Blockchain

Trusted shared services and digital business solutions

Introduction to the <u>Basic</u> Concepts

ICC | international computing centre | ICT SOLUTIONS FOR THE UN FAMILY

7 May 2019

:About Us:

Trusted shared services and digital business solutions

Shashank Rai

ICC international computing centre ICT SOLUTIONS FOR THE UN FAMILY

The ICC Story

Pursuant to GA Resolution 2741 (XXV) of 17 Dec 1970, ICC was created as an UN inter-organization facility.

Setup to provide services for mainframe and data communications – using Cost-Recovery Model *(not-for-profit)*

We still run two mainframe systems!!

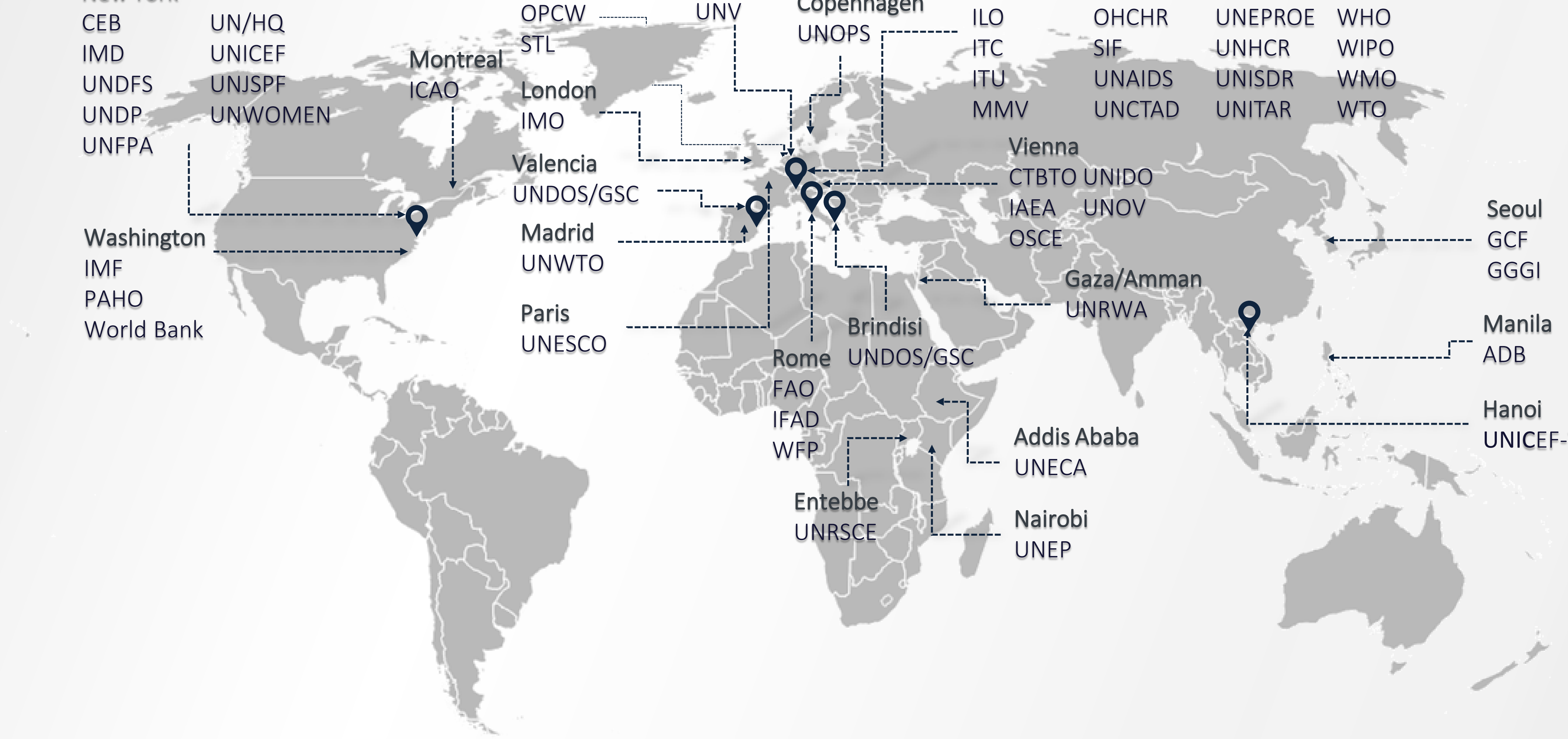
Over 50 Clients and nearly 40 service offerings across strategic consulting, emerging technologies, solution development, information security, on premise UN cloud as well as various *aaS cloud solutions.

Emerging Technology:
- Blockchain
- Machine Learning
- RPA
- Cloud Native Applications

Team of circa 420 UN Staff and consultants – almost entirely with ICT skill-set

Data Centres in Geneva (x2), Switzerland; New Jersey, USA; and Valencia, Spain – all within UN jurisdiction *(covered by P&I)*

ICC's Client Organizations



New York
CEB
IMD
UNDFS
UNDP
UNFPA
UN/HQ
UNICEF
UNJSPF
UNWOMEN

Washington
IMF
PAHO
World Bank

Montreal
ICAO

The Hague
ICJ
OPCW
STL

London
IMO

Valencia
UNDOS/GSC

Madrid
UNWTO

Paris
UNESCO

Bonn
UNFCCC
UNV

Copenhagen
UNOPS

Geneva
CITES
ILO
ITC
ITU
MMV
OCHA
OHCHR
SIF
UNAIDS
UNCTAD
UNECE
UNEPROE
UNHCR
UNISDR
UNITAR
UNOG
WHO
WIPO
WMO
WTO

Vienna
CTBTO
IAEA
OSCE
UNIDO
UNOV

Gaza/Amman
UNRWA

Brindisi
UNDOS/GSC

Rome
FAO
IFAD
WFP

Entebbe
UNRSCE

Addis Ababa
UNECA

Nairobi
UNEP

Seoul
GCF
GGGI

Manila
ADB

Hanoi
UNICEF-VN

ICC offices

ICC international computing centre | ICT SOLUTIONS FOR THE UN FAMILY

Today's Talk

The map…

Functional Context

petite Lexicon

Add it up

Dive into Blockchain…

Trusted shared services and digital business solutions

…Or is it Distributed Ledger?

