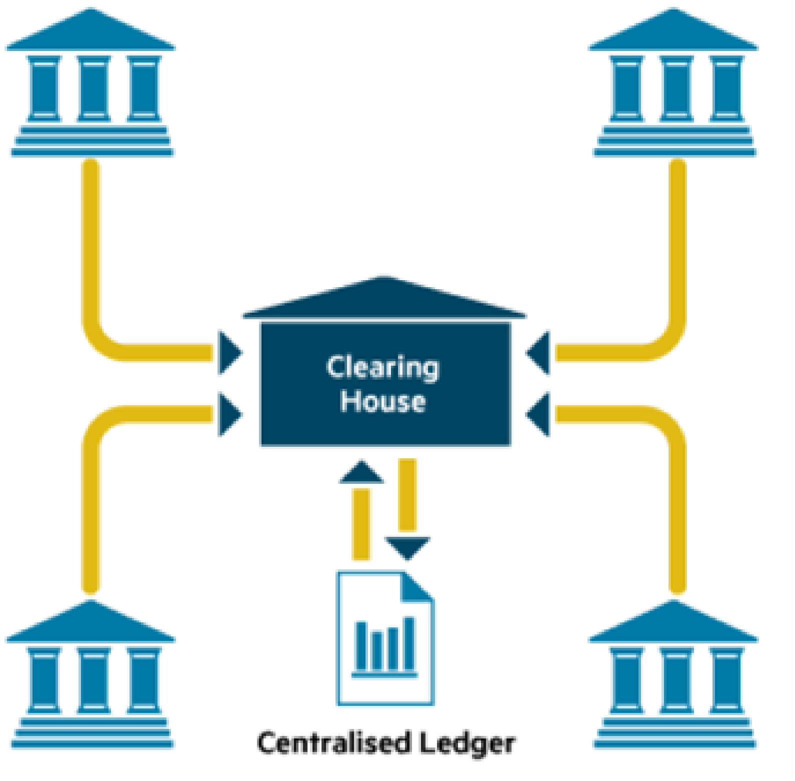
Introduction to Blockchain

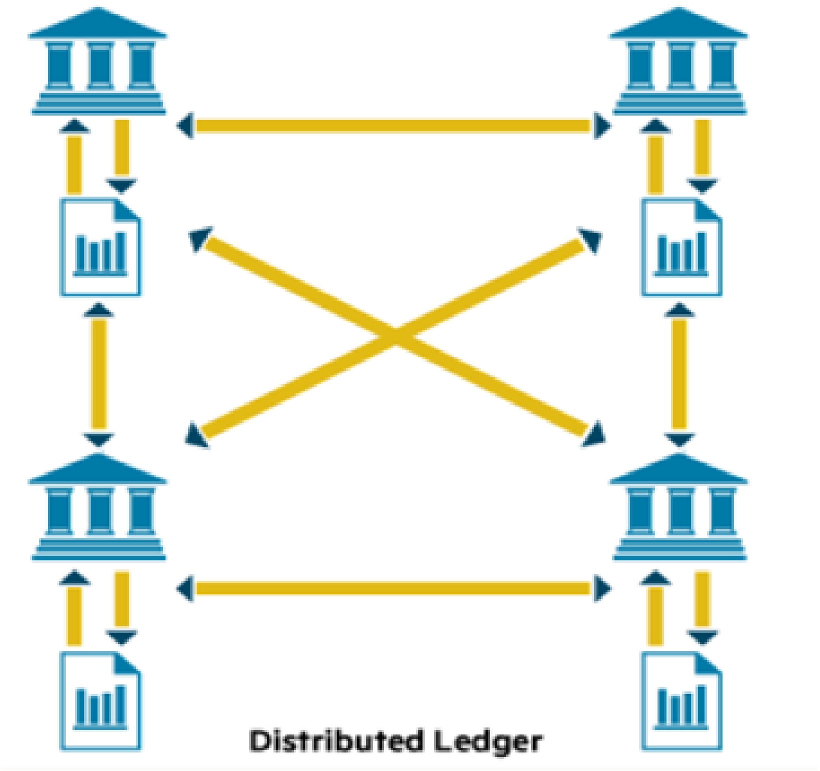
2018. 07. 26
Samuel Hyun

1. Essense of Blockchain: Infrastructure for Trust
2. Bitcoin, Ethereum
3. Private Blockchain
4. Blockchain Applications
5. Next Generation Blockchain

Trust Network


Clearing House
Centralised Ledger

vs.


Distributed Ledger

Santander InnoVentures
OLIVER WYMAN

Key Factors of Blockchain

By design, no one party can modify, delete, or even append any record to the ledger without the consensus, making the system useful for ensuring **the immutability of transaction, contract, and other legal documents.**

Append-only system of record shared across business network

Distributed DB

Shared Ledger

Cryptography

Ensuring secure, authenticated & verifiable transactions

Hash, PKI

+

All parties agree to network verified transaction

P2P, Consensus

Consensus

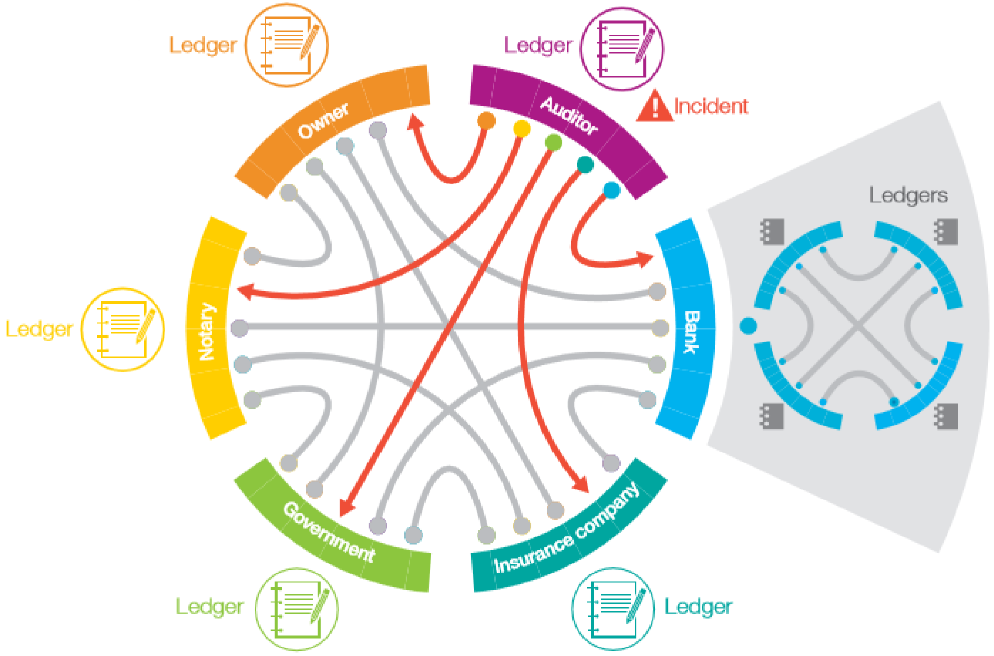
Smart Contract

Business terms embedded in transaction database & executed with transactions

Broader participation, lower cost, increased efficiency

Shared Ledger

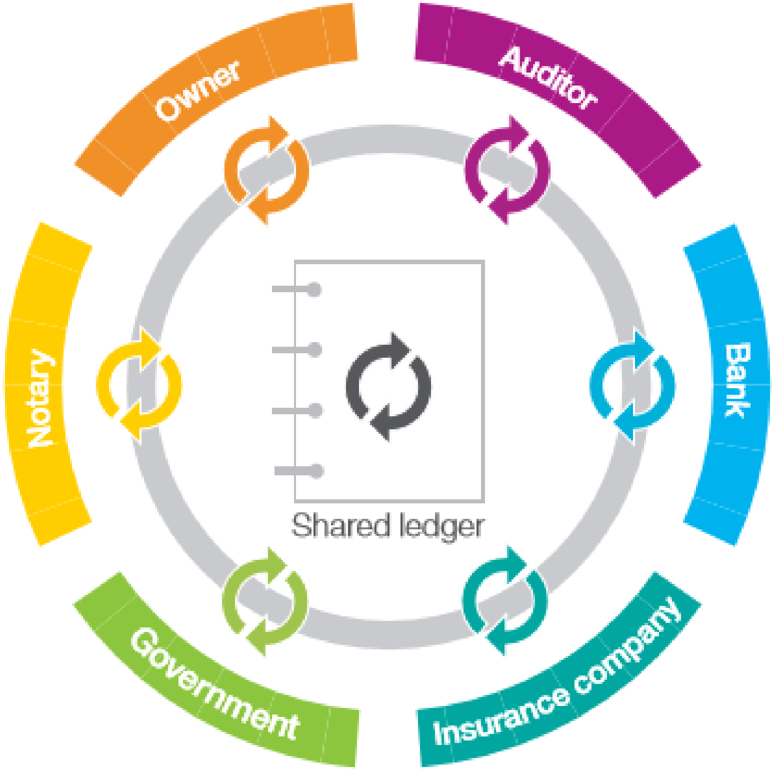
***Current view:** Individual ledgers and organizational siloes complicate how information and incidents are managed in the network*


Ledger
Ledger
Incident
Owner
Auditor
Ledgers
Ledger
Notary
Bank
Government
Insurance company
Ledger
Ledger

Source: IBM Institute for Business Value analysis.

VS.

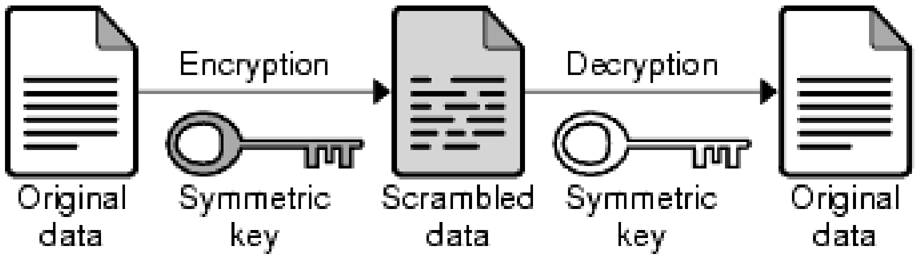
***Future view:** A shared ledger built on blockchain offers visibility, trust and permanence*


Owner
Auditor
Notary
Bank
Shared ledger
Government
Insurance company

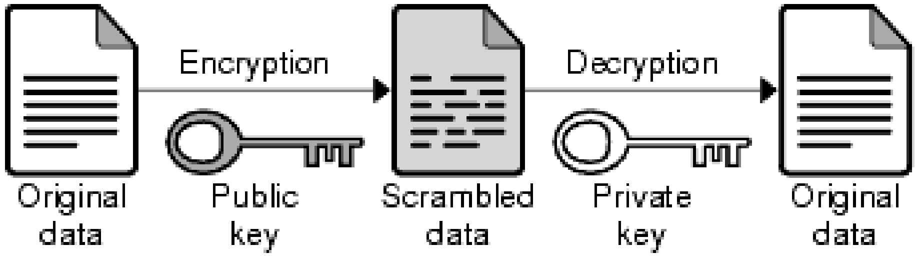
Source: IBM Institute for Business Value analysis.

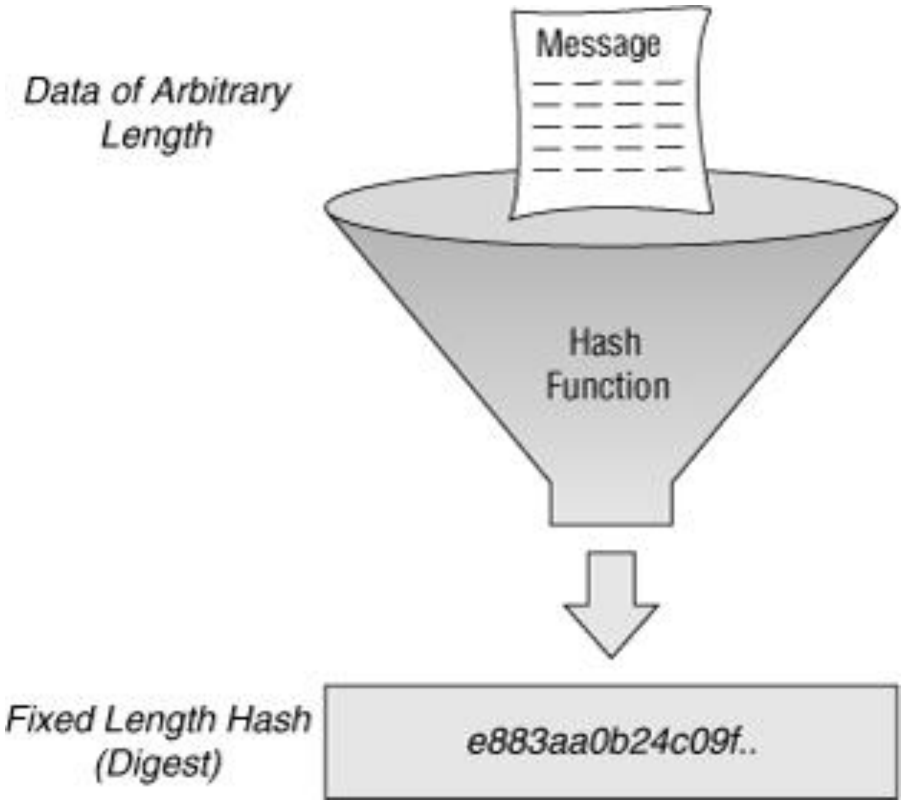
PKI & Hash

Symmetric Key Encryption

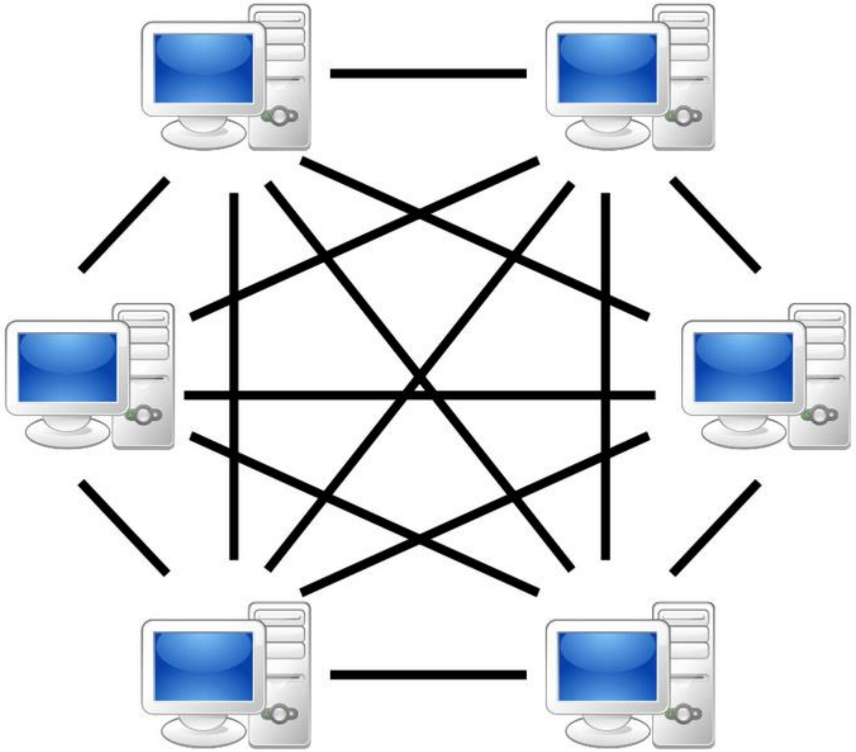

Encryption
Decryption
Original data
Symmetric key
Scrambled data
Symmetric key
Original data

Public Key Encryption

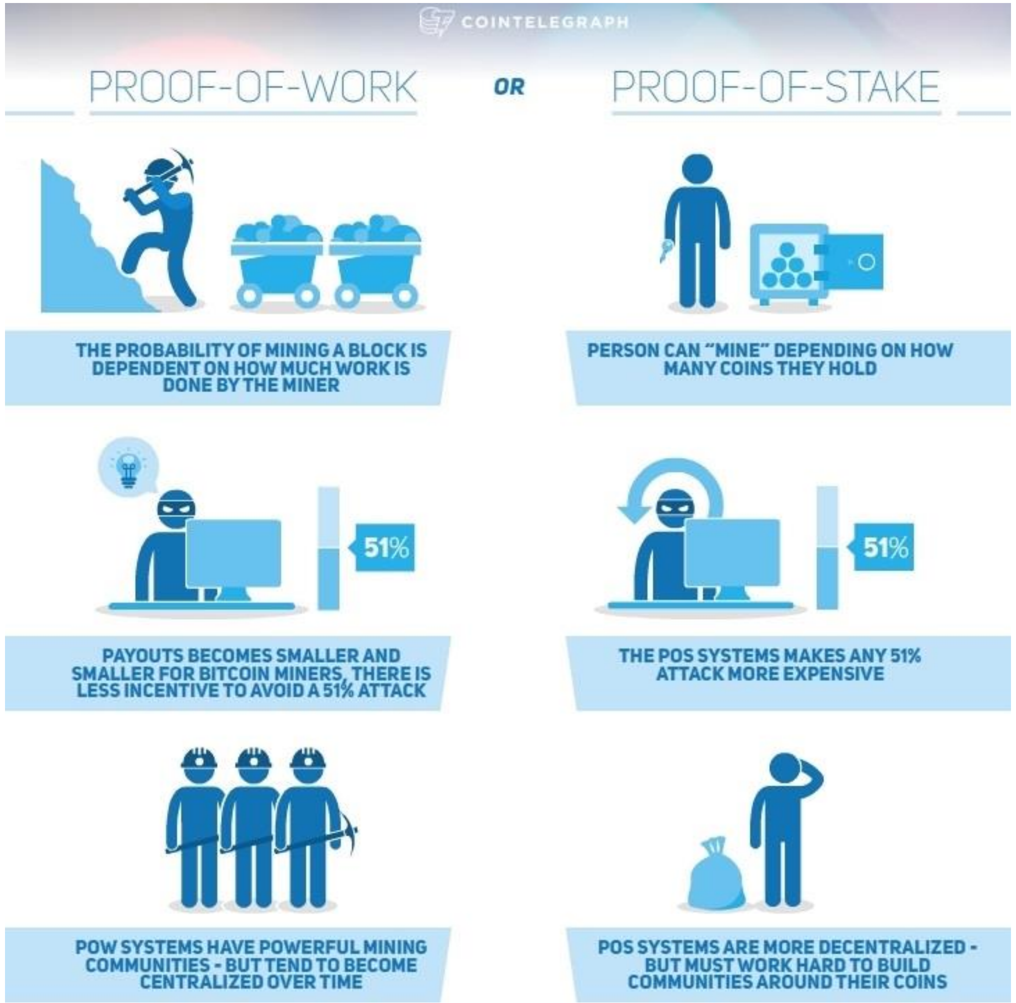

Encryption
Decryption
Original data
Public key
Scrambled data
Private key
Original data


Message
Data of Arbitrary Length
Hash Function
Fixed Length Hash (Digest)
e883aa0b24c09f..

P2P Protocol & Consensus Algorithm



Distributed P2P Network



THE PROBABILITY OF MINING A BLOCK IS DEPENDENT ON HOW MUCH WORK IS DONE BY THE MINER

PERSON CAN "MINE" DEPENDING ON HOW MANY COINS THEY HOLD

PAYOUTS BECOMES SMALLER AND SMALLER FOR BITCOIN MINERS, THERE IS LESS INCENTIVE TO AVOID A 51% ATTACK

THE POS SYSTEMS MAKES ANY 51% ATTACK MORE EXPENSIVE

POW SYSTEMS HAVE POWERFUL MINING COMMUNITIES - BUT TEND TO BECOME CENTRALIZED OVER TIME

POS SYSTEMS ARE MORE DECENTRALIZED - BUT MUST WORK HARD TO BUILD COMMUNITIES AROUND THEIR COINS

Blockchain: Infrastructure of Trust

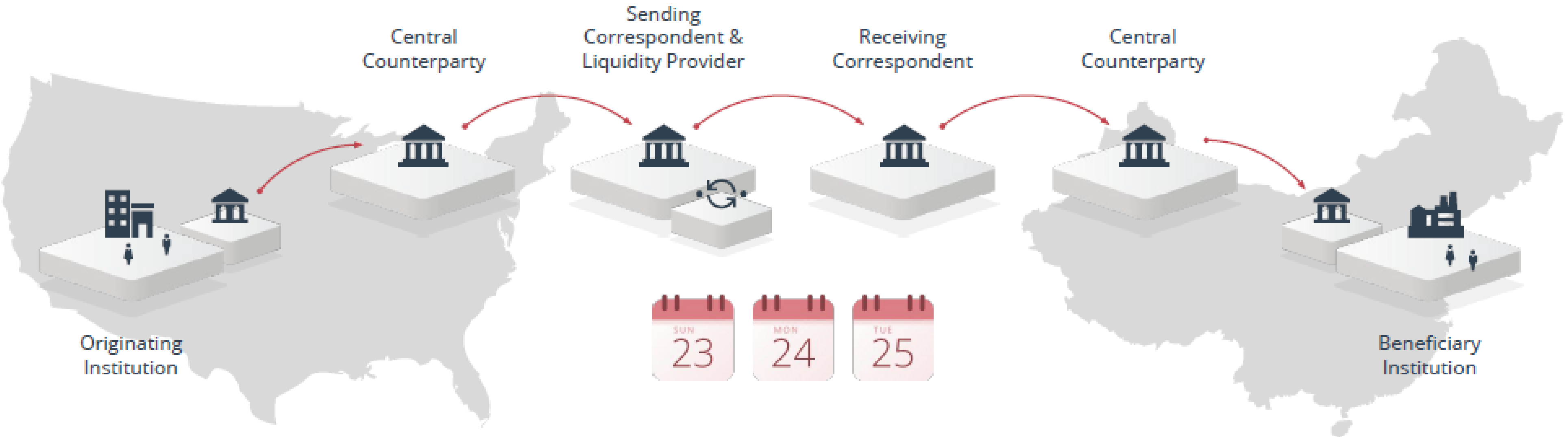
"Blockchain : Distributed Trust Network"

Blockchain's Big Innovation is Trust, Not Money

immutability | transparency | autonomy

coinplug

Cross-Border Payment on Trust Network



Central Counterparty

Sending Correspondent & Liquidity Provider

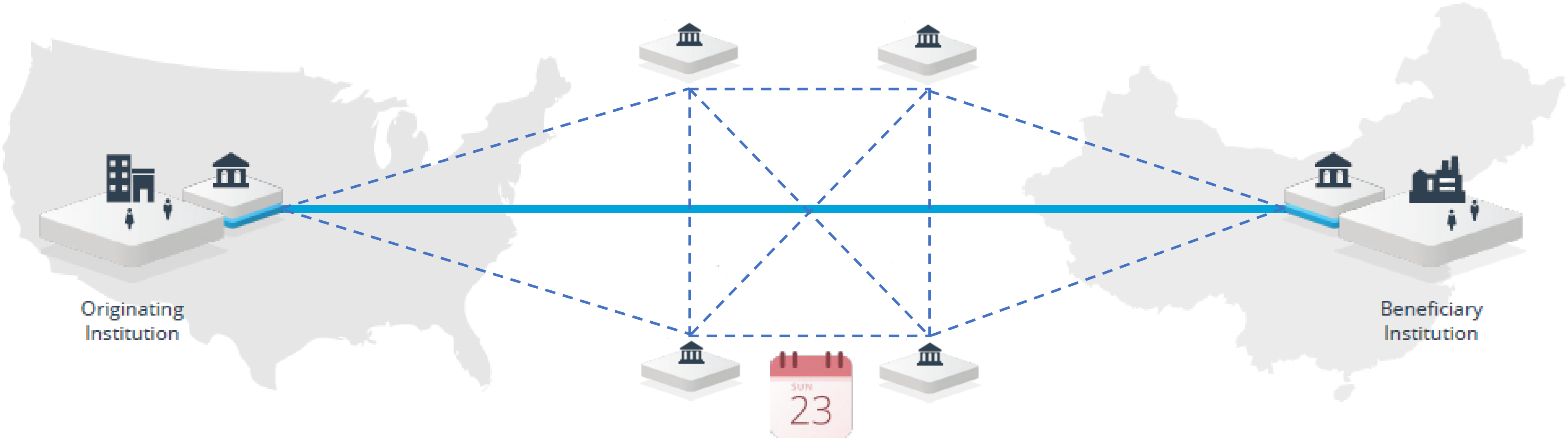
Receiving Correspondent

Central Counterparty

Originating Institution

Beneficiary Institution

VS.



Originating Institution

Beneficiary Institution

Evolution of Blockchain

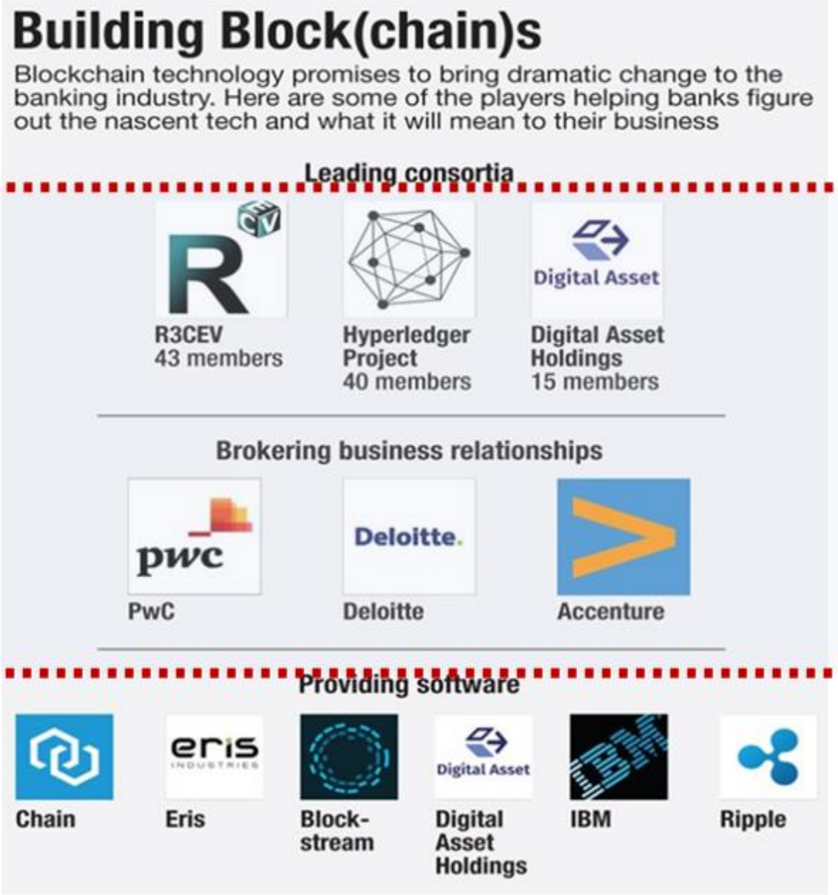
blockchain based services
(bitcoin → blockchain)

bitcoin

Blockchain 1.0:

Blockchain for Digital Currency

Private blockchain
(Public → Private)



Building Block(chain)s

Blockchain technology promises to bring dramatic change to the banking industry. Here are some of the players helping banks figure out the nascent tech and what it will mean to their business

Leading consortia

R3CEV
43 members

Hyperledger Project
40 members

Digital Asset Holdings
15 members

Brokering business relationships

PwC

Deloitte

Accenture

Providing software

Chain

Eris

Block-stream

Digital Asset Holdings

IBM

Ripple

Smart contract
(Ethereum...)

