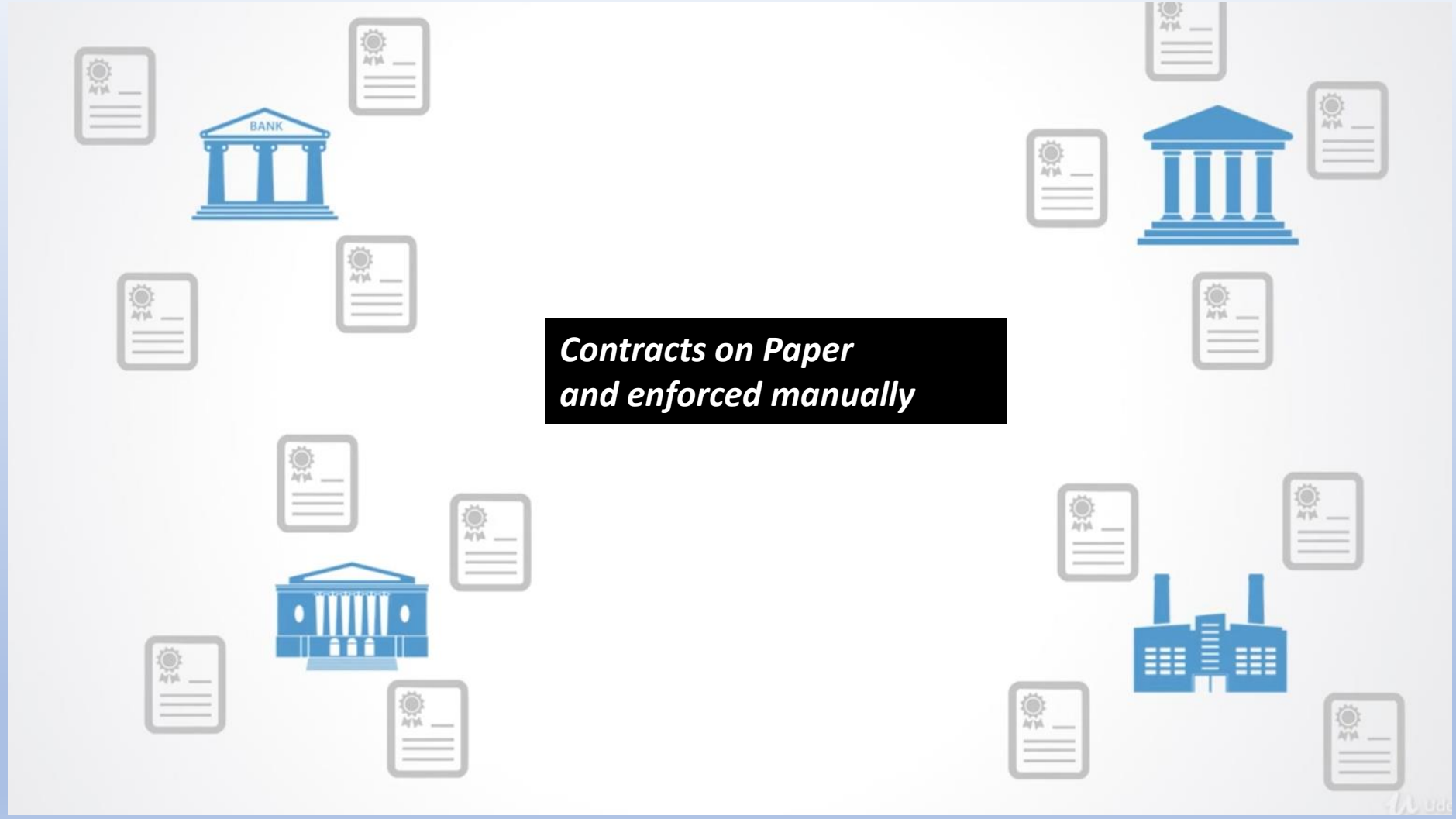
Automated

Advantages of Dapps

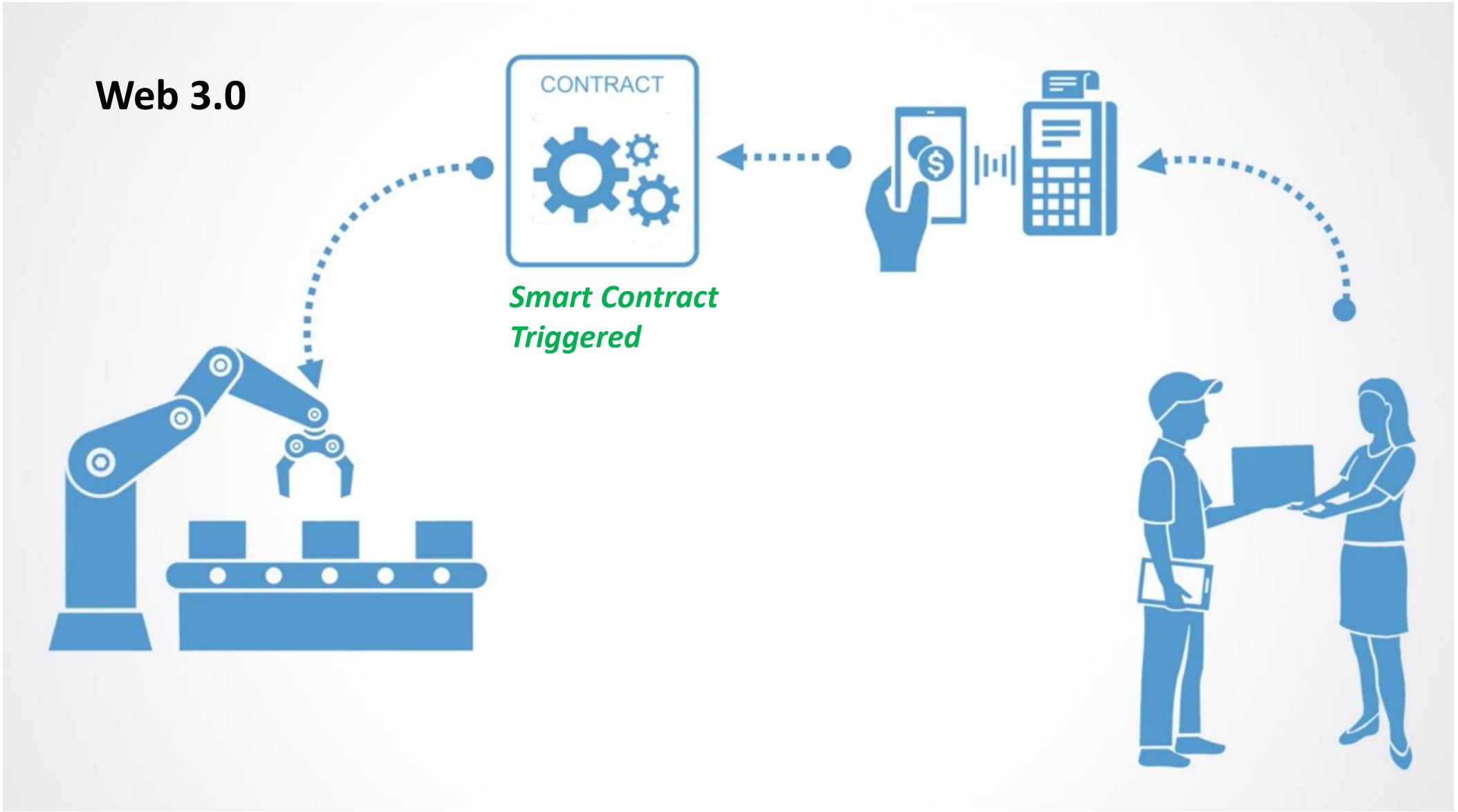
Smart Contracts

- **Smart Contract**:
  - A smart contract is a piece of code that resides on a Blockchain and is identified by a unique address.
  - A smart contract includes a set of executable functions and state variables.
  - The functions are executed when transactions are made to these functions.

