
ELEMENTAL CONCEPT

Hyperledger Fabric Workshop
Overview

Paul Sitoh
10-11 November 2018

Disclaimer

- Not representing Hyperledger or speaking from a “fan-boy” perspective
- Sharing practical experience from the perspective of a solution architect/developers’ perspective NOT from the perspective of Fabric maintainer

Workshop Agenda

- Blockchain 101
- Fabric Architecture
- Fabric Operations
- Fabric Development
- Q & A + Feedback

Blockchain 101

Agenda

- Transactions and consensus
- Decentralisation
- Types of Blockchain
- Why Fabric?

Transactions and consensus

Blockchain 101

Blockchain 101

- Transactions
  - Participants (people organisations) exchanging value
  - Value can be anything, tangible (car, house, cash, etc) or intangible (sense of security, happiness, education, etc)
  - Exchange has to be final
  - A change of state occurs to value being transacted – e.g. ownership of house
- Ledger
  - A record of transactions
  - Who transfer what to whom and when did it occur

Blockchain 101

Back to basic ….. bitcoin

Before

- Adam 10
- Eve 2

After

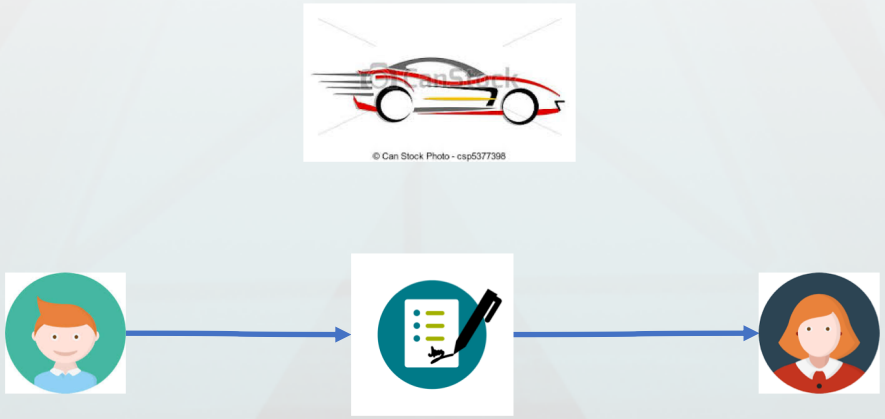
- Adam 9
- Eve 3

Blockchain 101

Back to basic ….. smart contracts == computer program NOT legal contract

Before

- Adam { model: super car, id: 1234, owner: Adam} <smart contract>
- Eve {model: nil, id: nil, owner: nil} <smart contract>



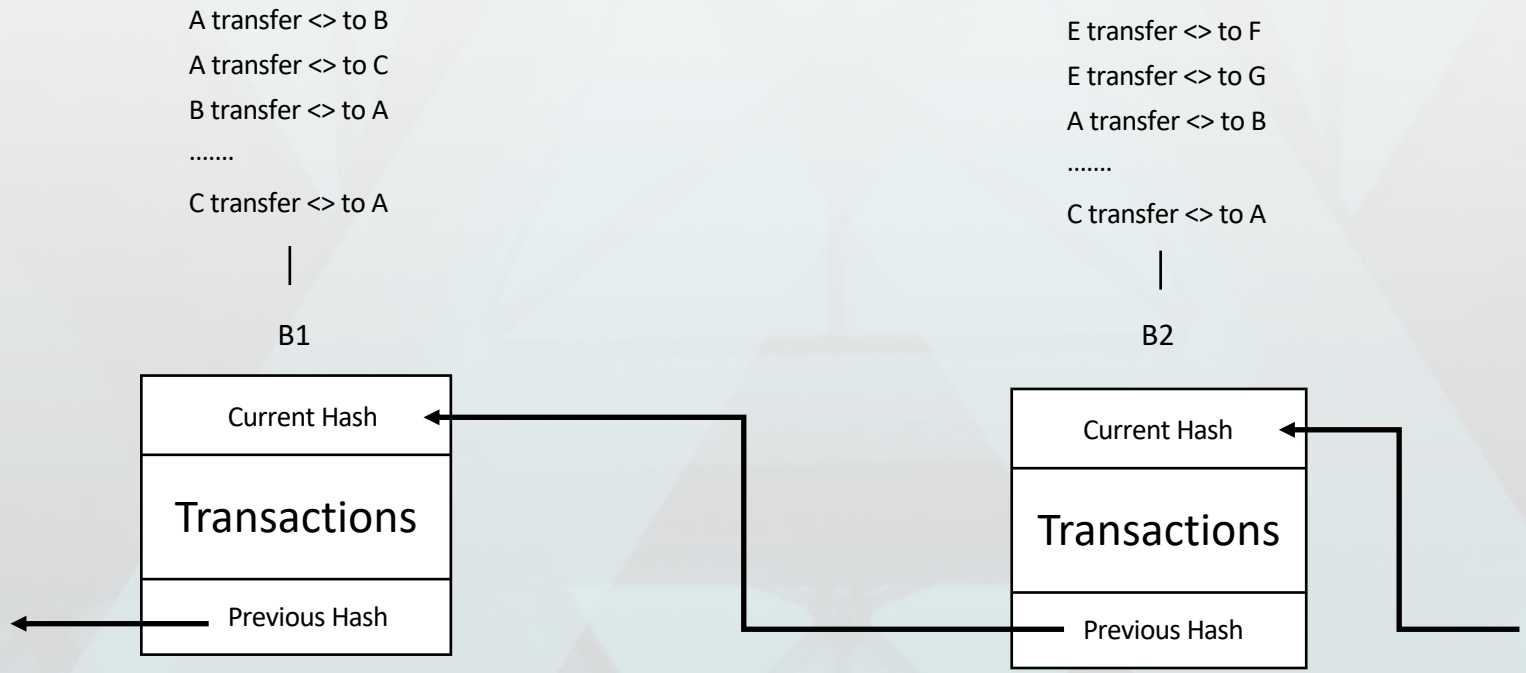
Adam transfer car to Eve via smart contract

After

- Adam { model: nil, id: nil, owner: nil} <smart contract>
- Eve {model: super, id:1234, owner: Eve} <smart contract>

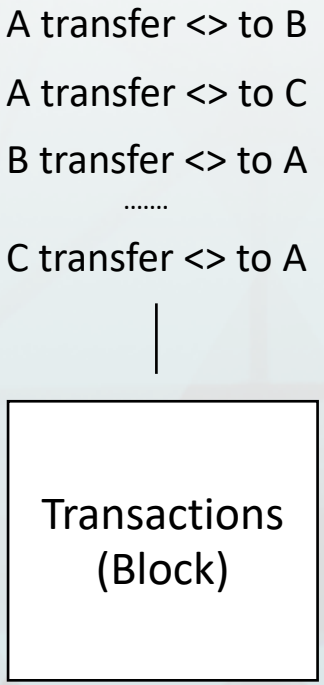
Blockchain 101

Ideal world: transaction occur in sequence that can easily be packed into blocks …..



