Scale-Out Blockchains
Off-Chain Scaling

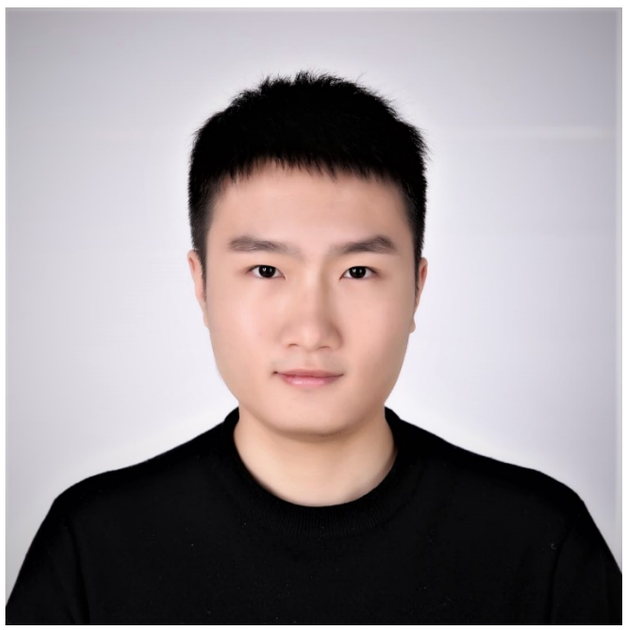
Fangyu Gai, Ph.D. student, supervised by Dr. Chen Feng

University of British Columbia – Okanagan Campus

April 23, 2019

https://medium.com/coinmonks/blockchain-101-4acc9902b3a4

Fangyu Gai



https://fangyugai.me
fangyu.gai@ubc.ca

Ph.D. student, UBC – Okanagan Campus,
supervised by Dr. Chen Feng

- **Education**
  - *B.Sc in Software Engineering, Beijing Institute of Technology, China, since 2011*
  - *M.Sc in Computer Science, National University of Defense Technology, China, since 2015*
  - *Ph.D. in Electrical Engineering, University of British Columbia, Canada, since 2018*
- **Research in Blockchain**
  - *Off-chain scaling*
  - *Consensus algorithms*

THE UNIVERSITY OF BRITISH COLUMBIA

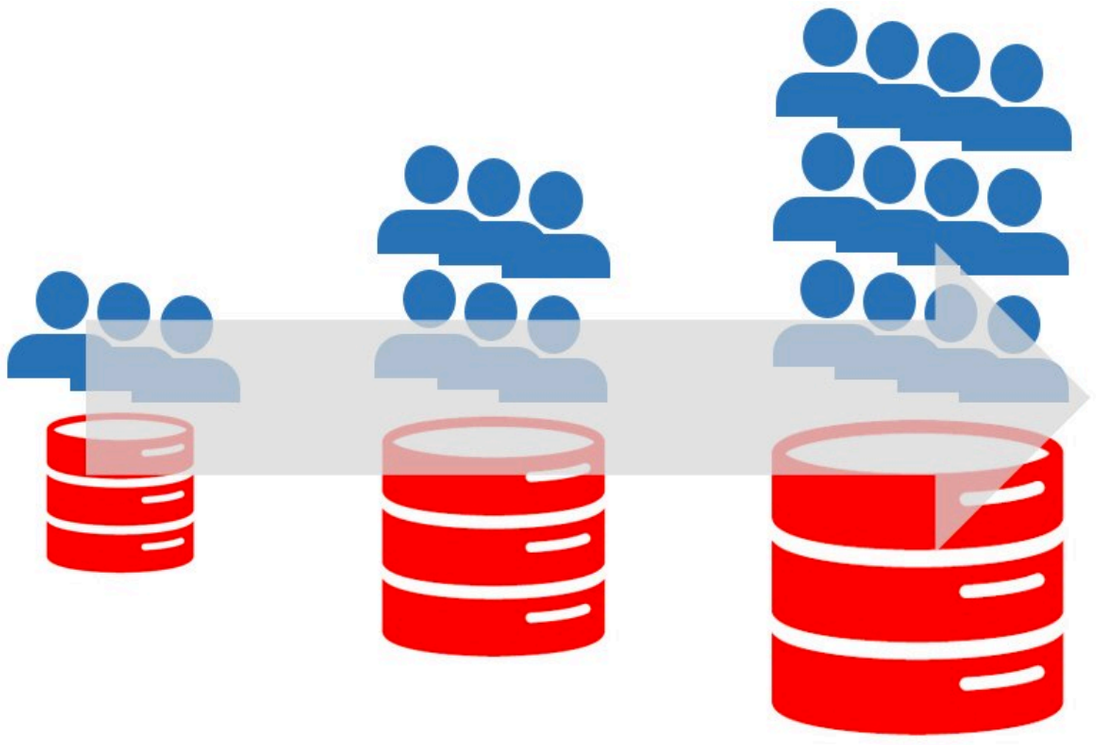
Overview

- Why does the blockchain need scaling?
- What is off-chain scaling?
- How do off-chain protocols work?

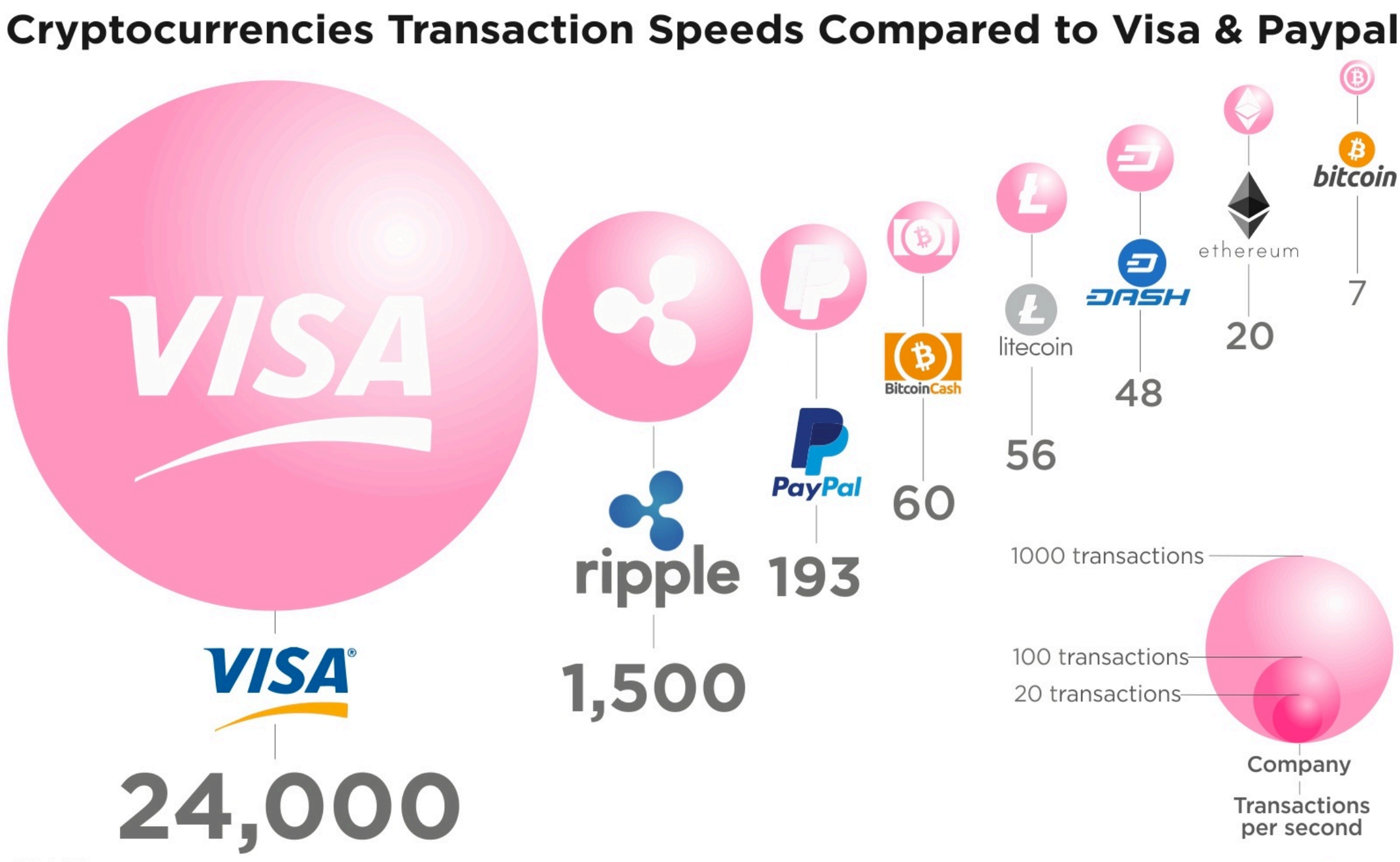
Why does the blockchain need scaling?