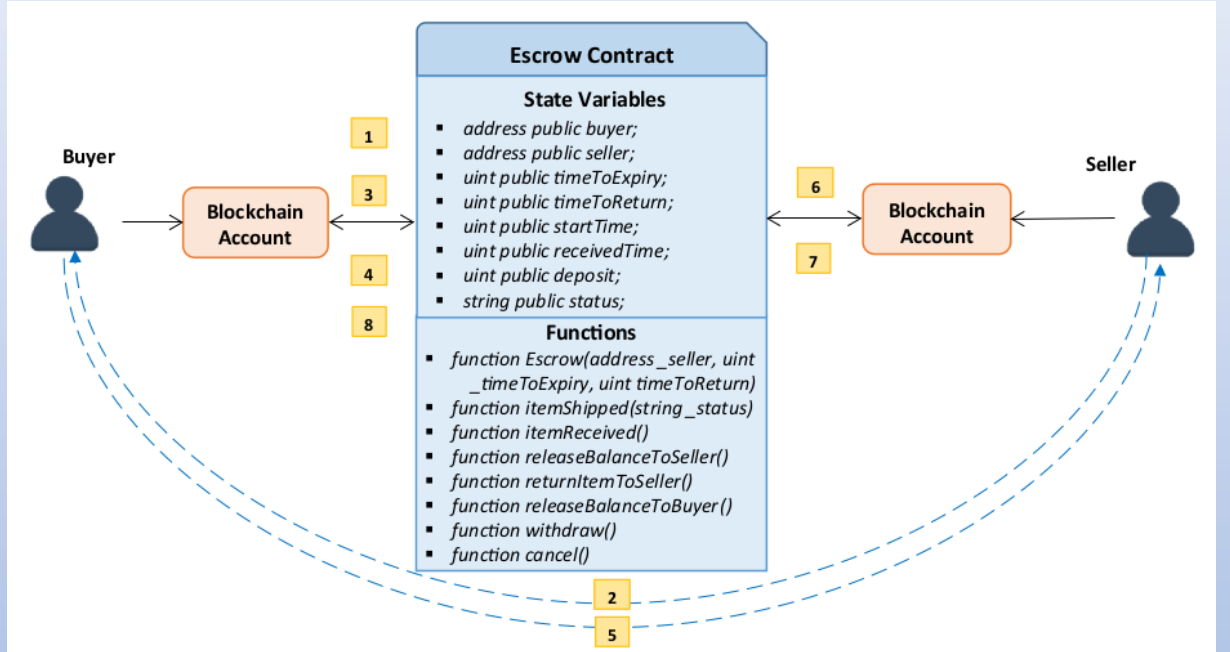



BANK
Contracts on Paper
and enforced manually

Web 3.0

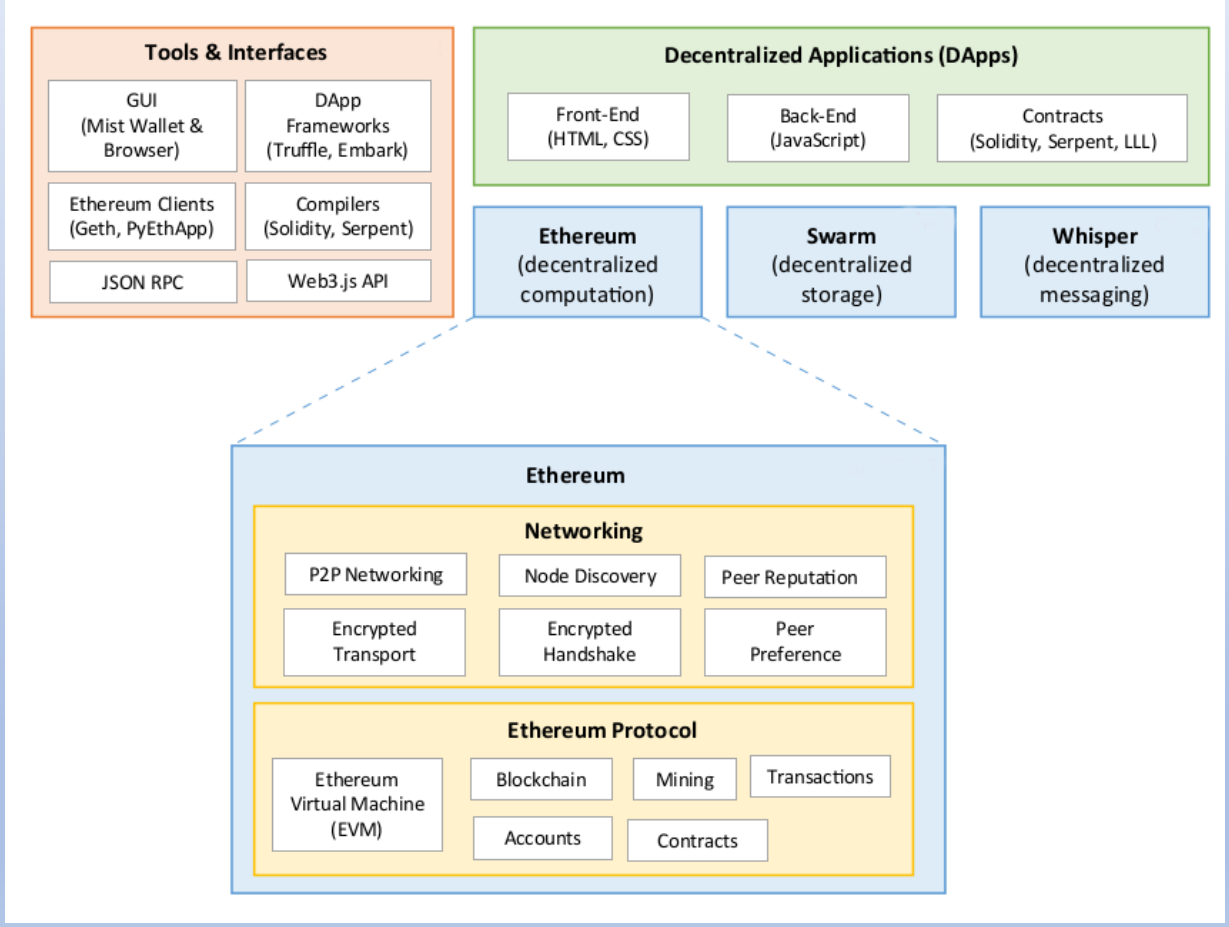


Escrow Smart Contract



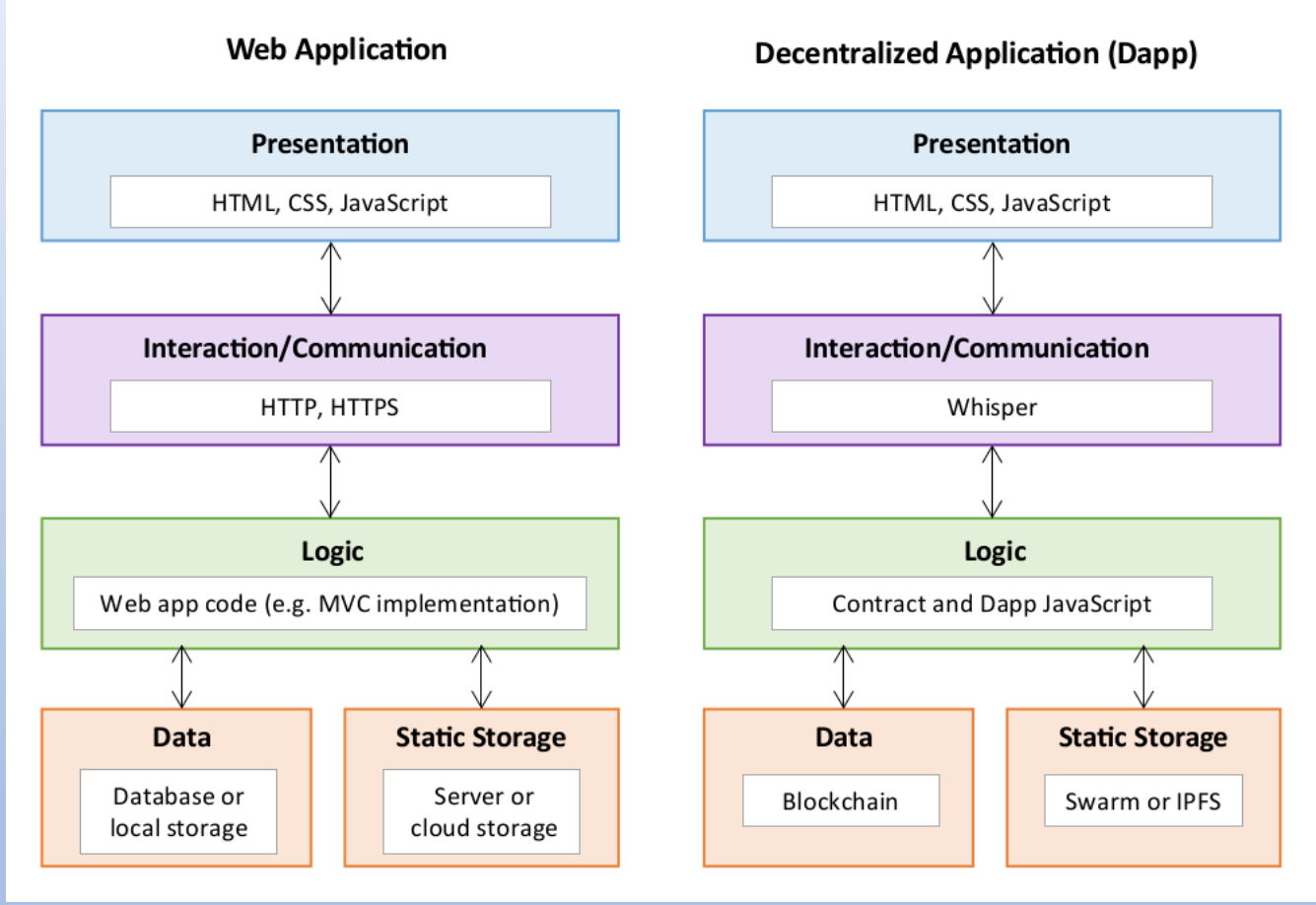
1. Buyer sets up Escrow contract and makes deposit. Deposit is held in the contract account.
2. Seller ships item to buyer and updates item shipment information.
3. Buyer checks the delivered item and releases 20% of the Escrow deposit.
4. If the buyer is satisfied with the item, the buyer releases the balance deposit to the seller.
5. If the buyer is not satisfied with the item, the buyer can return the item.
6. Seller releases the balance deposit to buyer upon receiving the item returned by the buyer. Seller keep 20% as restocking fees.
7. Seller can cancel the escrow and return the deposit held in the contract account to buyer.
8. Buyer can withdraw the deposit upon the expiry of the contract, if the item is not received.

Blockchain Stack



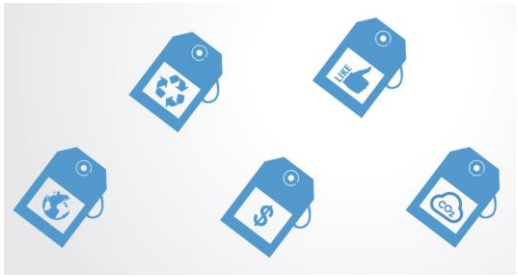
Web App vs Decentralized App

- Web Apps
  - Most Web 2.0 applications are centralized in nature and are deployed on one or more server instances under the control of a single organization or a cloud platform.
- Dapps
  - Dapps are decentralized in nature with no single entity or organization controlling the infrastructure on which the applications are deployed. In the context of Ethereum, Dapps are backed by smart contracts which are deployed on the Ethereum blockchain platform that is maintained by the Ethereum nodes or peers worldwide.