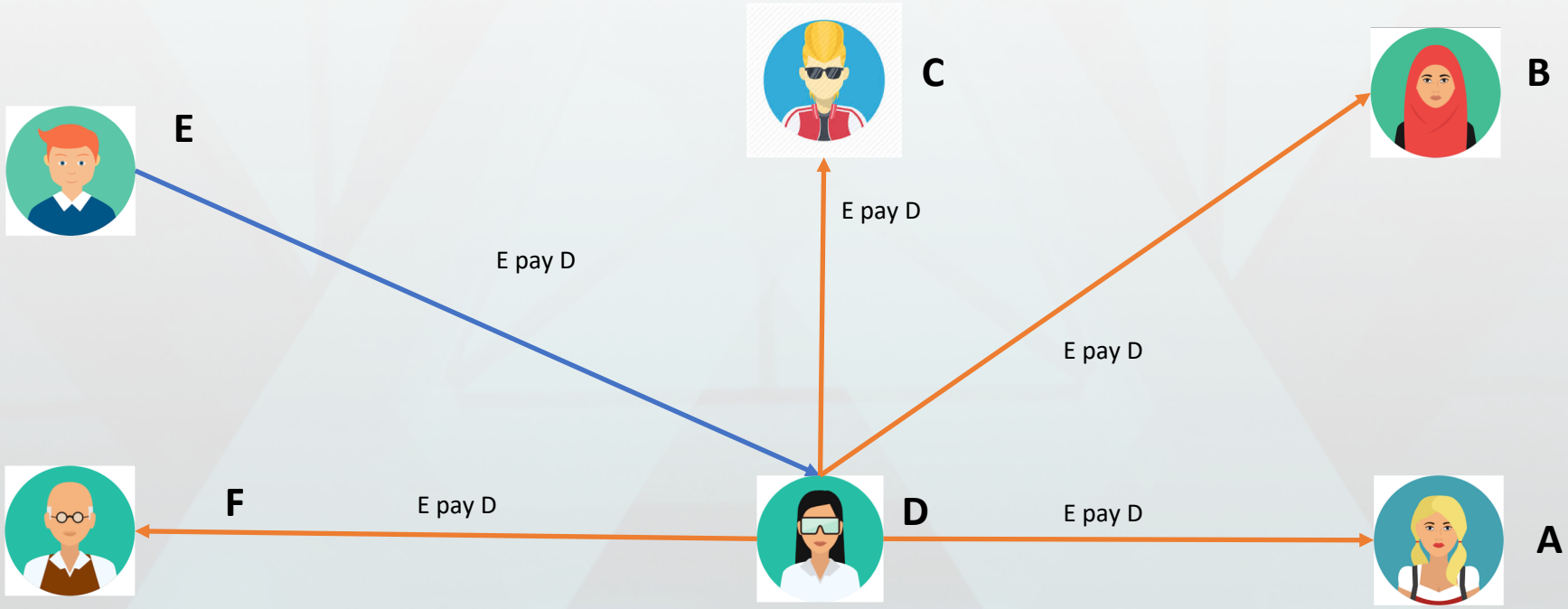
Blockchain 101

A block is simply a container of transaction hash ….