ICC | international computing centre | ICT SOLUTIONS FOR THE UN FAMILY

Blockchain / Distributed Ledger

you like tomato, and I like tomahto

The Jury is out -

- Blockchain (truly public owned) Vs Distributed Ledger (anything but completely open) OR
- Blockchain subset of Distributed Ledger

Focus on the characteristics of ‘prominent’ technologies

…while we are at it: Distributed Databases Vs Distributed Ledger – the lines are blurring (*hint* AWS QLDB) but ‘logical control / ownership’ is the key difference

It is very easy

Or so I’ve been told by a friend…

Not one of my references

Functional Context

Trusted shared services and digital business solutions

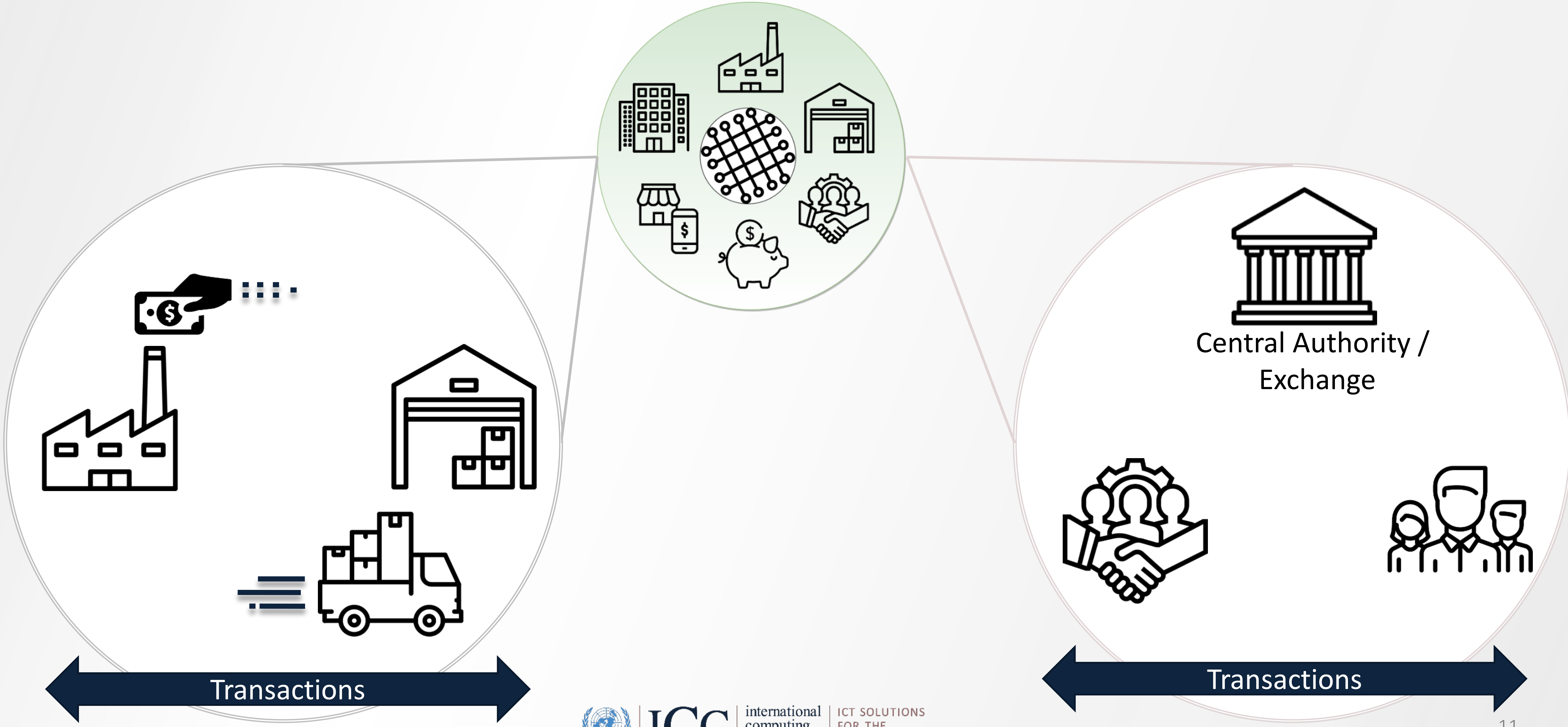
ICC international computing centre ICT SOLUTIONS FOR THE UN FAMILY

A Simple view

Of the everyday business…

- Entities carry out transactions – Buy / Sell
  - Goods and Services
  - Financial instruments
- Maintain records in ledgers *(such as)*:
  - General Ledger
  - Inventory Ledger
  - Assets ownership