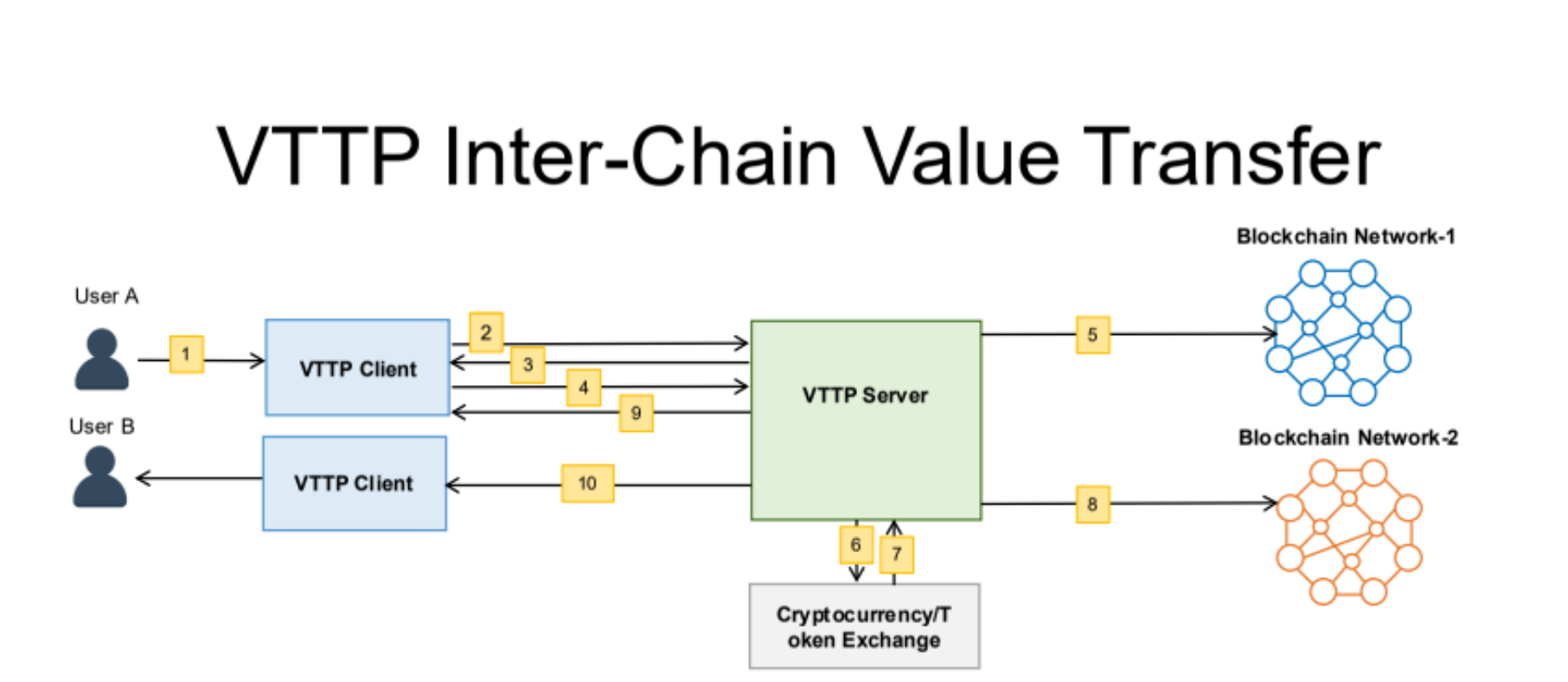
Internet of Value

- Allow seamless exchange of value between peers without central authorities
- Today even sending money across the world has significant barriers, let alone value exchange
- In a services oriented world value is defined differently



Value Token Transfer Protocol (VTTP)

- Does to the token-based economy what **http** did to Internet



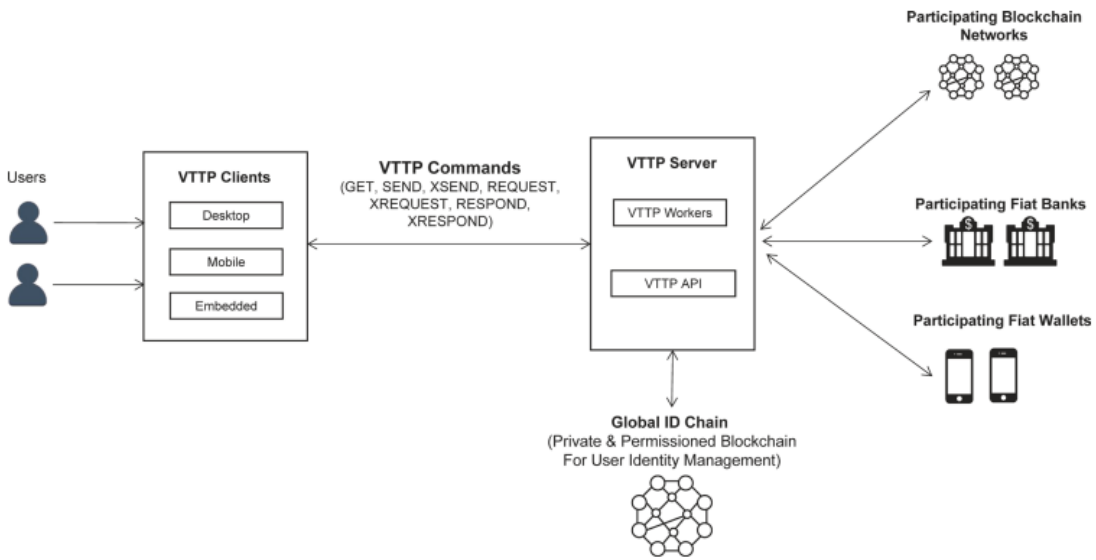


Figure 1. VTTP components.

Scientific Research Publishing

Journal of Software Engineering and Applications, 2020, 13, 303-311
https://www.scirp.org/journal/jsea
ISSN Online: 1945-3124
ISSN Print: 1945-3116

A Value Token Transfer Protocol (VTTP) for Decentralized Finance

Arshdeep Bahga, Vijay K. Madisetti

Georgia Institute of Technology, Atlanta, GA, USA
Email: arshdeepbahga@gmail.com, vkm@gatech.edu

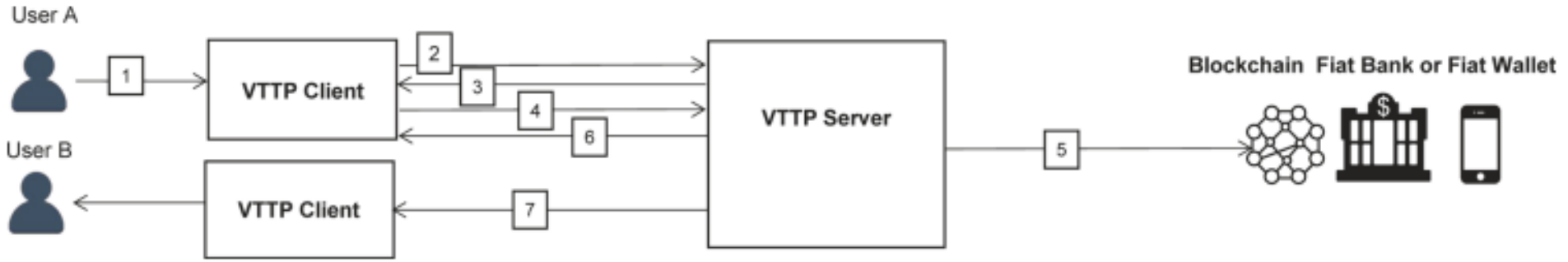


Figure 3. VTTP intra-chain value transfer process.

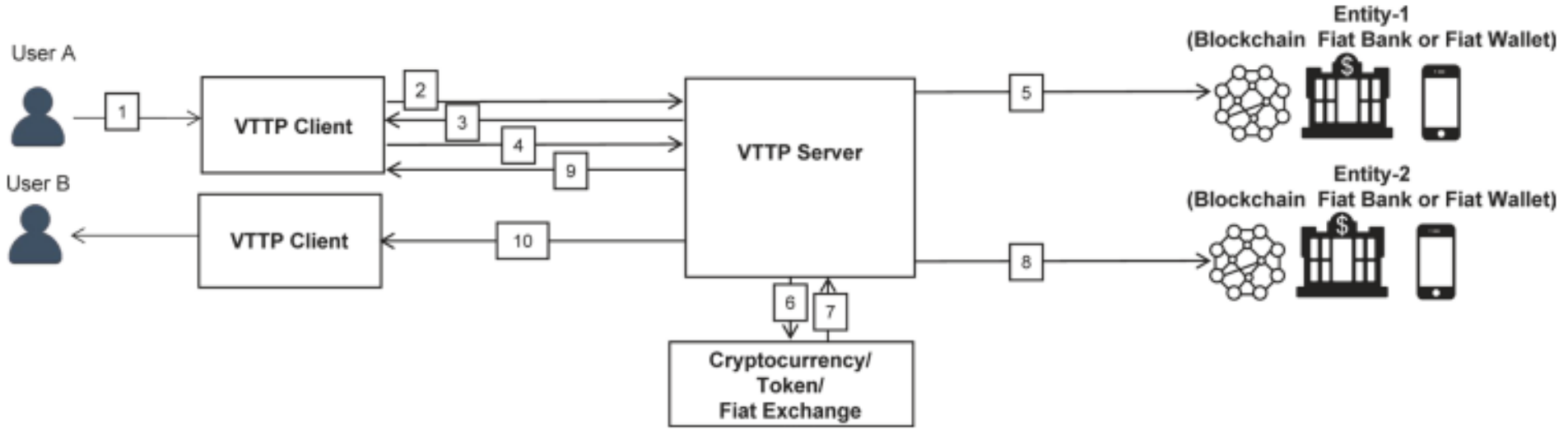


Figure 4. VTTP inter-chain value transfer process.

Method and system for tuning blockchain scalability for fast and low-cost ...

US • US10394845B2 • Vijay **Madisetti** • Vijay K. Madisetti

Priority 2017-04-12 • Filed 2018-12-18 • Granted 2019-08-27 • Published 2019-08-27

A method of synchronizing transactions between blockchains including receiving a first plurality of transactions and recording the first plurality of transactions to a first private block on a private blockchain network, receiving a second plurality of transactions and recording the second ...

Method and system for blockchain-based combined identity, ownership, integrity ...

US • US10204339B2 • Vijay K. **Madisetti** • Vijay K. Madisetti

Priority 2017-03-31 • Filed 2018-08-31 • Granted 2019-02-12 • Published 2019-02-12

A method of issuing blockchain-based digital certificates including receiving from a user hashed user identification information and object information, recording to a digital certificate smart contract deployed at a digital certificate smart contract address on a blockchain network the hashed ...

Method and system for tuning blockchain scalability, decentralization, and ...

US • US10579643B2 • Vijay **Madisetti** • Vijay Madisetti

Priority 2017-04-12 • Filed 2019-09-09 • Granted 2020-03-03 • Published 2020-03-03

A method for sharing data between blockchains in a multi-chain network including receiving a first plurality of account addresses associated with first and second blockchains and an account state for each account associated with the first plurality of account addresses, generating a first hash ...