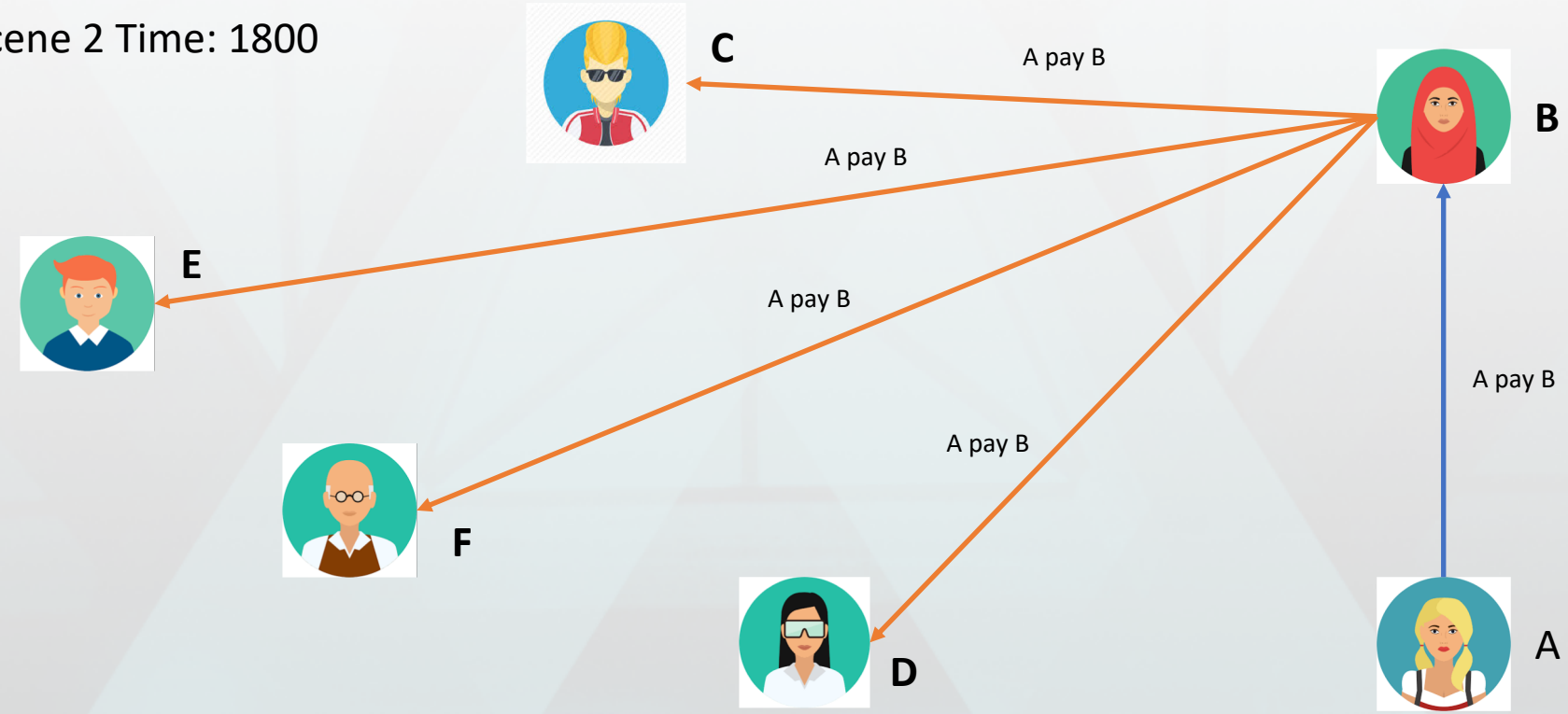
Blockchain 101

Reality ……. Scene 1 Time: 1800



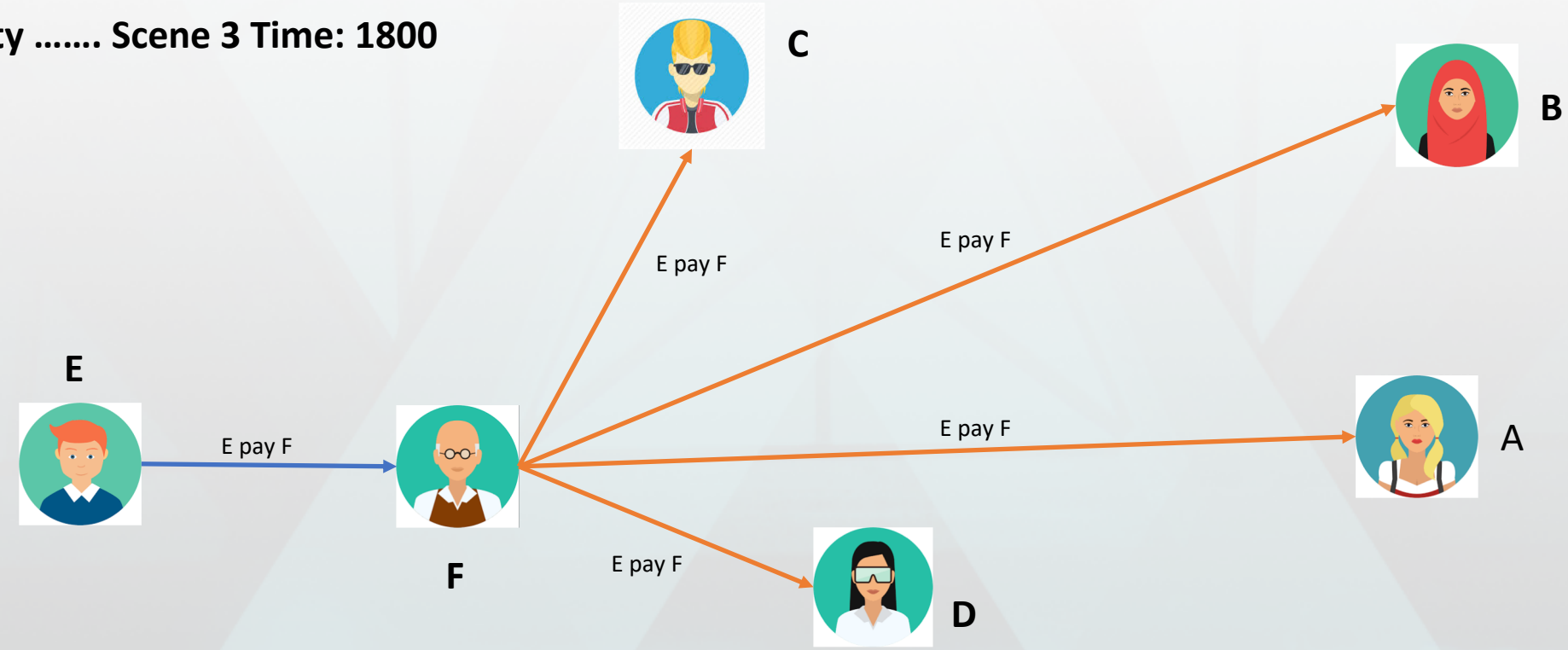
Blockchain 101

Reality ……. Scene 2 Time: 1800



Blockchain 101

Reality ……. Scene 3 Time: 1800



Blockchain 101

Reality ……. Scene 1 Time: 1800

E transfer <> to D

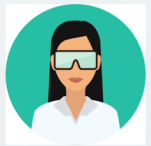
A transfer <> to C

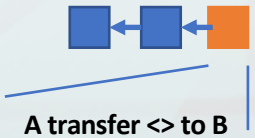
B transfer <> to A

…….

C transfer <> to A

Reality ……. Scene 2 Time: 1800





A transfer <> to B

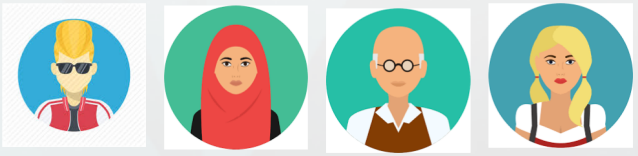
A transfer <> to C

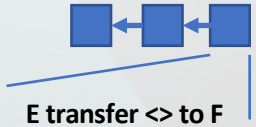
B transfer <> to A

…….