Why does the blockchain need scaling?

- Scaling? Scalable? Scalability?
  - In a scalable system, as we move from small to large, things should not get incrementally worse.

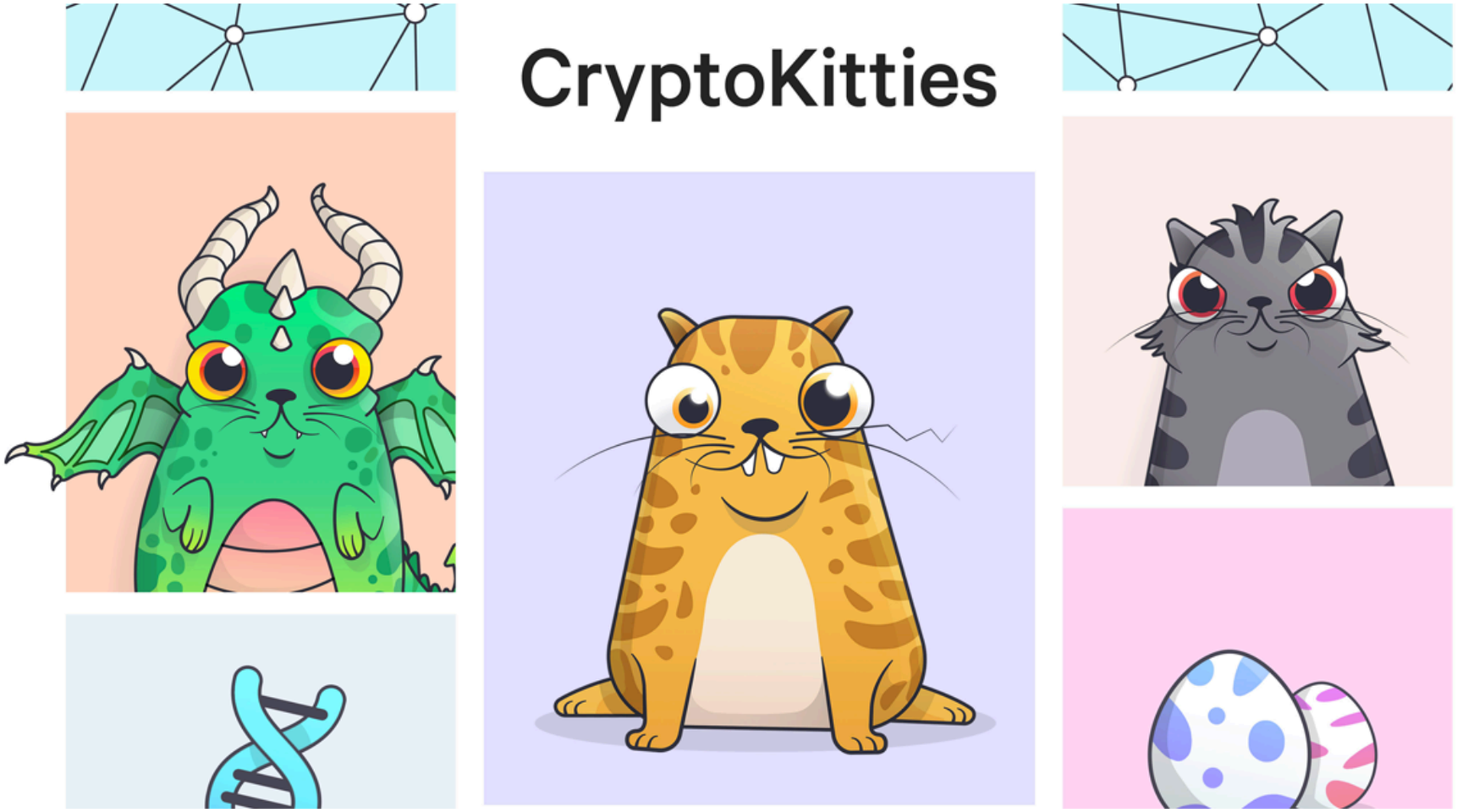


Why does the blockchain need scaling?