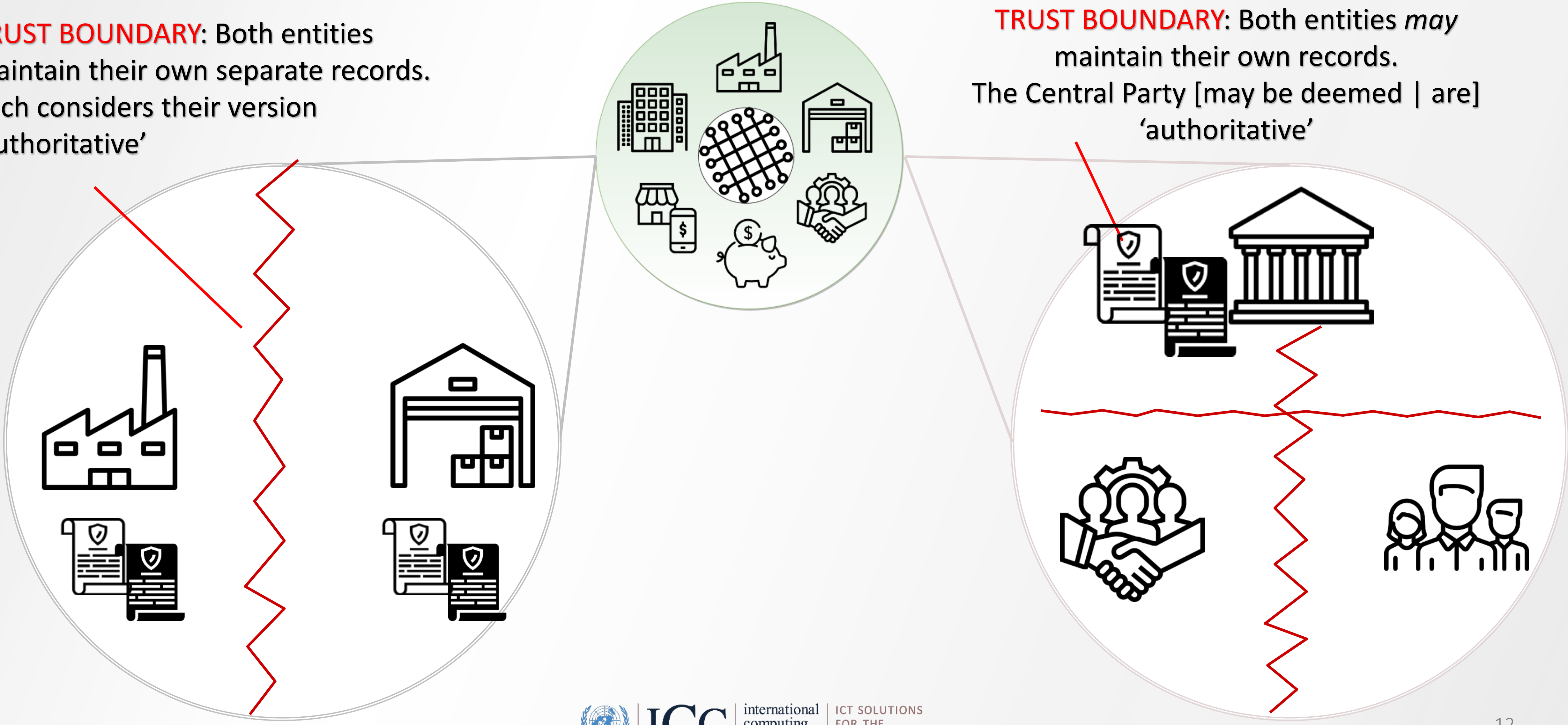
Transaction between Entities



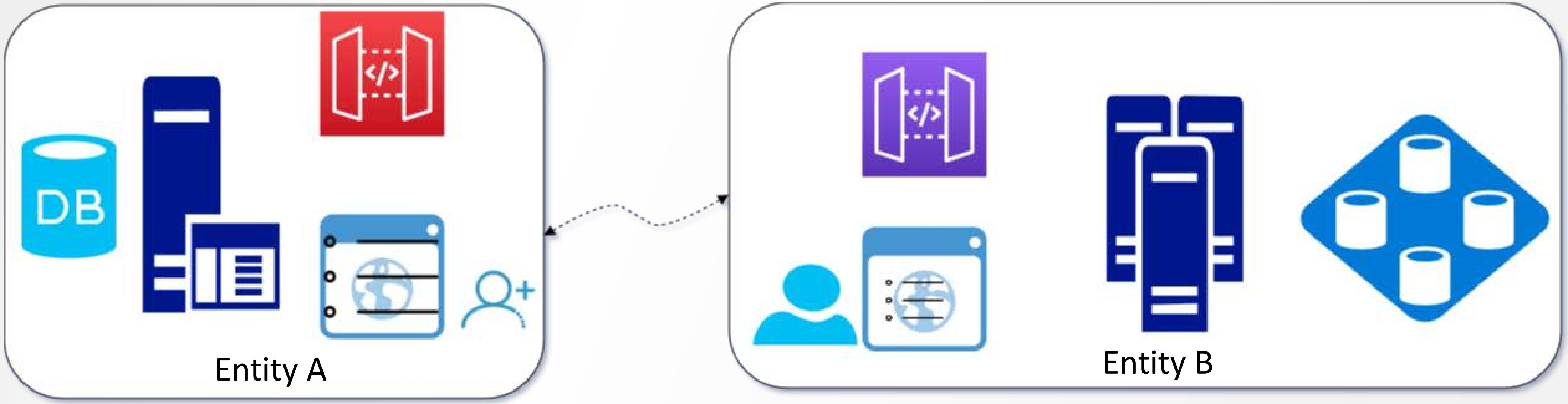
Records of Transactions: Ledgers

TRUST BOUNDARY: Both entities maintain their own separate records. Each considers their version 'authoritative'

TRUST BOUNDARY: Both entities *may* maintain their own records.
The Central Party [may be deemed | are] 'authoritative'



Records of Transactions: Technical Schematic



- API / UI based access to applications for maintaining records.
- The data is stored in databases – which can be geographically distributed
  - Nature of application determines ‘type’ of database
- In case of ‘geographically distributed servers’ **within an entity**
  - Multiple nodes (servers) coordinate to keep a consistent view of records
  - Nodes trust each other
  - Logical central control

What if, we can have a single ‘ledger’ across the two entities? – One source of ‘truth’!