C transfer <> to A

Reality ……. Scene 3 Time: 1800





E transfer <> to F

A transfer <> to C

B transfer <> to A

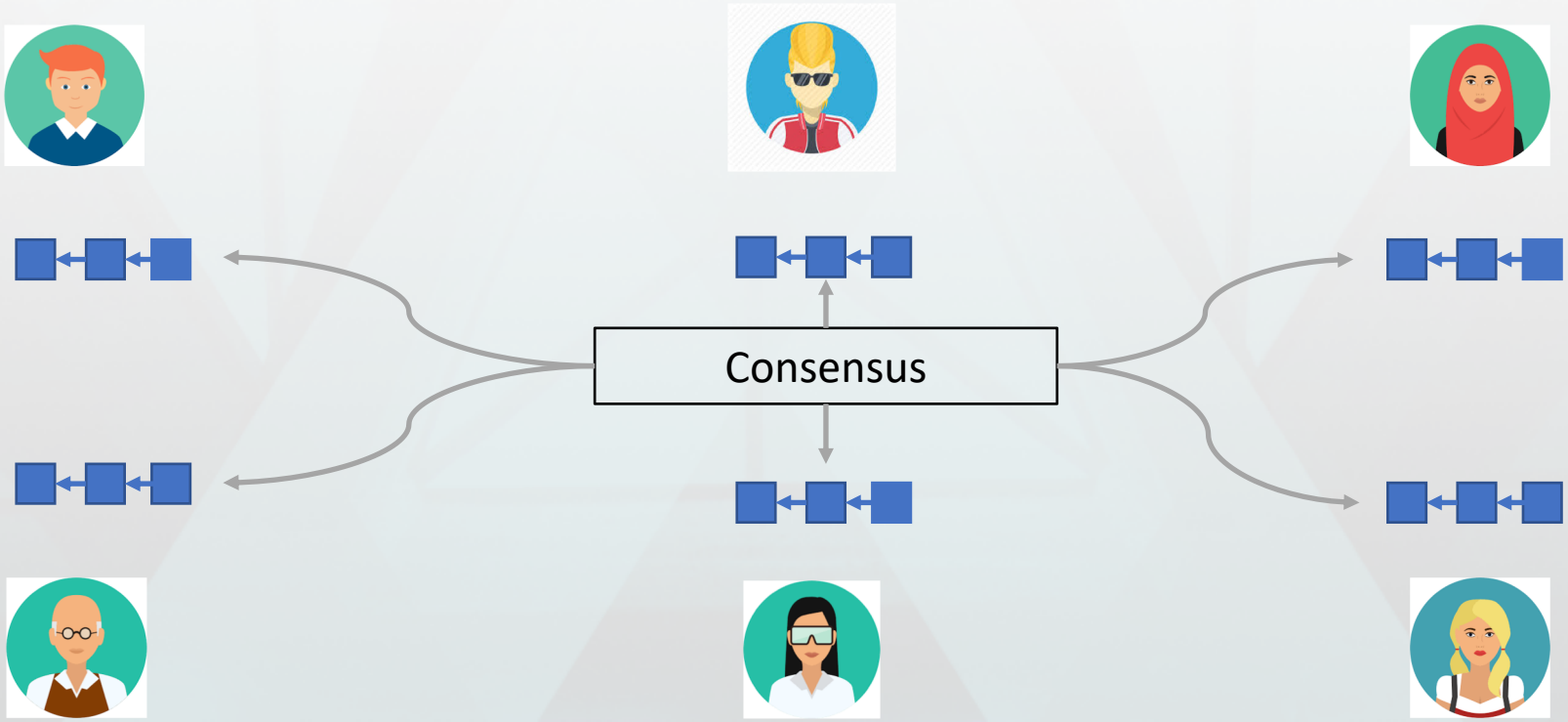
…….

C transfer <> to A

Blockchain 101

Which chain is the right one?