Ethereum is a "world computer" you can't shut down

ethereum

Blockchain 2.0:

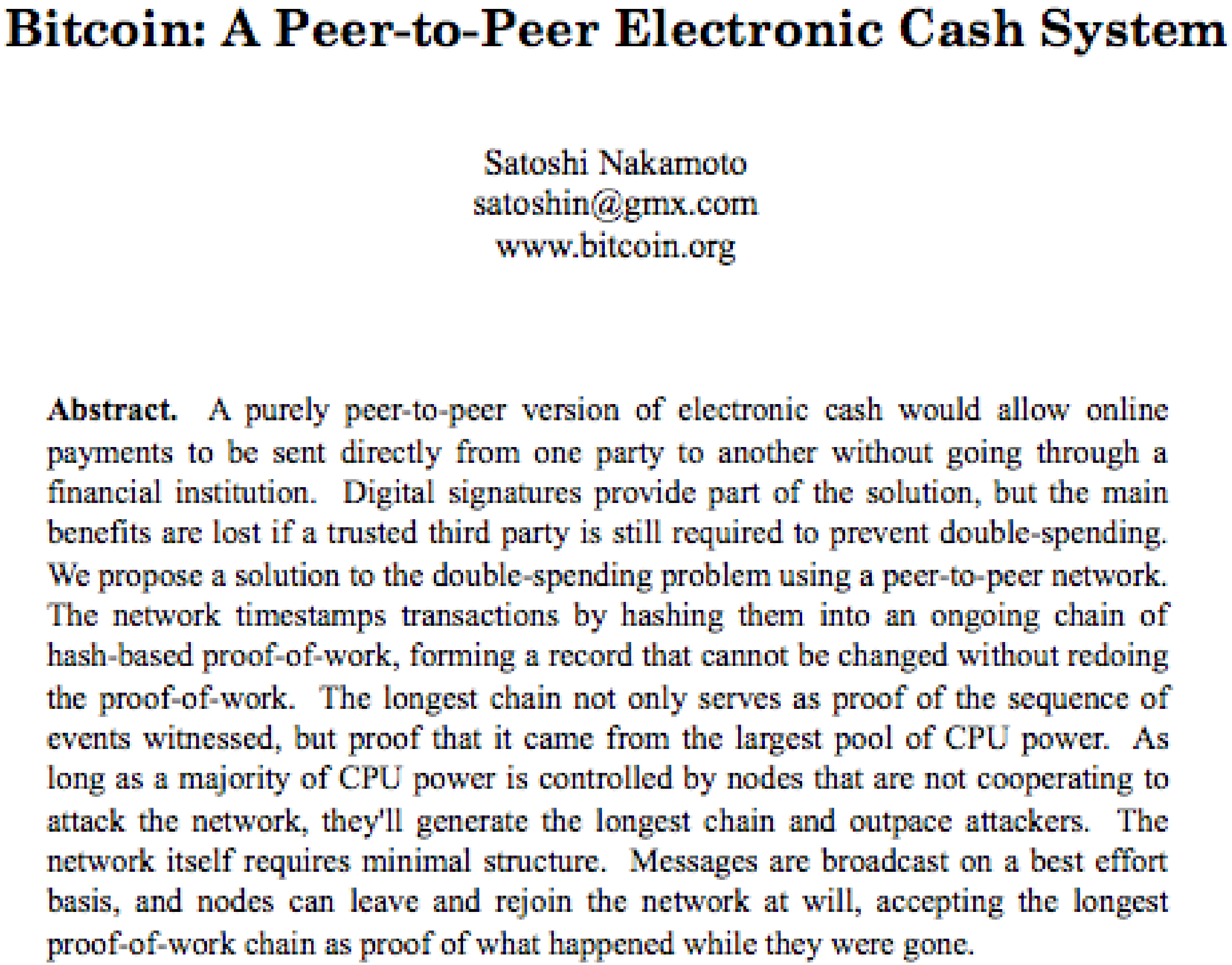
Blockchain as a Platform

1. Essense of Blockchain: Infrastructure for Trust
2. **Bitcoin, Ethereum**
3. Private Blockchain
4. Blockchain Applications
5. Next Generation Blockchain

Bitcoin

VIRES IN NUMERIS
2013
1 BITCOIN

bitcoin
ACCEPTED HERE



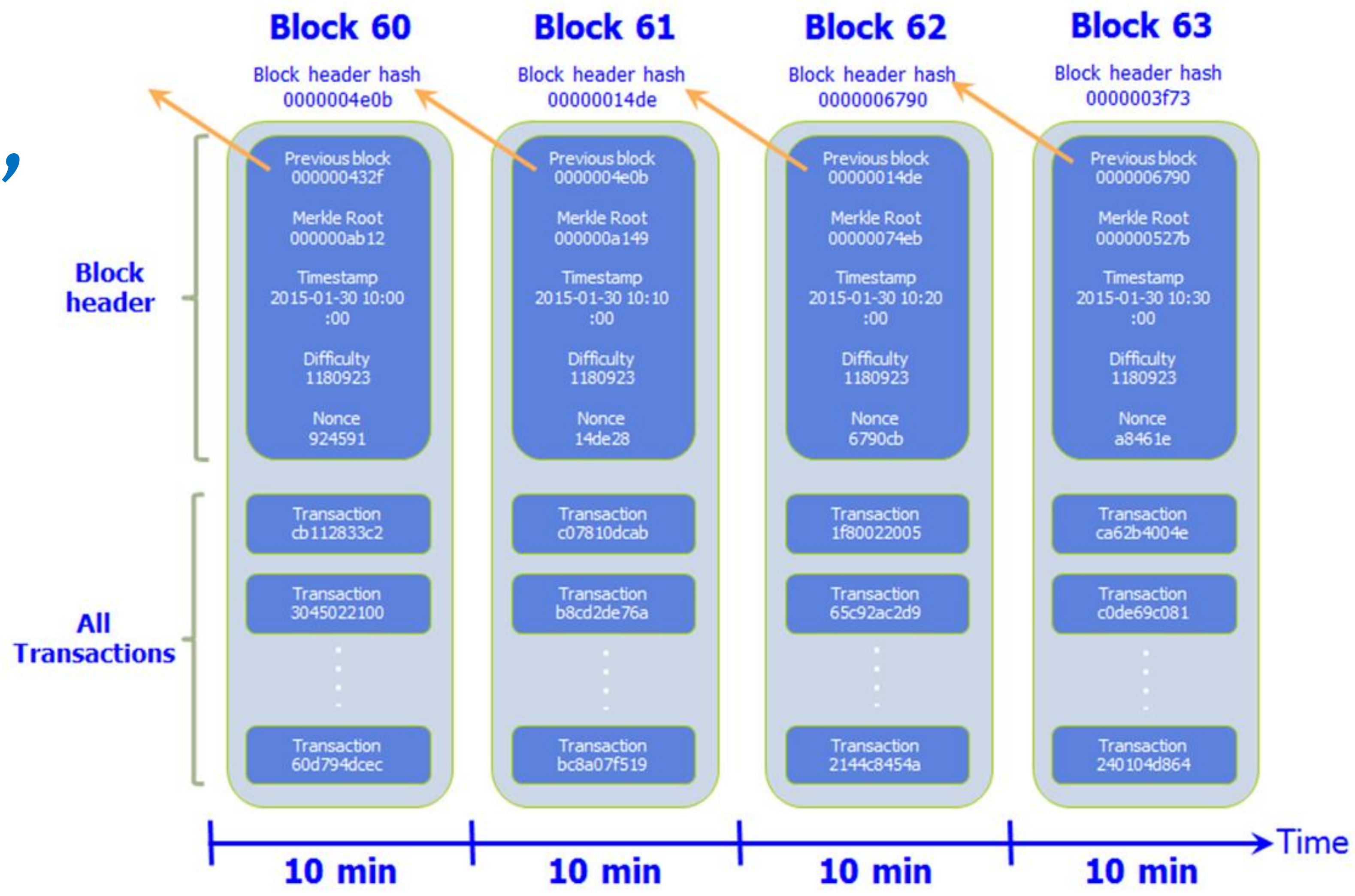
Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

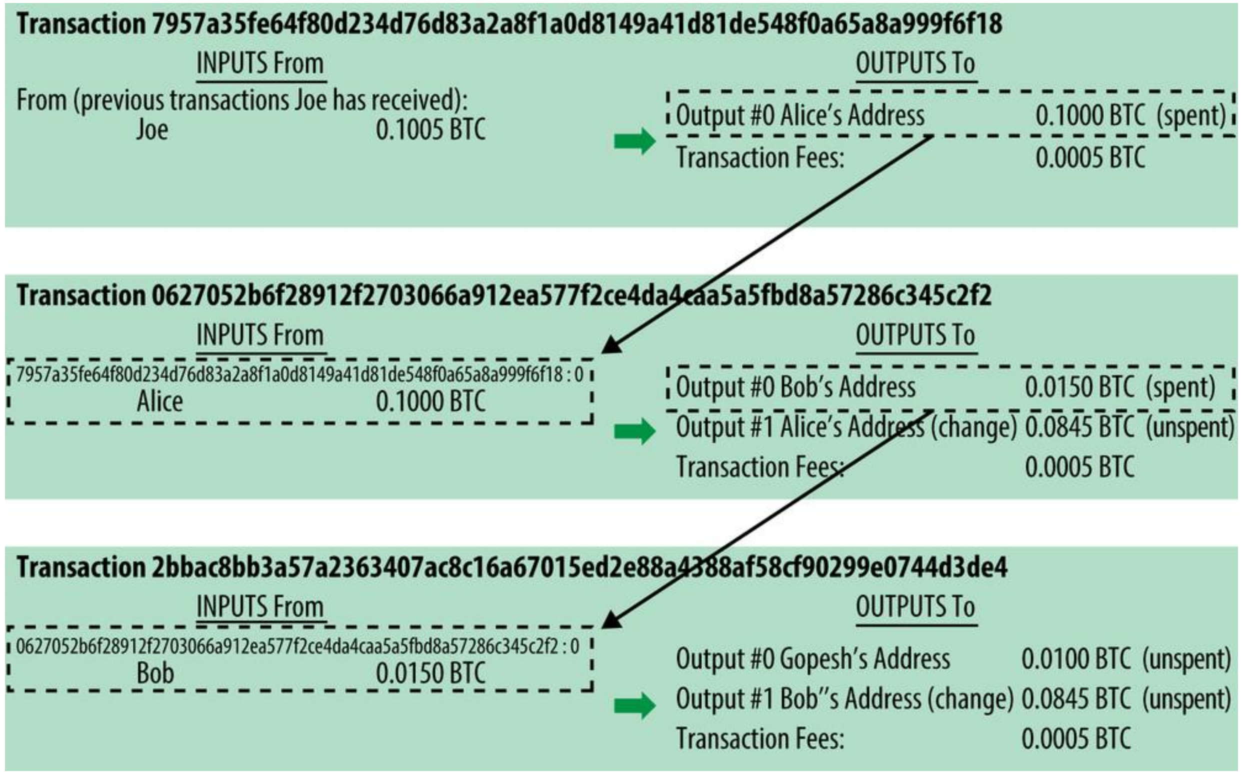
Block of Bitcoin

"Tamper-Proof Distributed Ledger"


Block 60
Block header hash
0000004e0b
Previous block
000000432f
Merkle Root
000000ab12
Timestamp
2015-01-30 10:00:00
Difficulty
1180923
Nonce
924591
Transaction
cb112833c2
Transaction
3045022100
Transaction
60d794dcec
Block 61
Block header hash
00000014de
Previous block
0000004e0b
Merkle Root
000000a149
Timestamp
2015-01-30 10:10:00
Difficulty
1180923
Nonce
14de28
Transaction
c07810dcab
Transaction
b8cd2de76a
Transaction
bc8a07f519
Block 62
Block header hash
0000006790
Previous block
00000014de
Merkle Root
00000074eb
Timestamp
2015-01-30 10:20:00
Difficulty
1180923
Nonce
6790cb
Transaction
1f80022005
Transaction
65c92ac2d9
Transaction
2144c8454a
Block 63
Block header hash
0000003f73
Previous block
0000006790
Merkle Root
000000527b
Timestamp
2015-01-30 10:30:00
Difficulty
1180923
Nonce
a8461e
Transaction
ca62b4004e
Transaction
c0de69c081
Transaction
240104d864
Block header
All Transactions
10 min
10 min
10 min
10 min
Time

Bitcoin Transaction

“UTXO”



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

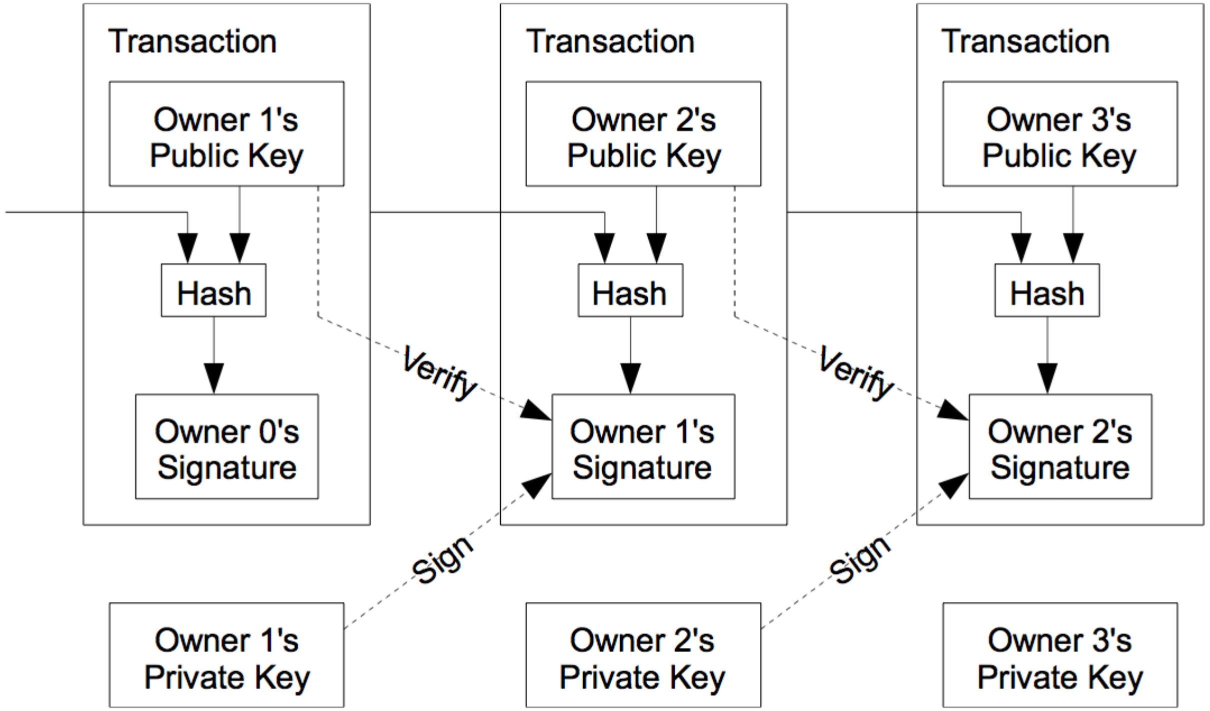
OUTPUTS To
Output #0 Bob’s Address 0.0150 BTC (spent)
Output #1 Alice’s Address (change) 0.0845 BTC (unspent)
Transaction Fees: 0.0005 BTC

Transaction 2bbac8bb3a57a2363407ac8c16a67015ed2e88a4388af58cf90299e0744d3de4

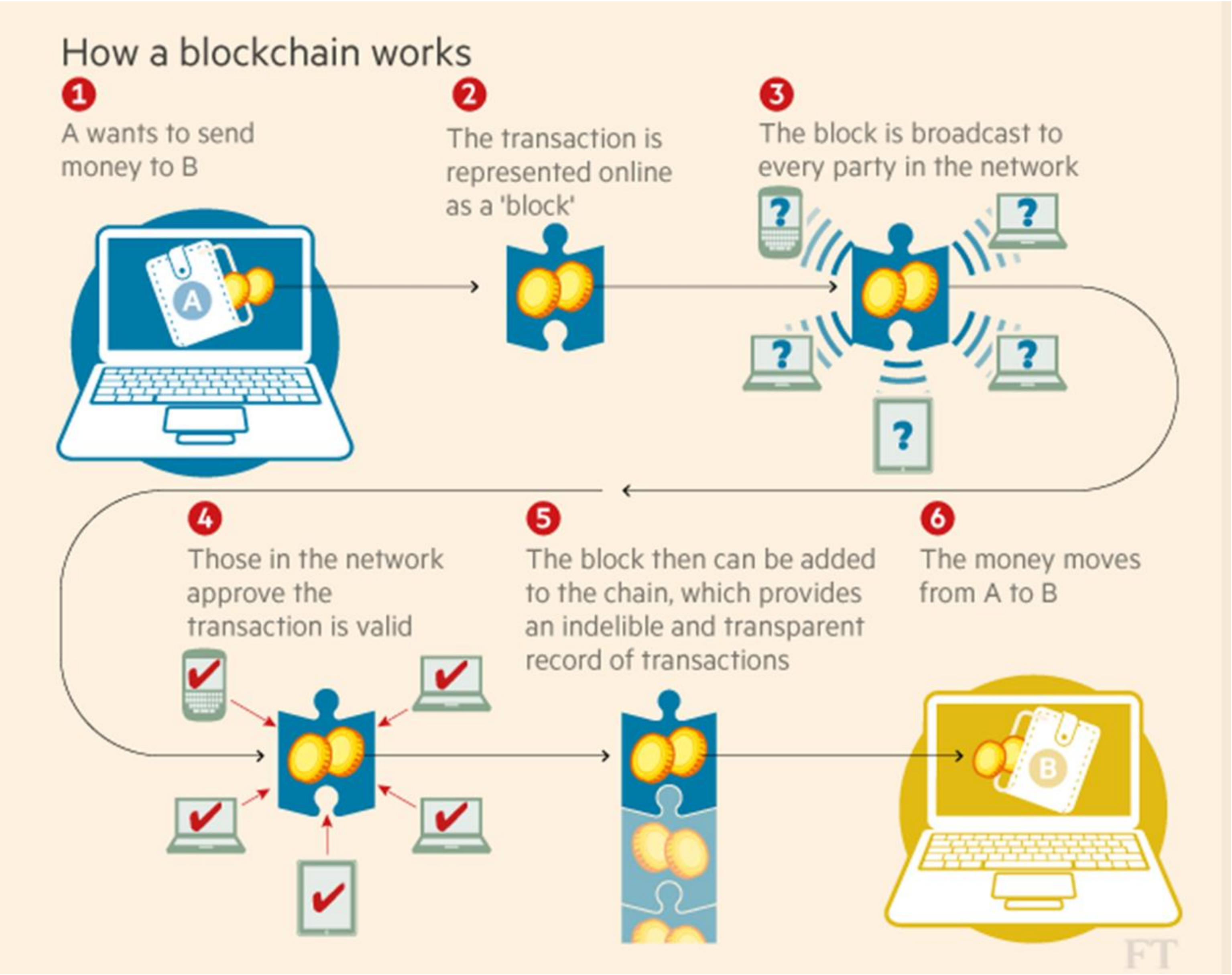
INPUTS From
0627052b6f28912f2703066a912ea577f2ce4da4caa5a5fbd8a57286c345c2f2 : 0
Bob 0.0150 BTC

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

“Verification”


Transaction
Owner 1's Public Key
Hash
Owner 0's Signature
Owner 1's Private Key
Verify
Sign
Transaction
Owner 2's Public Key
Hash
Owner 1's Signature
Owner 2's Private Key
Verify
Sign
Transaction
Owner 3's Public Key
Hash
Owner 2's Signature
Owner 3's Private Key

How Bitcoin Works



How a blockchain works

1. A wants to send money to B
2. The transaction is represented online as a 'block'
3. The block is broadcast to every party in the network
4. Those in the network approve the transaction is valid
5. The block then can be added to the chain, which provides an indelible and transparent record of transactions
6. The money moves from A to B

Global Bitcoin Network

GLOBAL BITCOIN NODES DISTRIBUTION

Reachable nodes as of Tue Dec 12 2017 13:39:17 GMT+0900 (대한민국 표준시).

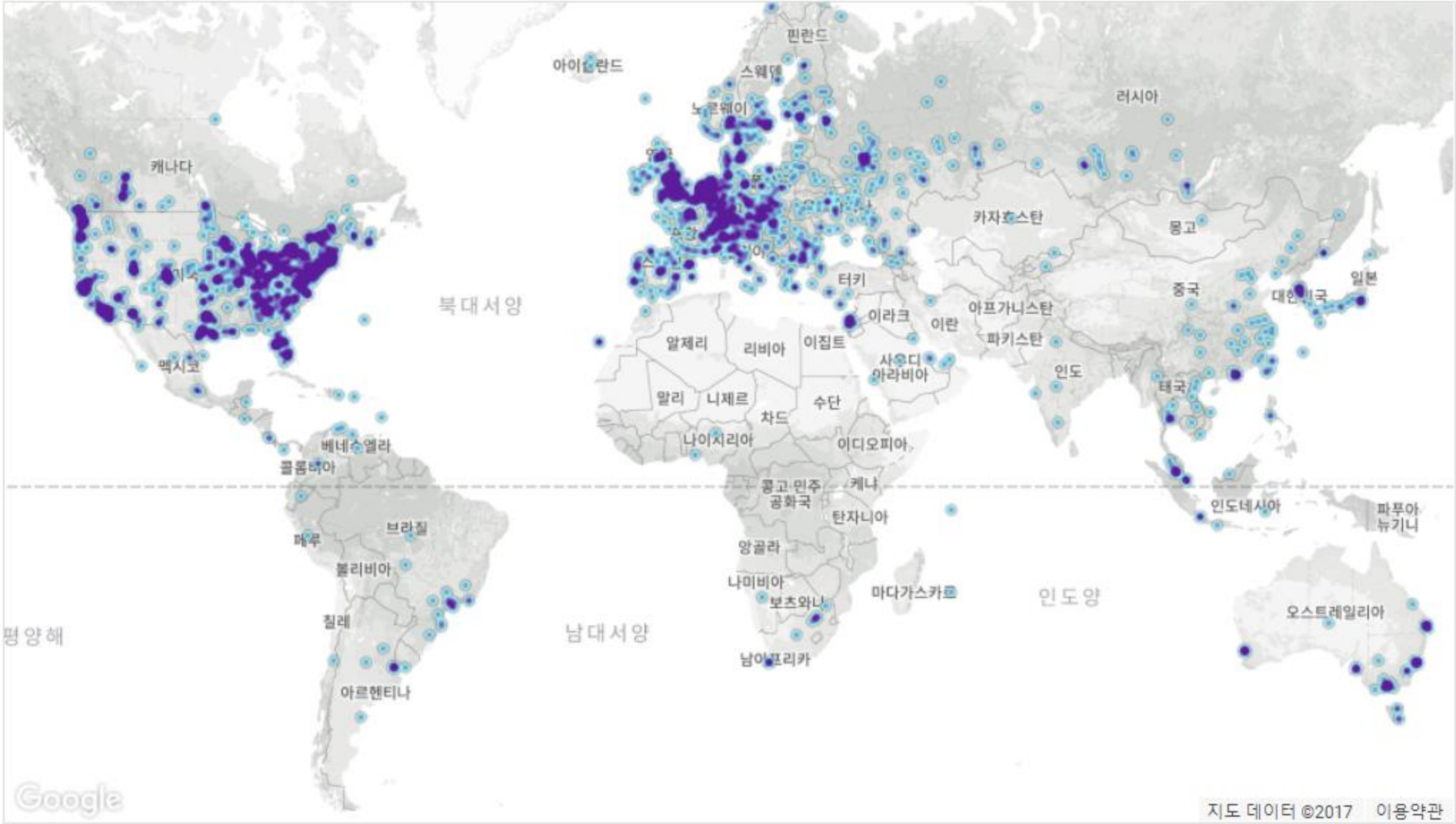
11684 NODES

24-hour charts »

Top 10 countries with their respective number of reachable nodes are as follow.

RANK	COUNTRY	NODES
1	United States	3247 (27.79%)
2	Germany	1951 (16.70%)
3	France	810 (6.93%)
4	China	769 (6.58%)
5	Netherlands	525 (4.49%)
6	Canada	501 (4.29%)
7	United Kingdom	443 (3.79%)
8	Russian Federation	395 (3.38%)
9	n/a	350 (3.00%)
10	Singapore	242 (2.07%)

More (101) »



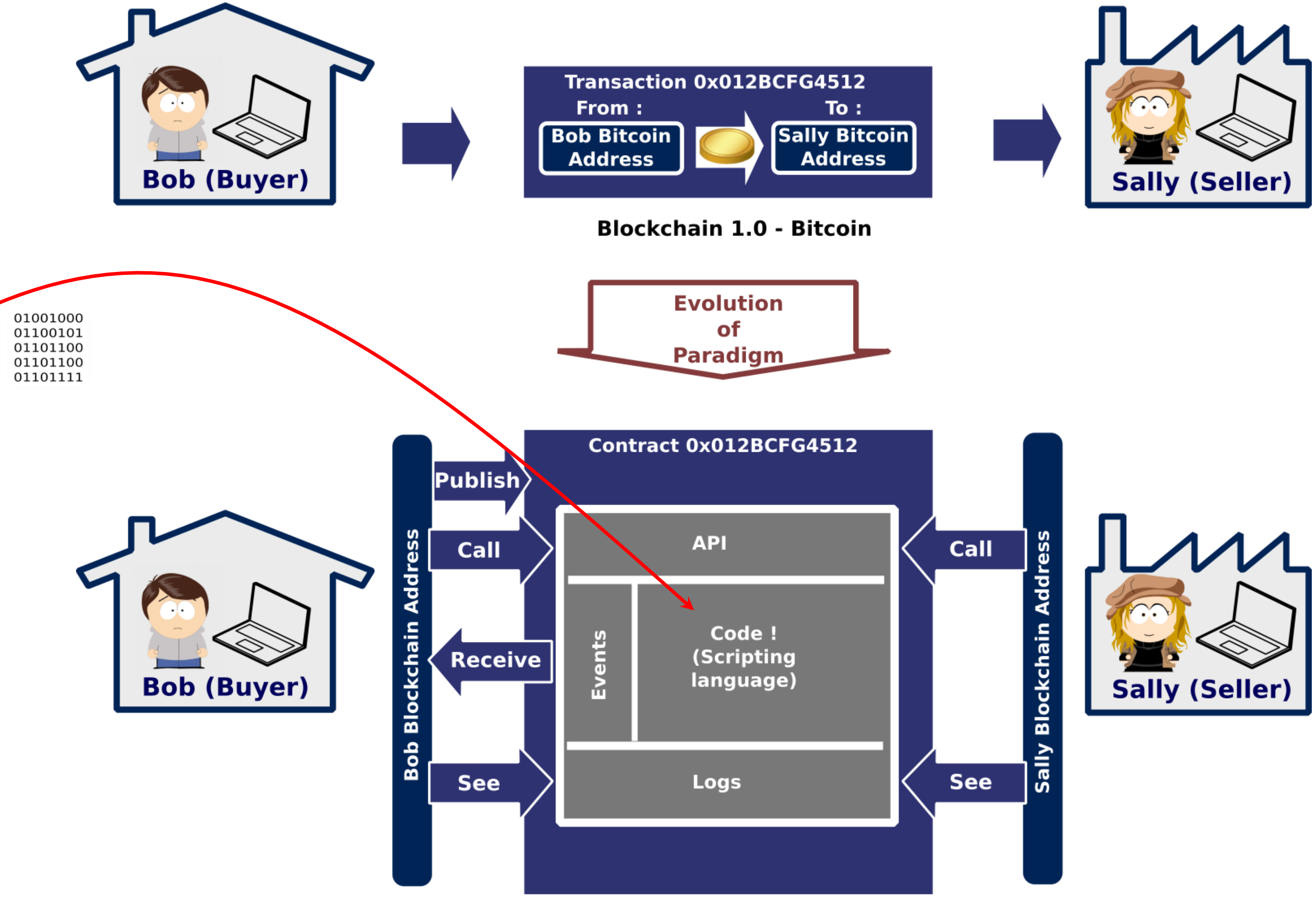
핀란드
아이슬란드
스웨덴
노르웨이
러시아
캐나다
카자흐스탄
몽고
북대서양
터키
중국
일본
대한민국
이라크
이란
아프가니스탄
파키스탄
알제리
리비아
이집트
사우디아라비아
인도
멕시코
말리
니제르
수단
차드
태국
베네수엘라
나이지리아
이디오피아
콜롬비아
콩고 민주 공화국
케냐
인도네시아
파푸아 뉴기니
탄자니아
브라질
페루
앙골라
볼리비아
나미비아
마다가스카르
인도양
보츠와나
오스트레일리아
칠레
남대서양
평양해
남아프리카
아르헨티나
Google
지도 데이터 ©2017
이용약관

Map shows concentration of reachable Bitcoin nodes found in countries around the world.