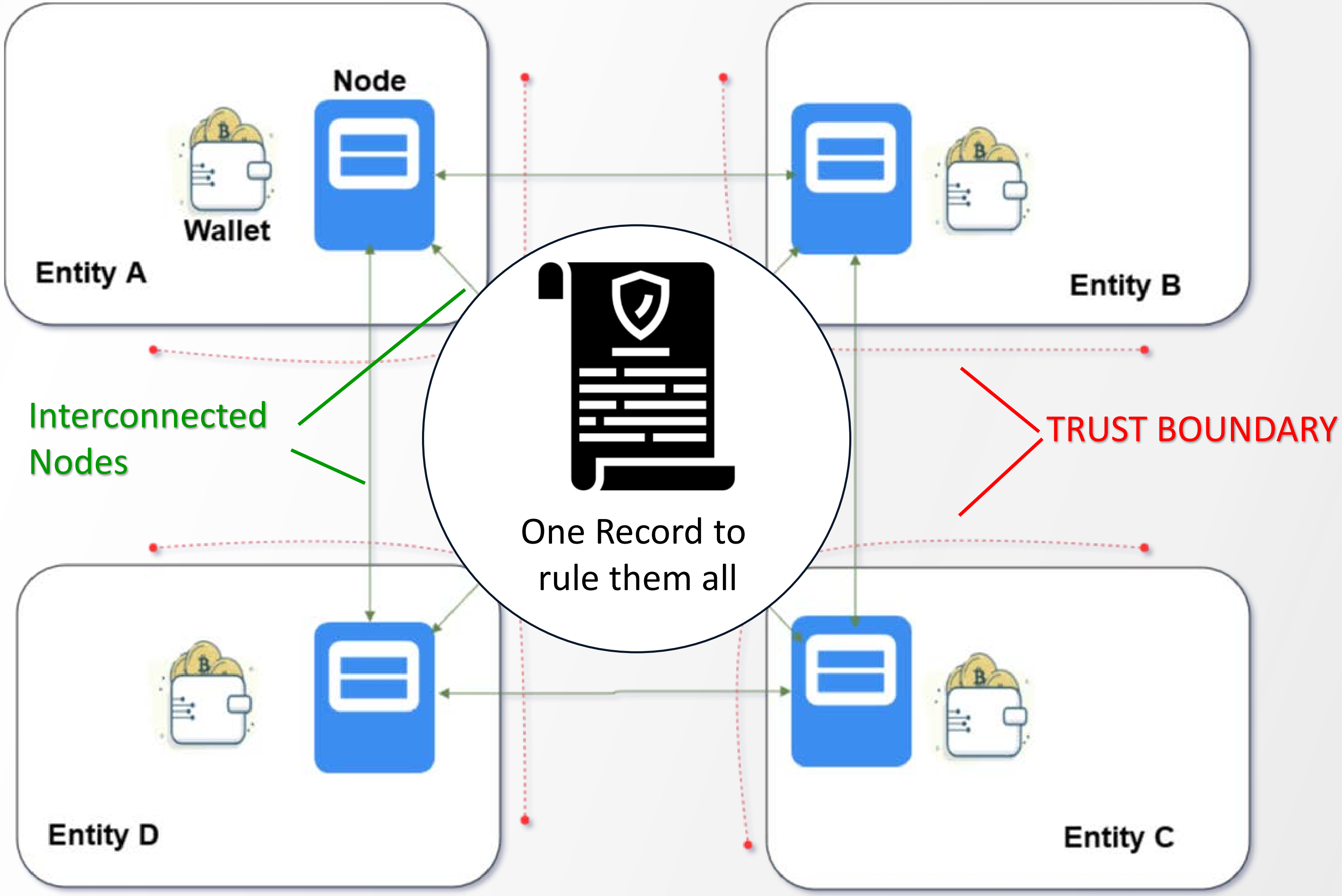
Distributed Ledger for Records

Business Transactions:
Take place ‘as usual’

Entities have a common/same view of records; through:

- Consensus on *transactions*
- Peer-to-peer network for data exchange
- Agreement on who can participate in this P2P network (and their roles)
- Ensure records can’t be tampered

Side effect: All nodes store all data



One Record to rule them all

DLT Terminology

Trusted shared services and digital business solutions

ICC international computing centre ICT SOLUTIONS FOR THE UN FAMILY

Keywords we picked up

Nodes:

- End-point (computing device) participating in the Distributed Ledger (DL) network.
- *Can have different roles depending on the DLT (Technology)*

P2P:

- Communication Protocols used to establish such a network *(think Bittorrent)*
- *Starts with a ‘genesis’ file -> genesis block*

Permissioned:

- Single Central OR a set of delegated members decide which node can participate in the DL *(and a few other nuances in between)*

Permissionless:

- Anyone and everyone can join

Another term: Wallet

Public Key Private Key

Mathematically related, large random numbers used in asymmetric cryptography

- Message encrypted with public key can be decrypted only by private key
- Message signed by private key- digital signature can be verified by using the public key

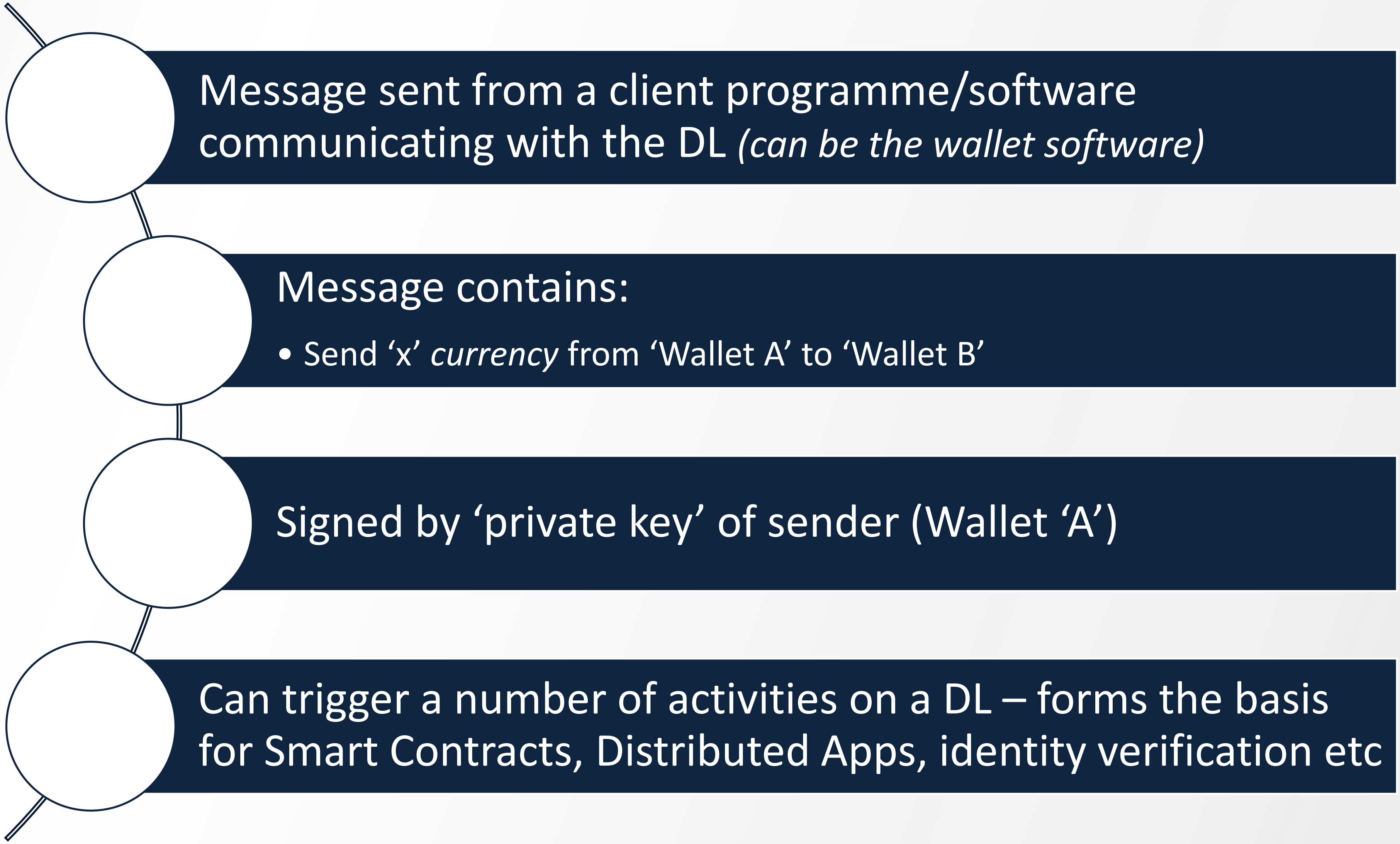
- A collection of multiple pairs of public and private keys
- Transaction Address: Created from a private key
- Use varies from one DLT to another