Tokens or crypto currency using smart contracts and blockchains

US • US10243743B1 • Vijay K. **Madisetti** • Vijay K. Madisetti

Priority 2017-09-13 • Filed 2018-09-11 • Granted 2019-03-26 • Published 2019-03-26

A method of exchanging value across a blockchain network comprising receiving first and second transaction smart contracts, recording the first transaction smart contract to the second transaction smart contract, and registering global variable names and defining values thereof. The method further ...

Methods and systems for operating secure digital management aware applications

US • US9935772B1 • Vijay K **Madisetti** • Vijay K Madisetti

Priority 2016-02-19 • Filed 2017-08-15 • Granted 2018-04-03 • Published 2018-04-03

A system and method for servicing secure data object management aware applications using a cloud-based host environment and a local secure container. The cloud-based host environment creates a controlled digital object from a master digital object, and activates a tether associated with the ...

(12) **INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)**

(19) **World Intellectual Property Organization**
International Bureau

(43) **International Publication Date**
24 September 2020 (24.09.2020)

WIPO | PCT

(10) **International Publication Number**
WO 2020/190720 A1

(51) **International Patent Classification:**
G06Q 20/36 (2012.01) *H04L 9/08* (2006.01)
G06Q 20/38 (2012.01)

(21) **International Application Number:**
PCT/US2020/022632

(22) **International Filing Date:**
13 March 2020 (13.03.2020)

(25) **Filing Language:** English

(26) **Publication Language:** English

(30) **Priority Data:**
62/818,798 15 March 2019 (15.03.2019) US

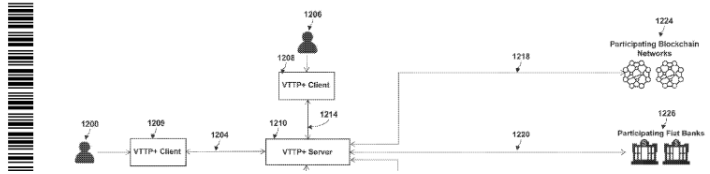
(72) **Inventor; and**
(71) **Applicant: MADISETTI, Vijay** [US/US]; 56 Creekside Park Drive, Johns Creek, Georgia 30022 (US).

(72) **Inventor: BAHGA, Arshdeep;** No 335 RCS - CPS En-clave, Sector 48A, Chandigarh 160047 (IN).

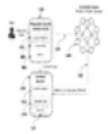
(74) **Agent: PIERRON, Daniel;** 1990 W. New Haven Avenue, Second Floor, Melbourne, Florida 32904 (US).

(81) **Designated States** *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, WS, ZA, ZM, ZW.

(54) **Title:** METHOD AND SYSTEM FOR EXCHANGE OF VALUE OR TOKENS BETWEEN BLOCKCHAIN NETWORKS



Method and system for tuning blockchain scalability for fast and low-cost ...



US • US10394845B2 • Vijay **Madisetti** • Vijay K. Madisetti

Priority 2017-04-12 • Filed 2018-12-18 • Granted 2019-08-27 • Published 2019-08-27

A method of synchronizing transactions between blockchains including receiving a first plurality of transactions and recording the first plurality of transactions to a first private block on a private blockchain network, receiving a second plurality of transactions and recording the second ...

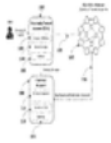
Method and system for blockchain-based combined identity, ownership, integrity ...

US • US10204339B2 • Vijay K. **Madisetti** • Vijay K. Madisetti

Priority 2017-03-31 • Filed 2018-08-31 • Granted 2019-02-12 • Published 2019-02-12

A method of issuing blockchain-based digital certificates including receiving from a user hashed user identification information and object information, recording to a digital certificate smart contract deployed at a digital certificate smart contract address on a blockchain network the hashed ...

Method and system for tuning blockchain scalability, decentralization, and ...



US • US10579643B2 • Vijay **Madisetti** • Vijay Madisetti

Priority 2017-04-12 • Filed 2019-09-09 • Granted 2020-03-03 • Published 2020-03-03

A method for sharing data between blockchains in a multi-chain network including receiving a first plurality of account addresses associated with first and second blockchains and an account state for each account associated with the first plurality of account addresses, generating a first hash ...

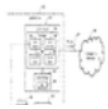
Tokens or crypto currency using smart contracts and blockchains

US • US10243743B1 • Vijay K. **Madisetti** • Vijay K. Madisetti

Priority 2017-09-13 • Filed 2018-09-11 • Granted 2019-03-26 • Published 2019-03-26

A method of exchanging value across a blockchain network comprising receiving first and second transaction smart contracts, recording the first transaction smart contract to the second transaction smart contract, and registering global variable names and defining values thereof. The method further ...

Methods and systems for operating secure digital management aware applications

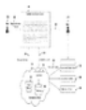


US • US9935772B1 • Vijay K **Madisetti** • Vijay K Madisetti

Priority 2016-02-19 • Filed 2017-08-15 • Granted 2018-04-03 • Published 2018-04-03

A system and method for servicing secure data object management aware applications using a cloud-based host environment and a local secure container. The cloud-based host environment creates a controlled digital

Method and system for real-time collaboration and annotation-based action …

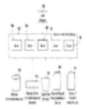


US • US20210081366A1 • Vijay **Madisetti** • Vijay Madisetti

Priority 2019-09-12 • Filed 2020-09-10 • Published 2021-03-18

A method of collaborating in real-time via action creation comprising detecting an annotation on a document, parsing the annotation; generating an action record responsive to information identified from parsing the annotation, and recording a generated action record to the action database. Action …

Method and system for persistent helpers for functions as a service (faas) in …



US • US20210042098A1 • Vijay **Madisetti** • Vijay Madisetti

Priority 2019-08-09 • Filed 2020-07-29 • Published 2021-02-11

A method for improving the performance of functions-as-a-service including receiving a first function call comprising a first argument, performing a first function responsive to the first argument comprised by the first function call, producing a first function result, generating a first …

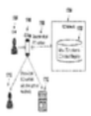
Method and system for securing cloud storage and databases from insider threats …

WO **US** • US10503927B1 • Vijay **Madisetti** • Vijay Madisetti

Priority 2018-12-20 • Filed 2019-07-09 • Granted 2019-12-10 • Published 2019-12-10

A method of optimizing performance of and securing cloud storage and databases comprising analyzing data comprised by a data request by an agent application on a computerized device, the data request being generated by a client application and inserting a tag into the data request responsive to …

System and Method for Processing Payments in Fiat Currency Using Blockchain and …

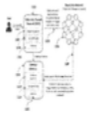


US • US20200005290A1 • Vijay **Madisetti** • Vijay Madisetti

Priority 2017-12-04 • Filed 2019-09-11 • Published 2020-01-02

A method of processing a payment including receiving a payment lookup request, identifying a user network account on a blockchain network, sending a payment authorization request to and receiving authorization from a user, transferring ownership of an in-network token responsive to the …

Method and System for Exchange of Value or Tokens Between Blockchain Networks



US • US20200151716A1 • Vijay **Madisetti** • Vijay Madisetti

Priority 2018-04-04 • Filed 2020-01-16 • Published 2020-05-14

A blockchain value transfer method including receiving a plurality of transaction requests, performing a balance check procedure on each transaction, determining a net transaction for each user account address for each transaction in an aggregate transaction record, and executing the net …

Example – *nCASH*

The **perfect** payments app for crypto & fiat currencies

nCash is a unique smartphone application that interfaces to a blockchain-based eCommerce platform that utilizes patent-pending technologies to allow its users to efficiently and securely conduct payments and transactions with affiliated merchants and other users.