LIVE MAP

Smart Contract

Nick Szabo



01001000
01100101
01101100
01101100
01101111

Bob (Buyer)

Transaction 0x012BCFG4512

From : Bob Bitcoin Address

To : Sally Bitcoin Address

Sally (Seller)

Blockchain 1.0 - Bitcoin

Evolution of Paradigm

Bob (Buyer)

Bob Blockchain Address

Publish

Call

Receive

See

Contract 0x012BCFG4512

API

Events

Code ! (Scripting language)

Logs

Call

See

Sally Blockchain Address

Sally (Seller)

Blockchain 2.0 - e.g. Ethereum, …

Ethereum

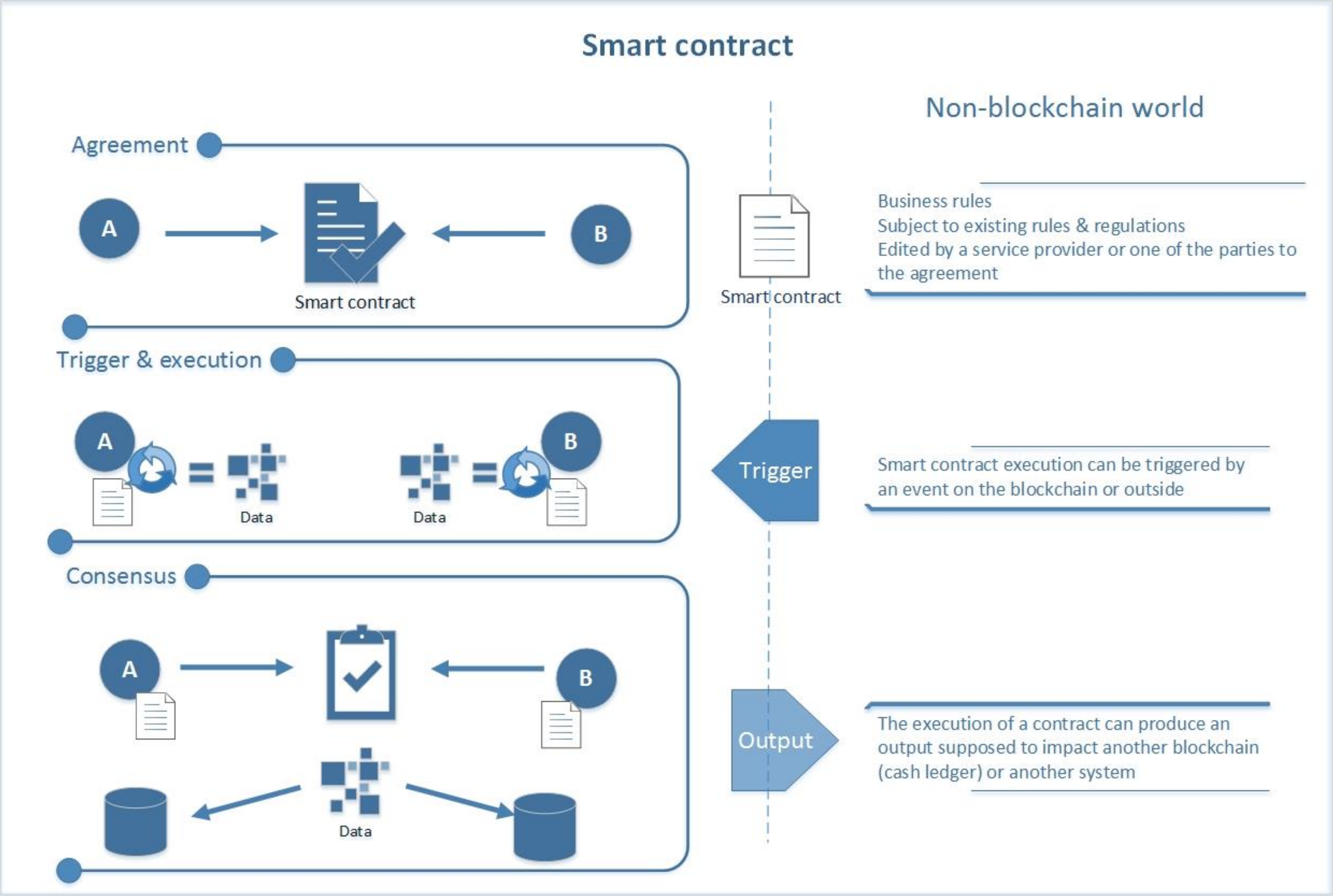
ethereum
HOMESTEAD RELEASE
BLOCKCHAIN APP PLATFORM

DISRUPT
Crunch

"World Computer"

- In 2014, Vitalik launched Ethereum project and successfully funded 20 mil worth of Ether by ICO
- While the goal of bitcoin is to build a platform that makes the digital currency to be exchanged safely on the internet without any interfering with governments or financial institutions, the goal of Ethereum is to build a platform that makes a genuine free web by expanding the territory of blockchain to encompass real-world applications
- Gas, Ethereum Virtual Machine

Smart Contract on Blockchain



Smart contract
Non-blockchain world
Agreement
A
B
Smart contract
Trigger & execution
A
B
Data
Data
Consensus
A
B
Data
Smart contract
Trigger
Output

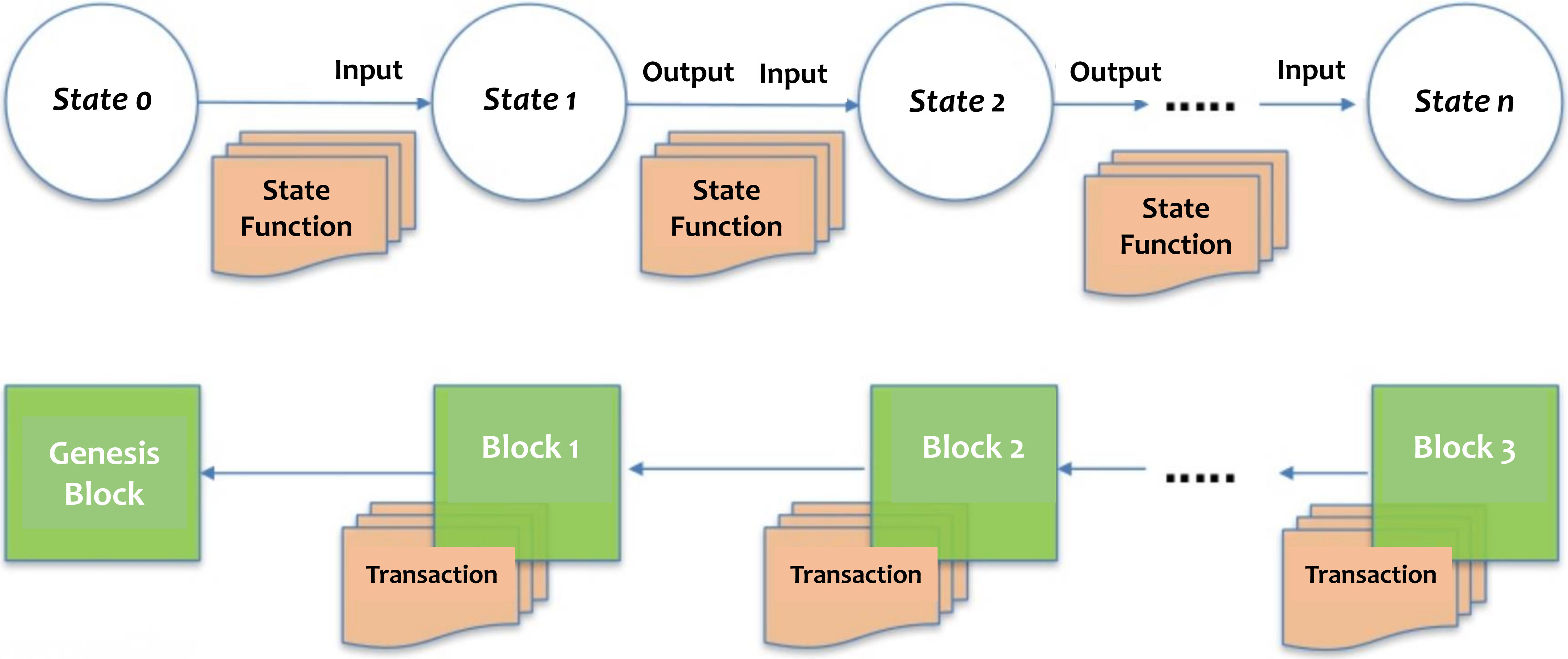
Business rules
Subject to existing rules & regulations
Edited by a service provider or one of the parties to the agreement

Smart contract execution can be triggered by an event on the blockchain or outside

The execution of a contract can produce an output supposed to impact another blockchain (cash ledger) or another system

FUNDCHAIN

State Transition


State 0
Input
State 1
Output
Input
State 2
Output
......
Input
State n
State Function
State Function
State Function
Genesis Block
Block 1
Block 2
......
Block 3
Transaction
Transaction
Transaction

Etherem Research Forum

Ethereum Transaction

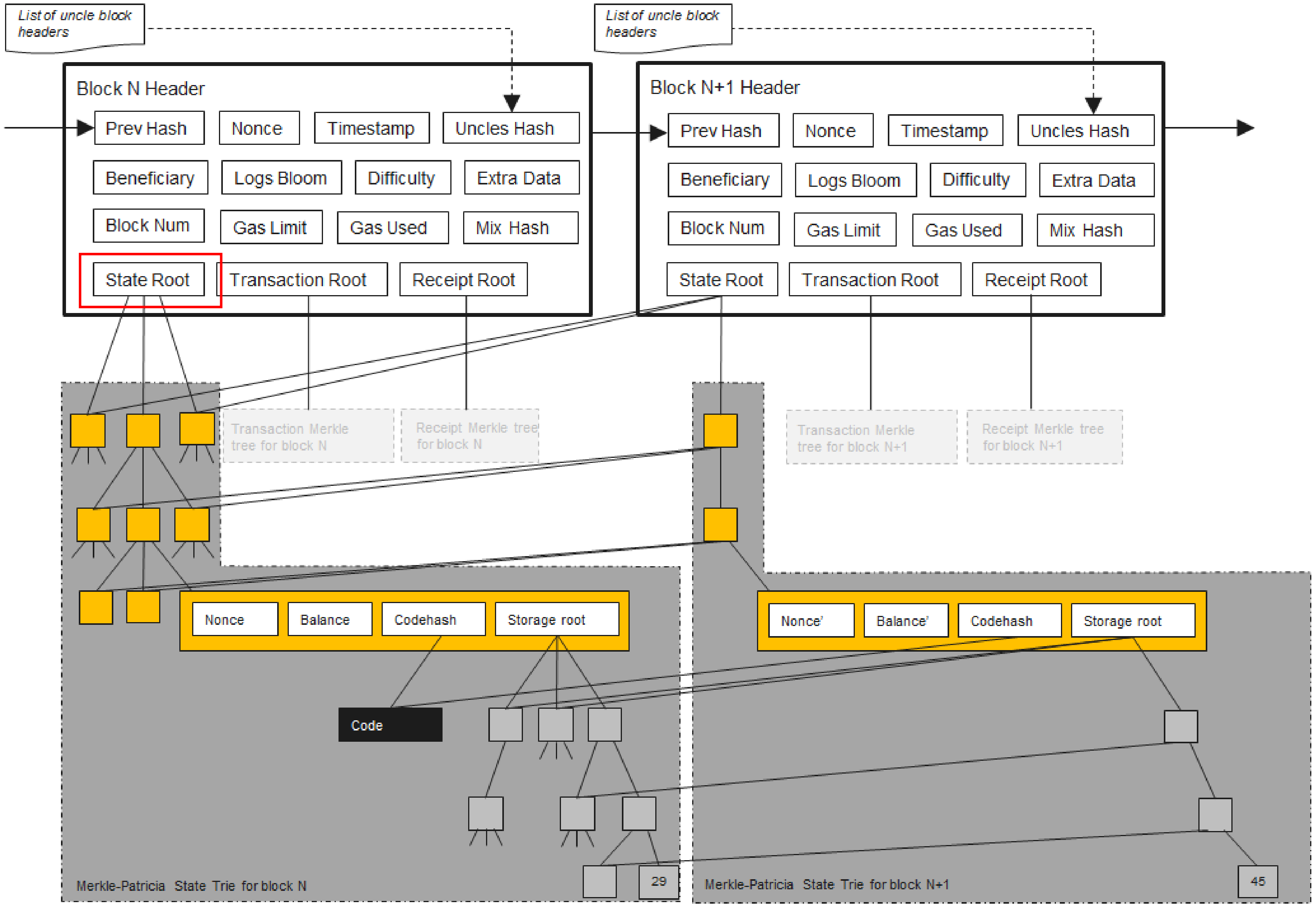
"Transaction"

Nounce	How many times the sender has sent a transaction
Sender	Address of sender
Recipient	Address of smart contract account
Value	Amount of ether to send
Gasprice	Amount of ether the sender pay per unit gas
Gaslimit	Maximum units of gas to consume
Data	Message to smart contract
Signature	Signature of sender

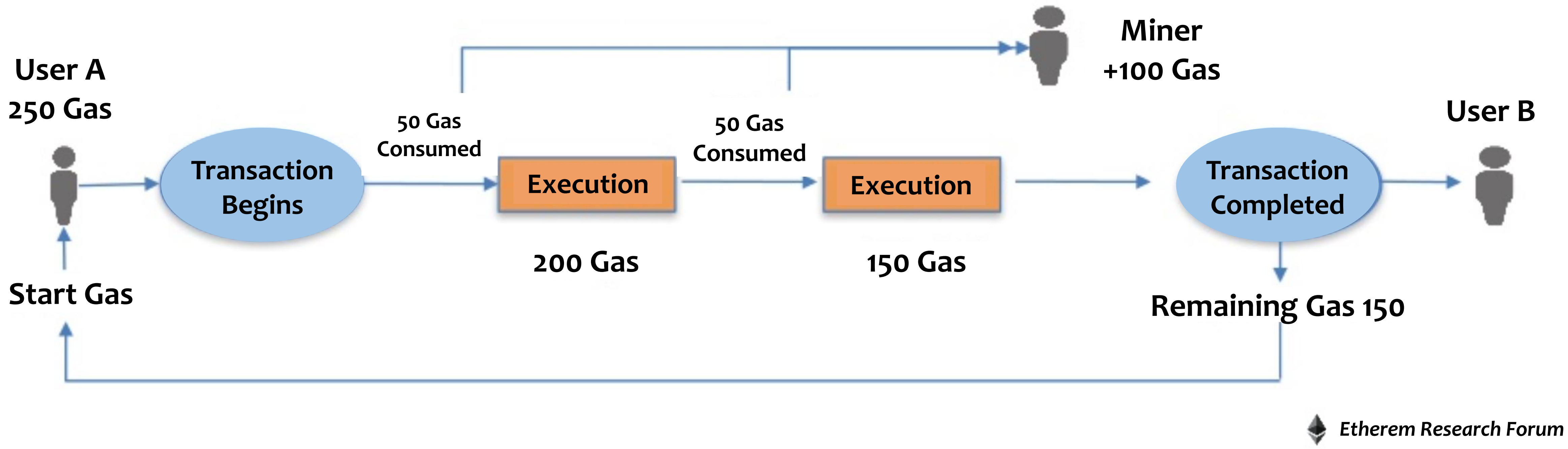
"Message"

Nounce	How many times the sender has sent a transaction
Sender	Address of sender
Recipient	Address of smart contract account
Value	Amount of gas to send
Gaslimit	Maximum units of gas to consume
Data	Message to smart contract
Signature	Signature of sender

Block of Ethereum


List of uncle block headers
Block N Header
Prev Hash
Nonce
Timestamp
Uncles Hash
Beneficiary
Logs Bloom
Difficulty
Extra Data
Block Num
Gas Limit
Gas Used
Mix Hash
State Root
Transaction Root
Receipt Root
List of uncle block headers
Block N+1 Header
Prev Hash
Nonce
Timestamp
Uncles Hash
Beneficiary
Logs Bloom
Difficulty
Extra Data
Block Num
Gas Limit
Gas Used
Mix Hash
State Root
Transaction Root
Receipt Root
Transaction Merkle tree for block N
Receipt Merkle tree for block N
Transaction Merkle tree for block N+1
Receipt Merkle tree for block N+1
Nonce
Balance
Codehash
Storage root
Code
29
Merkle-Patricia State Trie for block N
Nonce'
Balance'
Codehash
Storage root
45
Merkle-Patricia State Trie for block N+1

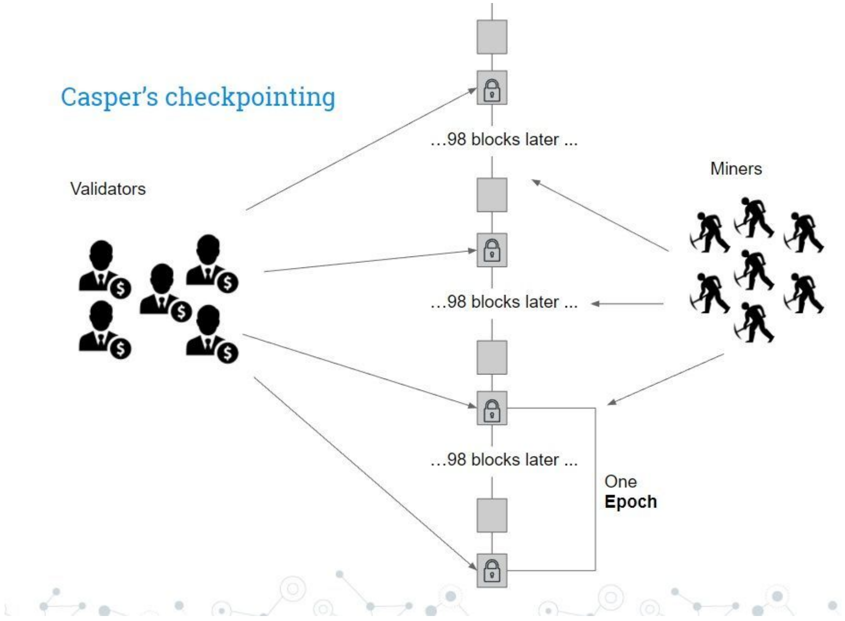
Gas

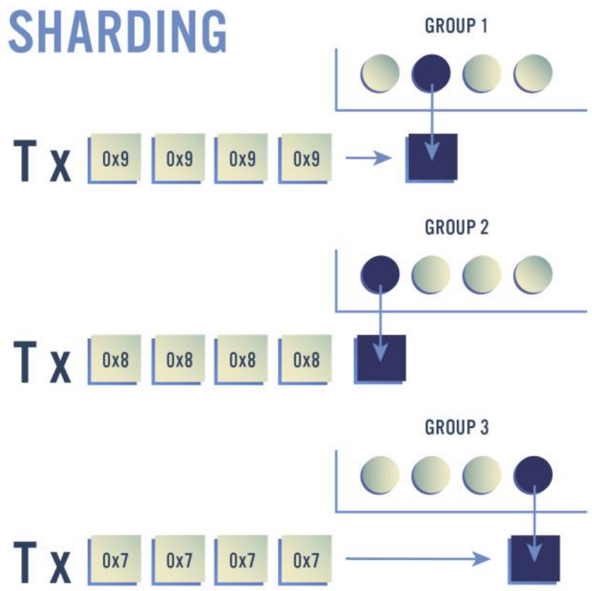

User A
250 Gas
Transaction Begins
50 Gas Consumed
Execution
200 Gas
50 Gas Consumed
Execution
150 Gas
Miner
+100 Gas
Transaction Completed
User B
Remaining Gas 150
Start Gas

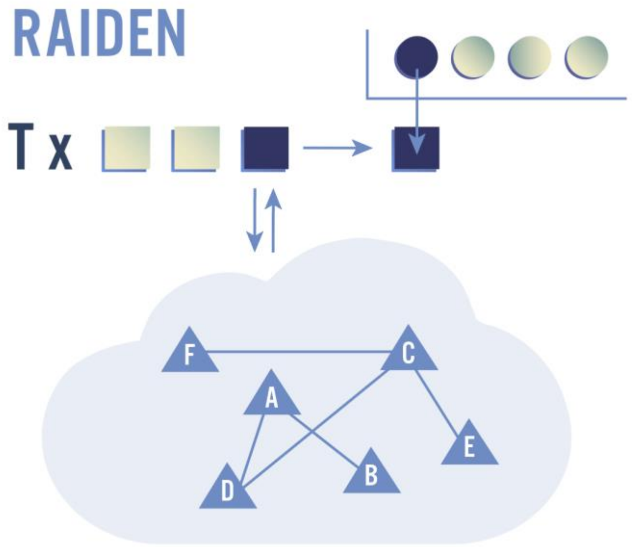
Etherem Research Forum

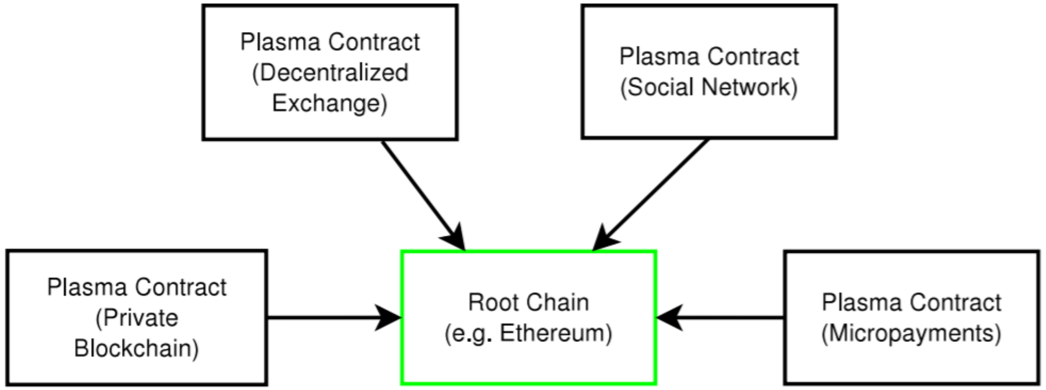
- Maximum transaction execution cost = gasLimit * gasPrice
- Min gasLimit : 21,000
- Max gasLimit per a block : 6,700,000

Scalability Improvements


Casper's checkpointing
Validators
Miners
...98 blocks later ...
...98 blocks later ...
...98 blocks later ...
One
Epoch


SHARDING
GROUP 1
Tx
0x9
0x9
0x9
0x9
GROUP 2
Tx
0x8
0x8
0x8
0x8
GROUP 3
Tx
0x7
0x7
0x7
0x7


RAIDEN
Tx
F
C
A
E
D
B



Plasma Contract (Decentralized Exchange)

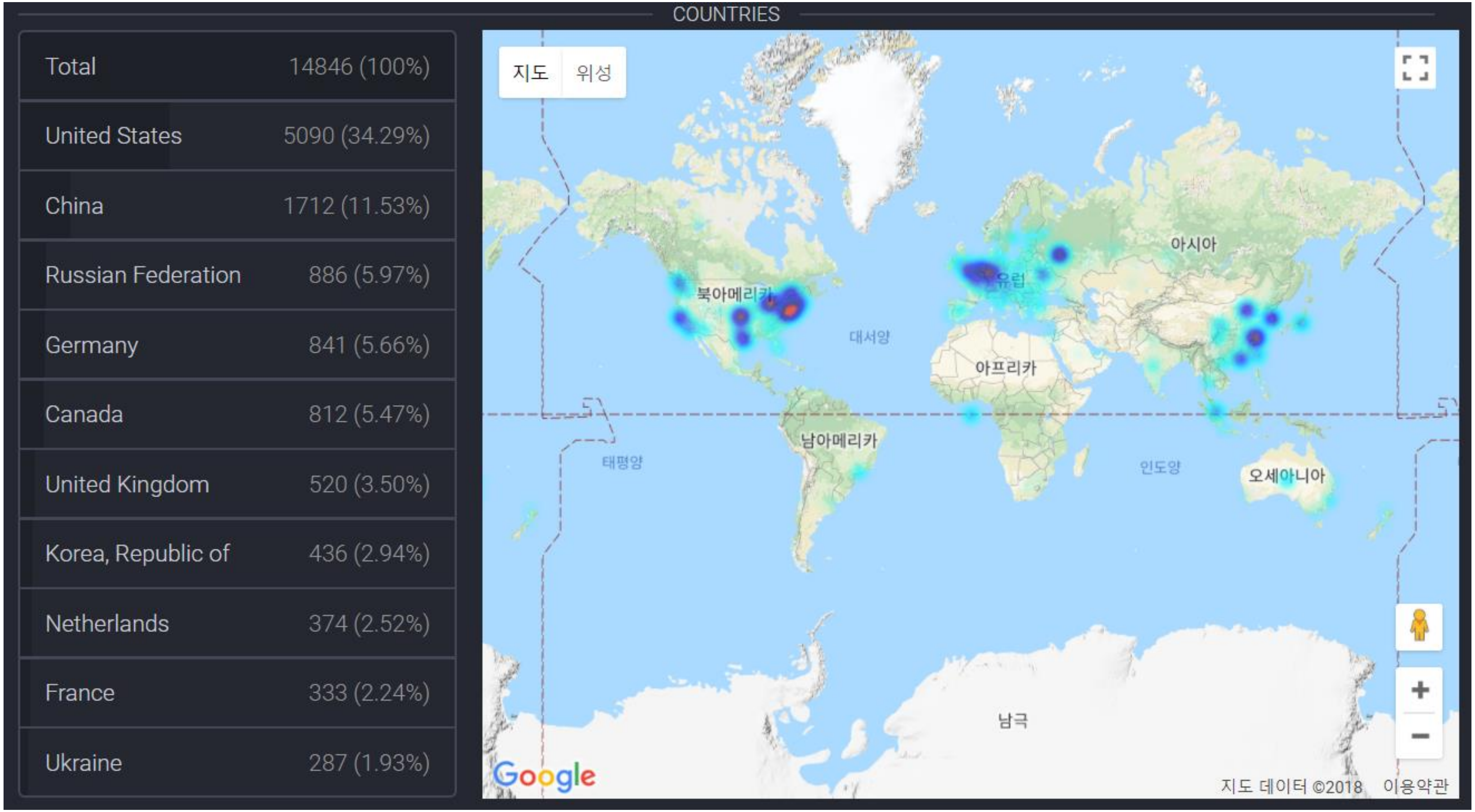
Plasma Contract (Social Network)