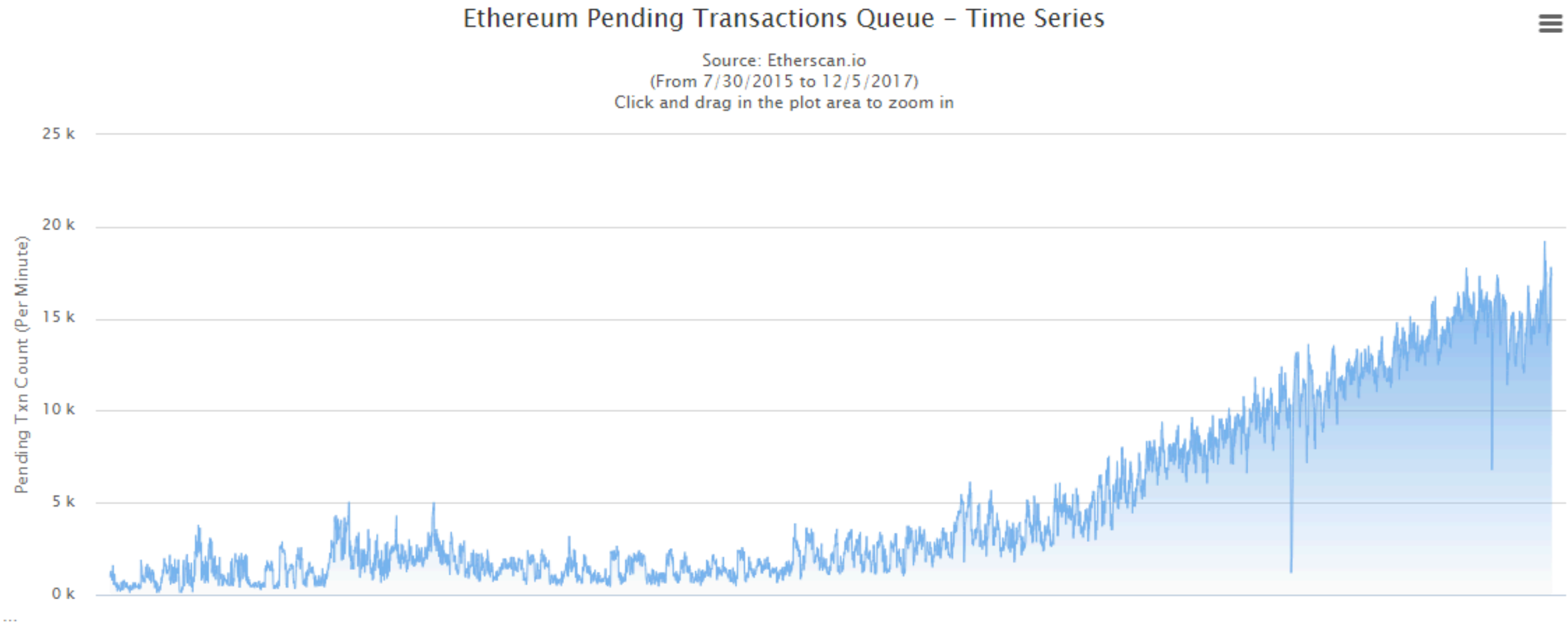


Article & Sources:
https://howmuch.net/articles/crypto-transaction-speeds-compared
https://howmuch.net/sources/crypto-transaction-speeds-compared

Why does the blockchain need scaling?



Why does the blockchain need scaling?

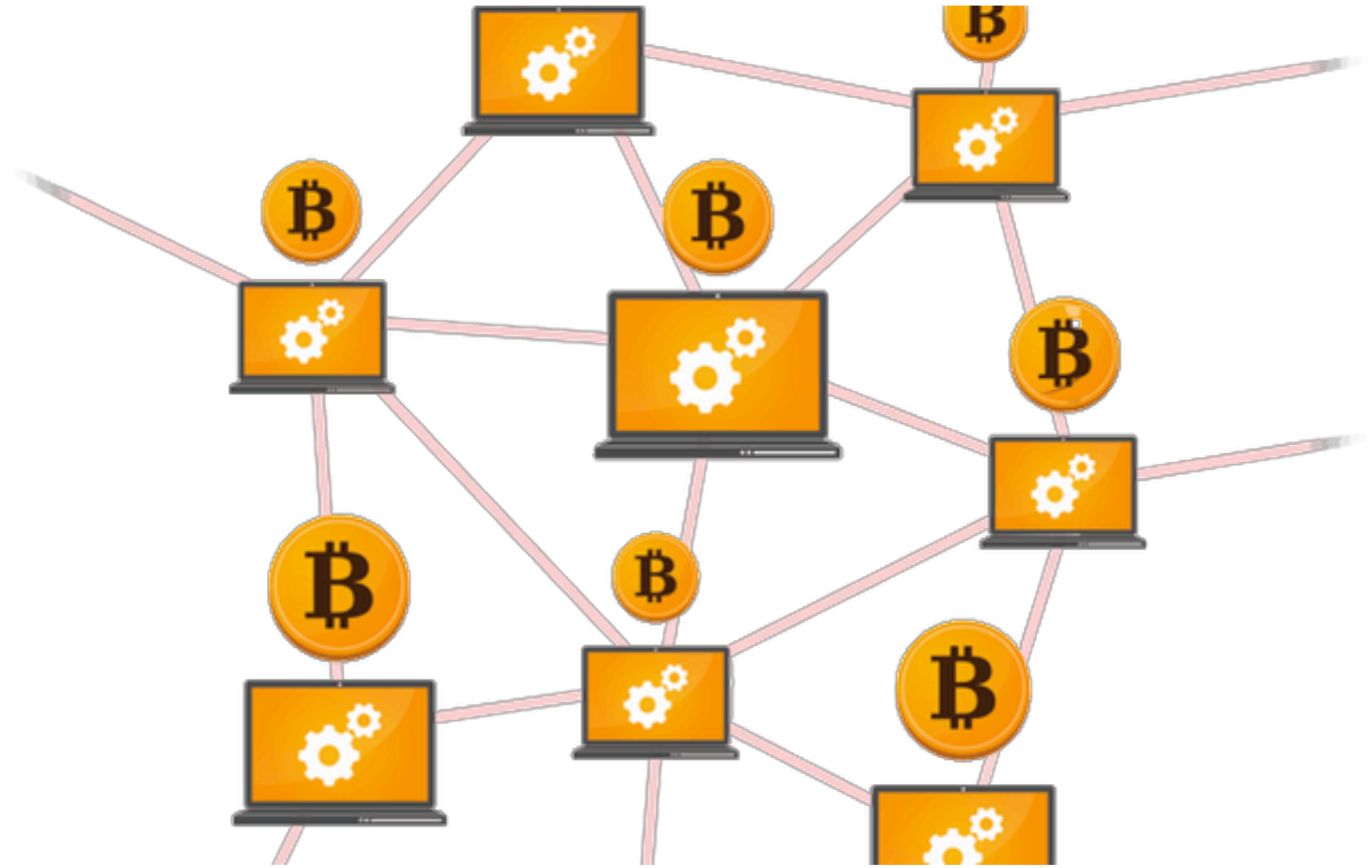


Why does the blockchain need scaling?

Because the current blockchains (e.g. Bitcoin, Ethereum) are not scalable.