GET APP NOW

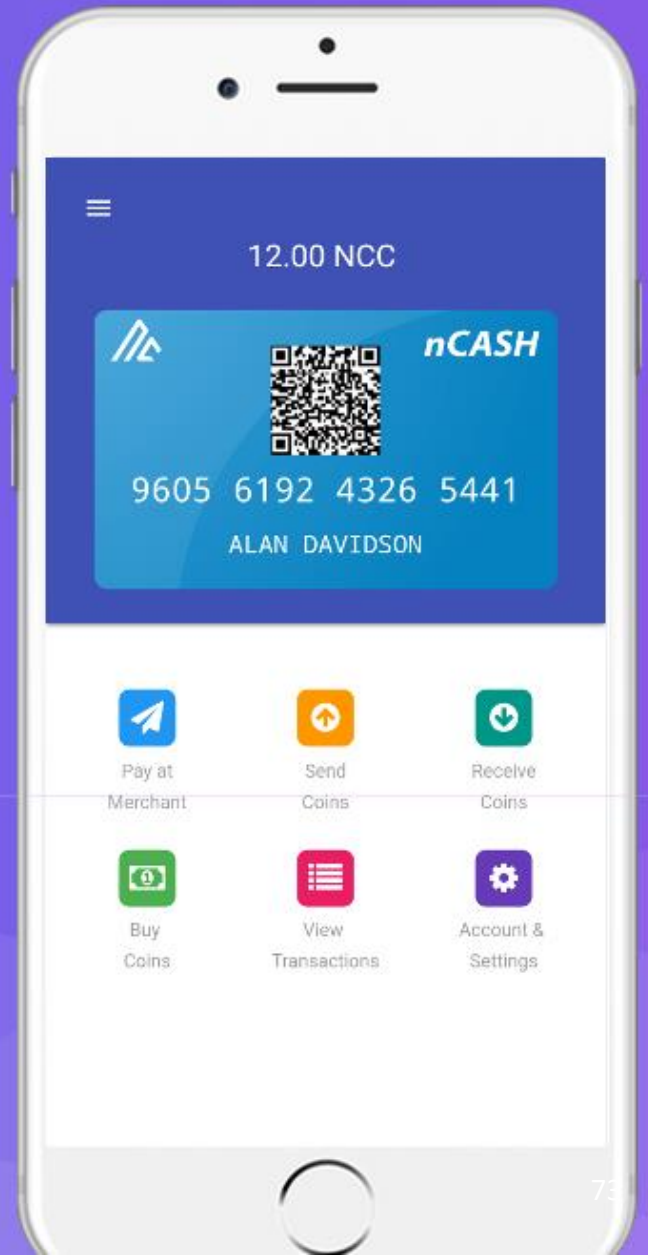
DISCOVER MORE

GET NCASH

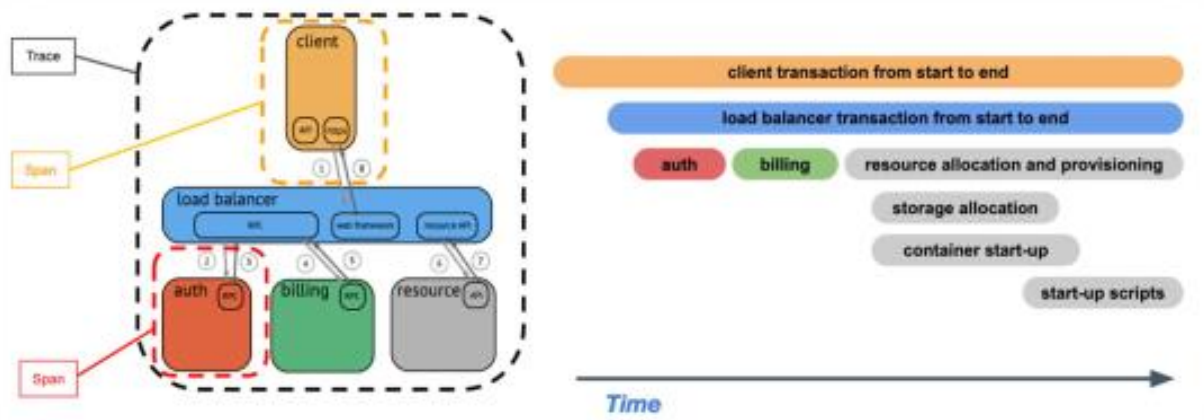
Get the nCash mobile wallet application and start sending and receiving payments in the supported currencies and tokens.

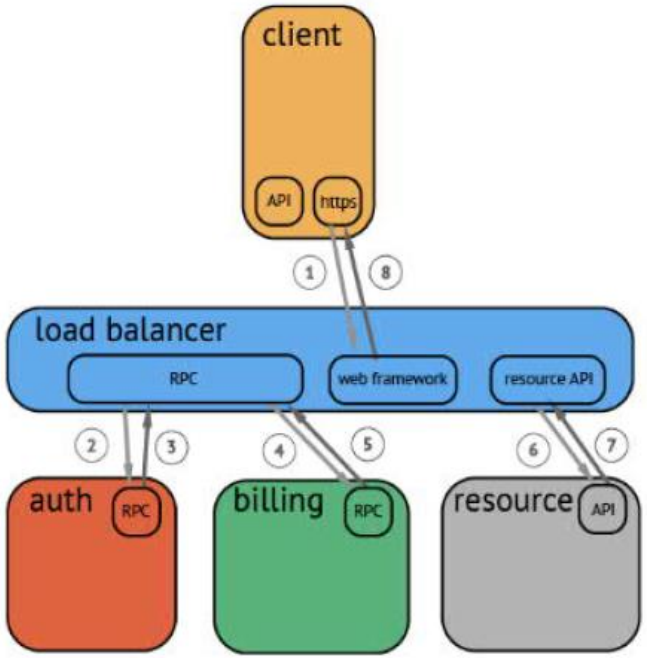
Download on the App Store

Get it on Google play



Using Traces/Spans for Optimizing Performance and Security





(12) **United States Patent**
Madisetti et al.

(10) **Patent No.: US 10,402,589 B1**
(45) **Date of Patent: Sep. 3, 2019**

(54) **METHOD AND SYSTEM FOR SECURING CLOUD STORAGE AND DATABASES FROM INSIDER THREATS AND OPTIMIZING PERFORMANCE**

(71) Applicant: **Vijay Madisetti**, Johns Creek, GA (US)

(72) Inventors: **Vijay Madisetti**, Johns Creek, GA (US); **Arshdeep Bahga**, Chandigarh (IN)

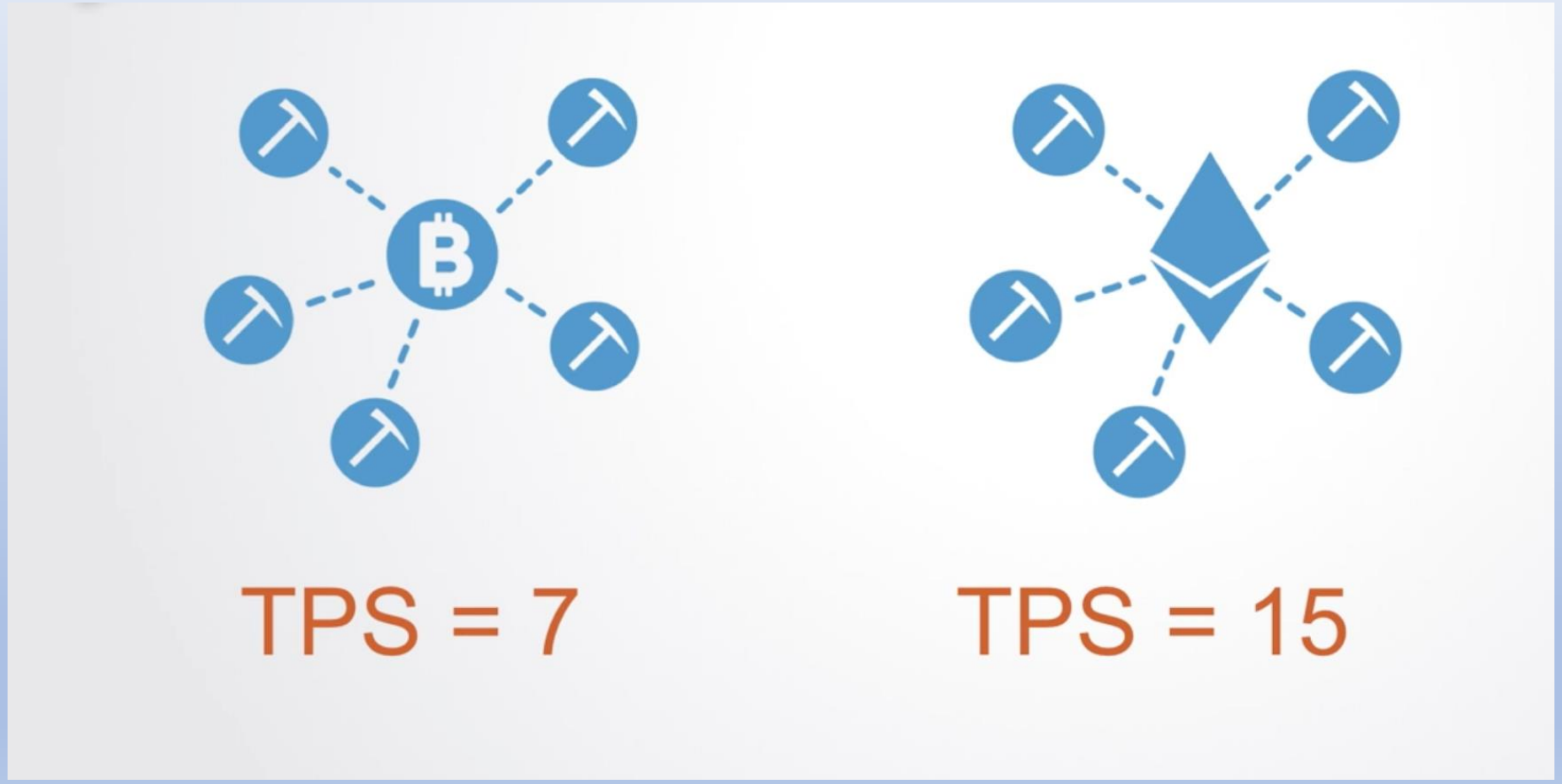
(73) Assignee: **Vijay K. Madisetti**, Johns Creek, GA (US)

2013/0167109 A1* 6/2013 Nucci G06F 9/44 717/105
2013/0219176 A1* 8/2013 Akella H04L 63/0815 713/165
2014/0164758 A1* 6/2014 Ramamurthy G06F 21/77 713/150
2015/0188949 A1* 7/2015 Mahaffey H04L 63/20 726/1
2016/0283996 A1* 9/2016 Bakhshaie G06Q 30/0613
2017/0041296 A1* 2/2017 Ford G06F 16/951
2017/0123677 A1* 5/2017 Singhai G06F 16/174
2017/0180372 A1* 6/2017 Bezold G06F 21/6209