Plasma Contract (Private Blockchain)

Root Chain (e.g. Ethereum)

Plasma Contract (Micropayments)

Global Ethereum network



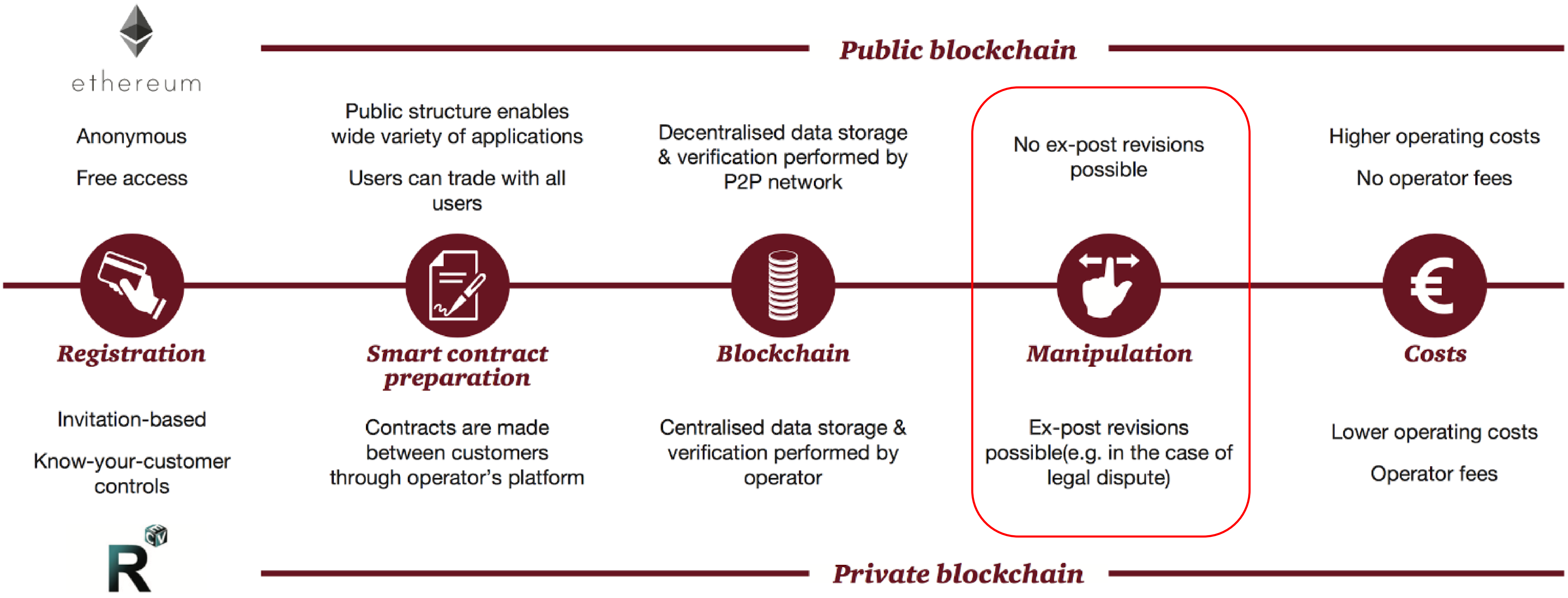
COUNTRIES

Total	14846 (100%)
United States	5090 (34.29%)
China	1712 (11.53%)
Russian Federation	886 (5.97%)
Germany	841 (5.66%)
Canada	812 (5.47%)
United Kingdom	520 (3.50%)
Korea, Republic of	436 (2.94%)
Netherlands	374 (2.52%)
France	333 (2.24%)
Ukraine	287 (1.93%)

지도
위성
북아메리카
유럽
아시아
대서양
아프리카
남아메리카
태평양
인도양
오세아니아
남극
Google
지도 데이터 ©2018
이용약관

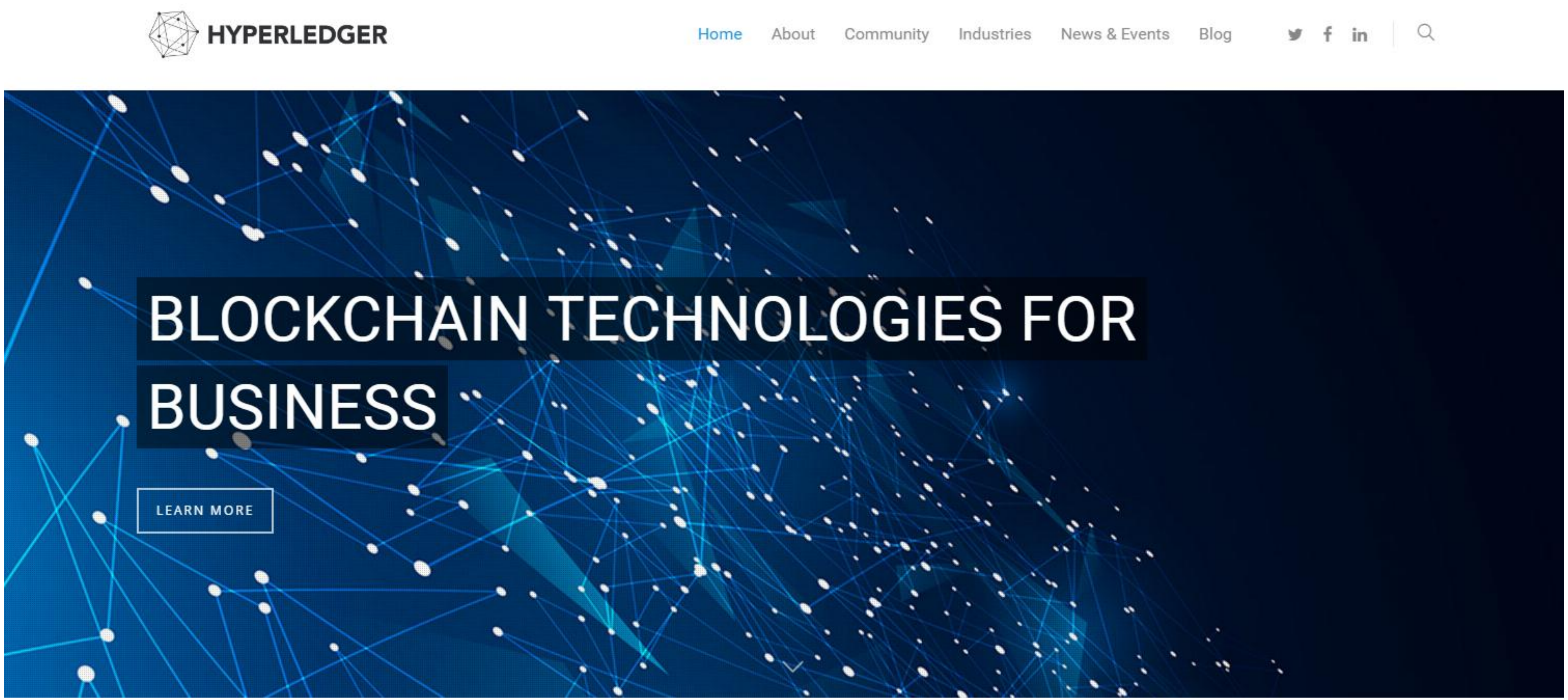
1. Essense of Blockchain: Infrastructure for Trust
2. Bitcoin, Ethereum
3. **Private Blockchain**
4. Blockchain Applications
5. Next Generation Blockchain

Public Blockchain vs. Private Blockchain



	Registration	Smart contract preparation	Blockchain	Manipulation	Costs
Public blockchain	Anonymous Free access	Public structure enables wide variety of applications Users can trade with all users	Decentralised data storage & verification performed by P2P network	No ex-post revisions possible	Higher operating costs No operator fees
Private blockchain	Invitation-based Know-your-customer controls	Contracts are made between customers through operator's platform	Centralised data storage & verification performed by operator	Ex-post revisions possible(e.g. in the case of legal dispute)	Lower operating costs Operator fees

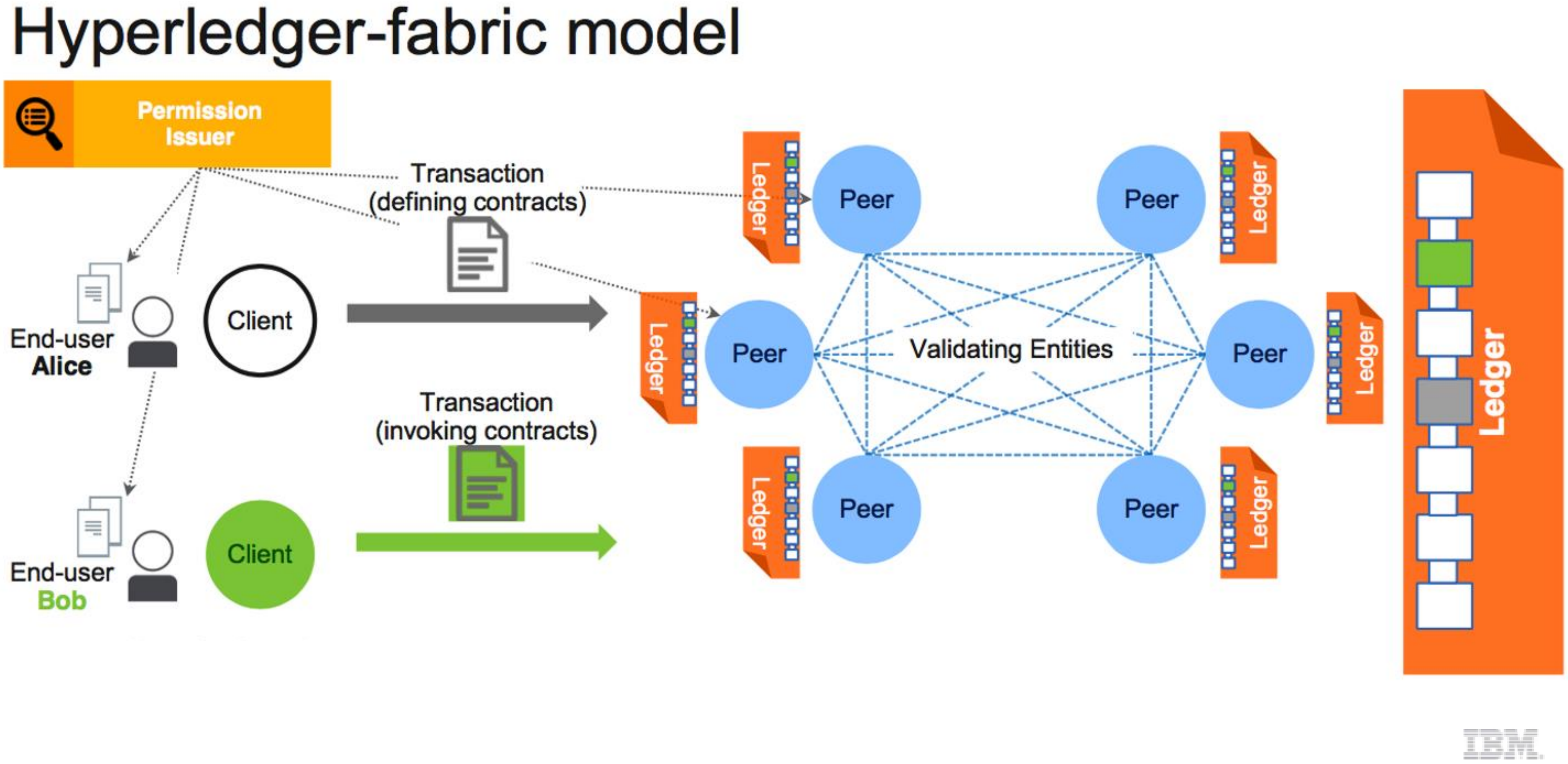
Hyperledger Project


HYPERLEDGER
Home
About
Community
Industries
News & Events
Blog
LEARN MORE

BLOCKCHAIN TECHNOLOGIES FOR BUSINESS

- Hosted by Linux Foundation & IBM
- Open source collaborative effort to advance cross-industry blockchain platform
- +100 startups, companies, organizations joined throughout the world

Hyperledger Fabric

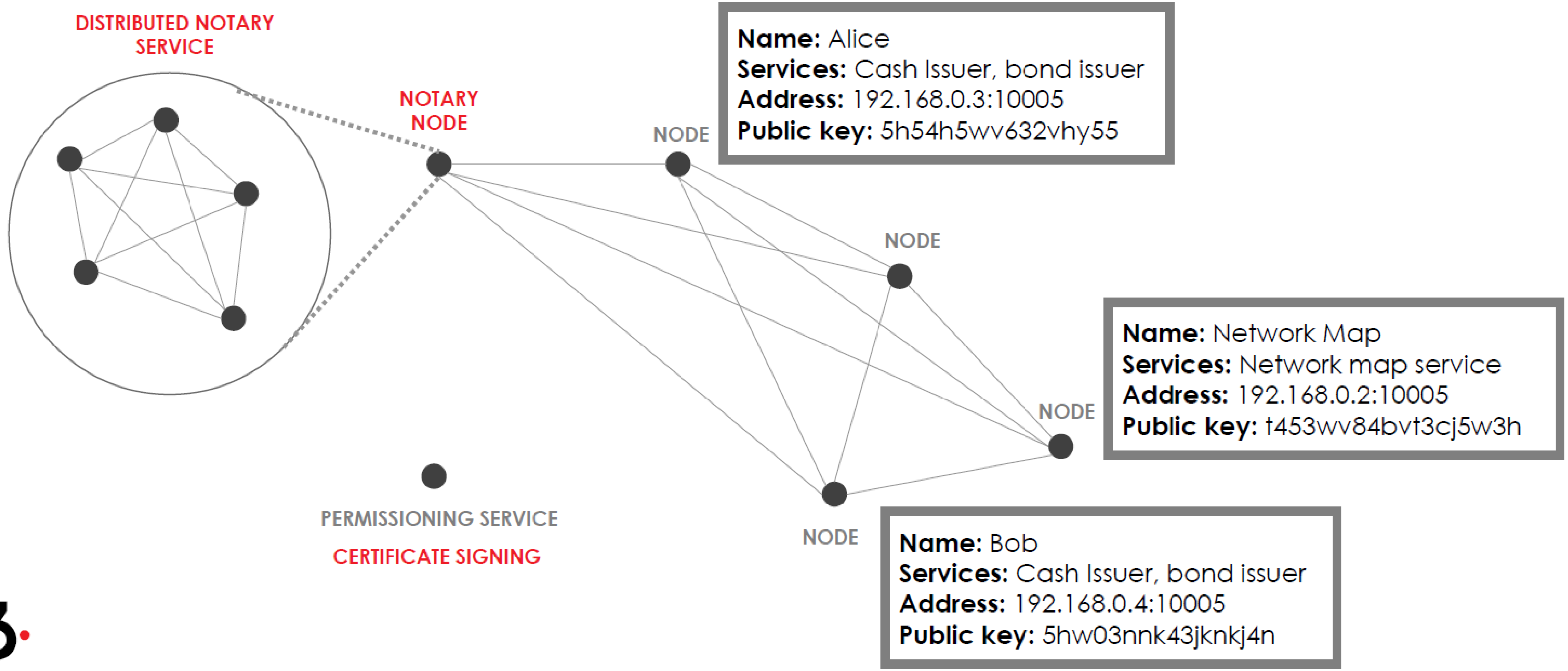

Hyperledger-fabric model
Permission Issuer
Transaction (defining contracts)
End-user Alice
Client
Transaction (invoking contracts)
End-user Bob
Client
Ledger
Peer
Peer
Ledger
Ledger
Peer
Validating Entities
Peer
Ledger
Ledger
Peer
Peer
Ledger
Ledger
IBM

Corda Project

R3 CEV
WE EMPOWER INNOVATION WITH EXPERTISE

- World first blockchain-based global bank consortium project
- Founders : David Rutter, Jesse Edwards, Todd McDonald
- +80 banks joined throughout the world
- **Distributed ledger platform for recording and processing financial agreement**

Corda Network



DISTRIBUTED NOTARY SERVICE
NOTARY NODE
NODE
NODE
NODE
NODE
PERMISSIONING SERVICE
CERTIFICATE SIGNING

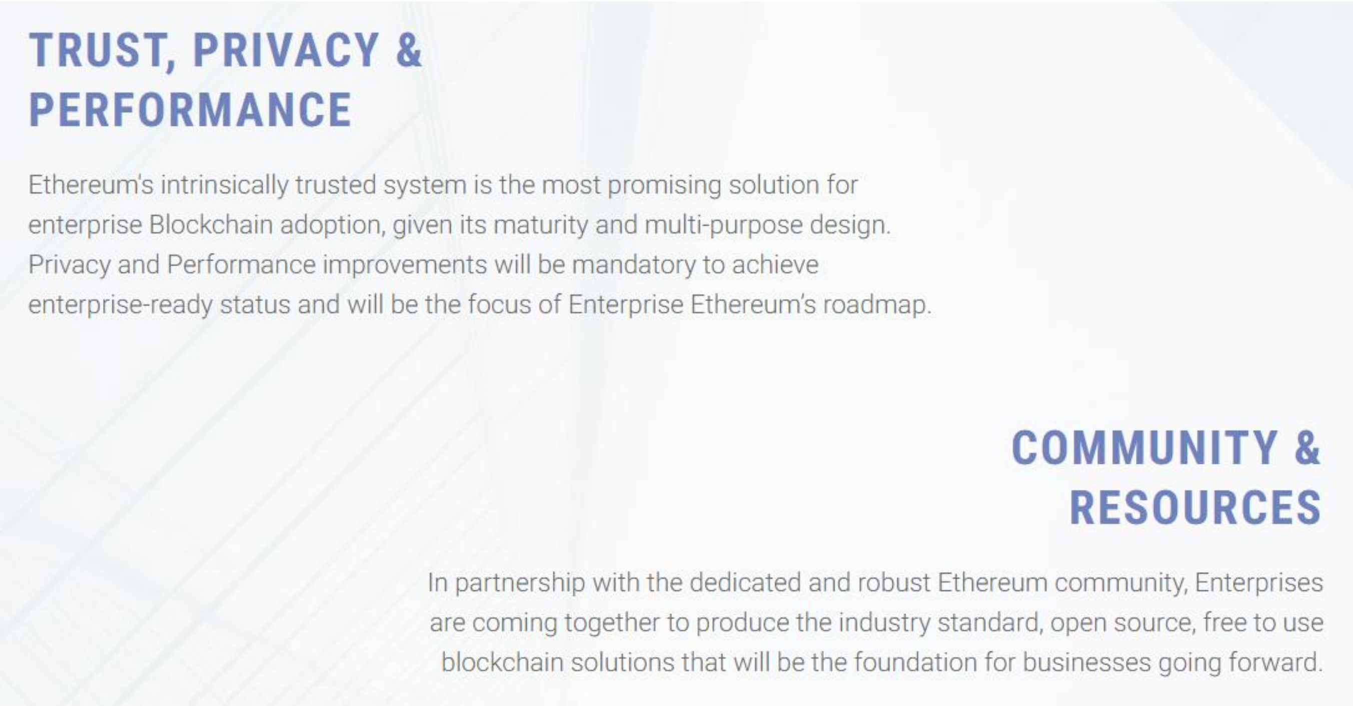
Name: Alice
Services: Cash Issuer, bond issuer
Address: 192.168.0.3:10005
Public key: 5h54h5wv632vhy55

Name: Network Map
Services: Network map service
Address: 192.168.0.2:10005
Public key: t453wv84bvt3cj5w3h

Name: Bob
Services: Cash Issuer, bond issuer
Address: 192.168.0.4:10005
Public key: 5hw03nnk43jknkj4n

Enterprise Ethereum Project

ENTERPRISE
ETHEREUM
ALLIANCE



TRUST, PRIVACY & PERFORMANCE

Ethereum's intrinsically trusted system is the most promising solution for enterprise Blockchain adoption, given its maturity and multi-purpose design. Privacy and Performance improvements will be mandatory to achieve enterprise-ready status and will be the focus of Enterprise Ethereum's roadmap.

COMMUNITY & RESOURCES

In partnership with the dedicated and robust Ethereum community, Enterprises are coming together to produce the industry standard, open source, free to use blockchain solutions that will be the foundation for businesses going forward.

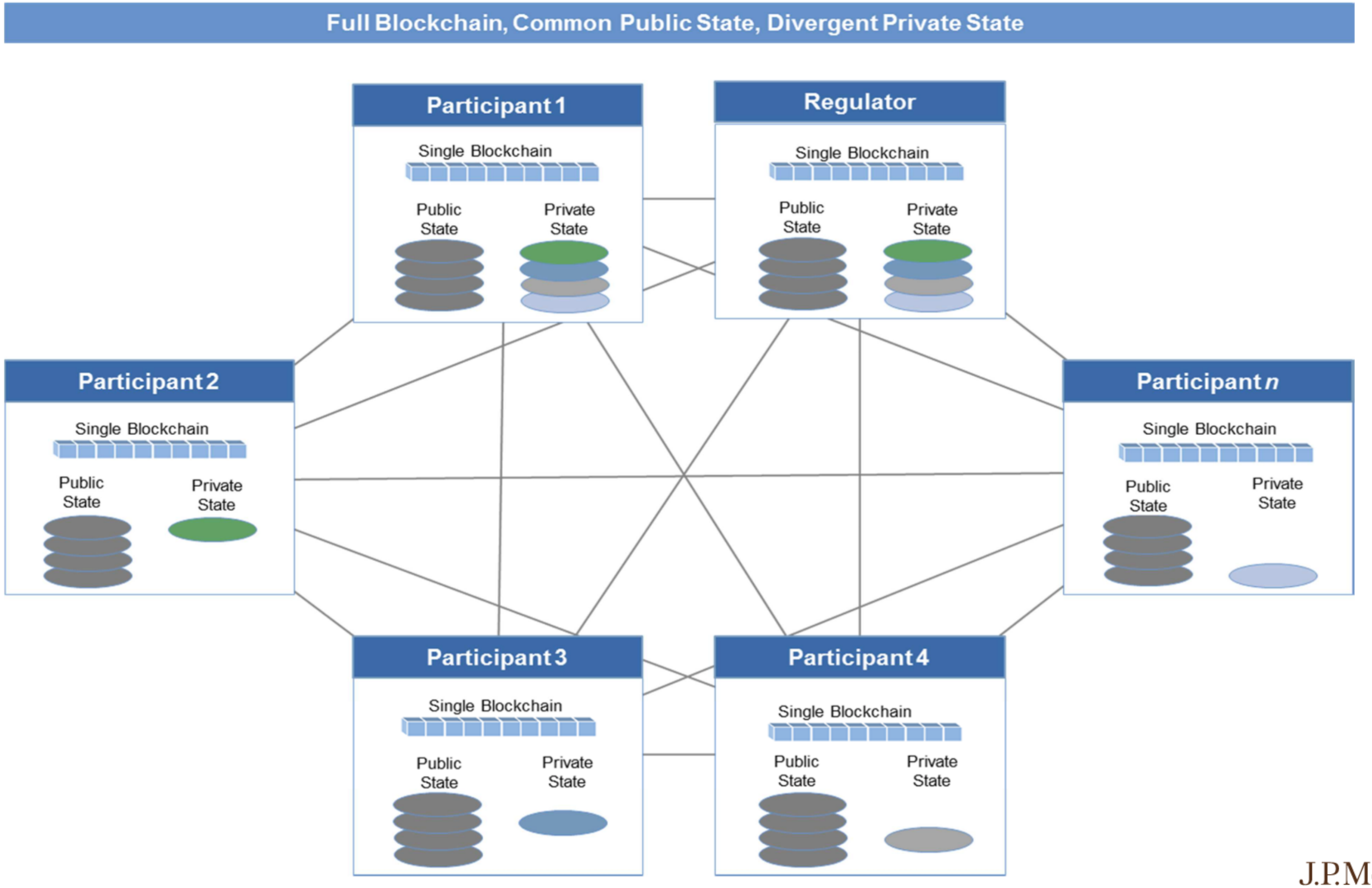
Quorum

nuco

BLOCKAPPS
STRATO

STRATO IS THE FULL-STACK TECHNOLOGY SOLUTION THAT ALLOWS YOU TO BUILD INDUSTRY-SPECIFIC BLOCKCHAIN APPLICATIONS

Quorum


Full Blockchain, Common Public State, Divergent Private State
Participant 1
Single Blockchain
Public State
Private State
Regulator
Single Blockchain
Public State
Private State
Participant 2
Single Blockchain
Public State
Private State
Participant *n*
Single Blockchain
Public State
Private State
Participant 3
Single Blockchain
Public State
Private State
Participant 4
Single Blockchain
Public State
Private State

J.P.Morgan

1. Essense of Blockchain: Infrastructure for Trust
2. Bitcoin, Ethereum
3. Private Blockchain
4. **Blockchain Applications**
5. Next Generation Blockchain

Blockchain Consortium

BY THE NUMBERS

- 32 global consortiums
- 18 in financial services
- 24 started in 2016
- Average # of members in each : 30
- Largest memberships : 100

R3

Number • 74
Location • New York, USA
Sector • Financial Services
Start Date • 2014
Goal • General purpose platform and technology to design and deliver advanced distributed ledger technologies to the global financial markets.
Members • See this list: https://en.wikipedia.org/wiki/R3_(company)
Leaders • R3 CEV

(C) William Mougayar, 2016.

HYPERLEDGER FOUNDATION

Number • 100
Location • San Francisco, USA
Sector • Standards & Platform
Start Date • Dec-2015
Goal • Open source collaborative effort created to advance cross-industry blockchain technologies. It is a global collaboration including leaders in finance, banking, Internet of Things, supply chains, manufacturing and Technology. The Linux Foundation hosts Hyperledger as a Collaborative Project under the foundation.
Members • See this list: https://www.hyperledger.org/about/members
Leaders • Linux Foundation, IBM, DAH.

(C) William Mougayar, 2016.

DIGITAL ASSET HOLDINGS

Number • 15
Location • New York, USA
Sector • Financial Services
Start Date • 2014
Goal • Building distributed, encrypted straight through processing tools to improve efficiency, security, compliance and settlement speed.
Members • Deutsche Börse, Icap, JP Morgan, DTCC , ABN Amro, Accenture, ASX Limited, BNP Paribas, Broadridge Financial Solutions, Citi, CME Ventures, Santander InnoVentures, IBM, Goldman Sachs and The PNC Financial Services Group.
Leaders • DAH

(C) William Mougayar, 2016.