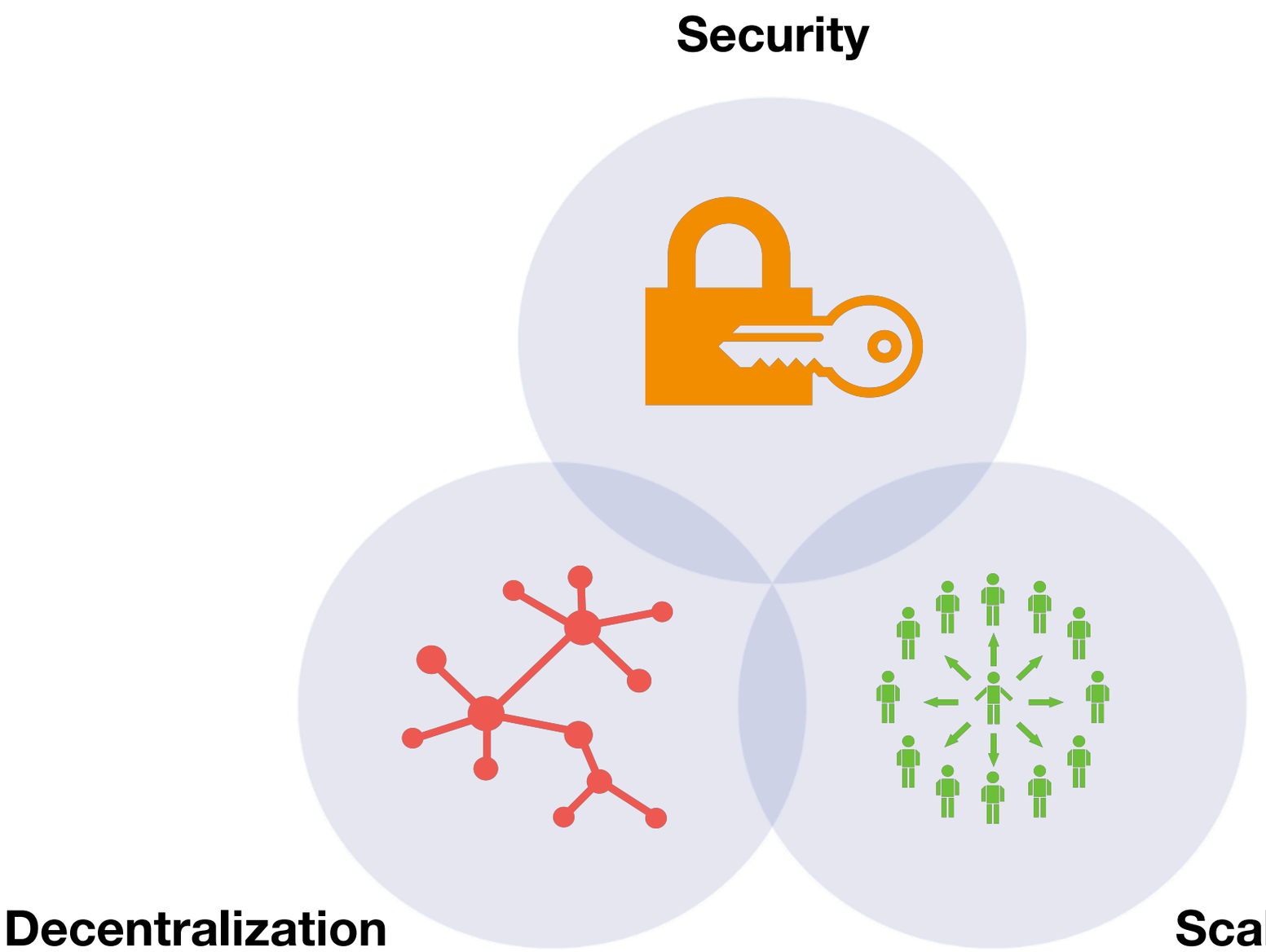
Why does the blockchain need scaling?

Why are the current blockchains not scalable?



Why does the blockchain need scaling?

Scalability Trilemma



https://medium.com/@aakash_13214/the-scalability-trilemma-in-blockchain-75fb57f646df

Why does the blockchain need scaling?

Conceptually, there are three main directions we might go about breaking the trilemma

- Alternative blockchain consensus architectures
  - PoS
  - New BFT
  - DAG (Directed Acyclic Graph)

Algorand

Tendermint

CARDANO

IOTA

- On-chain solutions (Layer 1)
  - Sharding
  - Parallel Chain

casper

- Off-chain solutions (Layer 2)
  - Payment Channels
  - Sidechain

LIGHTNING

RAIDEN NETWORK

Plasma

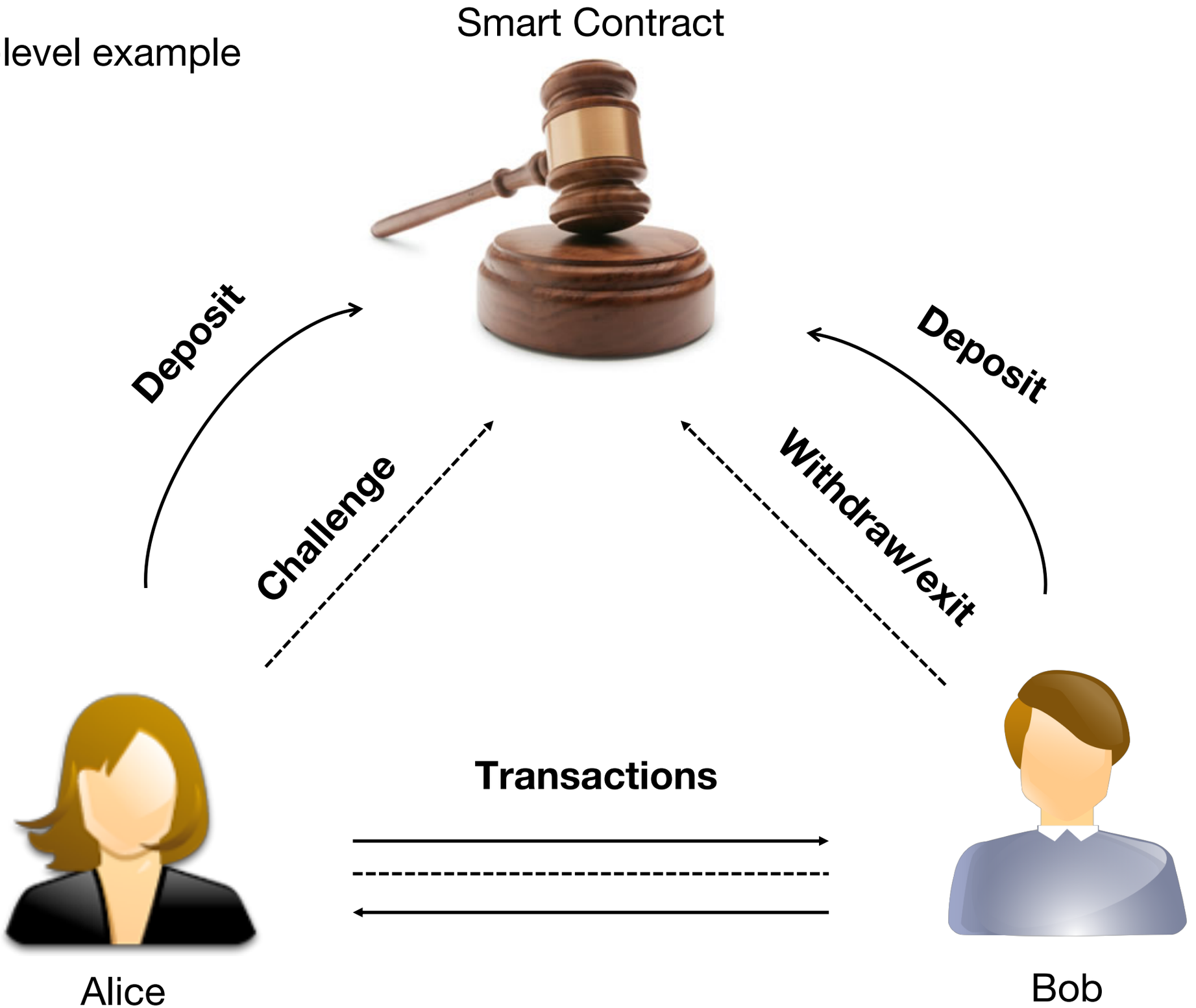
What is off-chain scaling?

What is off-chain scaling?