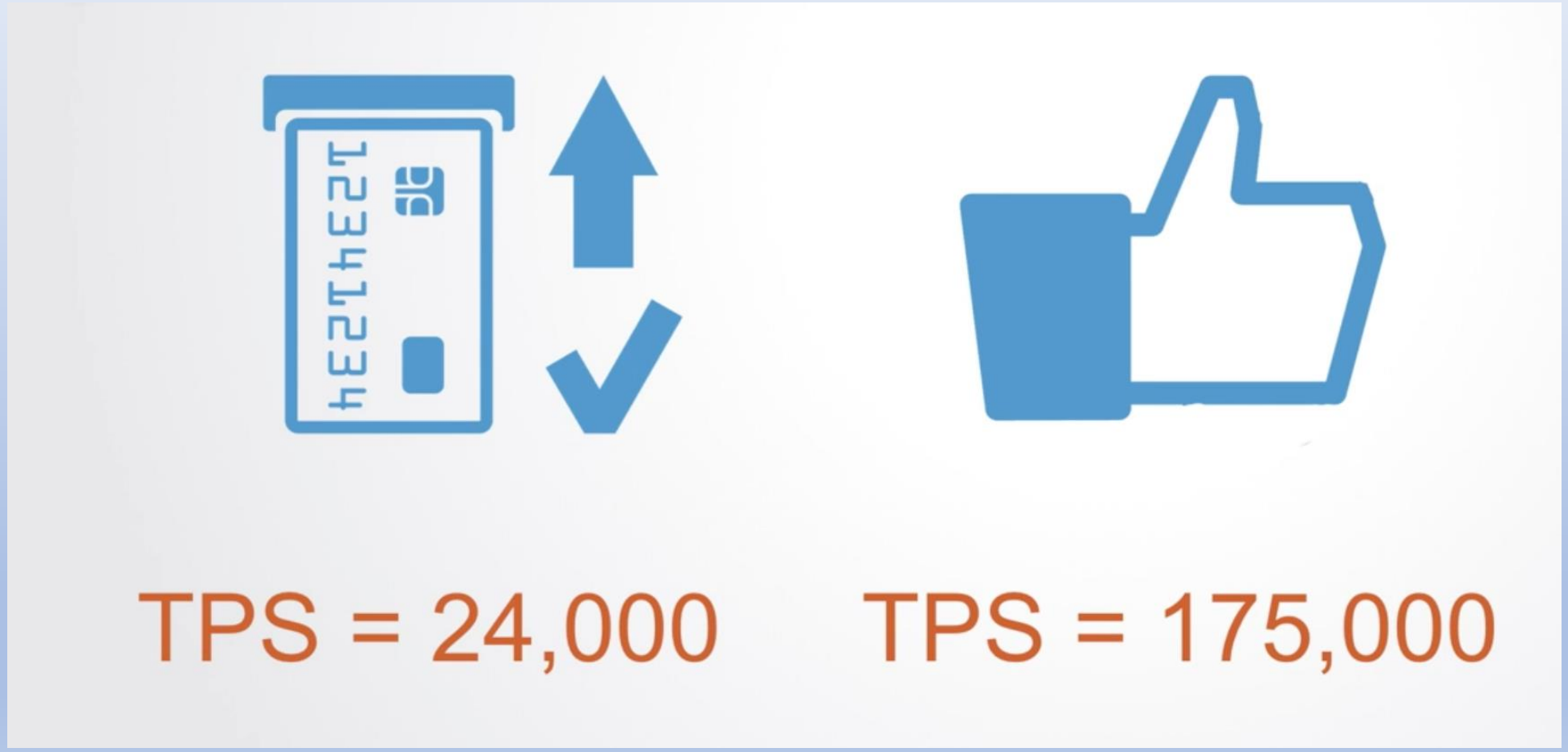
* cited by examiner

Blockchain – Rollout Perspectives

Are Blockchains “Slow” ?



Compared to Visa/MasterCard or Facebook?



What are big problems with Web 3.0 and using Blockchain

Scalability

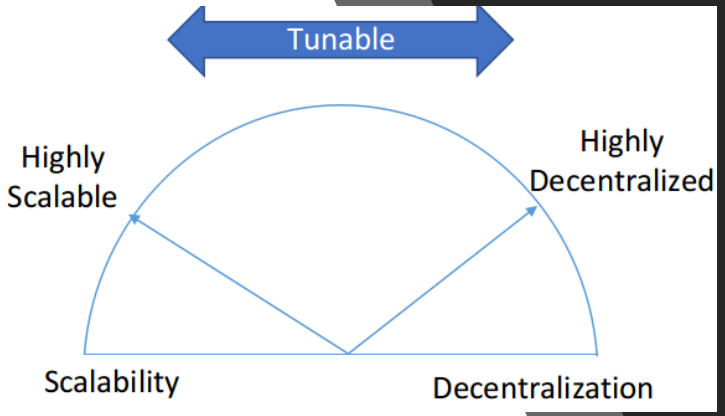
Identity

Regulatory Frameworks & Status Quo

Blockchain Scalability Concerns

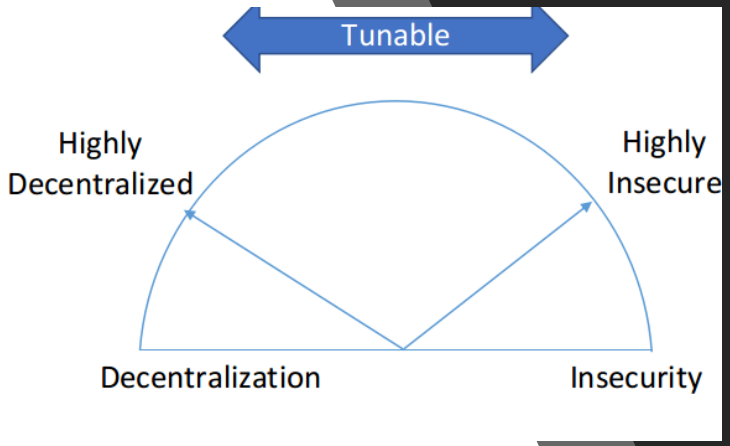
- While commercial payment networks can process thousands of transactions per second, for blockchain networks a user has to wait for several seconds for a transaction to be confirmed.
- The Bitcoin network has the block-time (time after which a new block is mined) of **10 minutes**, whereas Ethereum where the block-time is roughly **17 seconds**
- Ethereum blockchain currently supports roughly **15 transactions per second** compared to, say, the **45,000** transactions per second processed by Visa.
- The transaction validation and consensus mechanisms (such as proof-of-work) used in blockchain networks and the block-times determine how fast the network can process and confirm the transactions.
- Many blockchain applications require multiple confirmations for newly mined blocks to secure the transactions from double-spending. For such applications, it may take several minutes for a transaction to be confirmed.
- Another scalability concern for blockchain networks is the increasing size of the blockchain.
- As the size of the blockchain becomes larger, it can pose a centralization risk as it will make it difficult for small miners to function as full nodes.

Scalability & Decentralization



- The level of scalability in a blockchain network is inversely proportional to the level of decentralization.
- If a blockchain network is scaled-up to increase transaction throughput or decrease transaction latency, the level of decentralization of the network decreases.
- For example:
  - A scaling-up measure such as decreasing block size (to increase transaction throughput) reduces the level of decentralization as the computational and storage load on each node will increase and the nodes running on commodity hardware will not be able to catch-up and mine on the network.

Decentralization & Security



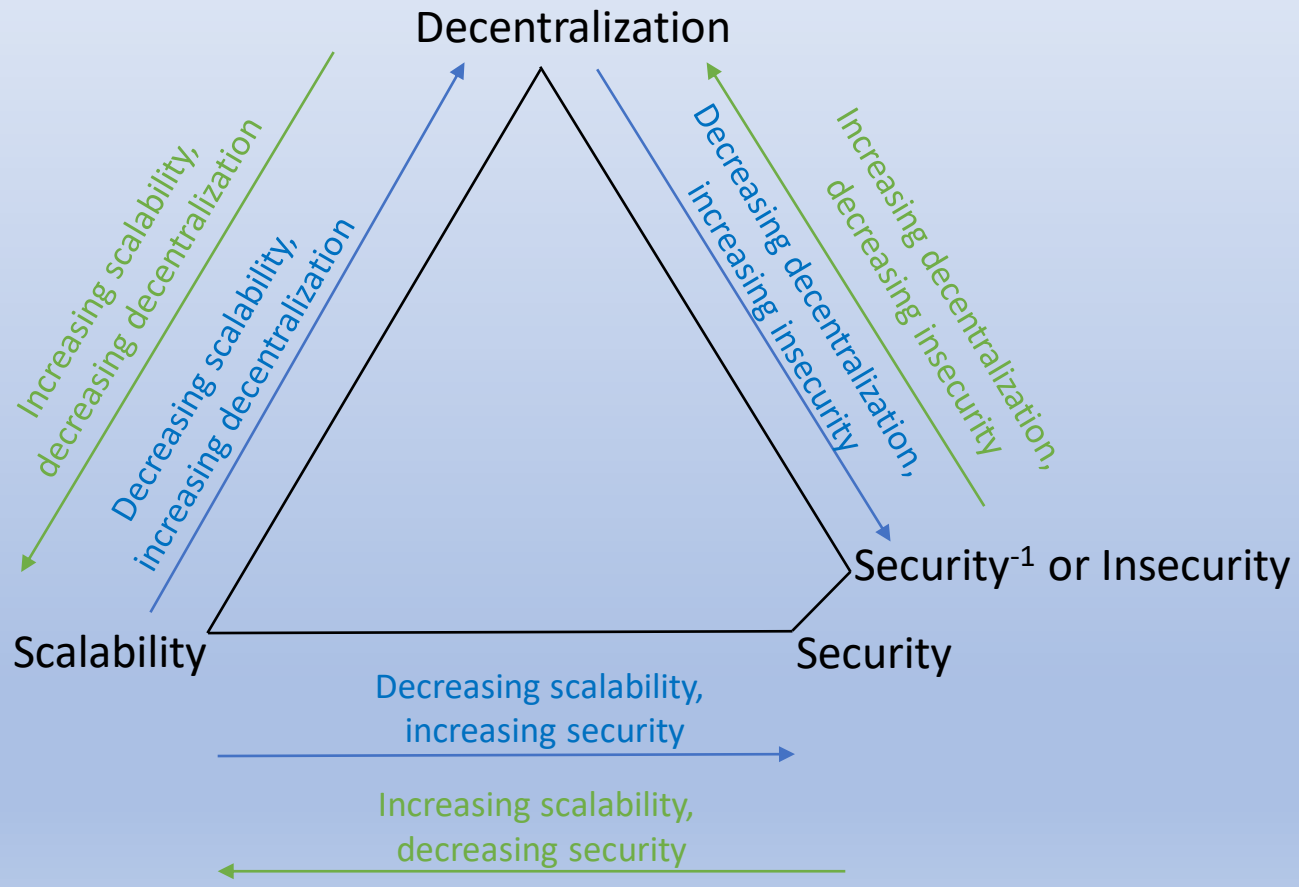
- The level of decentralization in a blockchain network is directly proportional to the level of security or inversely proportional to level of insecurity.
- If the level of decentralization of blockchain network is decreased, the security of the network decreases or insecurity increases.
- For example:
  - A lower-level of decentralization means that the network is controlled by groups of miners or mining pools. Mining pools can collude to compromise the security of the network and attempt a '51% attack'. In a 51% attack, the pool can rewrite the blockchain history and do double-spending to their advantage.

Decentralization, Scalability, Security (DSS)

- The levels of Decentralization (L_D), Scalability (L_{Sc}) and Security (L_{Se}) for blockchain networks are tunable subject to the following constraints:

$$L_{Sc} \propto (1/ L_D)^a \propto (1/ L_{Se})^b$$

where exponents *a* and *b* are dependent on the blockchain platform



Blockchain Scalability Approches

General approaches for blockchain scalability can be categorized into the following areas:

- Blockchain parameter tuning approaches
- On-chain Scaling with Sharding
- Off-chain Scaling with Channels
- Alternative blockchain designs and protocols

Blockchain Parameter Tuning

- Blockchain parameter tuning approaches involve tuning the blockchain parameters such as block-size and block-time (or block-interval) to increase the transaction throughput and reduce transaction latency using local and limited approaches that require client upgrades and lengthy consensus.