PROJECT JASPER

Number • 8
Location • Toronto, Canada
Sector • Financial Services
Start Date • Jun-2016
Goal • Exploring the possibility of issuing, transferring and settling central bank-issued assets on a distributed ledger network.
Members • CIBC, Bank of Montreal, Royal Bank of Canada, TD Bank, Scotiabank, Bank of Canada, Payments Canada, R3.
Leaders • Payments Canada, Bank of Canada.

(C) William Mougayar, 2016.

RIPPLE JAPANESE BANKS CONSORTIUM

Number • 30
Location • Japan
Sector • Financial Services
Start Date • Aug-2016
Goal • Enable round-the-clock settlement at a significant cost reduction to its members and their consumers. The consortium says banks will pay about 90% less in fees.
Members • SBI Holdings, the Bank of Yokohama and SBI Sumishin Net Bank.
Leaders • SBI Ripple Asia.

(C) William Mougayar, 2016.

CHINALEDGER ALLIANCE

Number
Location
Sector
Start Date
Goal
Members
Leaders

• 11 China Standards & Regulation April-2016 Adapt and develop existing blockchain technology to the needs of Chinese businesses and set standards across the industry to ensure regulatory compliance in an environment where regulators are very positive, open and interested in blockchain technology. Shanghai Stock Exchange and others Wangxiang Blockchain Labs, Internet Securities Commission of the Securities Association of China (SAC).

(C) William Mougayar, 2016.

FINANCIAL BLOCKCHAIN SHENZHEN CONSORTIUM

Number • 31
Location • Shenzhen, China
Sector • Financial Services
Start Date • May-2016
Goal • Communication tool for companies and a platform for information sharing concerning blockchain studies. Performing joint research on the blockchain application and create collective projects for its testing in the financial sphere. Special projects include the development of a prototype of a blockchain platform for securities trading and exploration of related services for credit, digital asset registry and invoice management.
Members • Ping An Bank, SIno Safe General Insurance, Huawai, etc. (31 total)
Leaders • Ping An.

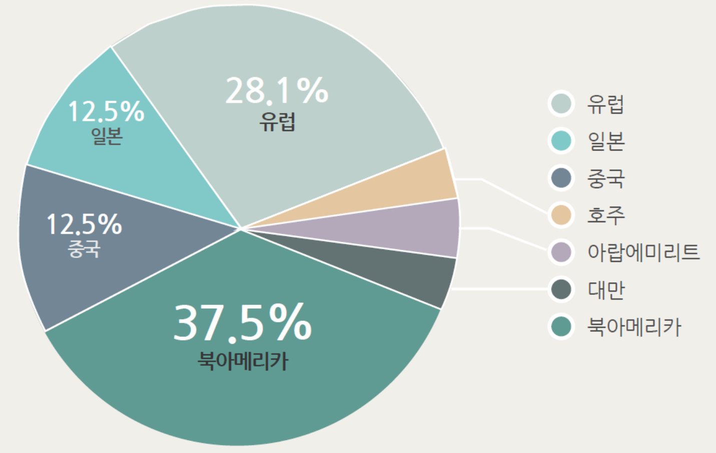
(C) William Mougayar, 2016.

GLOBAL BLOCKCHAIN COUNCIL

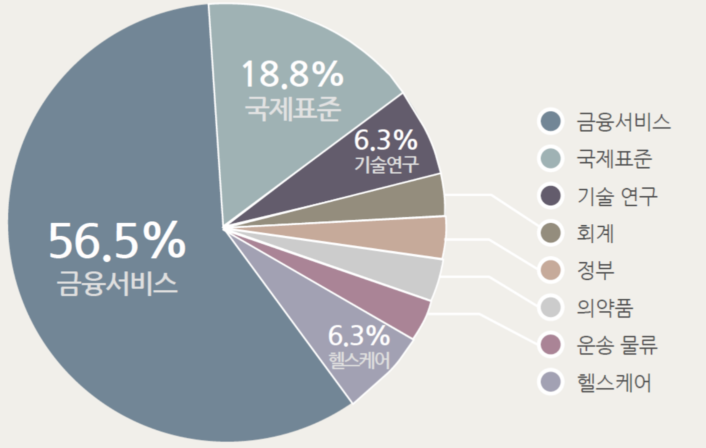
Number • 32
Location • UAE
Sector • Government
Start Date • Feb-2016
Goal • Help UAE authorities and corporations better understand this technology and consider its regulatory implications. Also, will conduct pilot projects testing the readiness of markets to adopt digital currencies.
Members • Du, SAP, IBM, TECOM, Dubai Holding, Privity FZ LLC, Vinay Gupta, Dubai Multi Commodities Centre (DMCC), Emirates Islamic, Microsoft, Infosys, Cisco, Dubai International Financial Center (DIFC), Souq.com, EmirateNBD, Careem, Michael Mainelli, Mashreq, Wamda, Propertyfinder.com, Kraken, Umbrellab, AstroLabs, YellowPay, SmartStart Fund, BitOasis, Ethereum, Viktor Koenig LLC, Digitus, Network int, Smart Dubai Office and Dubai Smart Government.
Leaders • Dubai International Financial Centre Authority.

(C) William Mougayar, 2016.

컨소시엄 지역별 비율 (2017.1.10)



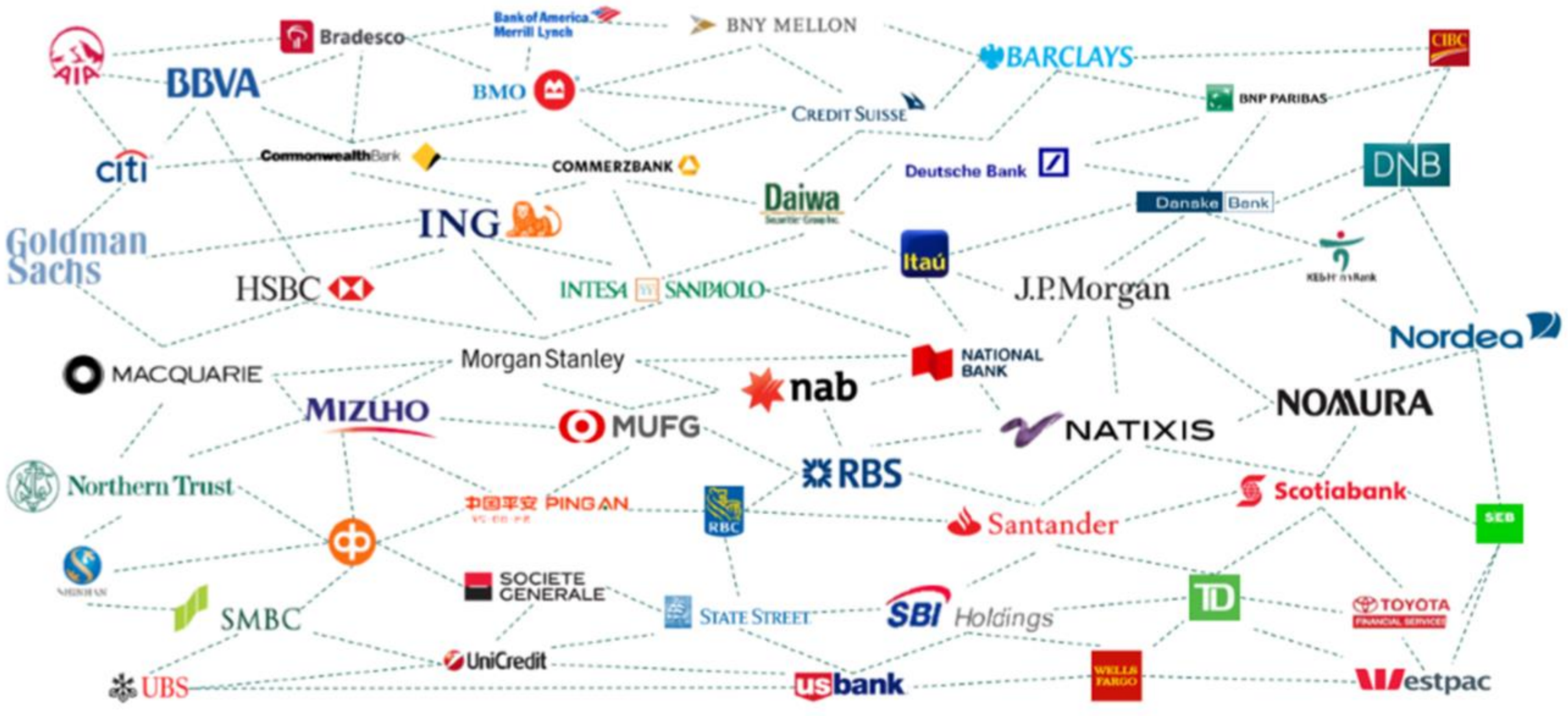
컨소시엄 분야별 비율 (2017.1.10)



R3 Consortium

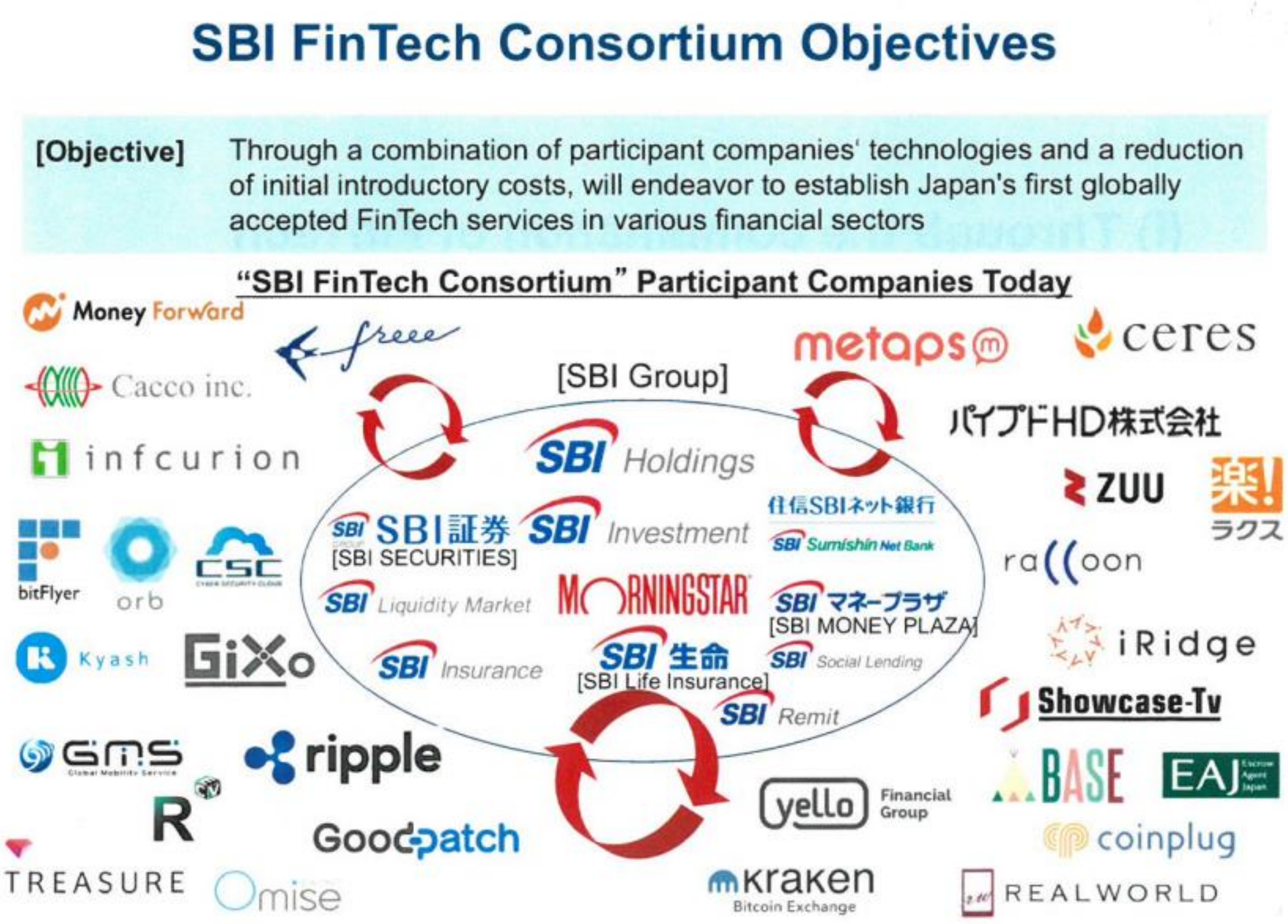
R3 Is the World's Largest Distributed Ledger Consortium

The 50+ Member initiative is focused exclusively on developing a next generation financial transaction network and commercial applications based on DLT


AIA
Bradesco
Bank of America Merrill Lynch
BNY MELLON
BARCLAYS
CIBC
BBVA
BMO
CREDIT SUISSE
BNP PARIBAS
citi
CommonwealthBank
COMMERZBANK
Daiwa
Deutsche Bank
DNB
Danske Bank
Goldman Sachs
ING
Itaú
HSBC
INTESA SANPAOLO
J.P.Morgan
Nordea
MACQUARIE
Morgan Stanley
nab
NATIONAL BANK
NOMURA
MIZUHO
MUFG
NATIXIS
Northern Trust
PING AN
RBC
RBS
Scotiabank
Santander
SEB
SMBC
SOCIETE GENERALE
STATE STREET
SBI Holdings
TD
TOYOTA FINANCIAL SERVICES
UBS
UniCredit
usbank
WELLS FARGO
Westpac

SBI Fintech Consortium

+30 Japanese fintech firms joined, Led by SBI Ripple Asia



SBI FinTech Consortium Objectives

[Objective] Through a combination of participant companies' technologies and a reduction of initial introductory costs, will endeavor to establish Japan's first globally accepted FinTech services in various financial sectors

"SBI FinTech Consortium" Participant Companies Today

Money Forward
freee
Cacco inc.
infcurion
bitFlyer
orb
CSC
Kyash
GiXo
GMS
ripple
R
TREASURE
Omise
Goodpatch
[SBI Group]
SBI Holdings
SBI証券
[SBI SECURITIES]
SBI Investment
住信SBIネット銀行
SBI Sumishin Net Bank
SBI Liquidity Market
MORNINGSTAR
SBI マネープラザ
[SBI MONEY PLAZA]
SBI Insurance
SBI 生命
[SBI Life Insurance]
SBI Social Lending
SBI Remit
metaps
ceres
パイプドHD株式会社
ZUU
楽! ラクス
raccoon
iRidge
Showcase-Tv
BASE
EAJ
coinplug
REALWORLD
yello Financial Group
kraken Bitcoin Exchange

Chinese Blockchain Consortium

Chinaledger Alliance

CHINALEDGER
WANXIANG
BLOCKCHAIN LABS

- Led by Wanxiang Group
- +11 financial institutions are joined

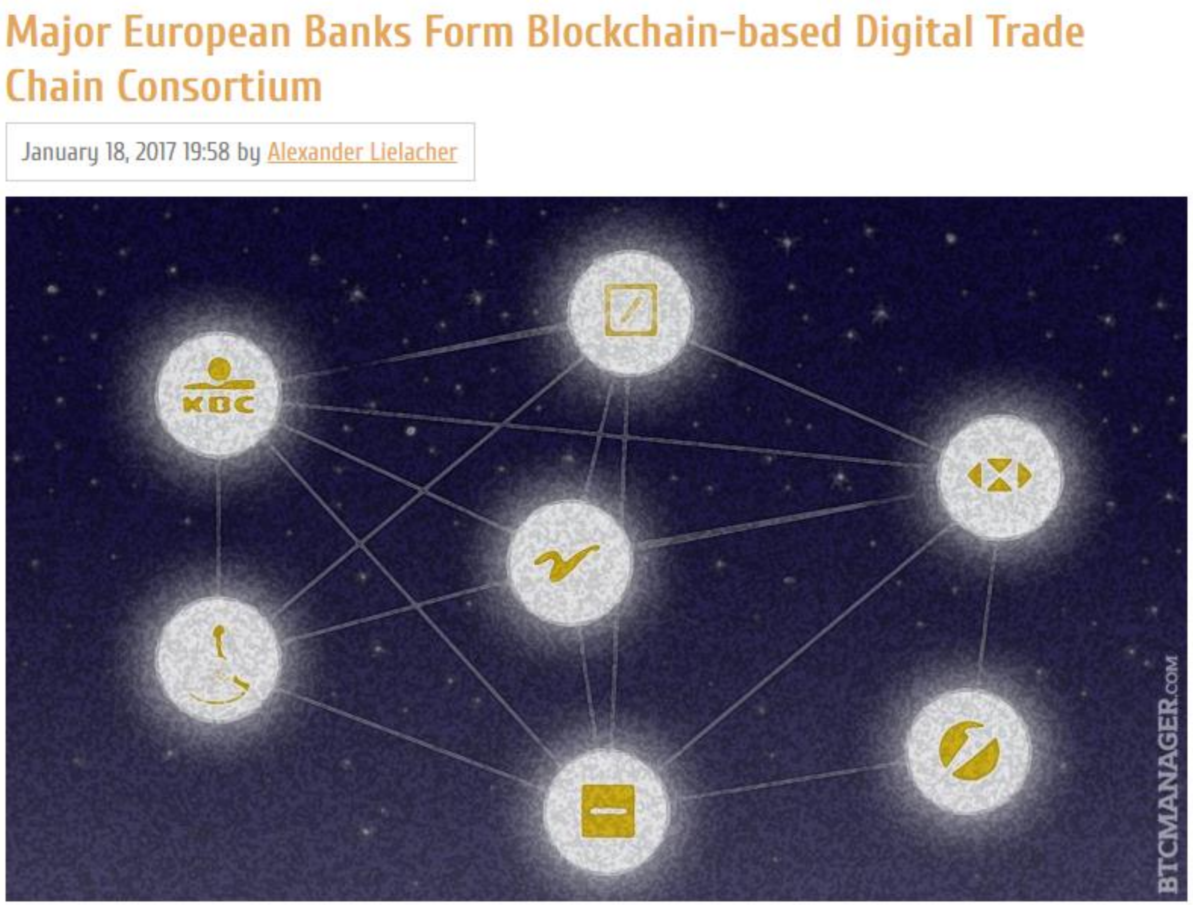
Blockchain Shenzhen Consortium

金融区块链合作联盟（深圳）成立大会
暨第一次联盟成员大会
中国平安
PING AN OF CHINA
专业·价值
Tencent

- Led by Ping An Bank and Tencent
- +31 technology and financial firms in China are joined

DTC Consortium

European banks' consortium for blockchain-based trade finance platform



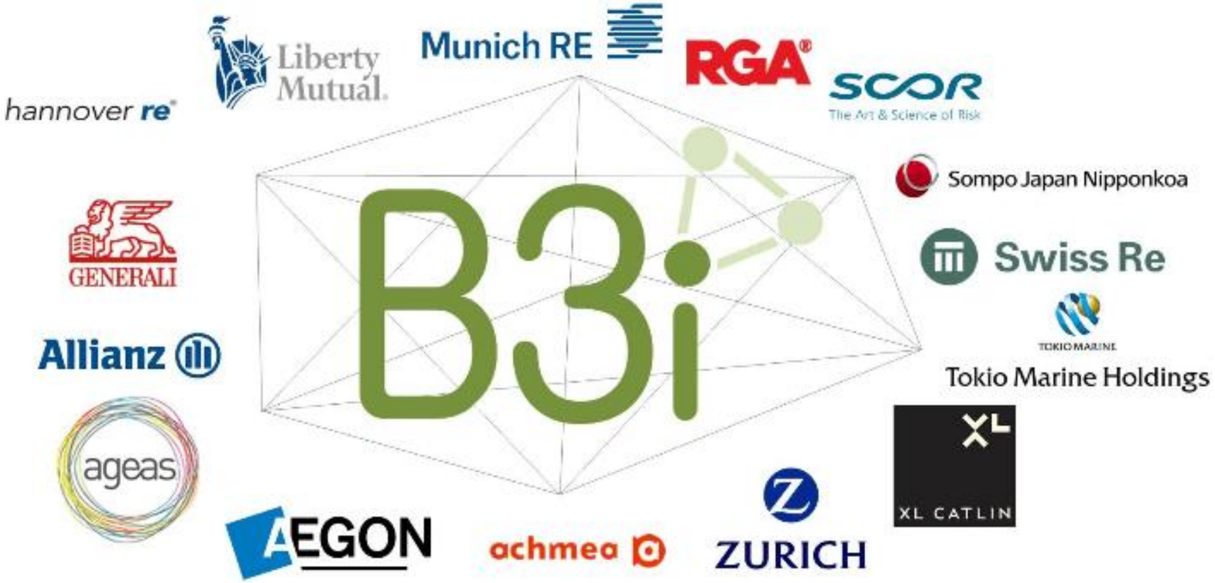
Major European Banks Form Blockchain-based Digital Trade Chain Consortium

January 18, 2017 19:58 by Alexander Lielacher

- Consortium members : Duetsche Bank, HSBC, Natixis, Rabobank, Societe Generale, UniCredit, KBC
- DTC : Digital Trading Chain
- Facilitate cross-border commerce for European small and medium-sized enterprises
- Leveraging distributed ledger technology to connect all parties involved in international trade transactions
- We.trade : digital platform for managing, tracking and protecting trade transactions between SMEs
- Registers entire trade process from order to payment, fully automated

B3i Consortium

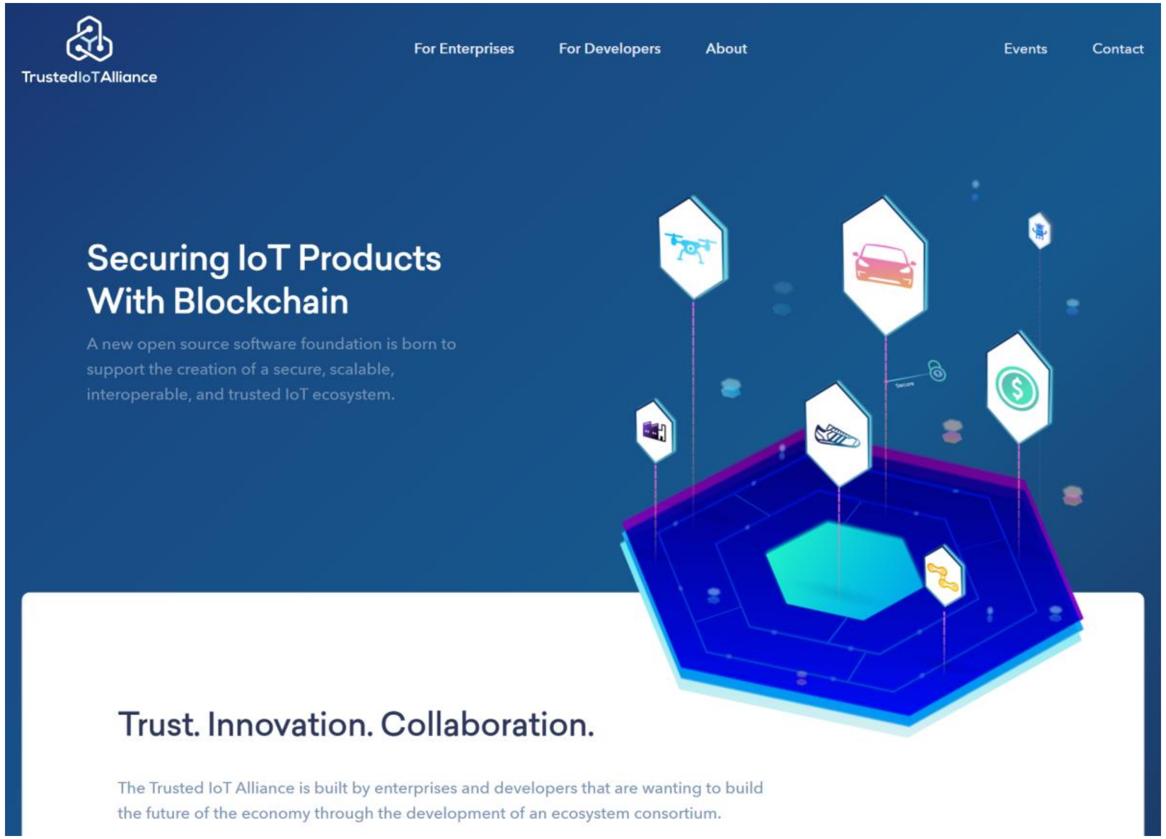
Switzerland Based Blockchain Insurance Initiative


hannover re
Liberty Mutual.
Munich RE
RGA
SCOR
The Art & Science of Risk
Sompo Japan Nipponkoa
Swiss Re
TOKIO MARINE
Tokio Marine Holdings
GENERALI
Allianz
B3i
ageas
AEGON
achmea
ZURICH
XL CATLIN

- Established : Oct. 2016
- Member : Aegon, Allianz, Munich Re, Swiss Re, Zurich, Achmea, Ageas, Generali, Hannover Re, RGA, Liberty Mutual, SCOR, Sompo Japan Nippoloa Insurance, Tokio Marine Holdings, XL Catin
- Streamlining insurance contract & settlement process using blockchain-based smart contract
- Acceleration of information & fund flow, Audit process improvement
- Developing new types of insurance service such as P2P insurance, microinsurance, parametric insurance
- Codex 1 : Blockchain-based smart contract prototype to automate catastrophic reinsurance processes

Trusted IoT Alliance

Tech Giants and start-ups have joined to form a consortium that will look to build a trusted IoT ecosystem with enhanced security and trust protocol



Securing IoT Products With Blockchain

A new open source software foundation is born to support the creation of a secure, scalable, interoperable, and trusted IoT ecosystem.

Trust. Innovation. Collaboration.

The Trusted IoT Alliance is built by enterprises and developers that are wanting to build the future of the economy through the development of an ecosystem consortium.