Blockchain 101

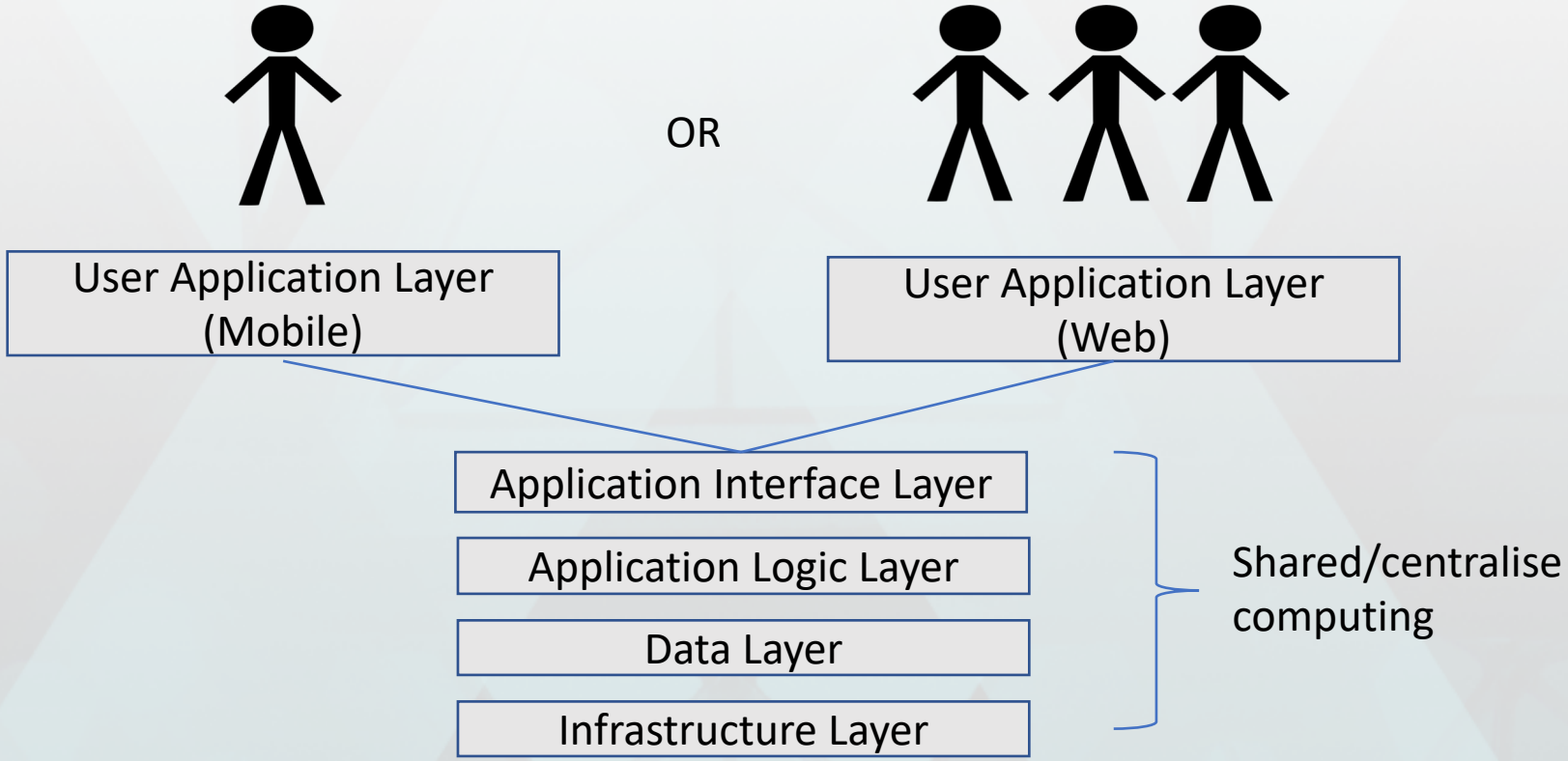


Decentralisation

Blockchain 101

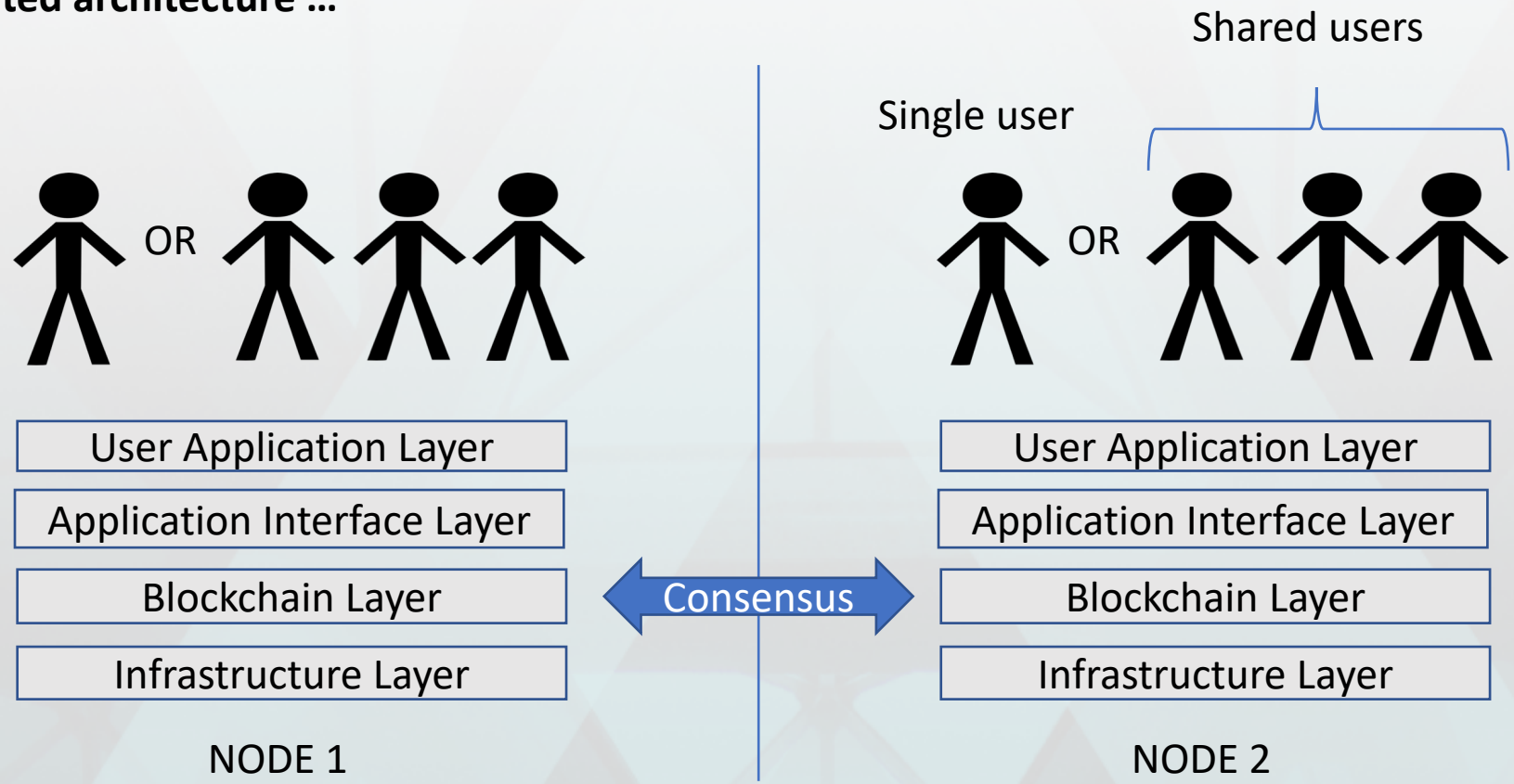
Blockchain 101

Non-blockchain architecture …



Blockchain 101

A distributed architecture …



Types of blockchain

Blockchain 101

Types of blockchain

There are many types of blockchain,
not one!

Types of blockchain

- According to Imperial College, London[(1)]
  - Permissionless public
  - Permissioned public
  - Permissioned private
- Cryptocurrency vs no currency
- Classification by technology/consensus algorithm

(1): Blockchain Beyond the Hype - A Practical Framework for Business Leaders. April 2018. World Economic Forum.