On-chain Scaling with Sharding

- On-chain Scaling with Sharding involves splitting the task of consensus among concurrently operating sets of nodes, to improve the transaction throughput and reduce the per-node processing and storage requirements.
- Sharding approaches for blockchain either shard transaction processing or shard the state.
- Related work on sharding - Elastico, Aspen

Off-chain Scaling with Channels

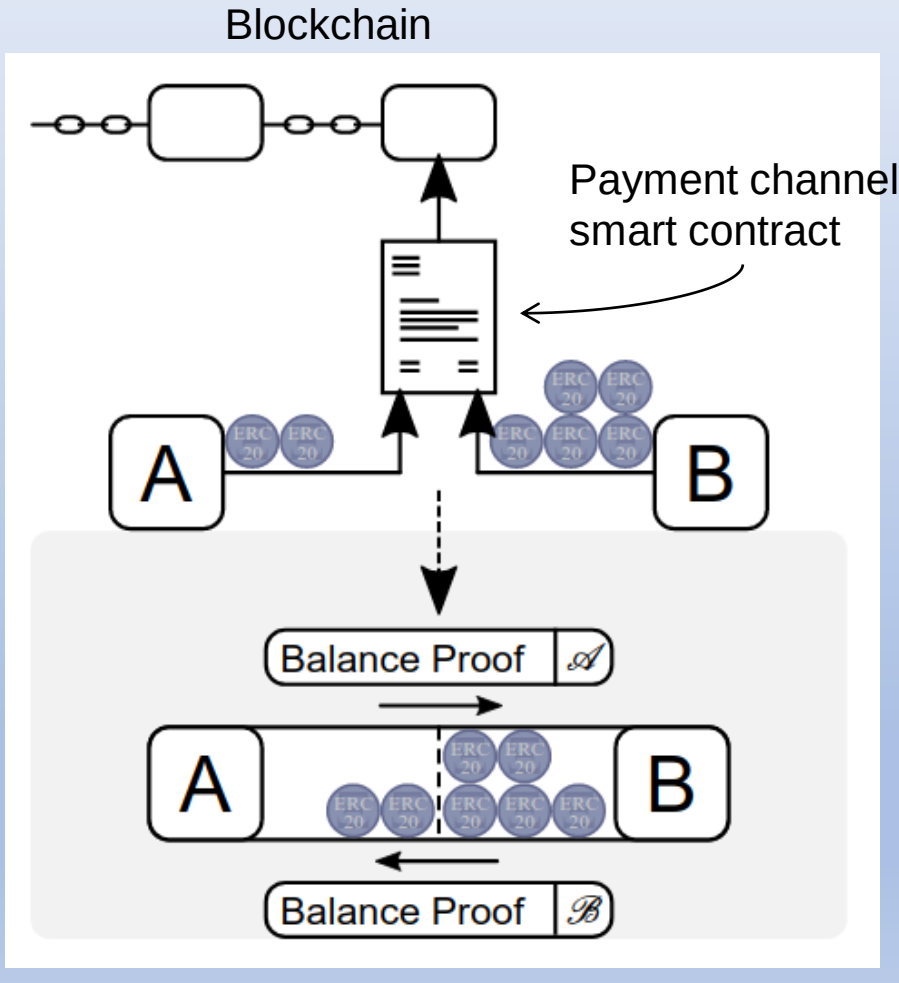
- Off-chain Scaling appoached with Channels, use off-chain peer-to-peer payment channels that allow transactions to occur directly between participants rather than sending transactions on the blockchain, and the blockchain is used as a settlement mechanism.
- Related work - Raiden, LightningNetwork

Lightning Network & Raiden Network

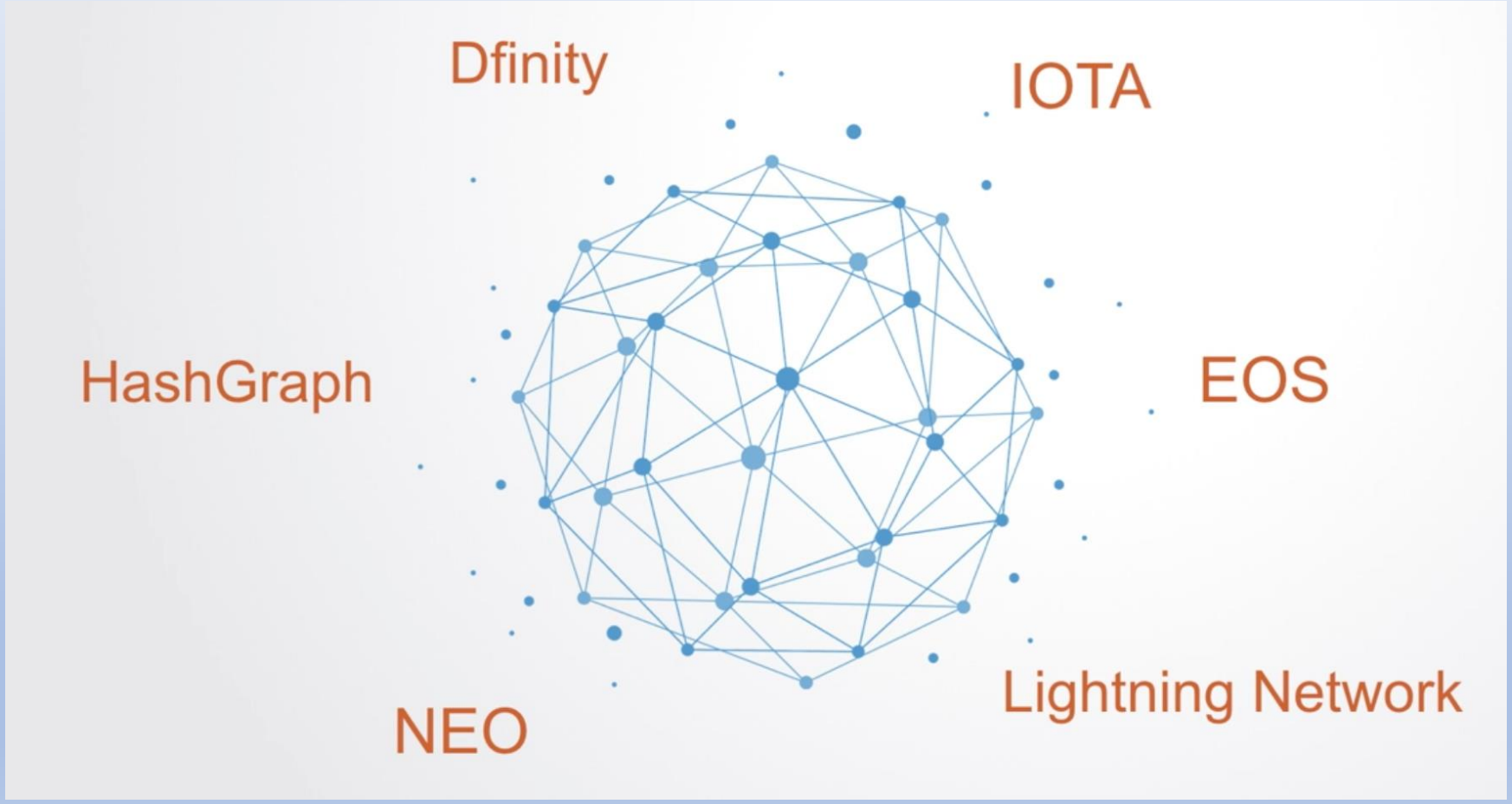
- Lightning Network and Raiden Network leverage bidirectional payment channels to address the issues of scalability, latency and transaction fees for blockchain based payment applications and token transfers.
- Lightning Network is the payment channel solution for the Bitcoin network.
- Raiden Network is the payment channel solution for the Ethereum network.

Payment Channels for Blockchain Scalability

- Payment channels allow off-chain transfer of on-chain tokens or cryptocurrencies.
- A payment channel is created between two participants by depositing a certain amount of tokens in smart contract.
- A payment channel is an agreement between two participants where the sender sets up a deposit in a smart contract for the receiver.
- Payments or transfer of tokens between the participants can then be done by sending signed messages without going through global consensus on the blockchain.
- Eventual settlement of payments between the participants happens when a payment channel is closed by either participant.
- The payment channel smart contract validates the last signed message and settles the claims.



Some Scalability Options Amongst Blockchains



Comparison of Some Blockchain Platforms

	Bitcoin	Ethereum	Neo	Lisk	EOS
Consensus	Proof of Work	Proof of Work	Proof of Stake	Delegated Proof of Stake	Delegated Proof of Stake
Smart Contracts	-	Solidity	C#, Java, Python, Go	JavaScript	C++
Average Block Time	10 min	12 s	15 s	10 s	2 s
Transactions per sec (max claimed)	7 tx/s	15 tx/s	10,000 tx/s	100,000 tx/s	100,000 tx/s
Cryptocurrency	BTC	ETH	NEO	LSK	EOS
Circulating Supply	16,944,000 BTC	98,464,403 ETH	65,000,000 NEO	103,248,830 LSK	756,241,354 EOS
Price	1 BTC ≃ $8,050	1 ETH ≃ $462	1 NEO ≃ $60	1 LSK ≃ $10	1 EOS ≃ $7
Market Cap	$136,294,316,640	$45,506,997,654	$3,870,951,500	$1,041,935,566	$4,904,573,054

Blockchain Identity Concerns

- Blockchain platforms lack identity management beyond the blockchain accounts and there is no way to know if two blockchain accounts belong to the same person
- Blockchain applications can be prone to Sybil attacks where the attacker can create a large number of pseudonymous identities and then use them to gain a large influence on the network
- In existing Blockchain platforms, there is no way to securely link a blockchain account to a real-user
- When using multiple private/permissioned blockchains within a single organization, there is no way for a user to work on multiple blockchains while maintaining the same identity and/or credentials

Problems with Existing KYC Processes

- Existing works linking blockchain accounts to real users is based on know your customer (KYC) processes that require the user to provide KYC documents such as a government issued identity card (such as passport or driving license).
- The KYC processes require manual verification by the platform or application team.
- When using multiple private and/or permissioned blockchain networks within a single organization, there is no way for a user to work on multiple blockchain networks while maintaining the same identity.
- For multiple blockchain networks within an organization or different applications deployed on the same blockchain network, existing solutions require the KYC process to be completed separately either for each blockchain network or for each application.