- Consortium includes Bank New York Mellon, Bosch, Cisco, Gemalto, Foxconn, BitSE, Chronicled, Consensys, Filament, Ledger, Skuchain, Slock.it, IOTA, Oaken Innovation, Chain of Things, BigChain DB
- Completed PoCs for trusted odometer, luxury goods identity verification, router firmware verification, trade finance automation, supply chain event logging, smart vehicle charging, deed of title registration, data logger provenance
- Value propositions for IoT product identity and provenance, Secure and transferable digital identities, Payments-enabled devices/machines, Immutable attestation of sensor data and event logs, Automation of business logic with smart contracts, Neutral support for business ecosystem, Elimination of silos in current IoT model

Blockchain SCM Initiative

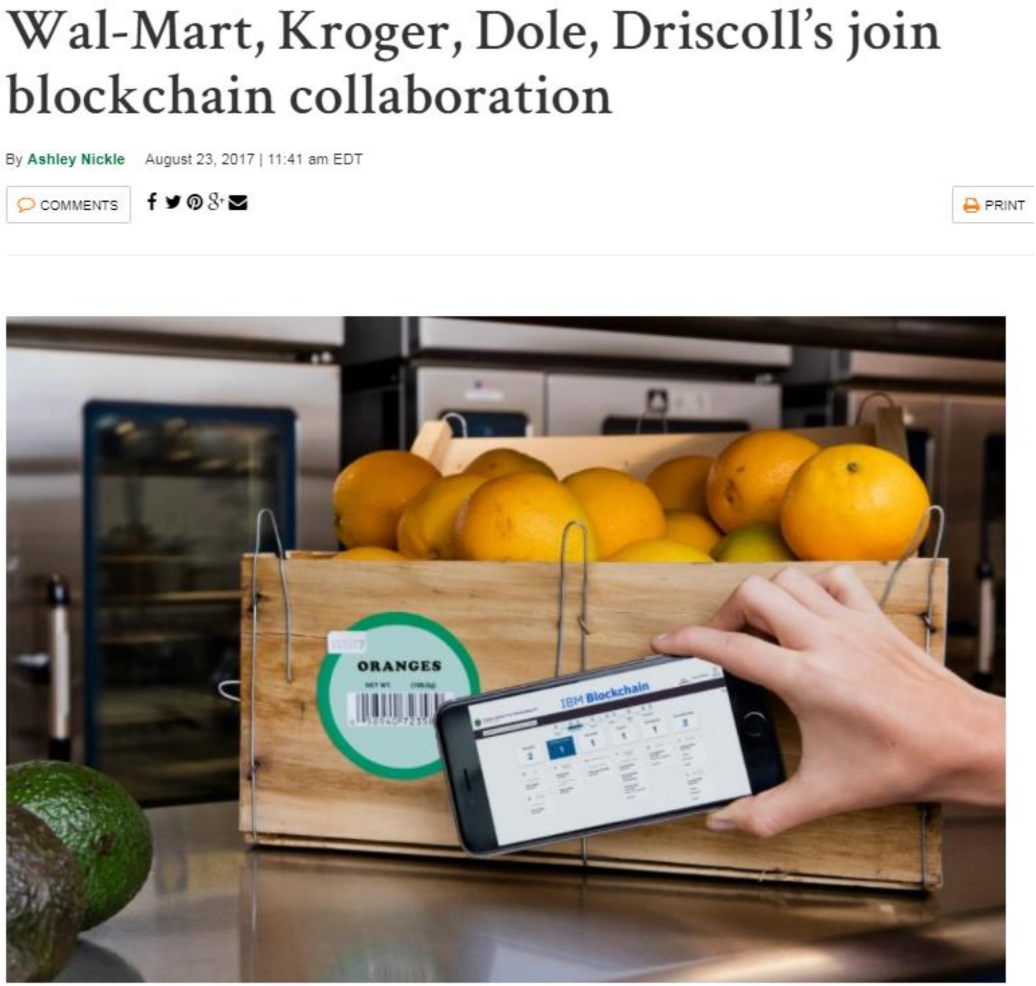
Maersk has joined forces with IBM to deploy blockchain technology for global cross-border supply chain applications

IBM. | MAERSK
Transforming supply chains using blockchain technology
#ibmblockchain

- Provide immutable, transparent visibility of the progress of goods through the supply chain, location of containers, status of customs, documents, BOL, and other data
- Provide efficiencies by reducing fraud and errors, improving inventory management, ultimately reducing cost and time
- Collaborating with shippers, freight forwarders, ocean carriers, ports, custom authorities
- Building global trade digitisation solution
- Completed PoC for tracking a container of flowers
- Custom administration of Netherlands, US Department of Homeland Security Science and Technology Directorate, US Customs and Border Protection

Blockchain in Food Supply

Major food suppliers' blockchain consortium for food safety initiative



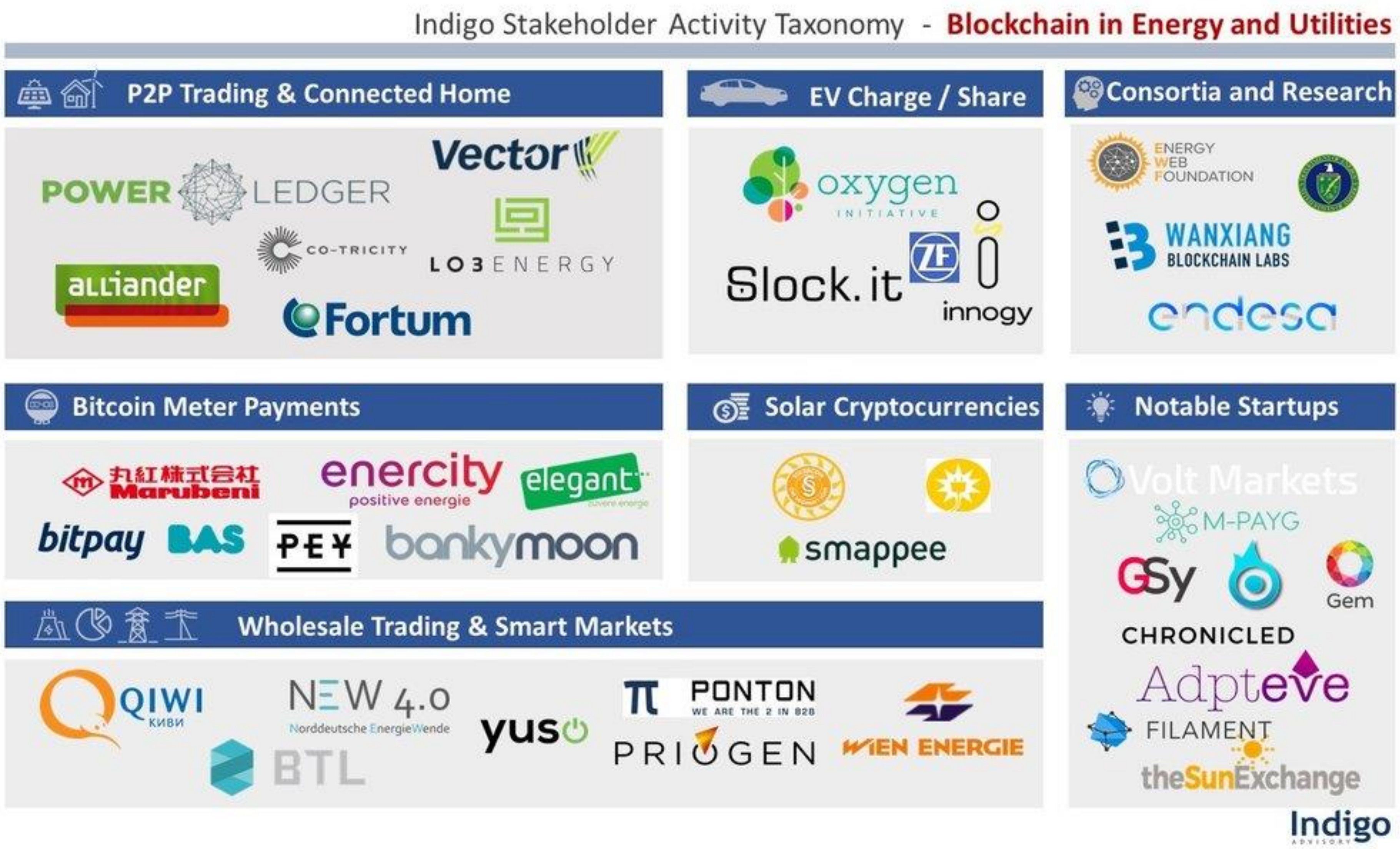
Wal-Mart, Kroger, Dole, Driscoll's join blockchain collaboration

By **Ashley Nickle** August 23, 2017 | 11:41 am EDT

COMMENTS PRINT

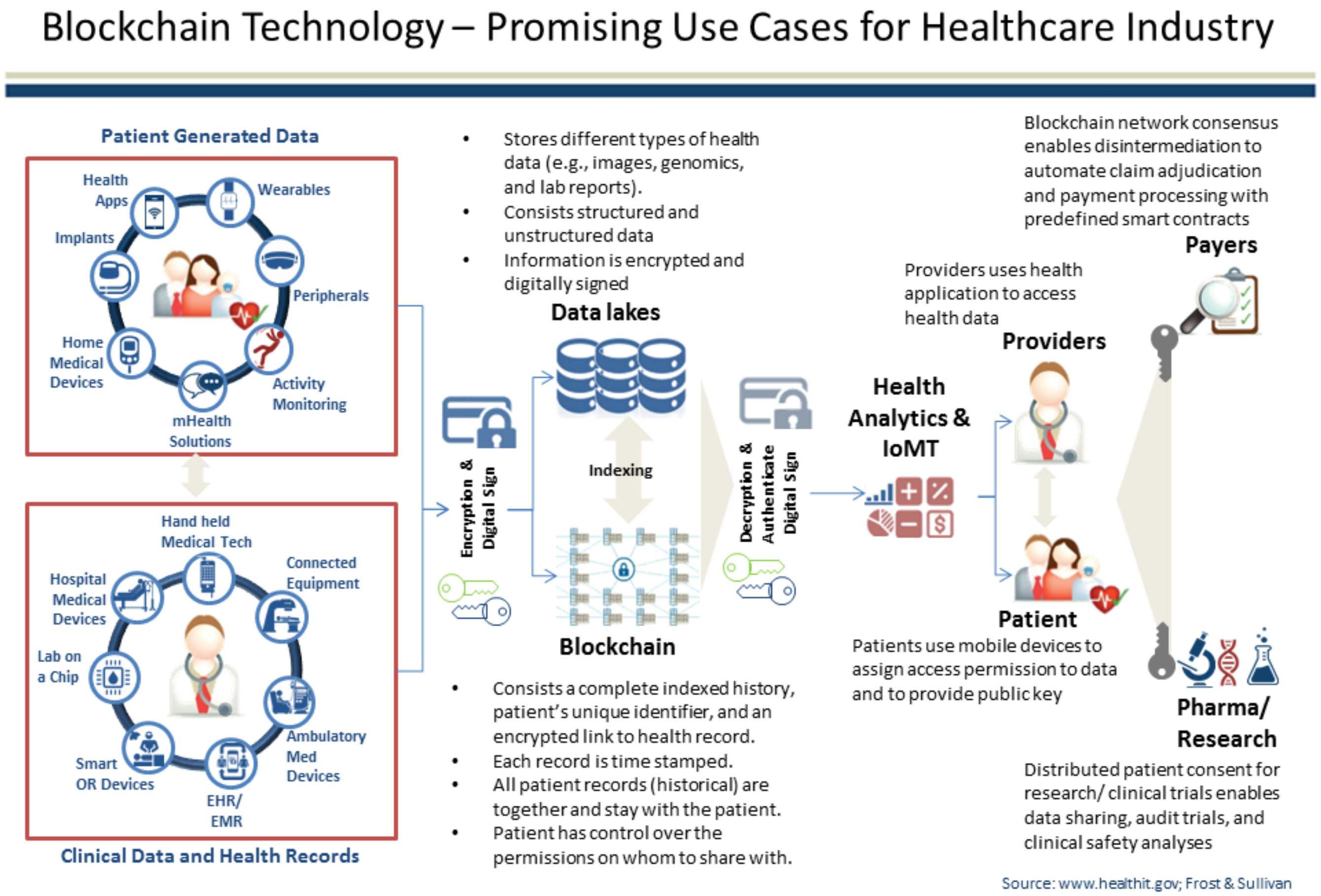
- Consortium includes Walmart, Kroger, Driscoll's, Doll, Golden State Food, McCormick and Co., McLane Co., Nestle, Tyson Foods, Unilever
- Explore and test blockchain technology as a solution for enhanced food safety across the business
- Provide benefits to customers with greater transparency and traceability in the supply chain

Blockchain in Energy Industry


Indigo Stakeholder Activity Taxonomy - Blockchain in Energy and Utilities
P2P Trading & Connected Home
POWER LEDGER
Vector
CO-TRICITY
LO3 ENERGY
alliander
Fortum
EV Charge / Share
oxygen INITIATIVE
Slock.it
ZF
innogy
Consortia and Research
ENERGY WEB FOUNDATION
WANXIANG BLOCKCHAIN LABS
endesa
Bitcoin Meter Payments
丸紅株式会社 Marubeni
enercity positive energie
elegant
bitpay
BAS
PEY
bankymoon
Solar Cryptocurrencies
smappee
Notable Startups
Volt Markets
M-PAYG
GSy
Gem
CHRONICLED
Adpteve
FILAMENT
theSunExchange
Wholesale Trading & Smart Markets
QIWI КИВИ
NEW 4.0 Norddeutsche EnergieWende
BTL
yuso
PONTON WE ARE THE 2 IN B2B
PRIOGEN
WIEN ENERGIE
Indigo ADVISORY

Blockchain in Healthcare

Blockchain challenges for clinical health data exchange and interoperability, drug supply chain integrity and provenance


Blockchain Technology – Promising Use Cases for Healthcare Industry

- Stores different types of health data (e.g., images, genomics, and lab reports).
- Consists structured and unstructured data
- Information is encrypted and digitally signed

- Consists a complete indexed history, patient's unique identifier, and an encrypted link to health record.
- Each record is time stamped.
- All patient records (historical) are together and stay with the patient.
- Patient has control over the permissions on whom to share with.

Blockchain network consensus enables disintermediation to automate claim adjudication and payment processing with predefined smart contracts

Providers uses health application to access health data

Patients use mobile devices to assign access permission to data and to provide public key

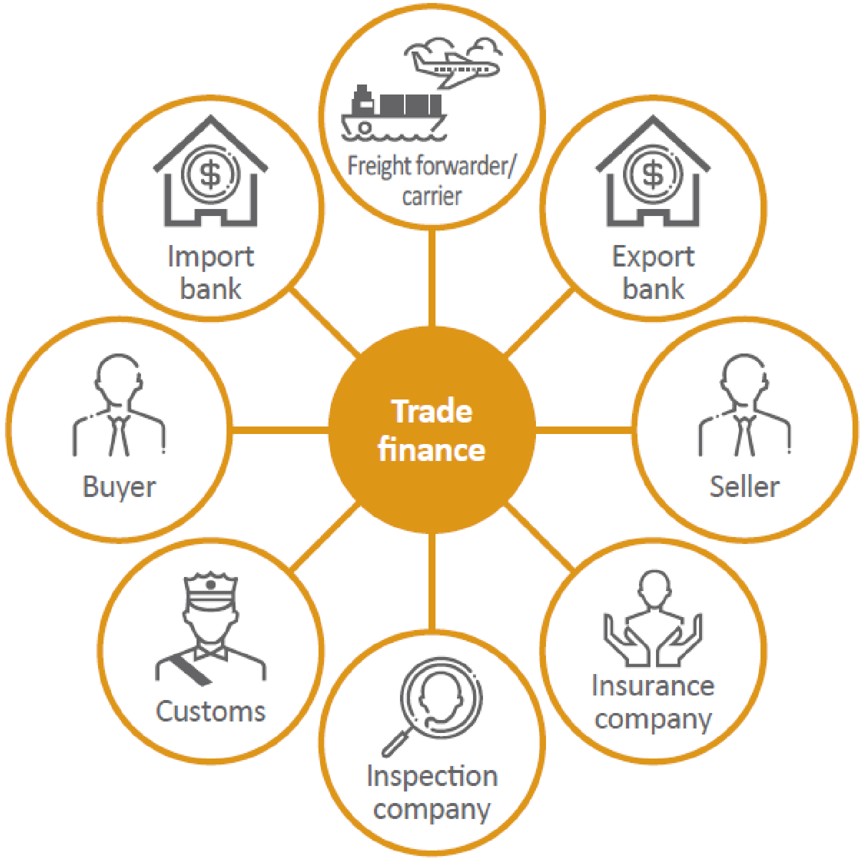
Distributed patient consent for research/ clinical trials enables data sharing, audit trials, and clinical safety analyses

Source: www.healthit.gov; Frost & Sullivan

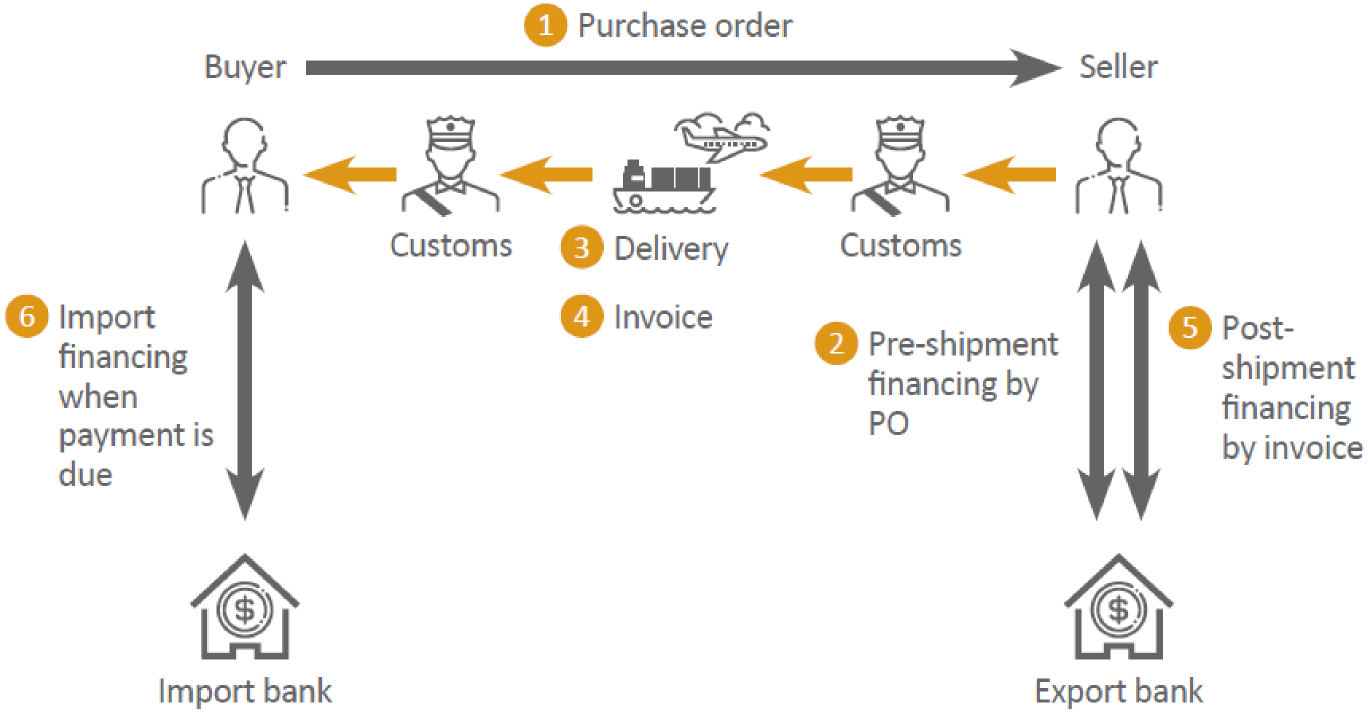
Patient Generated Data
Health Apps
Wearables
Implants
Peripherals
Home Medical Devices
Activity Monitoring
mHealth Solutions
Hand held Medical Tech
Connected Equipment
Hospital Medical Devices
Lab on a Chip
Ambulatory Med Devices
Smart OR Devices
EHR/ EMR
Clinical Data and Health Records
Encryption & Digital Sign
Data lakes
Indexing
Blockchain
Decryption & Authenticate Digital Sign
Health Analytics & IoMT
Providers
Payers
Patient
Pharma/ Research

- Clinical data sharing improvement
- Public health improvement
- Better and secured research and clinical trials
- More precise medicine
- Administrative and financial information
- Patient and provider identity

Blockchain for Trade Finance


Freight forwarder/ carrier
Import bank
Export bank
Trade finance
Buyer
Seller
Customs
Inspection company
Insurance company

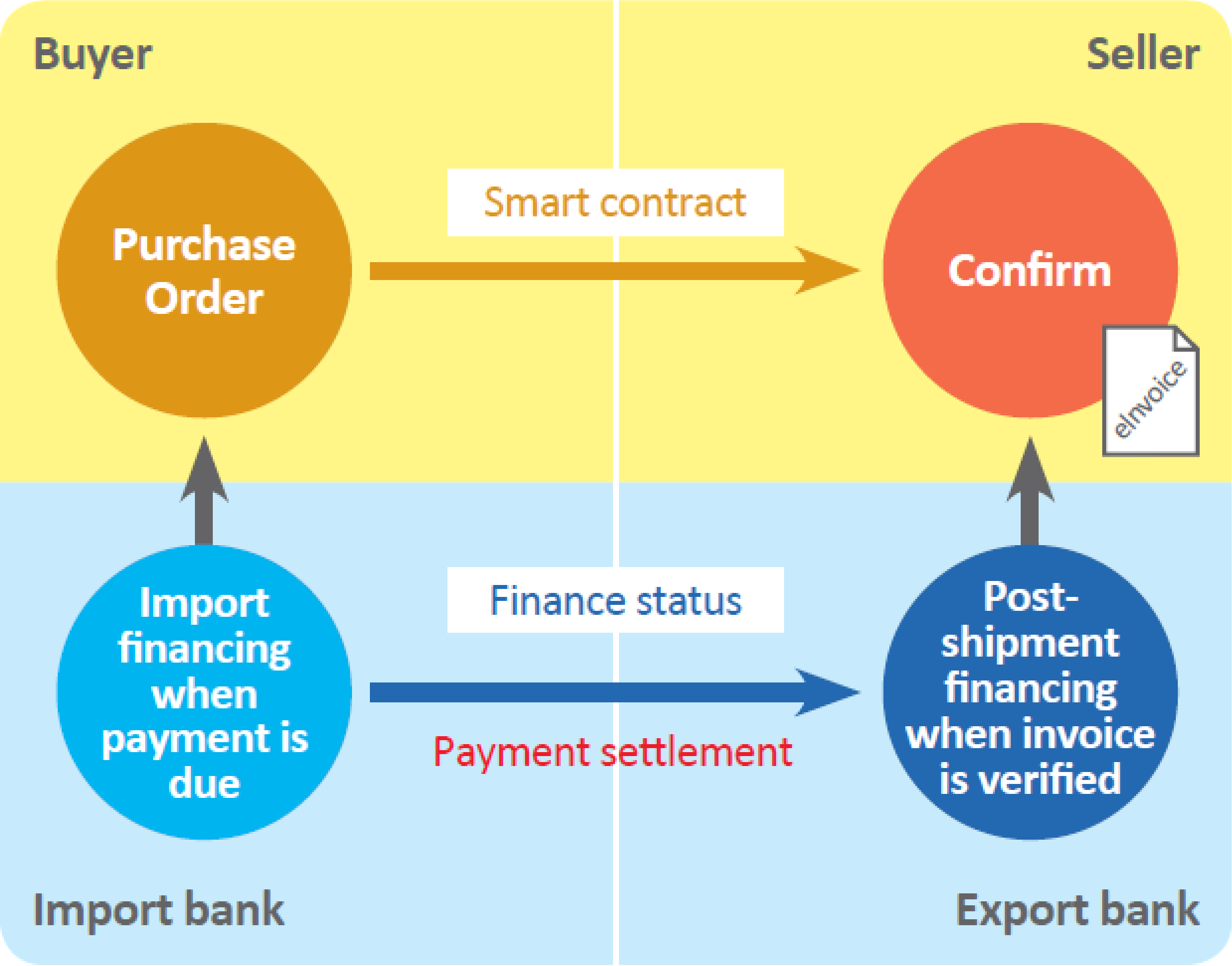
Key stakeholders in the trade finance ecosystem


① Purchase order
Buyer
Seller
Customs
③ Delivery
Customs
④ Invoice
⑥ Import financing when payment is due
② Pre-shipment financing by PO
⑤ Post-shipment financing by invoice
Import bank
Export bank

Current open account trading process

(Source : ASTRI Report)

Blockchain for Trade Finance


Buyer
Seller
Purchase Order
Smart contract
Confirm
eInvoice
Import financing when payment is due
Finance status
Payment settlement
Post-shipment financing when invoice is verified
Import bank
Export bank

An example of the workflow of a smart contract

Current process inefficiencies:

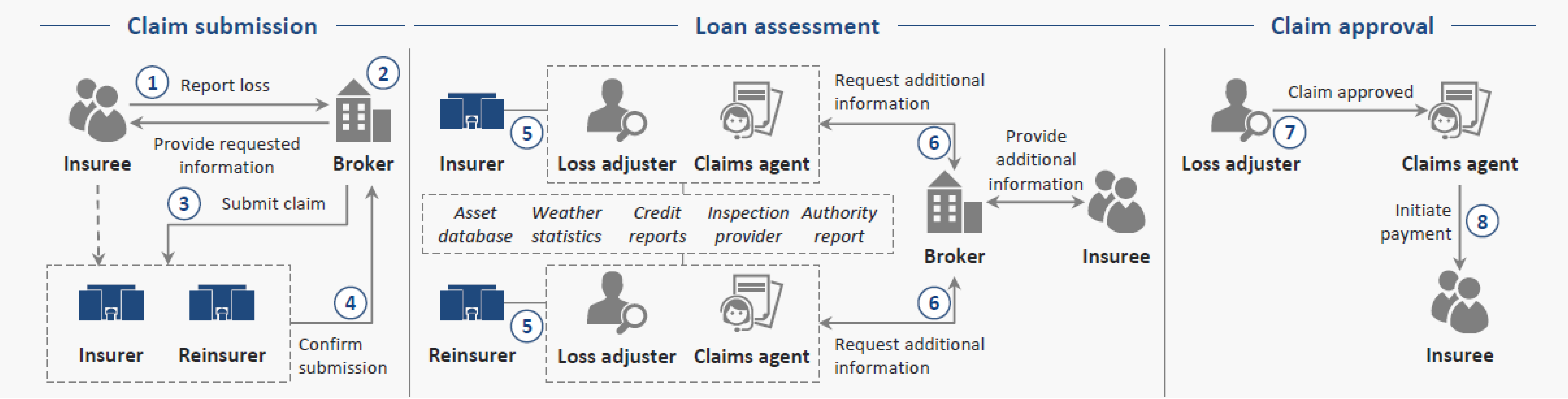
- No standardised structure of a PO
- No way to verify the latest version of a PO
- Low visibility of contract terms and amendments to banks
- High error rate due to manual mistakes
- Inefficient and costly due to:
  - Handling of paper-based documents
  - Difficulty in authentication by banks
- Risk of fraud

Improvements achieved by applying DLT:

- Digitised and standardised PO
- Deployment of smart contract automates trade execution
- Facilitate cross-border trade finance by collaboration with overseas DLT projects
- Financing to customer is faster and enable stage financing along the supply chain
- Lower risk of financing and avoid double financing

(Source : ASTRI Report)