Types of blockchain

- According to Imperial College, London
- Cryptocurrency vs no currency
- Classification by technology/consensus algorithm
  - Ethereum
  - Neo
  - Hyperledger Family
    - Fabric
    - Sawtooth
  - JP Morgan Quorum
  - More …

Types of Blockchain

Summary …

	Public	Permission
Currency	Ethereum Neo	
No currency		Fabric Sawtooth JP Morgan Quorum

Public blockchain

- Anyone permitted join the network, to write to the network and to read the transactions from those networks. These systems have no single owner – everyone on the network has an identical copy of the "ledger"(1)
- Users directly interact with Blockchain
- User identity based on cryptographic keys
- Cryptocurrency typically used to incentivise behavior or pay for computing power (such as mining operations)

(1): Blockchain Beyond the Hype - A Practical Framework for Business Leaders. April 2018. World Economic Forum.

Public blockchain

- Consensus algorithm: Proof of Work or Proof of Stake
- Goal is to replace third party organisations such as law firms, banks, etc with fully automated code or smart contracts – i.e. Distributed Autonomous Organisation (DAO)

Public blockchain

Architecture …	User 1	User 2	.....	User N
User application layer	Web/mobile	Web/mobile		Web/mobile
Blockchain access layer	Wallet/ledger/smart contract	Wallet/ledger/smart contract		Wallet/ledger/smart contract
Blockchain consensus layer	Proof of work	Proof of work		Proof of work
Currency layer	Ether (ETH)	Ether (ETH)		Ether (ETH)
Infrastructure networking layer	PC or Server	PC or Server		PC or Server

Permissioned blockchain(1)

- Permissioned public
  - These are are a form of hybrid system that provide for situations where whitelisted access is required but all the transactions should be publicly viewable. Examples of this are government applications where only certain people should be able to write to the network but all transactions can be publicly verified.
- Permissioned, private, shared systems

(1): Blockchain Beyond the Hype - A Practical Framework for Business Leaders. April 2018. World Economic Forum.

Permissioned blockchain(1)

- Permissioned public
- Permissioned, private, shared systems
  - These are those that have whitelisted access, meaning that only those people with permission can read or write to such systems. They may have one or many owners – often consortia are formed to manage the ownership.

(1): Blockchain Beyond the Hype - A Practical Framework for Business Leaders. April 2018. World Economic Forum.

Permissioned blockchain

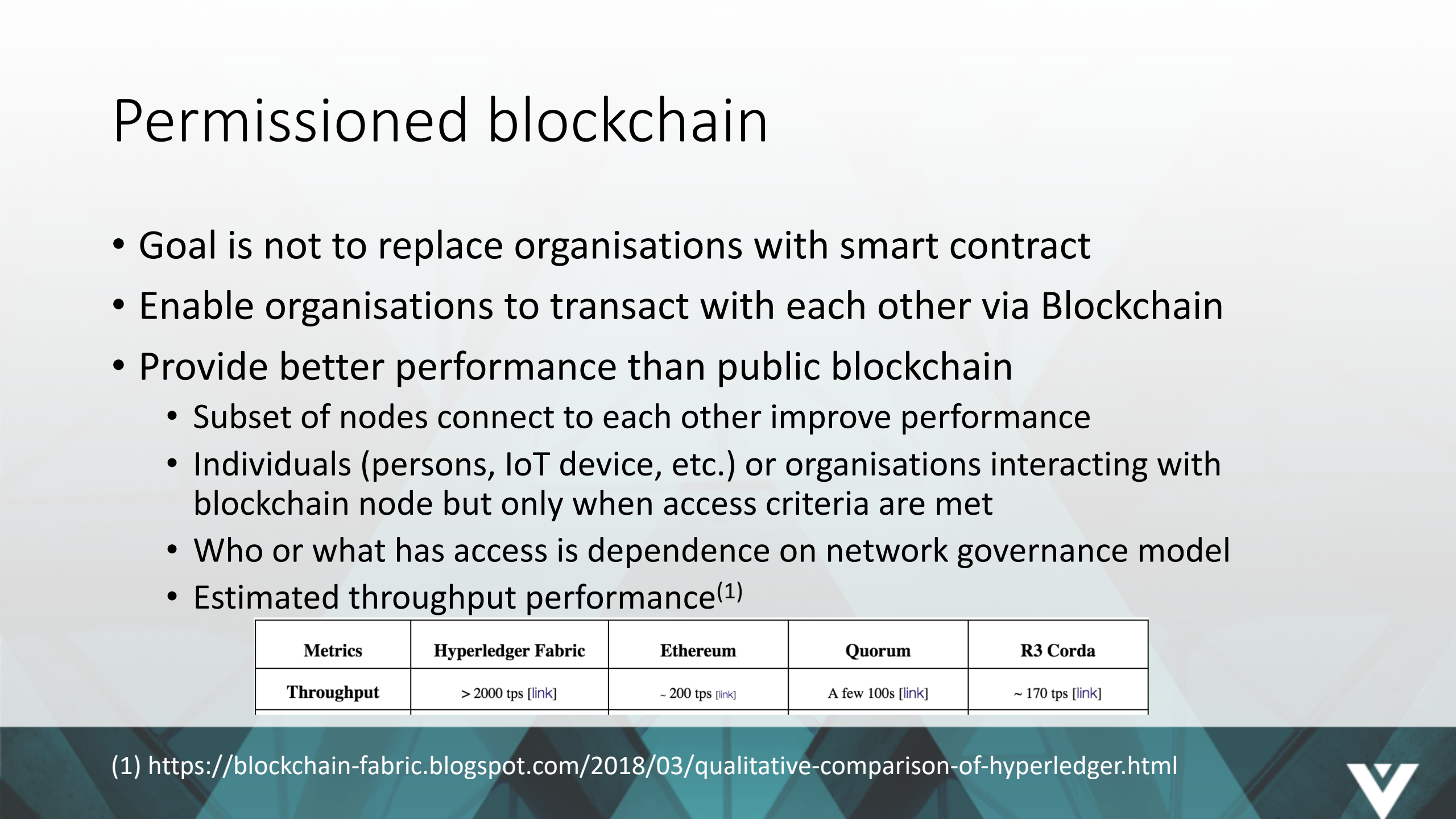
- Goal is not to replace organisations with smart contract
- Enable organisations to transact with each other via Blockchain
  - Representative of organisations interact with blockchain on behalf or organisation (i.e. cashier of a bank)
  - Individual don’t (normally) own a owned the nodes but nodes are owned by organisations
  - Using smart contract to automate business logic on behalf of organisation
- Provide better performance than public blockchain