  e.g. in case of Hyperledger Indy, it store identities issued by an identity provider

CryptoCurrency & Transactions

CryptoCurrency

Units created by the underlying software code and ownership stored in a ledger



Message sent from a client programme/software communicating with the DL *(can be the wallet software)*

Message contains:

- Send ‘x’ *currency* from ‘Wallet A’ to ‘Wallet B’

Signed by ‘private key’ of sender (Wallet ‘A’)

Can trigger a number of activities on a DL – forms the basis for Smart Contracts, Distributed Apps, identity verification etc

Terms we picked up: Consensus

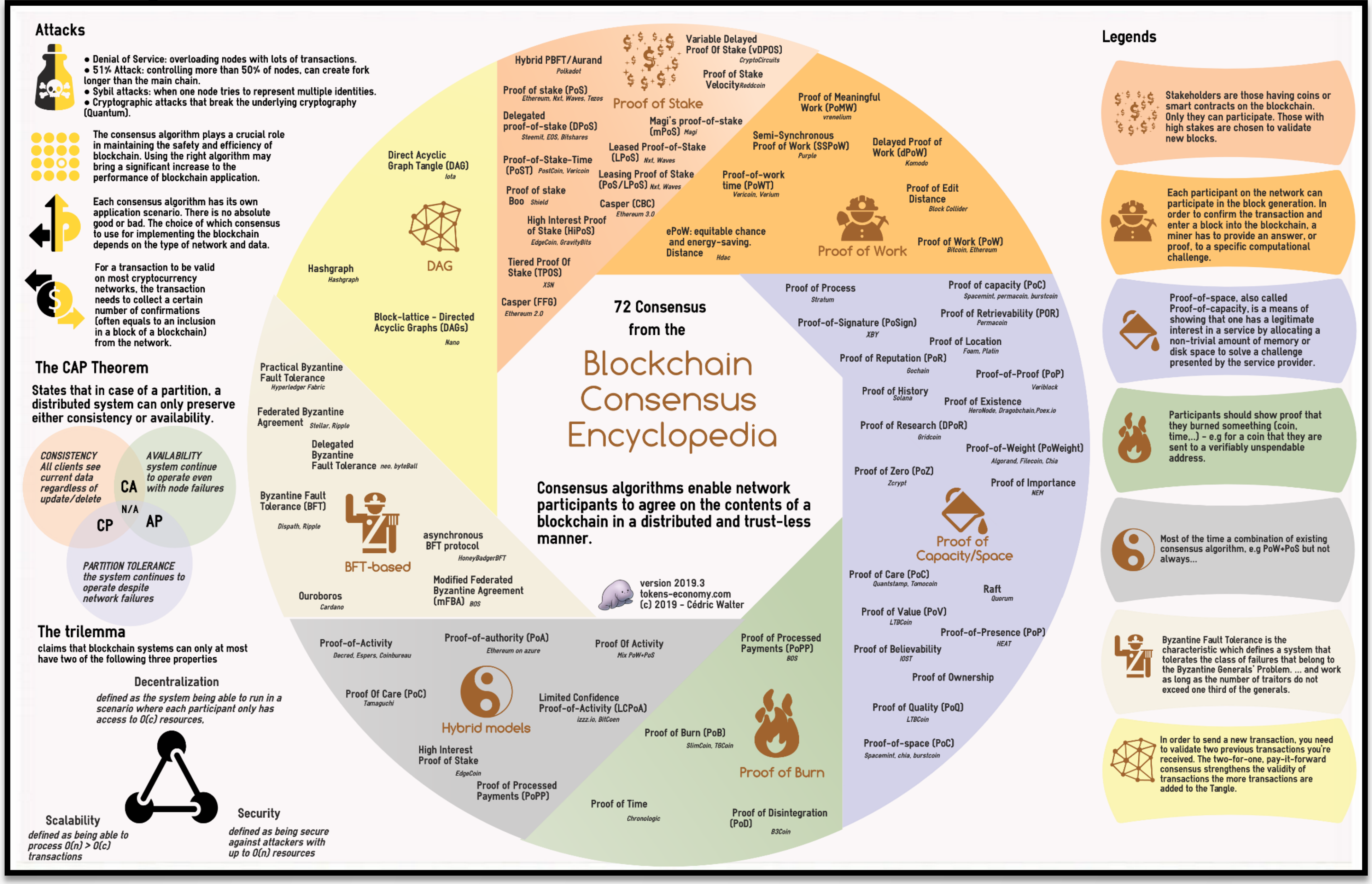
Methods by which the nodes in a DL reach agreement on the state of the ledger – i.e. which transaction are valid. Few examples:

- Proof of Work (aka mining)
  - *Also serves the purpose of ‘generating’ the crypto currency*
- Proof of Stake
- Practical Byzantine Fault Tolerance(PBFT)
- DAG: Direct Acyclic Graphs

Consensus algorithms are designed to avoid ‘double-spending’

Vulnerable to the ‘***x***’%age attack – if malicious entities control at least ‘x’% of the nodes, can influence the state of the DL

One picture worth…



Attacks

- Denial of Service: overloading nodes with lots of transactions.
- 51% Attack: controlling more than 50% of nodes, can create fork longer than the main chain.
- Sybil attacks: when one node tries to represent multiple identities.
- Cryptographic attacks that break the underlying cryptography (Quantum).

The consensus algorithm plays a crucial role in maintaining the safety and efficiency of blockchain. Using the right algorithm may bring a significant increase to the performance of blockchain application.

Each consensus algorithm has its own application scenario. There is no absolute good or bad. The choice of which consensus to use for implementing the blockchain depends on the type of network and data.

For a transaction to be valid on most cryptocurrency networks, the transaction needs to collect a certain number of confirmations (often equals to an inclusion in a block of a blockchain) from the network.

The CAP Theorem

States that in case of a partition, a distributed system can only preserve either consistency or availability.

CONSISTENCY All clients see current data regardless of update/delete

AVAILABILITY system continue to operate even with node failures

CA

N/A

CP

AP

PARTITION TOLERANCE the system continues to operate despite network failures

The trilemma

claims that blockchain systems can only at most have two of the following three properties

Decentralization

defined as the system being able to run in a scenario where each participant only has access to O(c) resources,

Scalability

defined as being able to process O(n) > O(c) transactions

Security

defined as being secure against attackers with up to O(n) resources

72 Consensus

from the

Blockchain Consensus Encyclopedia

Consensus algorithms enable network participants to agree on the contents of a blockchain in a distributed and trust-less manner.

version 2019.3
tokens-economy.com
(c) 2019 - Cédric Walter

DAG

Direct Acyclic Graph Tangle (DAG) *Iota*

Hashgraph *Hashgraph*

Block-lattice - Directed Acyclic Graphs (DAGs) *Nano*

Proof of Stake

Hybrid PBFT/Aurand *Polkadot*

Proof of stake (PoS) *Ethereum, Nxt, Waves, Tezos*

Delegated proof-of-stake (DPoS) *Steemit, EOS, Bitshares*

Proof-of-Stake-Time (PoST) *PostCoin, Vericoin*

Proof of stake Boo *Shield*

High Interest Proof of Stake (HiPoS) *EdgeCoin, GravityBits*

Tiered Proof Of Stake (TPOS) *XSN*

Casper (FFG) *Ethereum 2.0*

Variable Delayed Proof Of Stake (vDPOS) *CryptoCircuits*

Proof of Stake Velocity *Reddcoin*

Magi's proof-of-stake (mPoS) *Magi*

Leased Proof-of-Stake (LPoS) *Nxt, Waves*

Leasing Proof of Stake (PoS/LPoS) *Nxt, Waves*

Casper (CBC) *Ethereum 3.0*

Proof of Work

Proof of Meaningful Work (PoMW) *vrenelium*

Semi-Synchronous Proof of Work (SSPoW) *Purple*

Delayed Proof of Work (dPoW) *Komodo*

Proof-of-work time (PoWT) *Vericoin, Verium*

Proof of Edit Distance *Block Collider*

ePoW: equitable chance and energy-saving. Distance *Hdac*

Proof of Work (PoW) *Bitcoin, Ethereum*

Proof of Capacity/Space

Proof of Process *Stratum*

Proof of capacity (PoC) *Spacemint, permacoin, burstcoin*

Proof-of-Signature (PoSign) *XBY*

Proof of Retrievability (POR) *Permacoin*

Proof of Location *Foam, Platin*

Proof of Reputation (PoR) *Gochain*

Proof-of-Proof (PoP) *Veriblock*

Proof of History *Solana*

Proof of Existence *HeroNode, Dragobchain,Poex.io*

Proof of Research (DPoR) *Gridcoin*

Proof-of-Weight (PoWeight) *Algorand, Filecoin, Chia*

Proof of Zero (PoZ) *Zcrypt*

Proof of Importance *NEM*

Proof of Care (PoC) *Quantstamp, Tomocoin*

Raft *Quorum*

Proof of Value (PoV) *LTBCoin*

Proof-of-Presence (PoP) *HEAT*

Proof of Believability *IOST*

Proof of Ownership

Proof of Quality (PoQ) *LTBCoin*

Proof-of-space (PoC) *Spacemint, chia, burstcoin*

Proof of Burn

Proof of Processed Payments (PoPP) *BOS*

Proof of Burn (PoB) *SlimCoin, TGCoin*

Proof of Time *Chronologic*

Proof of Disintegration (PoD) *B3Coin*

Hybrid models

Proof-of-Activity *Decred, Espers, Coinbureau*

Proof-of-authority (PoA) *Ethereum on azure*

Proof Of Activity *Mix PoW+PoS*

Proof Of Care (PoC) *Tamaguchi*

Limited Confidence Proof-of-Activity (LCPoA) *izzz.io, BitCoen*

High Interest Proof of Stake *EdgeCoin*

Proof of Processed Payments (PoPP)

BFT-based

Practical Byzantine Fault Tolerance *Hyperledger Fabric*

Federated Byzantine Agreement *Stellar, Ripple*

Delegated Byzantine Fault Tolerance *neo, byteBall*

Byzantine Fault Tolerance (BFT) *Dispath, Ripple*

asynchronous BFT protocol *HoneyBadgerBFT*

Modified Federated Byzantine Agreement (mFBA) *BOS*

Ouroboros *Cardano*

Legends

Stakeholders are those having coins or smart contracts on the blockchain. Only they can participate. Those with high stakes are chosen to validate new blocks.