Blockchain for P&C Claim Processing

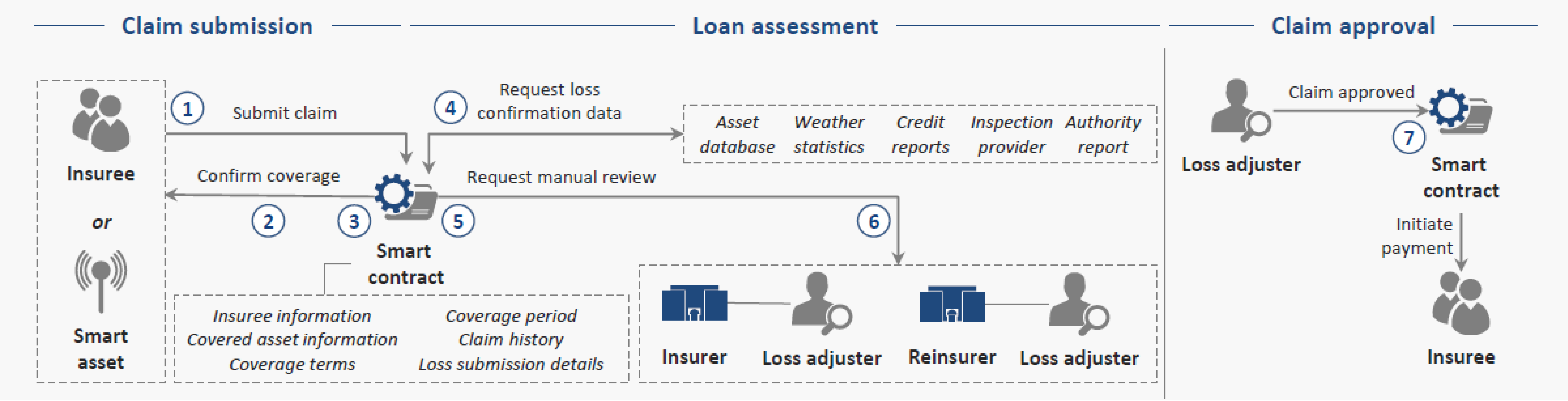

Claim submission
Loan assessment
Claim approval
① Report loss
②
Insuree
Provide requested information
Broker
③ Submit claim
Insurer
Reinsurer
④ Confirm submission
Insurer
⑤
Loss adjuster
Claims agent
Request additional information
⑥
Provide additional information
Asset database
Weather statistics
Credit reports
Inspection provider
Authority report
Broker
Insuree
Reinsurer
⑤
Loss adjuster
Claims agent
⑥
Request additional information
Claim approved
Loss adjuster
⑦
Claims agent
Initiate payment
⑧
Insuree

Current-state process description

- Complicated claim submission
- Cost for intermediaries
- Manual claim processing
- High potential for fraud and errors

(Source : World Economic Forum)

Blockchain for P&C Claim Processing


Claim submission
Loan assessment
Claim approval
Insuree
or
Smart asset
① Submit claim
② Confirm coverage
③
④ Request loss confirmation data
⑤ Request manual review
⑥
Smart contract
Insuree information
Covered asset information
Coverage terms
Coverage period
Claim history
Loss submission details
Asset database
Weather statistics
Credit reports
Inspection provider
Authority report
Insurer
Loss adjuster
Reinsurer
Loss adjuster
Loss adjuster
Claim approved
⑦
Smart contract
Initiate payment
Insuree

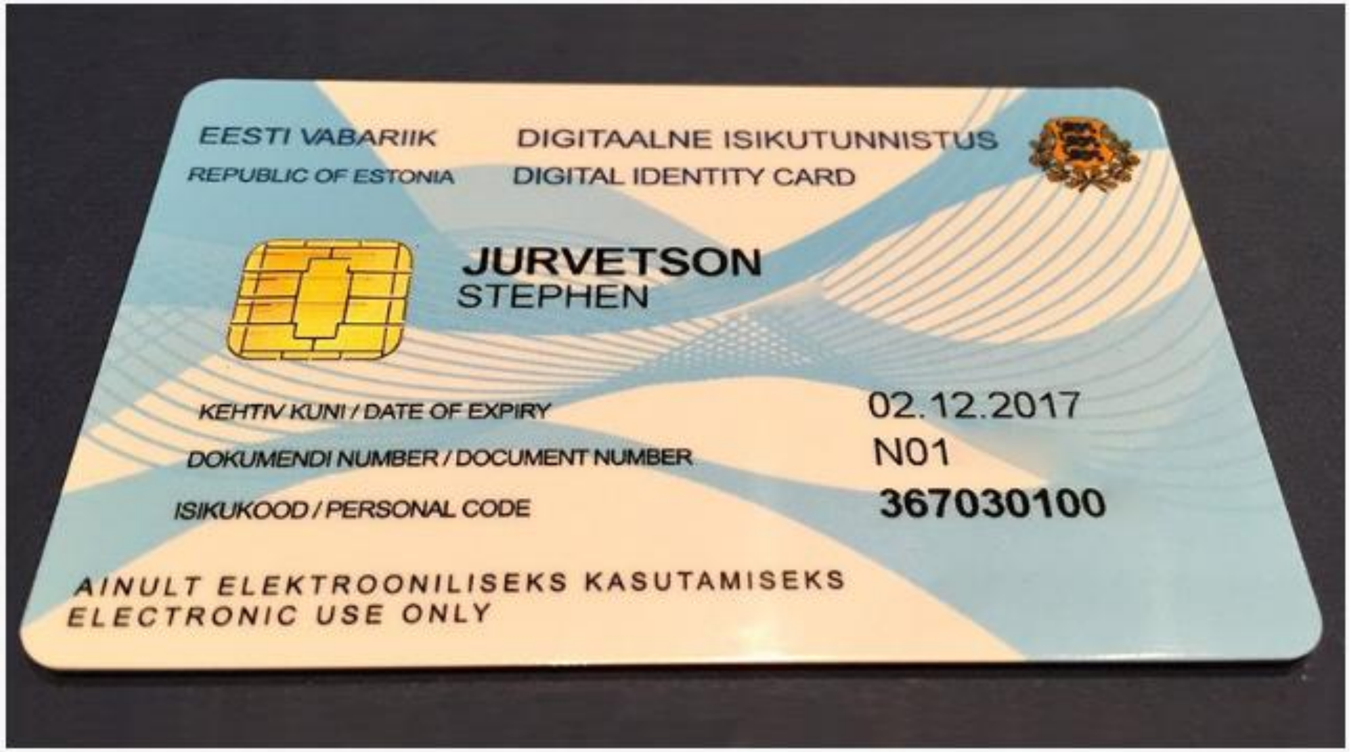
Future-state process description

- Simplified claim submission
- Streamlined transfer of information
- No intermediaries

- Automated claim processing
- Reduction in fraud and error
- Streamlined payment processing

(Source : World Economic Forum)

Blockchain for Identity



EESTI VABARIIK
REPUBLIC OF ESTONIA

DIGITAALNE ISIKUTUNNISTUS
DIGITAL IDENTITY CARD

JURVETSON
STEPHEN

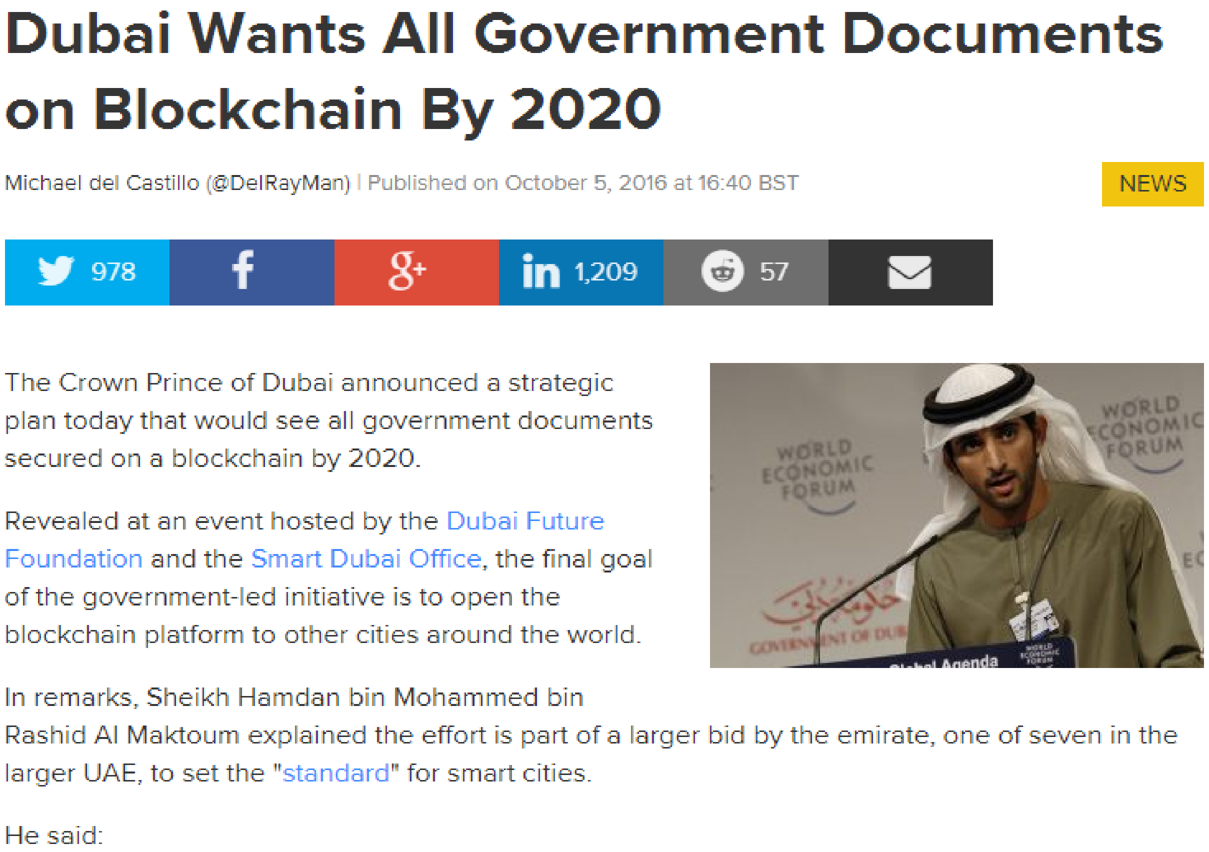
KEHTIV KUNI / DATE OF EXPIRY 02.12.2017
DOKUMENDI NUMBER / DOCUMENT NUMBER N01
ISIKUKOOD / PERSONAL CODE 367030100

AINULT ELEKTROONILISEKS KASUTAMISEKS
ELECTRONIC USE ONLY

open
24/7
AUSTRALIA POST
Self Service

- ➢ In Estonia, Digital Identity Card in connection with Blockchain
- ➢ Australian Postal Office is developing Blockchain-based digital ID platform

Blockchain for Document Service



Dubai Wants All Government Documents on Blockchain By 2020

Michael del Castillo (@DelRayMan) | Published on October 5, 2016 at 16:40 BST

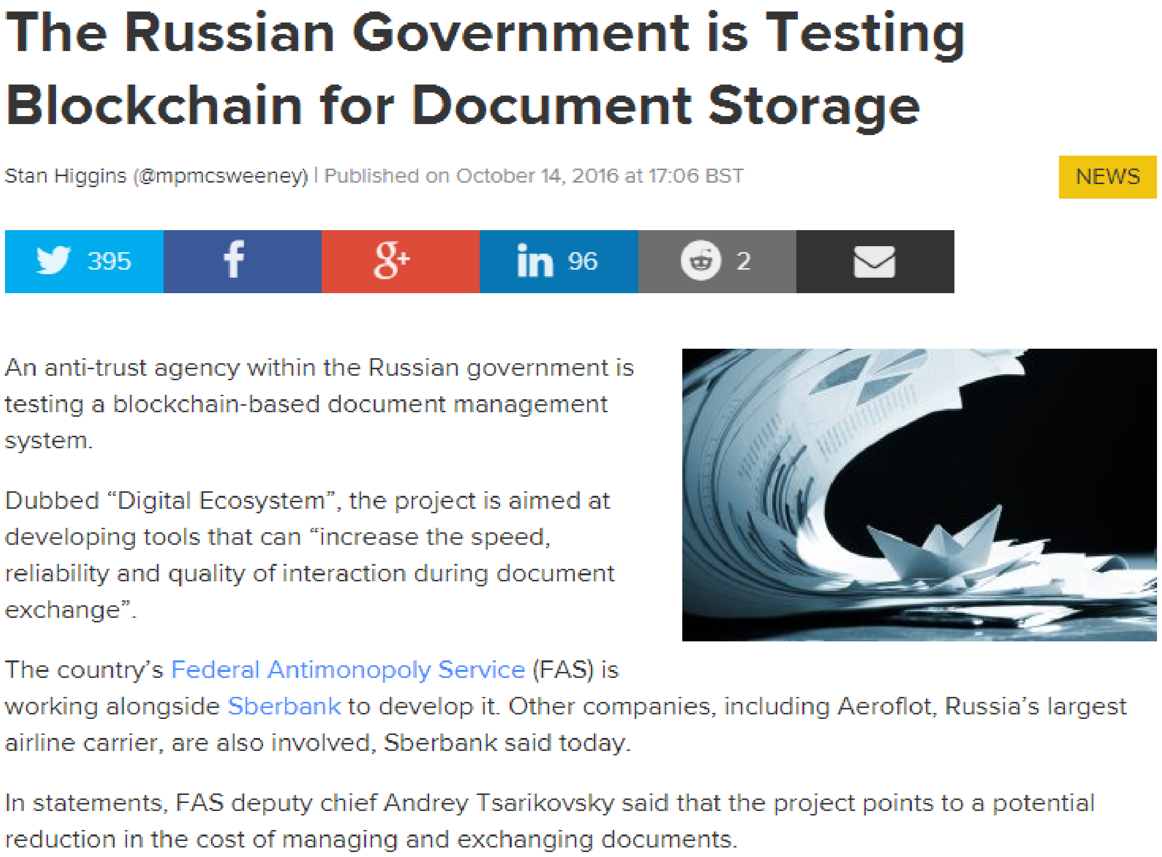
NEWS

The Crown Prince of Dubai announced a strategic plan today that would see all government documents secured on a blockchain by 2020.

Revealed at an event hosted by the Dubai Future Foundation and the Smart Dubai Office, the final goal of the government-led initiative is to open the blockchain platform to other cities around the world.

In remarks, Sheikh Hamdan bin Mohammed bin Rashid Al Maktoum explained the effort is part of a larger bid by the emirate, one of seven in the larger UAE, to set the "standard" for smart cities.

He said:



The Russian Government is Testing Blockchain for Document Storage

Stan Higgins (@mpmcsweeney) | Published on October 14, 2016 at 17:06 BST

NEWS

An anti-trust agency within the Russian government is testing a blockchain-based document management system.

Dubbed "Digital Ecosystem", the project is aimed at developing tools that can "increase the speed, reliability and quality of interaction during document exchange".

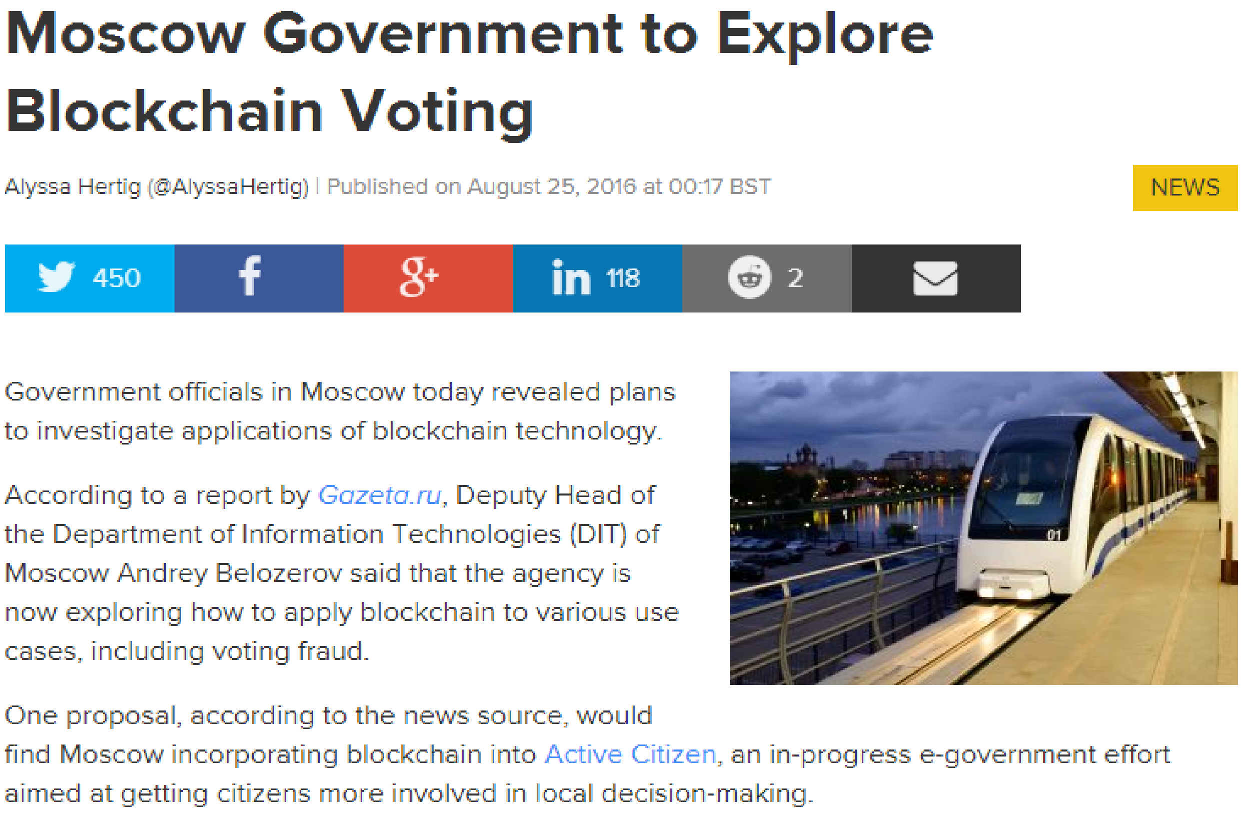
The country's Federal Antimonopoly Service (FAS) is working alongside Sberbank to develop it. Other companies, including Aeroflot, Russia's largest airline carrier, are also involved, Sberbank said today.

In statements, FAS deputy chief Andrey Tsarikovsky said that the project points to a potential reduction in the cost of managing and exchanging documents.

- Dubai government announced to register all public documents on the Blockchain until 2020

- Russian government in the process of testing feasibility of Blockchain as a public document depository

Blockchain for Voting



Moscow Government to Explore Blockchain Voting

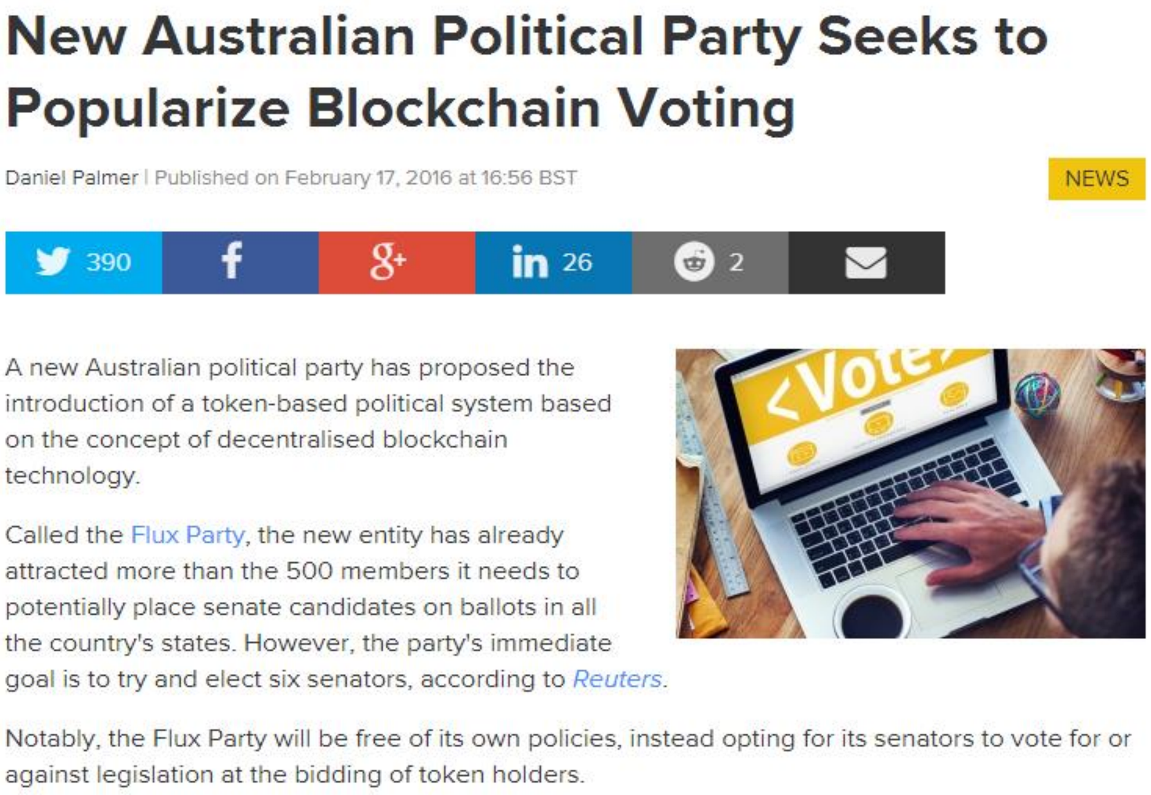
Alyssa Hertig (@AlyssaHertig) | Published on August 25, 2016 at 00:17 BST

NEWS

Government officials in Moscow today revealed plans to investigate applications of blockchain technology.

According to a report by *Gazeta.ru*, Deputy Head of the Department of Information Technologies (DIT) of Moscow Andrey Belozerov said that the agency is now exploring how to apply blockchain to various use cases, including voting fraud.

One proposal, according to the news source, would find Moscow incorporating blockchain into Active Citizen, an in-progress e-government effort aimed at getting citizens more involved in local decision-making.



New Australian Political Party Seeks to Popularize Blockchain Voting

Daniel Palmer | Published on February 17, 2016 at 16:56 BST

NEWS

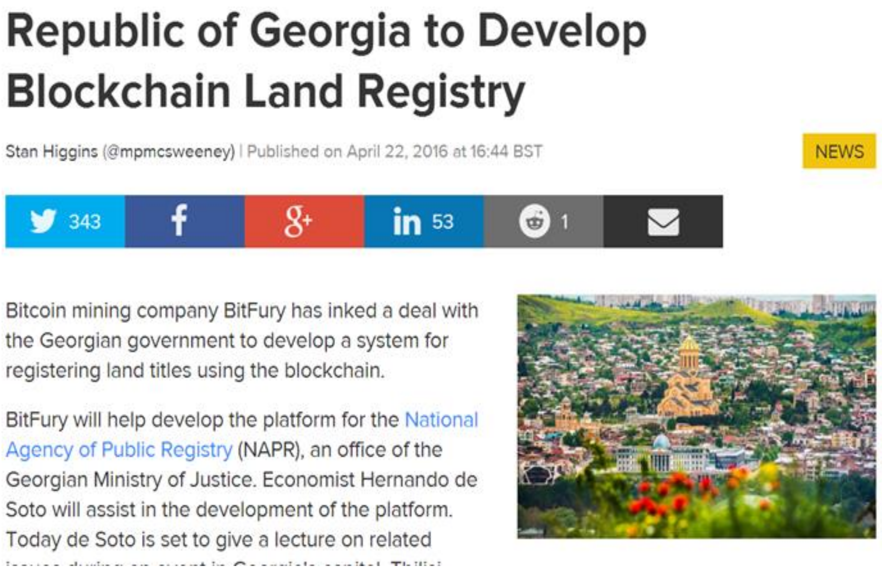
A new Australian political party has proposed the introduction of a token-based political system based on the concept of decentralised blockchain technology.

Called the Flux Party, the new entity has already attracted more than the 500 members it needs to potentially place senate candidates on ballots in all the country's states. However, the party's immediate goal is to try and elect six senators, according to *Reuters*.

Notably, the Flux Party will be free of its own policies, instead opting for its senators to vote for or against legislation at the bidding of token holders.

- Russian government is developing Blockchain-based E-Voting system
- Australian political party proposed Blockchain-based E-Voting system

Blockchain for Land Management



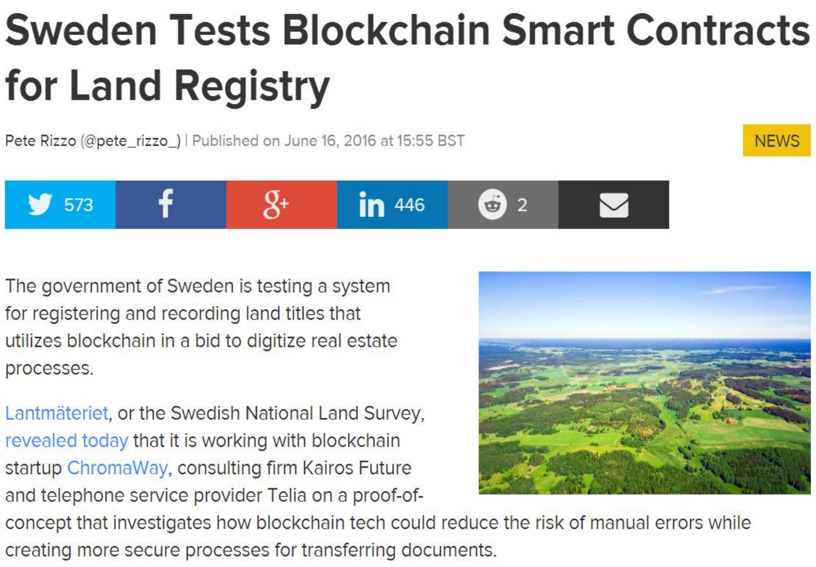
Republic of Georgia to Develop Blockchain Land Registry

Stan Higgins (@mpmcsweeney) | Published on April 22, 2016 at 16:44 BST

NEWS

Bitcoin mining company BitFury has inked a deal with the Georgian government to develop a system for registering land titles using the blockchain.

BitFury will help develop the platform for the National Agency of Public Registry (NAPR), an office of the Georgian Ministry of Justice. Economist Hernando de Soto will assist in the development of the platform. Today de Soto is set to give a lecture on related



Sweden Tests Blockchain Smart Contracts for Land Registry

Pete Rizzo (@pete_rizzo_) | Published on June 16, 2016 at 15:55 BST

NEWS

The government of Sweden is testing a system for registering and recording land titles that utilizes blockchain in a bid to digitize real estate processes.