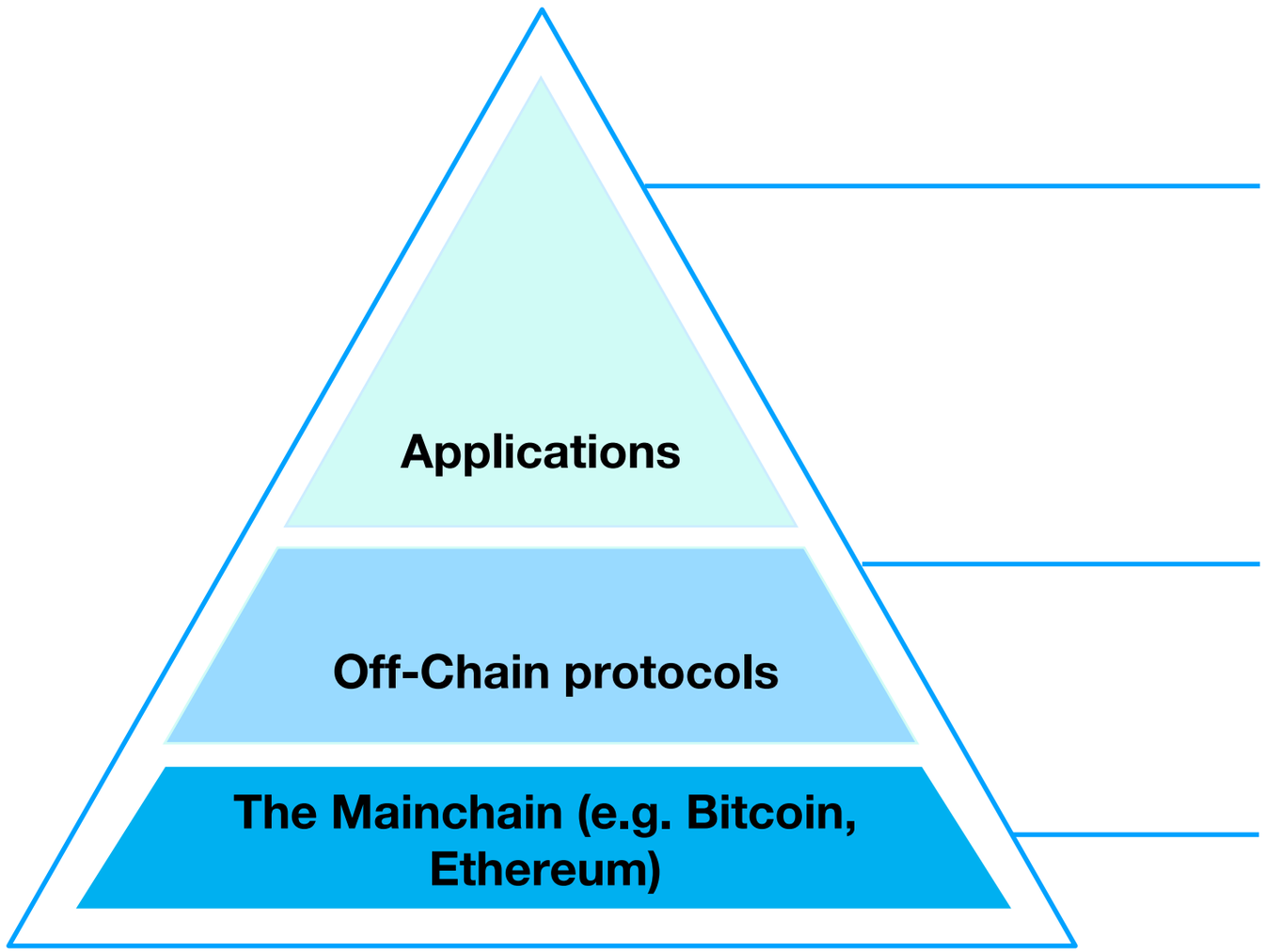
- Off-chain protocols use public blockchains as the **settle layer**, aka the “mainchain”.
- Every parties have some **deposits** frozen on the mainchain.
- Parties can do **unlimited transactions** off-chain and only touch the mainchain when it’s **necessary**.
- The mainchain has no idea what happens off-chain, but it can tell who is right or wrong when **conflicts happen**, and the result is **trusted**.
- When someone wants to **withdraw/exit**, he or she needs to provide the **proof of possession**.

What is off-chain scaling?

A high-level example



What is off-chain scaling?



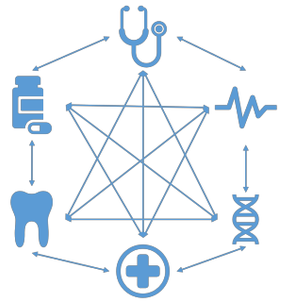
- Application in need of scalable, fast and reliable blockchain infrastructure
- Traditional database techniques can be used

- The implementation of off-chain protocols depend on the use case
- Expose an API to the upper layer, so that public nodes can verify the integrity inside the network

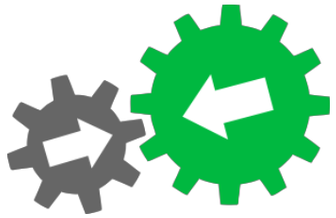
- Provides trustless services to the upper layer

What is off-chain scaling?

Privacy



Interoperability



Backward Compatibility

Benefits of off-chain solutions

Instant Transactions

Low Fees

Scalability

How do off-chain protocols work?