Permissioned blockchain

- Goal is not to replace organisations with smart contract
- Enable organisations to transact with each other via Blockchain
- Provide better performance than public blockchain
  - Subset of nodes connect to each other improve performance
  - Individuals (persons, IoT device, etc.) or organisations interacting with blockchain node but only when access criteria are met
  - Who or what has access is dependence on network governance model
  - Estimated throughput performance(1)

Metrics	Hyperledger Fabric	Ethereum	Quorum	R3 Corda
Throughput	> 2000 tps [link]	~ 200 tps [link]	A few 100s [link]	~ 170 tps [link]

(1) https://blockchain-fabric.blogspot.com/2018/03/qualitative-comparison-of-hyperledger.html

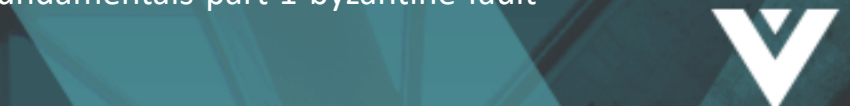


Permissioned blockchain

Architecture …	Entity 1	Entity 2	.....	Entity N
User application layer	Web/mobile	Web/mobile		Web/mobile
Blockchain access layer	Identity management	Identity management		Identity management
Blockchain Ledger layer	Ledger/smart contract	Ledger/smart contract		Ledger/smart contract
Blockchain consensus layer	BFT(1)	BFT (1)		BFT (1)
Infrastructure networking layer	PC or Server	PC or Server		PC or Server

Entity = individual or organisation

(1): BFT – Byzantine Fault Tolerance | https://medium.com/loom-network/understanding-blockchain-fundamentals-part-1-byzantine-fault-tolerance-245f46fe8419.

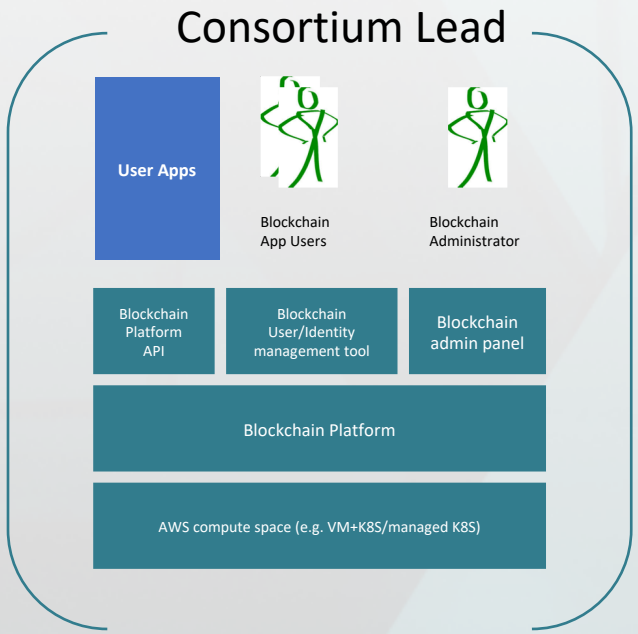


Permissioned blockchain

Governance …	Entity 1	Entity 2	…….	Entity N
Who can access blockchain?	Blockchain identity layer	Blockchain identity layer		Blockchain identity layer
Who can deploy smart contracts?	Blockchain layer	Blockchain layer		Blockchain
Who decides which pc is allowed to join?	Network layer	Network layer		Network layer

Permissioned blockchain

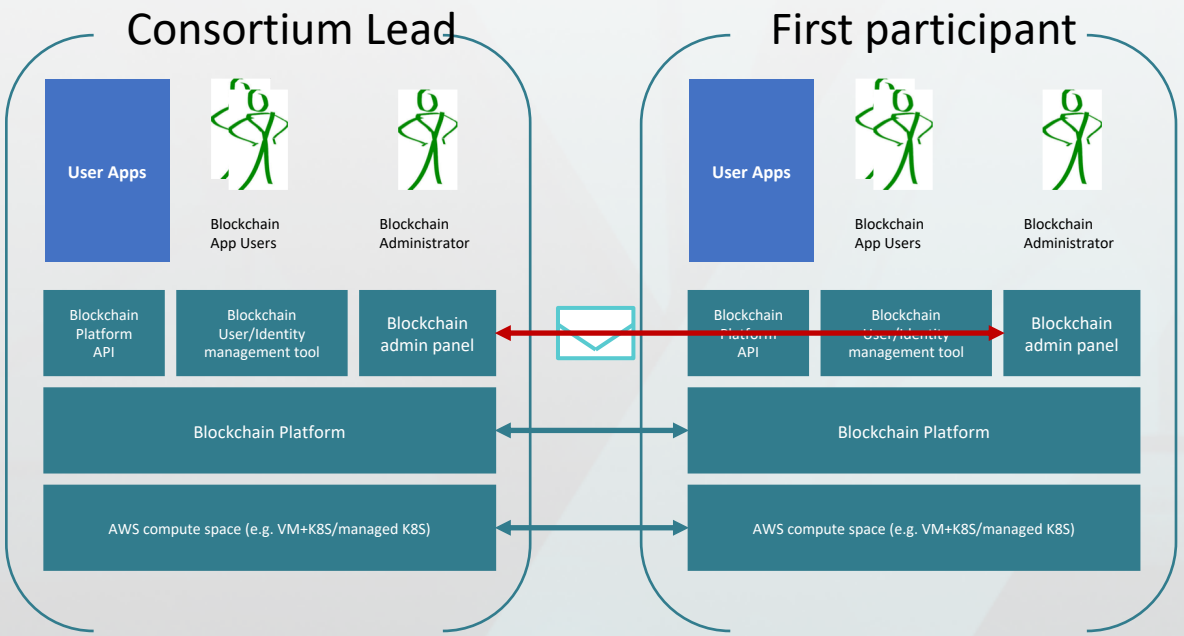
Decentralise governance model – purest form



- First organization – e.g. Hospital – create a nominally lead node.
- User app integrated with Blockchain Platform API
- User within the organization are assigned keys for signing transactions
- Next step – blockchain administrator send invite to another organization via email to create a node and join.