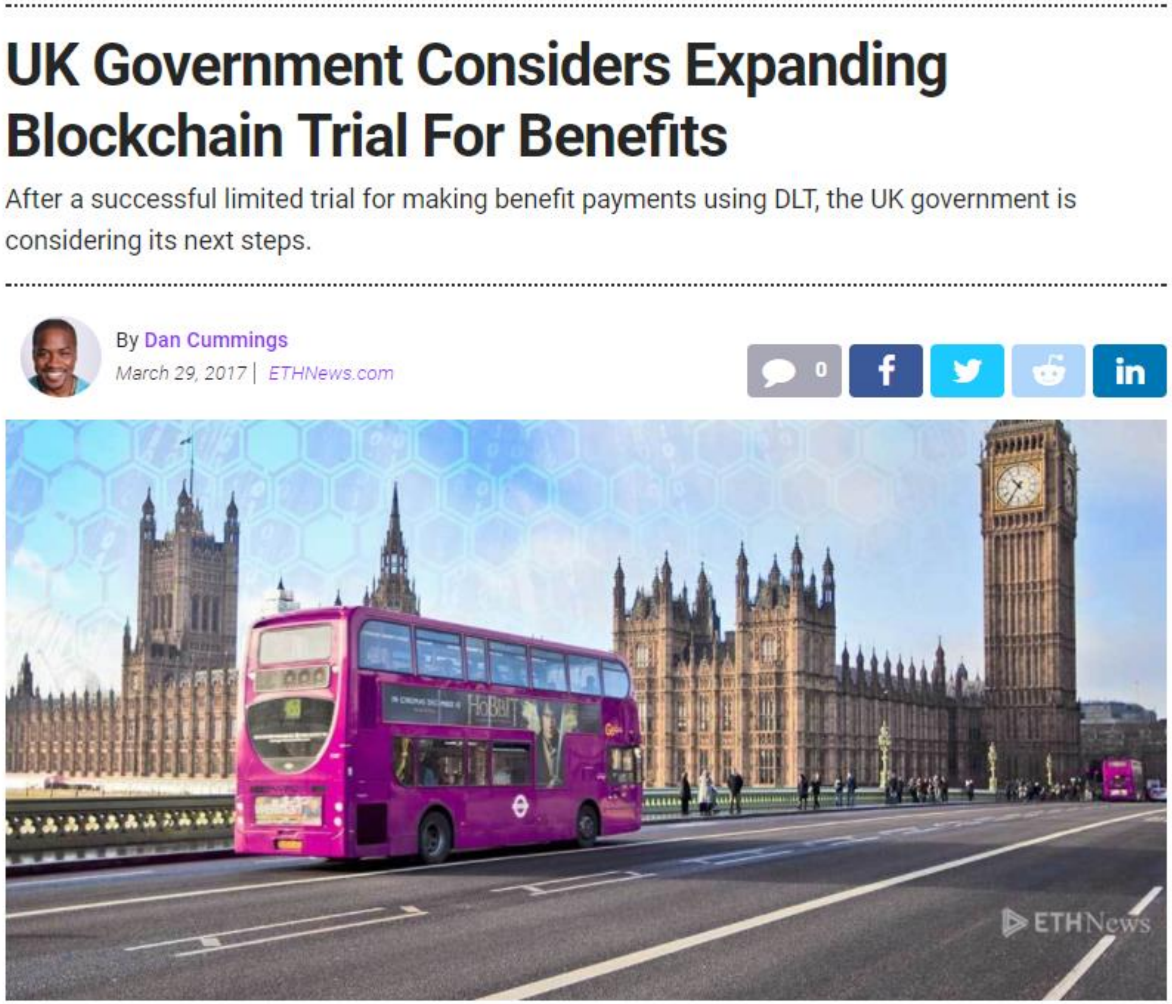
Lantmäteriet, or the Swedish National Land Survey, revealed today that it is working with blockchain startup ChromaWay, consulting firm Kairos Future and telephone service provider Telia on a proof-of-concept that investigates how blockchain tech could reduce the risk of manual errors while creating more secure processes for transferring documents.

Honduras to build land title registry using bitcoin technology

bitcoin
ACCEPTED HERE

- Georgia government is developing Blockchain-based platform to register land ownership and verify the transition of ownership
- Sweden completed the test for Smart Contract-based Land registration and transition record
- Honduras is developing Blockchain-based land registration system to prevent land registry fraud

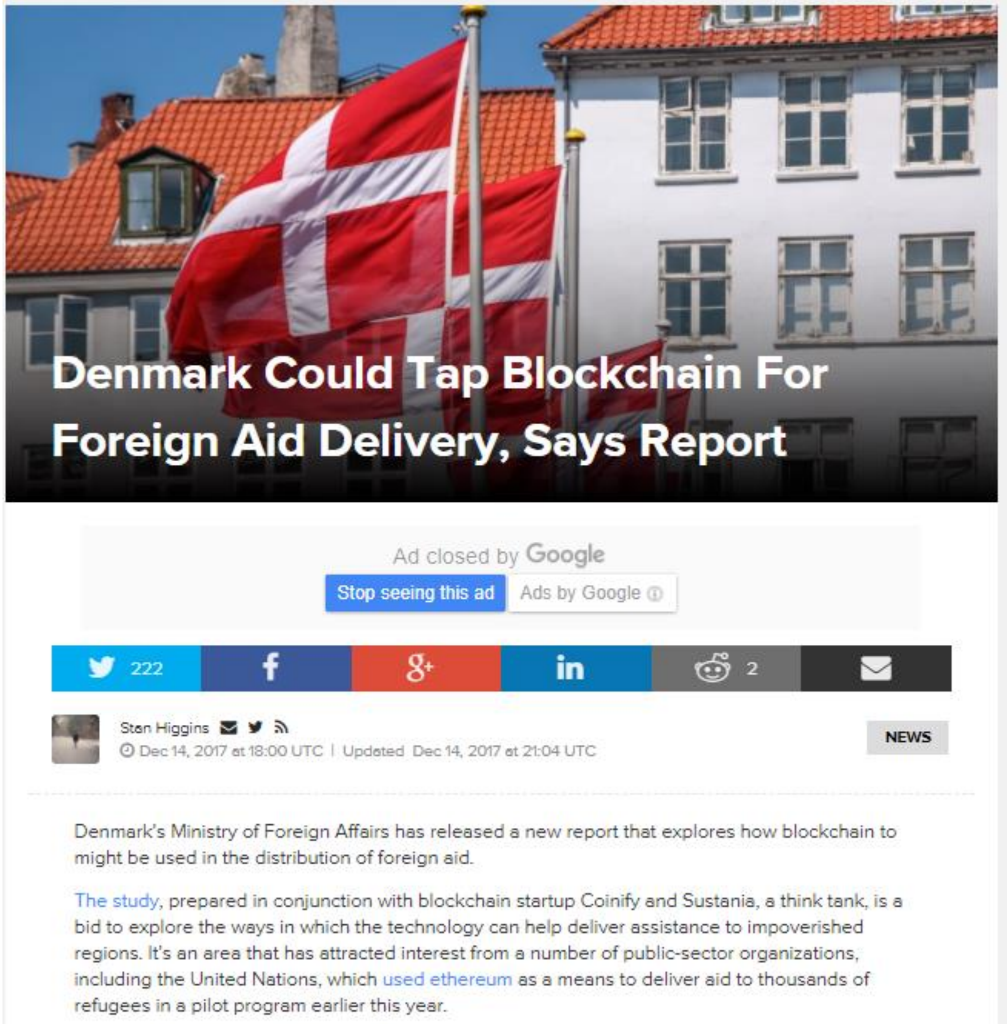
Blockchain for Financial Aid



UK Government Considers Expanding Blockchain Trial For Benefits

After a successful limited trial for making benefit payments using DLT, the UK government is considering its next steps.

By **Dan Cummings**
March 29, 2017 | ETHNews.com



Denmark Could Tap Blockchain For Foreign Aid Delivery, Says Report

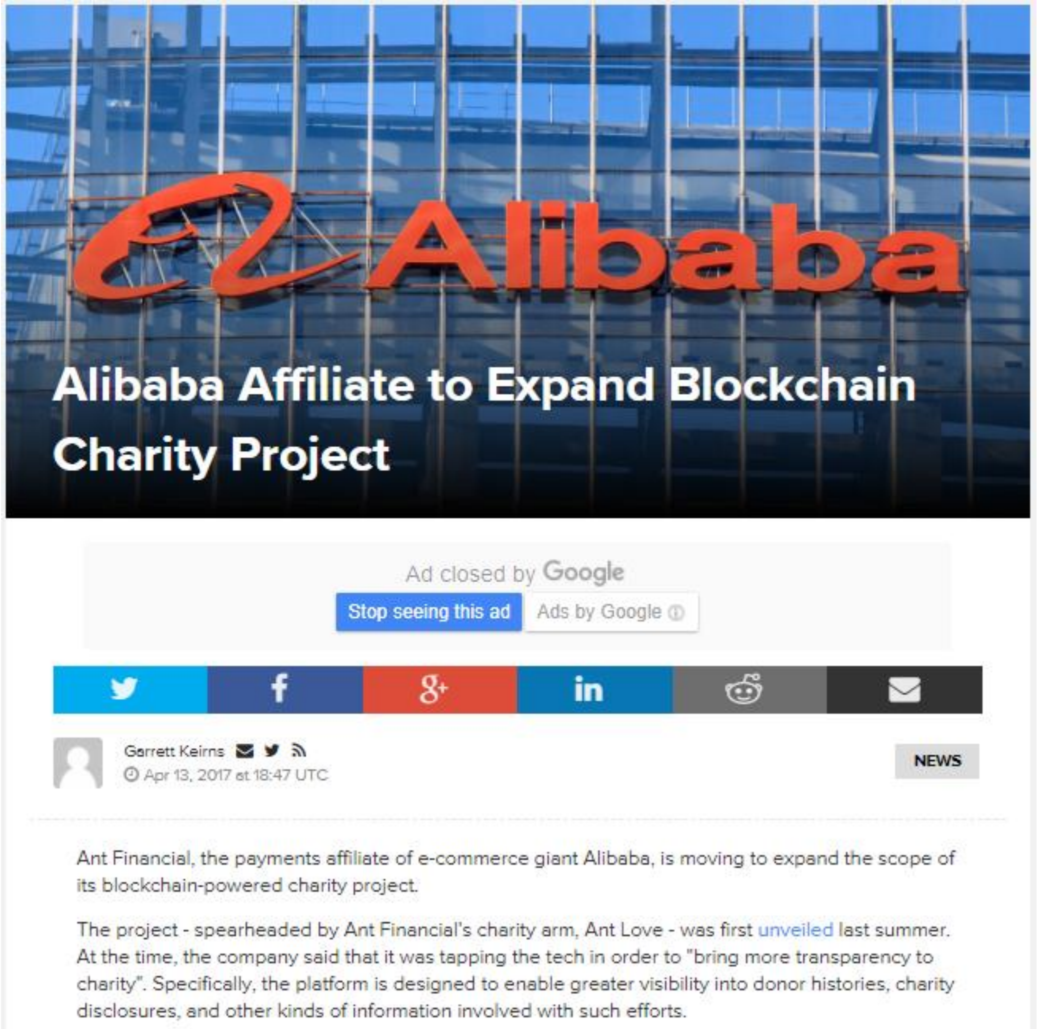
Stan Higgins
Dec 14, 2017 at 18:00 UTC | Updated Dec 14, 2017 at 21:04 UTC

Denmark's Ministry of Foreign Affairs has released a new report that explores how blockchain to might be used in the distribution of foreign aid.

The study, prepared in conjunction with blockchain startup Coinify and Sustania, a think tank, is a bid to explore the ways in which the technology can help deliver assistance to impoverished regions. It's an area that has attracted interest from a number of public-sector organizations, including the United Nations, which used ethereum as a means to deliver aid to thousands of refugees in a pilot program earlier this year.

- UK government is looking for the way to increase the transparency of pension payment using blockchain technology
- Denmart government in research of applying Blockchain to oversea aids program

Blockchain for Charity

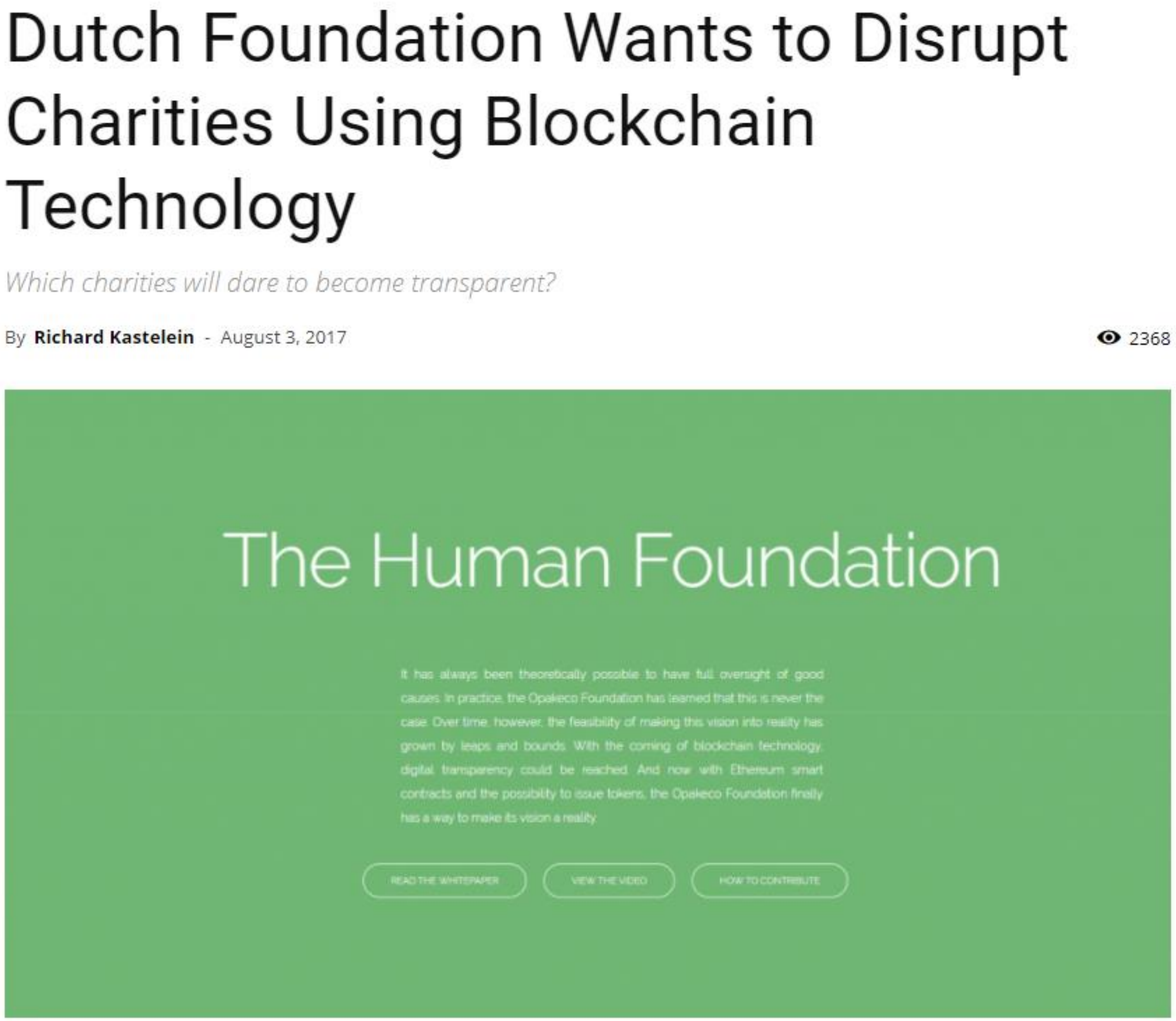


Alibaba Affiliate to Expand Blockchain Charity Project

Garrett Keirns
Apr 13, 2017 at 18:47 UTC

Ant Financial, the payments affiliate of e-commerce giant Alibaba, is moving to expand the scope of its blockchain-powered charity project.

The project - spearheaded by Ant Financial's charity arm, Ant Love - was first unveiled last summer. At the time, the company said that it was tapping the tech in order to "bring more transparency to charity". Specifically, the platform is designed to enable greater visibility into donor histories, charity disclosures, and other kinds of information involved with such efforts.



Dutch Foundation Wants to Disrupt Charities Using Blockchain Technology

Which charities will dare to become transparent?

By **Richard Kastelein** - August 3, 2017

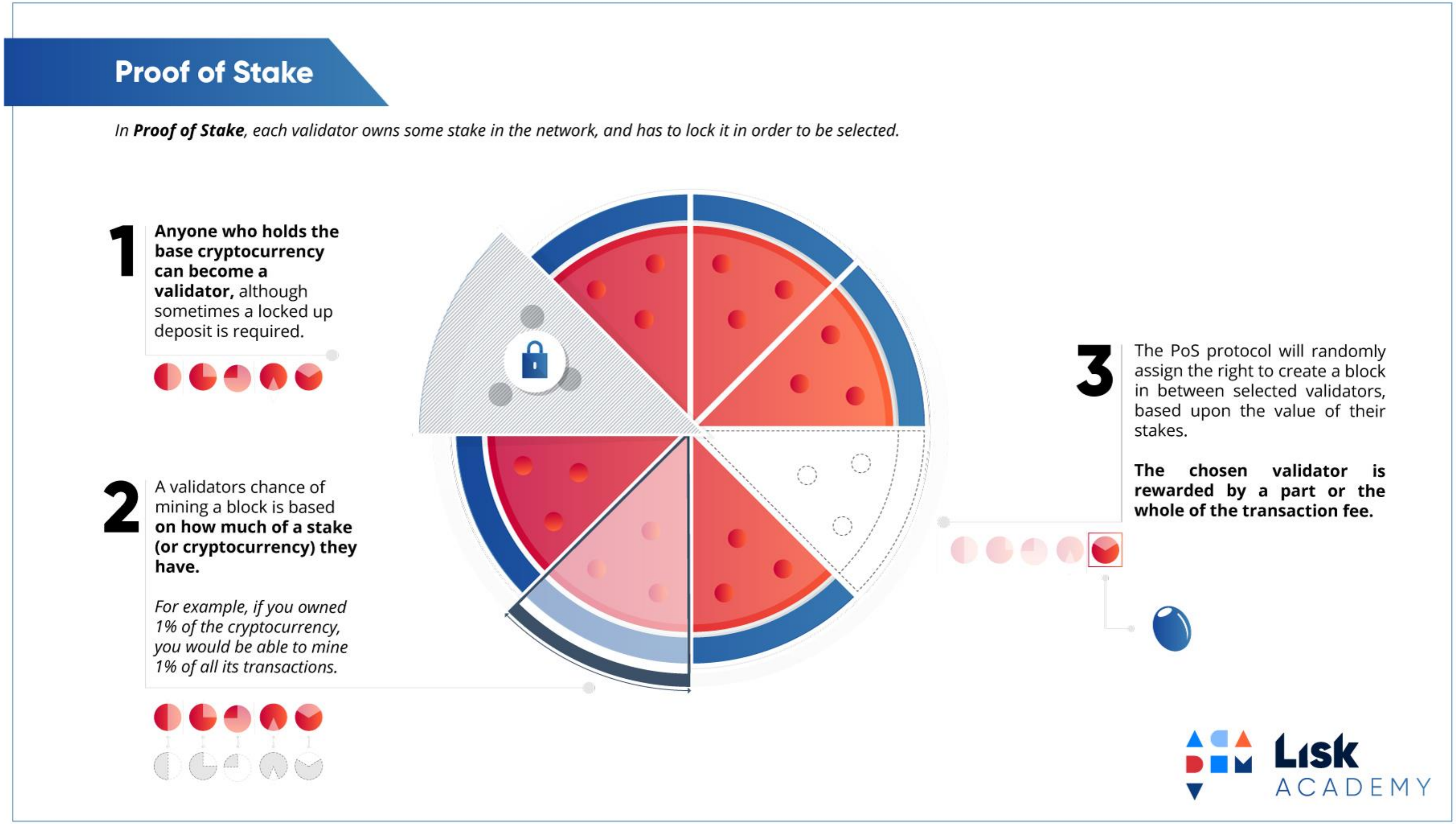
It has always been theoretically possible to have full oversight of good causes. In practice, the Opakeco Foundation has learned that this is never the case. Over time, however, the feasibility of making this vision into reality has grown by leaps and bounds. With the coming of blockchain technology, digital transparency could be reached. And now with Ethereum smart contracts and the possibility to issue tokens, the Opakeco Foundation finally has a way to make its vision a reality.

- ➢ Alibaba announced the project to develop Blockchain-based donation platform

- ➢ Dutch non-profit organization is developing Blockchain-based charity management platform

1. Essense of Blockchain: Infrastructure for Trust
2. Bitcoin, Ethereum
3. Private Blockchain
4. Blockchain Applications
5. **Next Generation Blockchain**

Proof of Stake(PoS)



Proof of Stake

*In **Proof of Stake**, each validator owns some stake in the network, and has to lock it in order to be selected.*

1 **Anyone who holds the base cryptocurrency can become a validator,** although sometimes a locked up deposit is required.

2 A validators chance of mining a block is based **on how much of a stake (or cryptocurrency) they have.**

For example, if you owned 1% of the cryptocurrency, you would be able to mine 1% of all its transactions.

3 The PoS protocol will randomly assign the right to create a block in between selected validators, based upon the value of their stakes.

The chosen validator is rewarded by a part or the whole of the transaction fee.

Delegated Proof of Stake(DPoS)

“PoS”

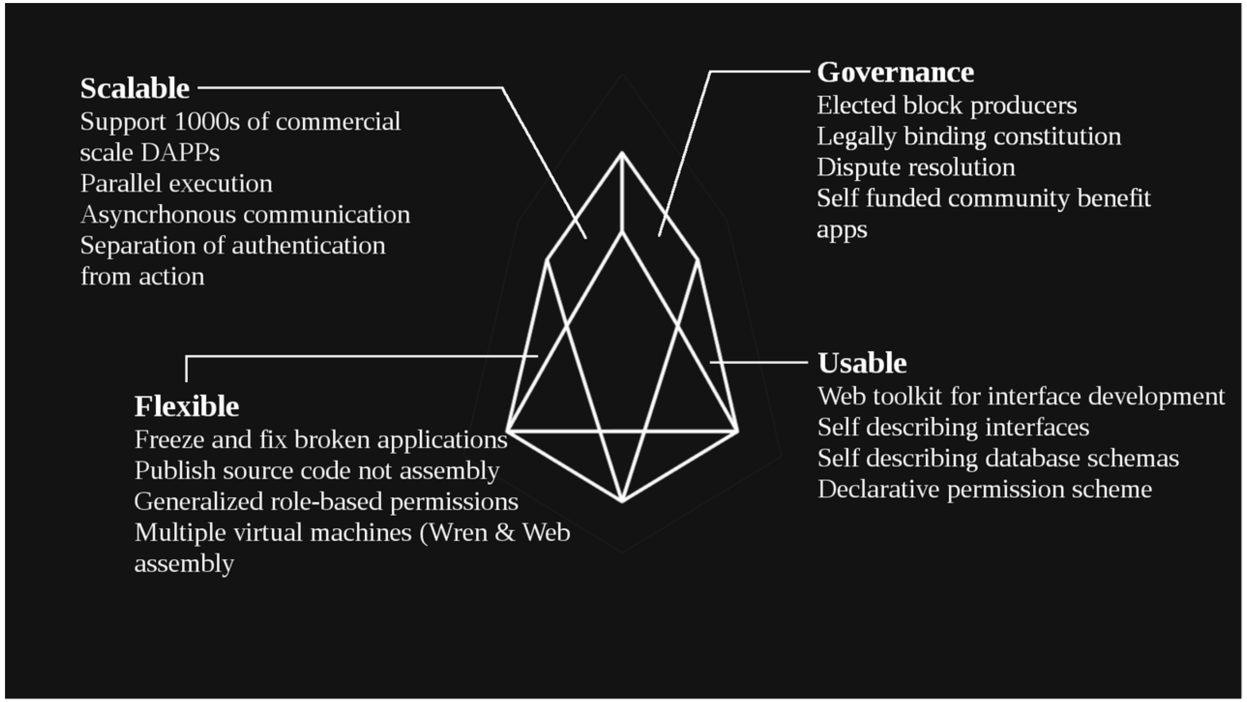
- Direct Democracy
- Voters: stakeholder with minimally required stake
- Voter’s duty: validate transactions, generate a block

“DPoS”

- Indirect Democracy
- Witness(Delegate): elected by stakeholder.
- Witness’s duty: validate transactions, generate a block

- Fast, efficient
- No need to purchase a tremendous amount of coin
- Higher participation rate – 99%
- Witness’s pledge
  - Return a portion of mining compensation(ARK, RISE)
  - Exempt transfer fee(EOS, Steem)

EOS vs. NEO



Scalable
Support 1000s of commercial scale DAPPs
Parallel execution
Asyncrhonous communication
Separation of authentication from action

Governance
Elected block producers
Legally binding constitution
Dispute resolution
Self funded community benefit apps

Flexible
Freeze and fix broken applications
Publish source code not assembly
Generalized role-based permissions
Multiple virtual machines (Wren & Web assembly

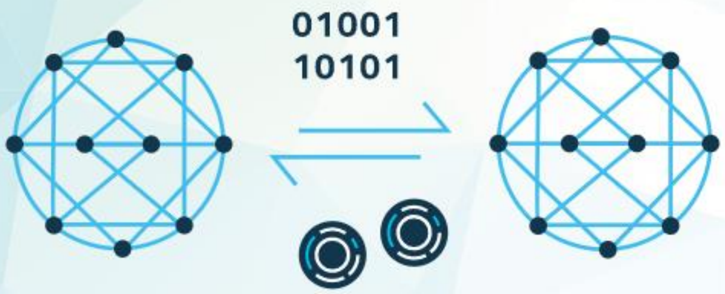
Usable
Web toolkit for interface development
Self describing interfaces
Self describing database schemas
Declarative permission scheme

NEO
smart economy

- Parallel computing
- Inter-app communication
- Consensus mechanism - DPoS
- Block time - 3 second
- Protocol update & constitution

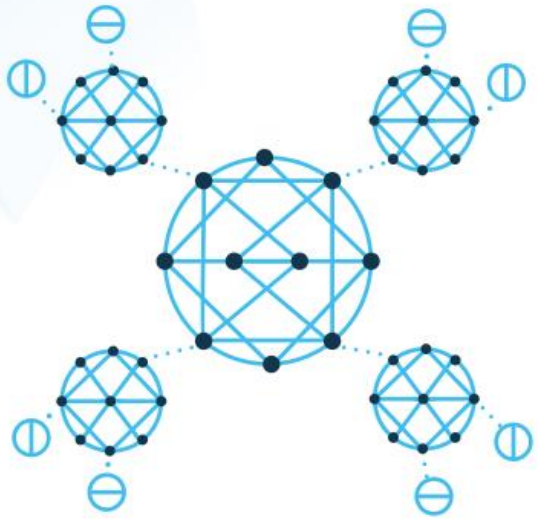
- Neo vs. Gas
- Neo Contract, NeoFS, NeoQS
- Consensus mechanism - DBFT
- Block time - 15 second
- Fast tps, immediate finality

Aion



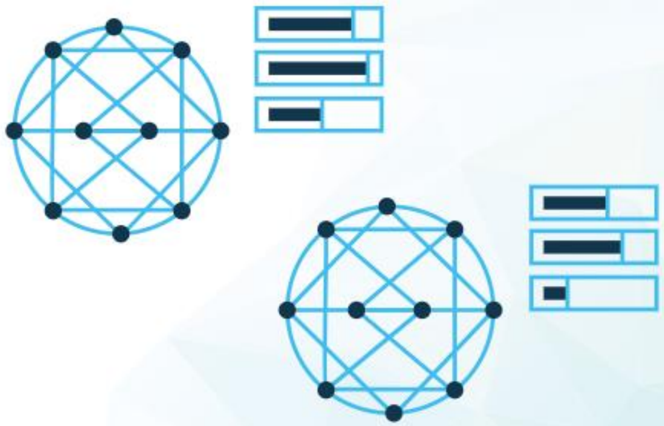
FEDERATE

Aion facilitates inter-blockchain communication via a high-performance bridging mechanism. Multiple bridges between pairs of chains allow both data and value to transfer between chains.



SCALE

Aion addresses the issues of scalability and performance by introducing a new high-performance virtual machine, and by enabling applications to operate across multiple chains.



SPOKE

Aion allows custom blockchain design, including different consensus algorithms and virtual machines, without sacrificing interoperability with other blockchains.

"Integrate dissimilar blockchain systems in a multi-tier hub-and-spoke model"

Thank You!