—— Take Payment Channels & Sidechain for example

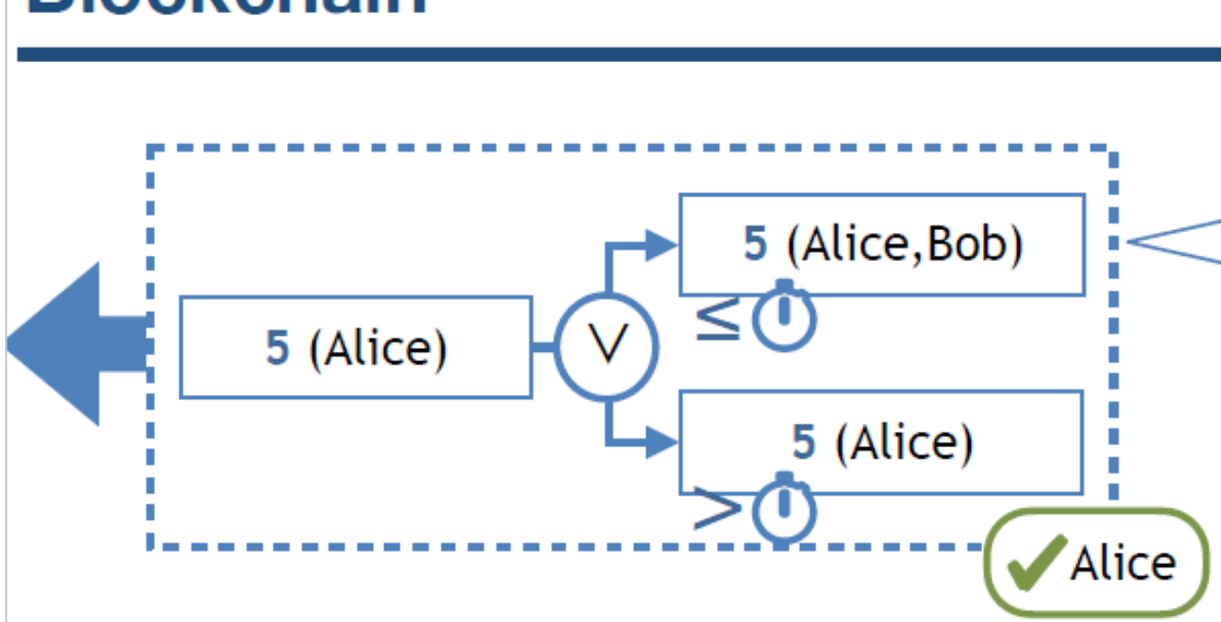
Payment Channels: Open

5

Alice

Bob

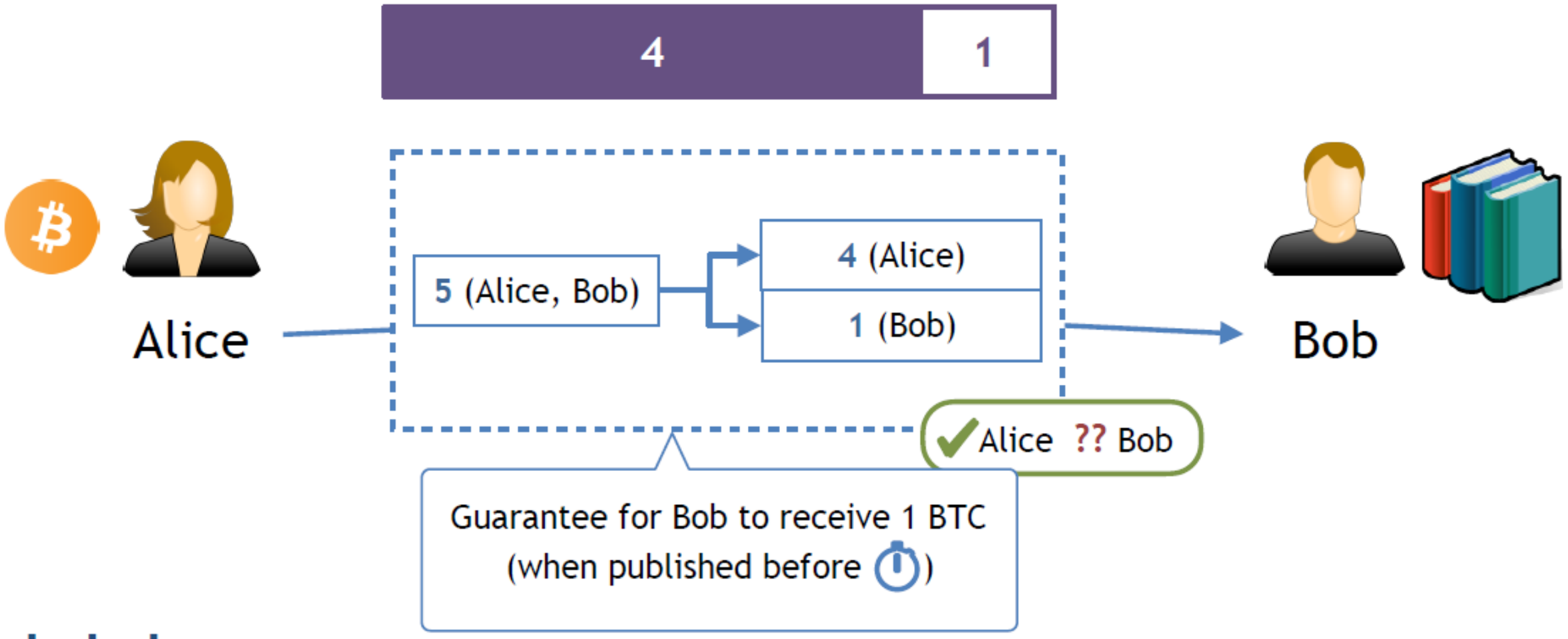
Blockchain



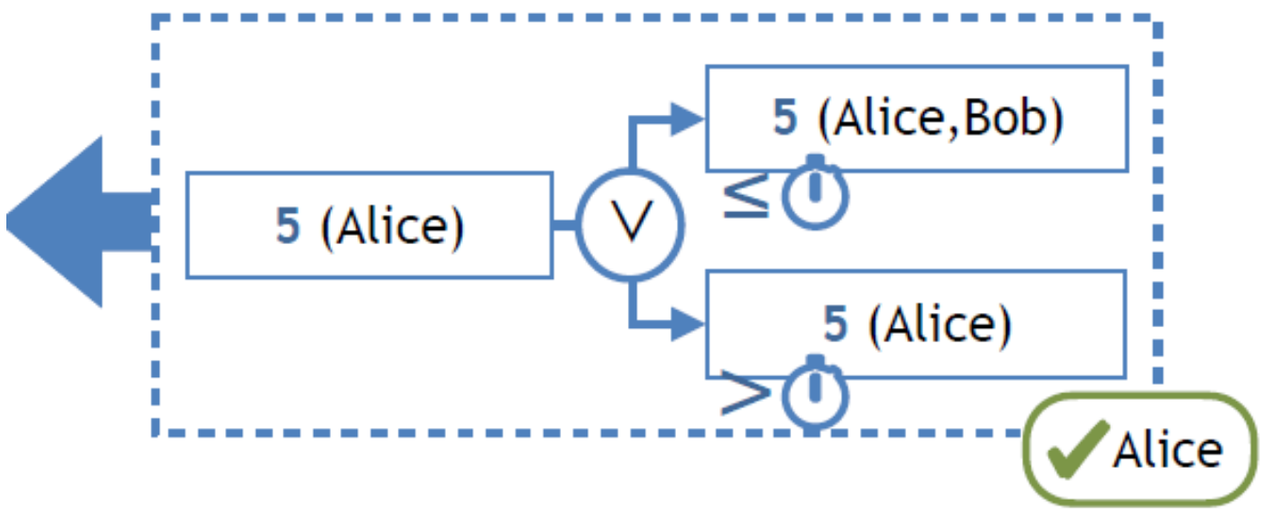
Multisig Contract