Permissioned blockchain

Decentralise governance model – purest form

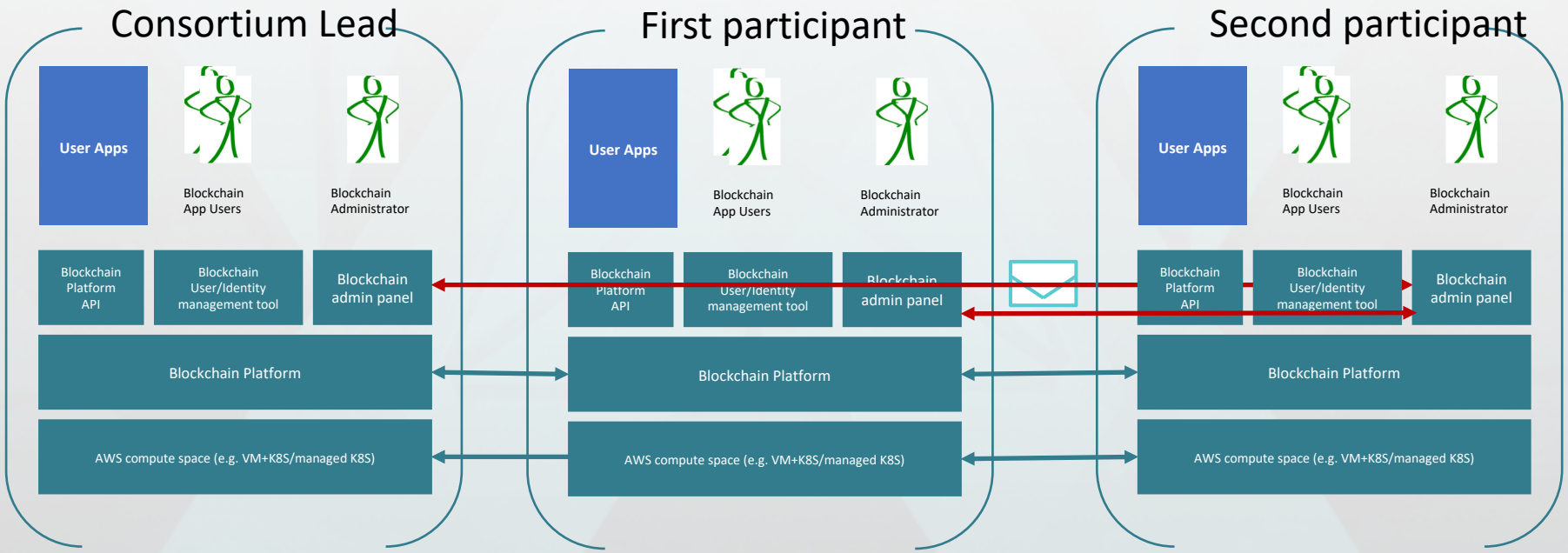


- A network is formed between the two entities at the blockchain level and networking level
- The lead and first participant together must sign off to add a new participant**

Notes:
** One possible consortium governance model

Permissioned blockchain

Decentralise governance model – purest form

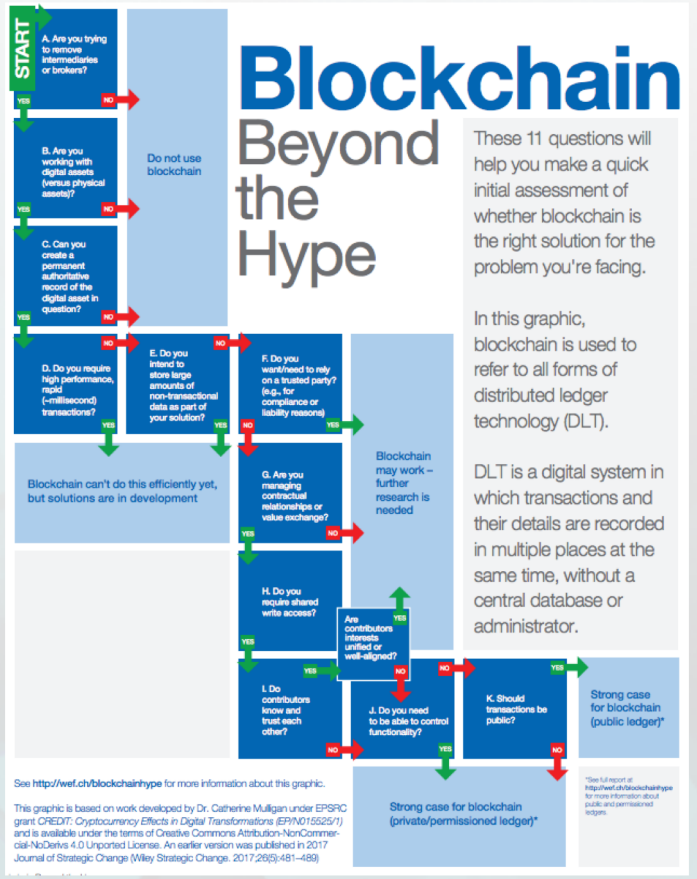


Second participant joins and all have equal rights to invite more.

Why Fabric?

Why Fabric?(1)

- For parties that don't trust each other **AND** improve efficiency
- Transfer trust from typically centralise intermediaries to distributed technology
- If you trust a 3rd Party to host your data and business logic, don't use blockchain there are better solution



(1): Blockchain Beyond the Hype - A Practical Framework for Business Leaders. April 2018. World Economic Forum.

Why Fabric?

- You are prepared to sacrifice aspects of your identity for performance
- If you don’t want crypto currency to be basis for consensus
- You want ensure communication privacy
- You would like to use general purpose programming language for smart contracts
- You want a pluggable solution

Q & A?