Each participant on the network can participate in the block generation. In order to confirm the transaction and enter a block into the blockchain, a miner has to provide an answer, or proof, to a specific computational challenge.

Proof-of-space, also called Proof-of-capacity, is a means of showing that one has a legitimate interest in a service by allocating a non-trivial amount of memory or disk space to solve a challenge presented by the service provider.

Participants should show proof that they burned something (coin, time,..) - e.g for a coin that they are sent to a verifiably unspendable address.

Most of the time a combination of existing consensus algorithm, e.g PoW+PoS but not always...

Byzantine Fault Tolerance is the characteristic which defines a system that tolerates the class of failures that belong to the Byzantine Generals' Problem. ... and work as long as the number of traitors do not exceed one third of the generals.

In order to send a new transaction, you need to validate two previous transactions you're received. The two-for-one, pay-it-forward consensus strengthens the validity of transactions the more transactions are added to the Tangle.

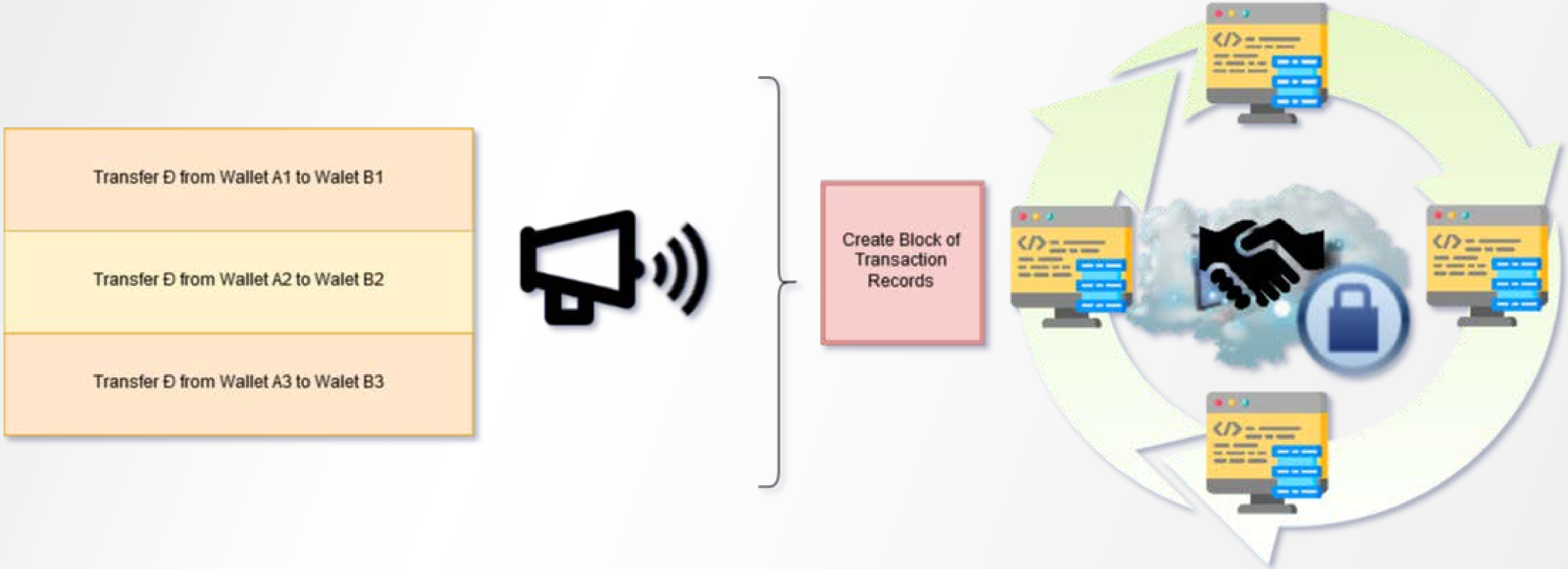
Credit: https://www.tokens-economy.com/wp-content/uploads/2019/02/Major-Blockchain-consensus-Infographics.png