Proposed Solution for Identity Management Across Multiple Chains

(12) **United States Patent**
Madisetti et al.

(10) **Patent No.: US 10,204,339 B2**
(45) **Date of Patent: Feb. 12, 2019**

(54) **METHOD AND SYSTEM FOR BLOCKCHAIN-BASED COMBINED IDENTITY, OWNERSHIP, INTEGRITY AND CUSTODY MANAGEMENT**

(71) Applicants: **Vijay K. Madisetti**, Johns Creek, GA (US); **Arshdeep Bahga**, Chandigarh (IN)

(72) Inventors: **Vijay K. Madisetti**, Johns Creek, GA (US); **Arshdeep Bahga**, Chandigarh (IN)

(73) Assignee: **Vijay K. Madisetti**, Johns Creek, GA (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

(21) Appl. No.: **16/118,599**

(52) **U.S. Cl.**
CPC ***G06Q 20/38215*** (2013.01); ***G06Q 20/065*** (2013.01); ***G06Q 20/367*** (2013.01); ***H04L 9/0637*** (2013.01); ***H04L 9/14*** (2013.01); ***H04L 9/30*** (2013.01); ***H04L 9/3242*** (2013.01); ***H04L 9/3247*** (2013.01); ***H04L 9/3263*** (2013.01); *H04L 2209/56* (2013.01)

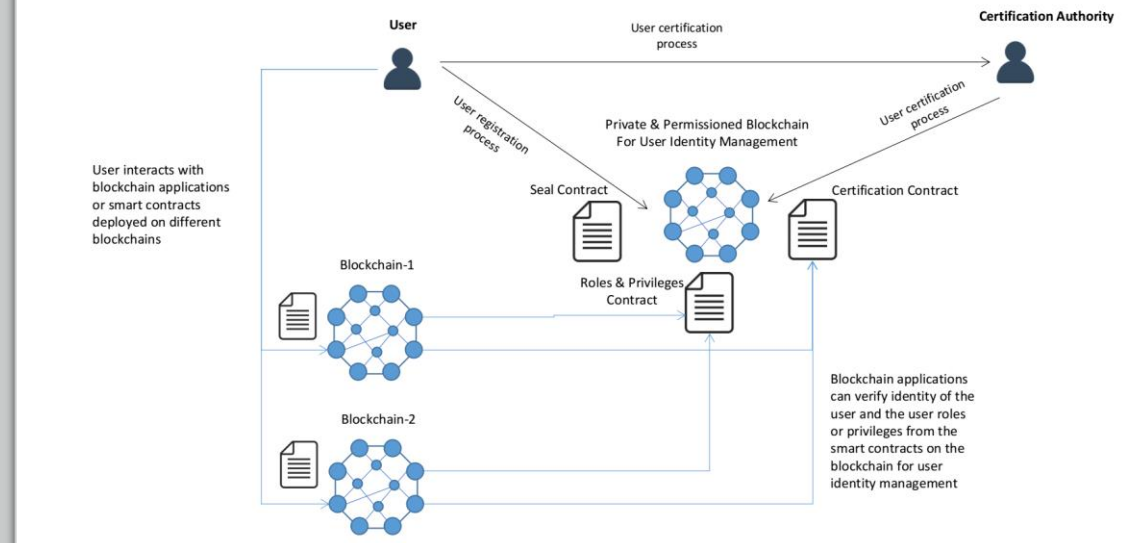
(58) **Field of Classification Search**
None
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

9,935,772 B1 * 4/2018 Madisetti G06F 21/6209
9,992,022 B1 * 6/2018 Chapman H04L 63/0861
(Continued)

Primary Examiner — Michael R Vaughan
(74) *Attorney, Agent, or Firm* — Daniel C. Pierron; Widerman Malek PL



IoT in Perspective

The Four Industrial Revolutions

Navigating the next industrial revolution

WORLD ECONOMIC FORUM
COMMITTED TO IMPROVING THE STATE OF THE WORLD

Revolution	Year	Information
1	1784	Steam, water, mechanical production equipment
2	1870	Division of labour, electricity, mass production
3	1969	Electronics, IT, automated production
4	?	Cyber-physical systems

Internet of Things (IoT) Plays Central Role in Cyber-Physical Systems

www.weforum.org

Characteristics of the 4th Revolution

Unlike the first three revolutions……..

the fourth revolution is different in:

- **VELOCITY** – exponential pace of adoption (NOT LINEAR)
- **SCOPE** – DISRUPTIONS in ALMOST EVERY INDUSTRY ON EARTH
- **SYSTEMS IMPACT** – Transformation of entire systems of production, management and governance

Dr. Klaus Schwab, Chairman WEF 2016

Impact of the IoT Revolution

EFFECT ON BUSINESS

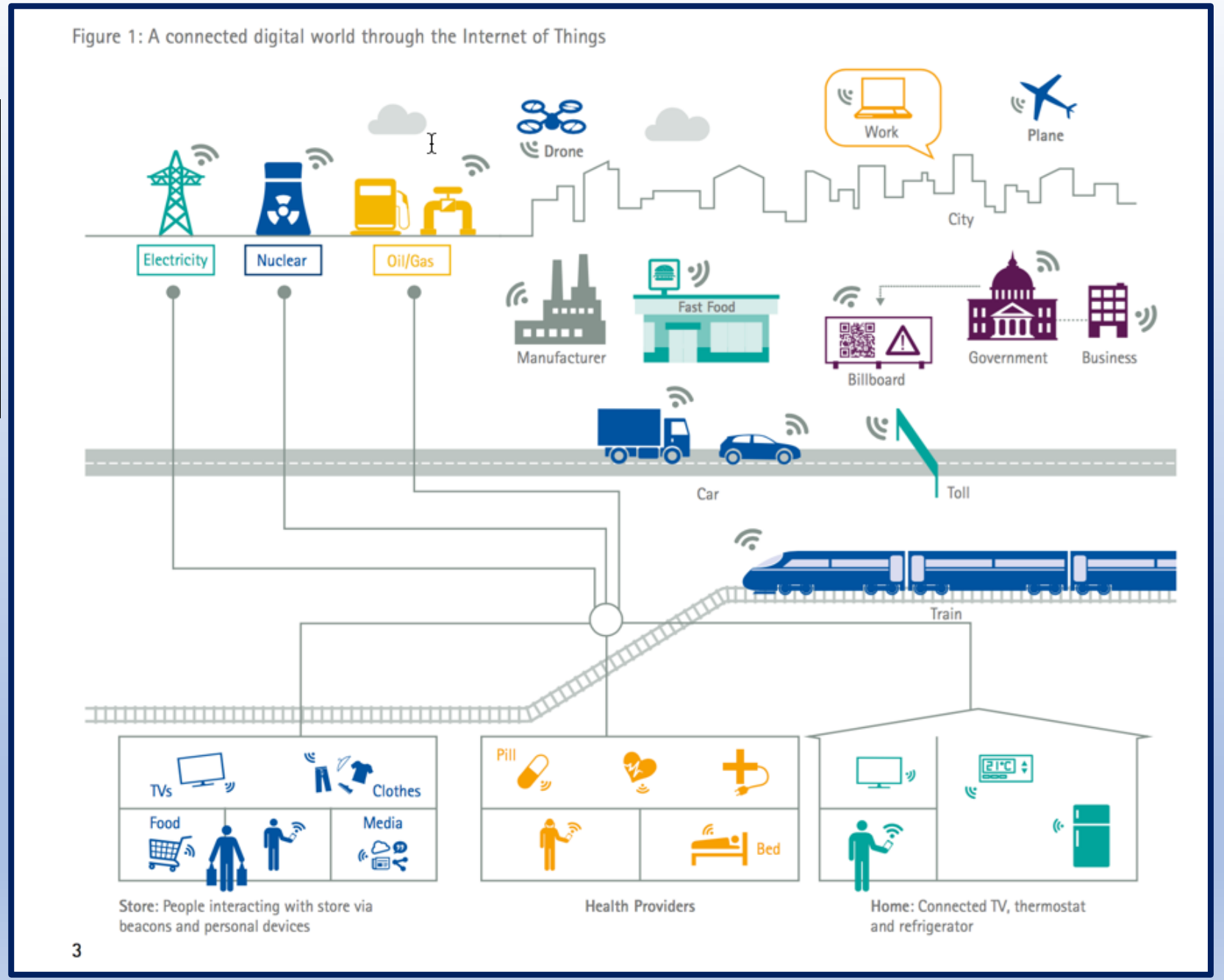
- Customer expectations at affordable cost
- Innovative product enhancements
- Collaborative approach to innovation – include customers, partners & universities
- ORGANIZATION FORMS – OLD HIERARCHICAL FORM was suitable for MASS PRODUCTION, new forms must emerge for the blockchain-type world

EFFECT ON GOVERNMENT

- NEW POLICIES FOR PRIVACY RIGHTS
- NEW SECURITY POLICIES
- FAIR DATA SHARING AND COLLABORATION contracts
- NEW REGULATIONS COVERING INTELLIGENT MACHINES & NETWORKS
- REGULATION OF CORPORATE ORGANIZATIONAL FORMS
- JOB CREATION FOR THE NEW ECONOMY
- ADOPTION OF "AGILE GOVERNANCE"

Adapted from
Dr. Klaus Schwab, WEF
www.weforum.org

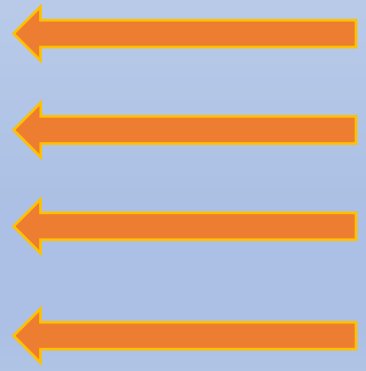
Connected Cyber-Physical World



Source: Accenture

The Seven Tenets of Successful IoT Deployment

- Confidentiality: Data is not available to unauthorized parties
- Integrity: Data or Code cannot be changed or damaged or erased by unauthorized parties (data at rest or in motion)
- Availability: Network and data is responsive and available to authorized parties
- Controllability
- Visibility
- Safety
- Standardization



New Tenets

Summary

- Web 3.0 is here
- Technology is based on **Blockchain, IoT** and **Analytics**
- New economic and business models, systems and applications are driving the development of **Internet of Value**