Can be spent only with the signatures of both Alice and Bob

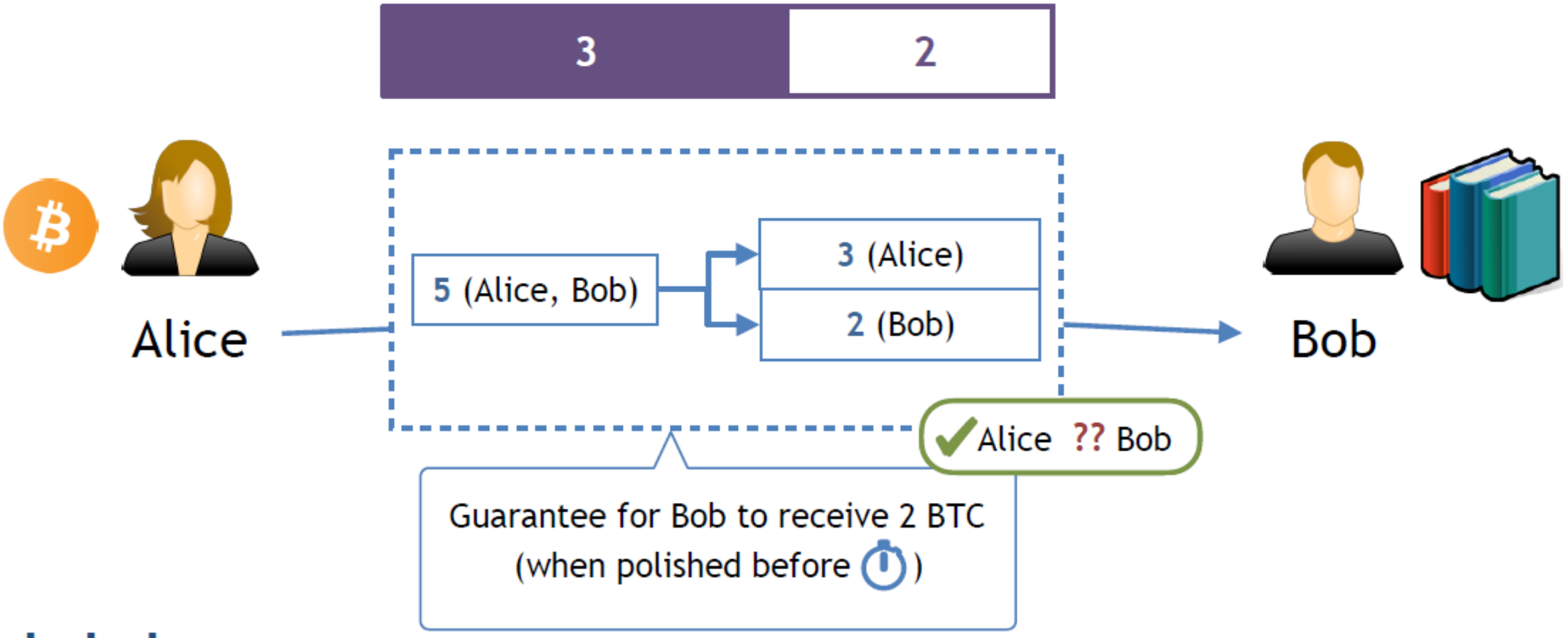
Payment Channels: Transactions



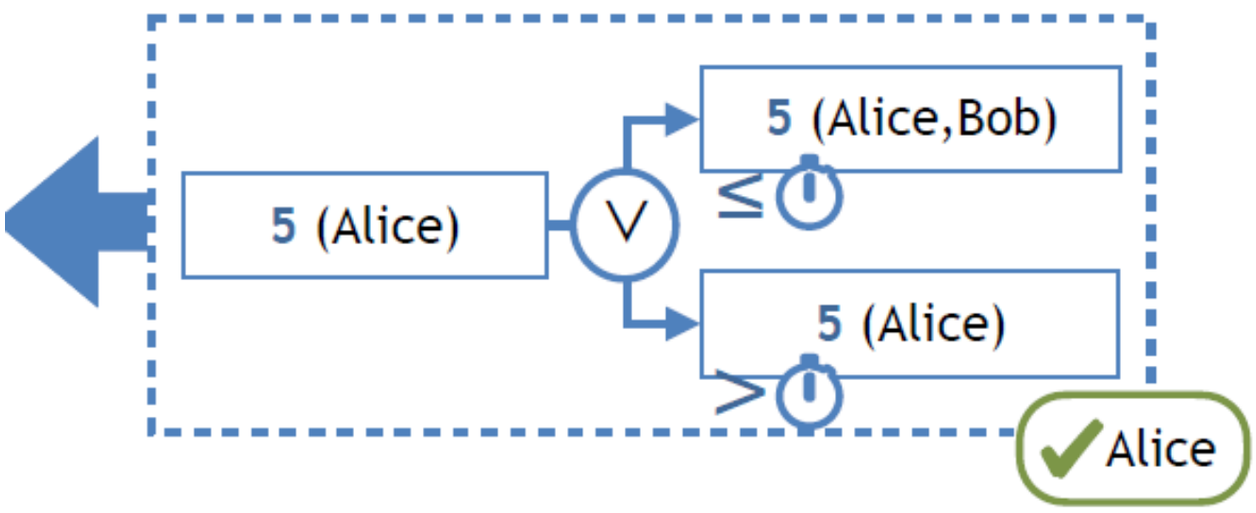
Blockchain



Payment Channels: Transactions



Blockchain