Joining the parts

Trusted shared services and digital business solutions

ICC international computing centre ICT SOLUTIONS FOR THE UN FAMILY

Blockchain - formation



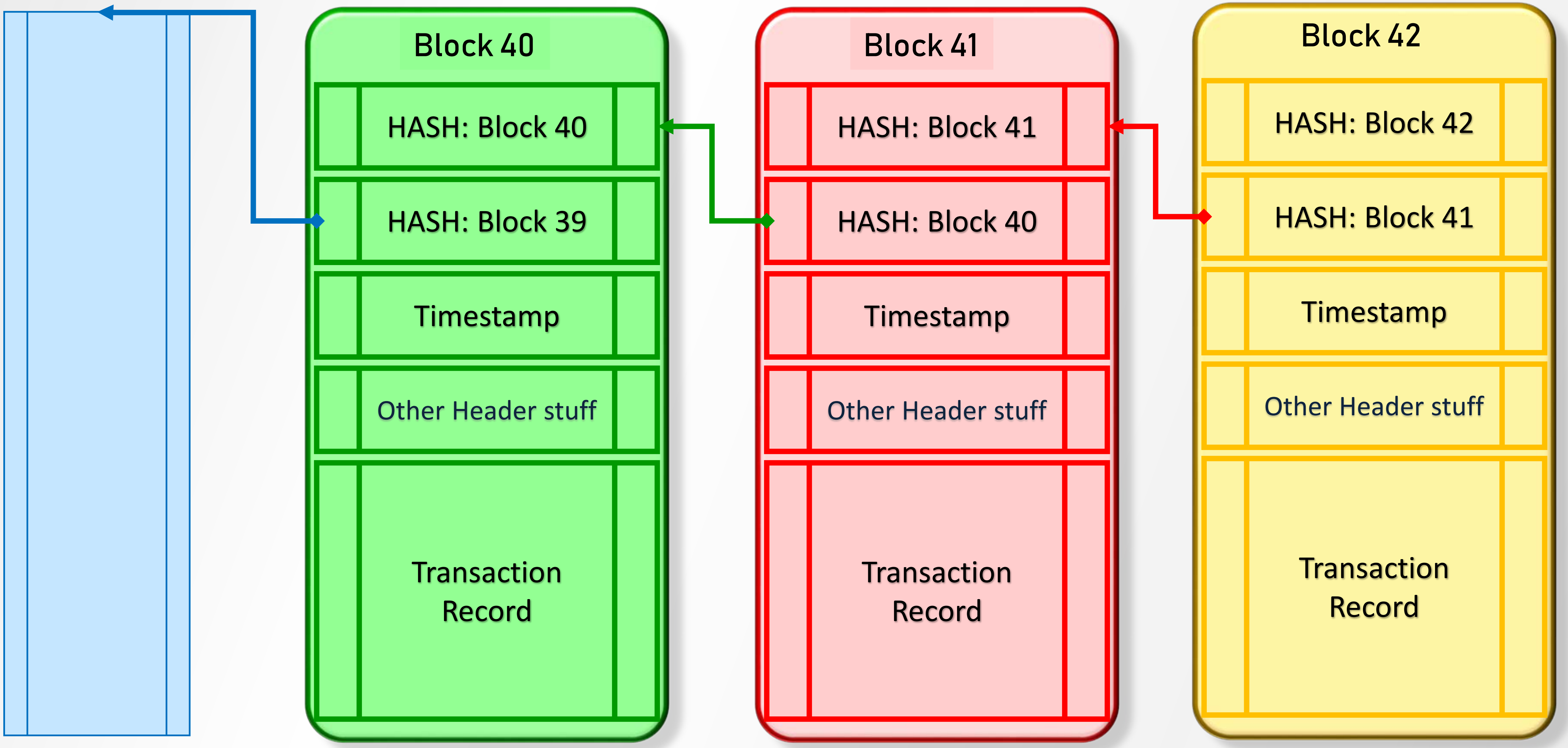
Transfer Ð from Wallet A1 to Walet B1

Transfer Ð from Wallet A2 to Walet B2

Transfer Ð from Wallet A3 to Walet B3

Create Block of Transaction Records

Blockchain - formation

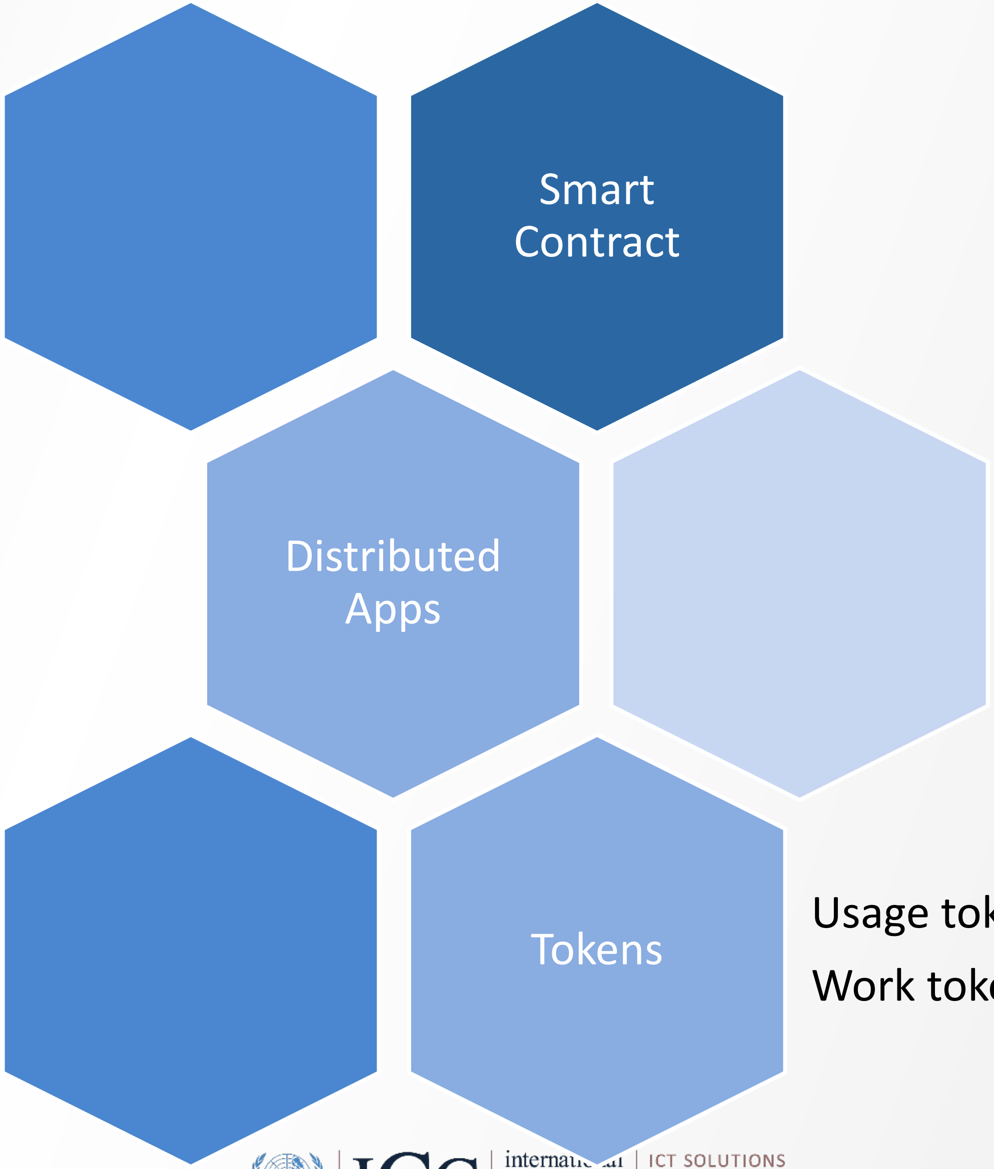


Is left as an exercise…

Trusted shared services and digital business solutions

ICC international computing centre ICT SOLUTIONS FOR THE UN FAMILY

Some other terms



Usage tokens

Work tokens

Thank you!

Trusted shared services and digital business solutions

Shashank Rai: raish@unicc.org

ICC international computing centre

ICT SOLUTIONS FOR THE UN FAMILY