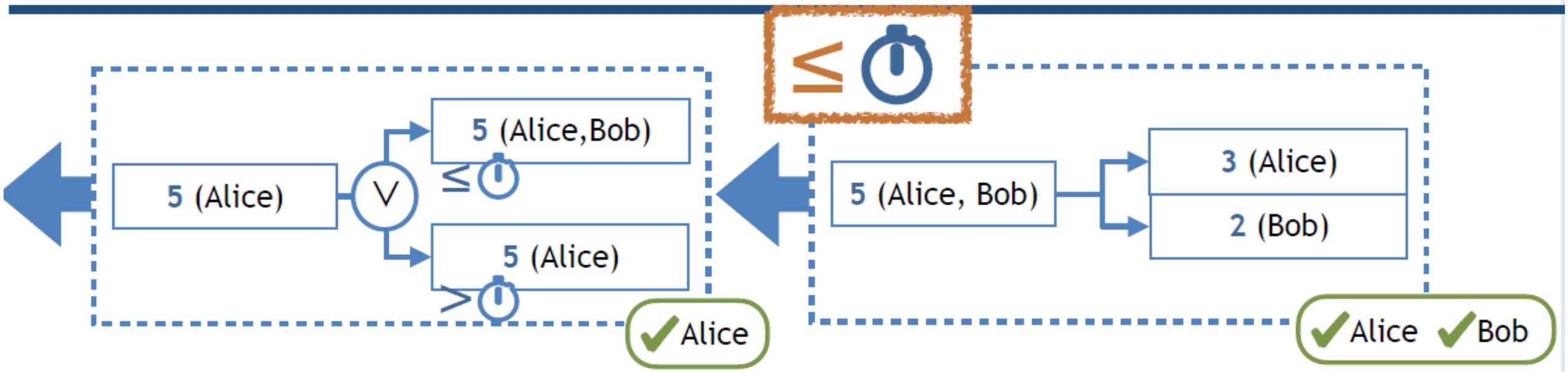


Payment Channels: Close

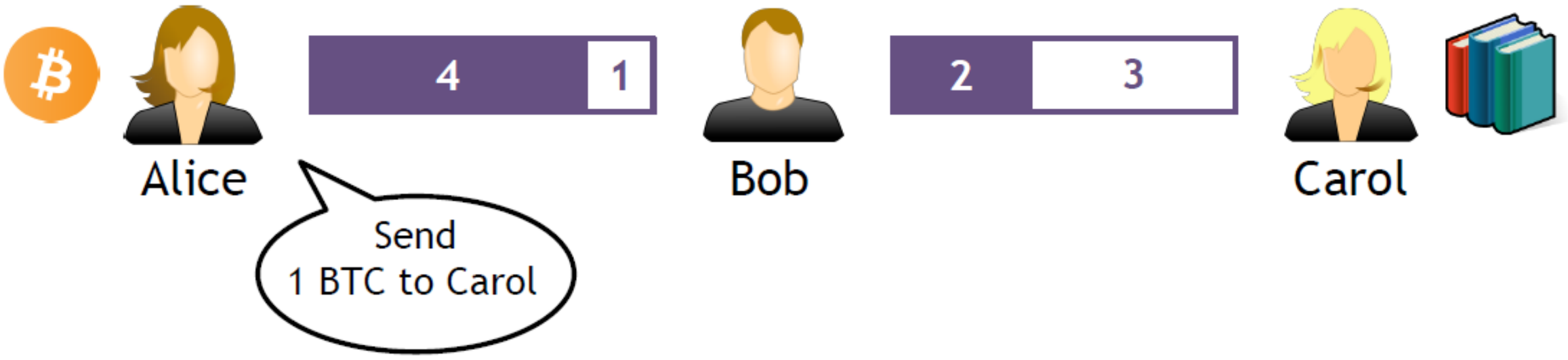
Alice

Bob

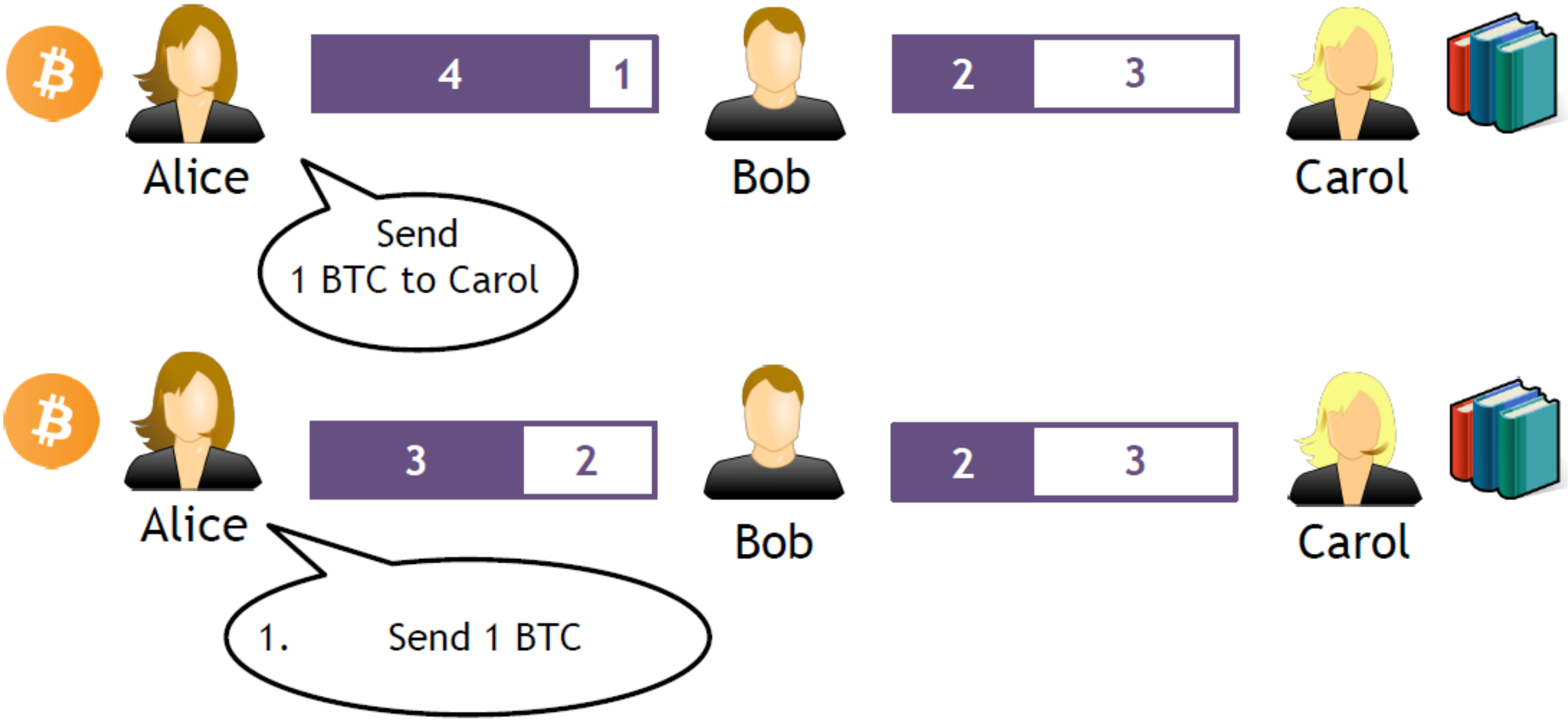
Blockchain



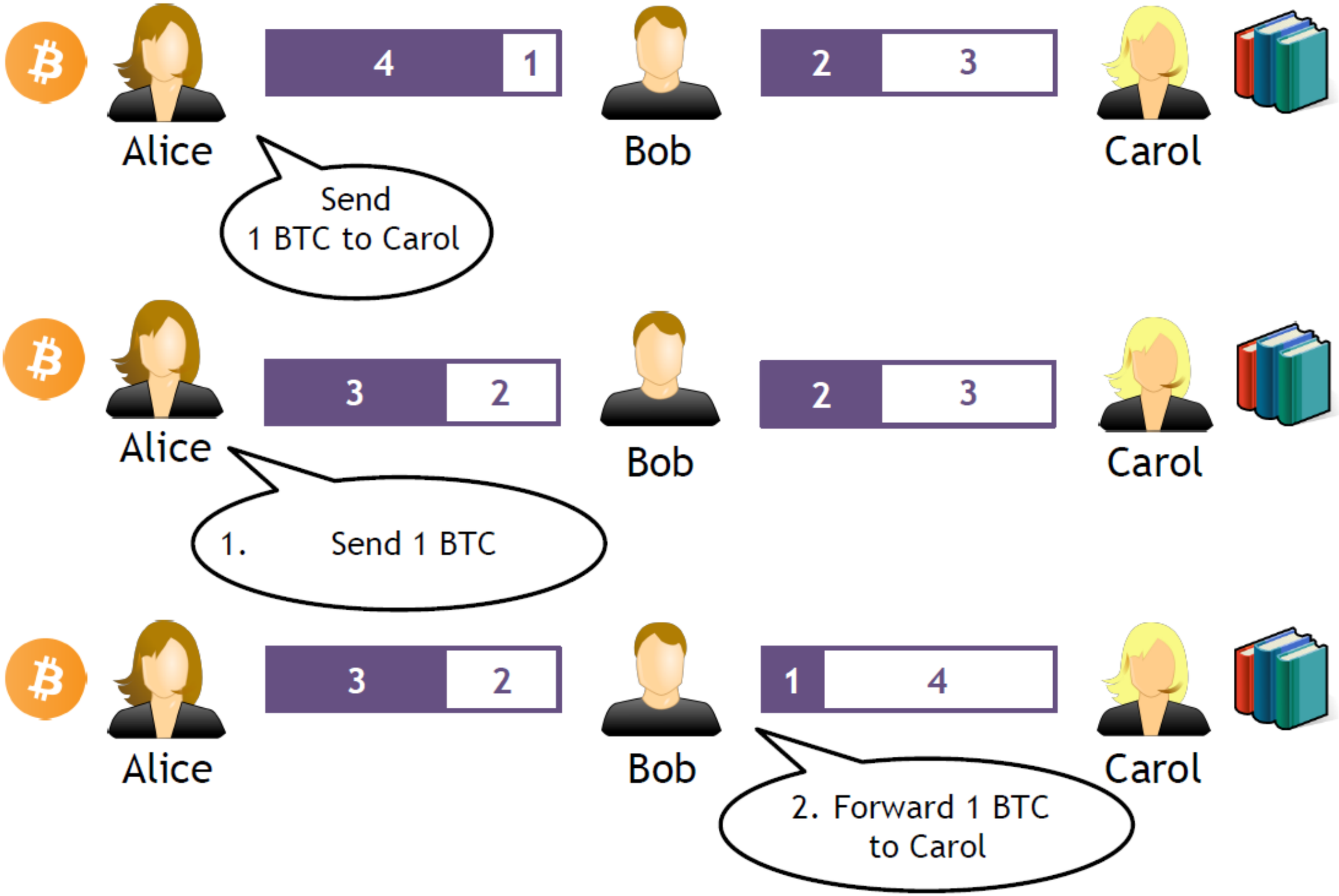
Payment Channel Networks



Payment Channel Networks

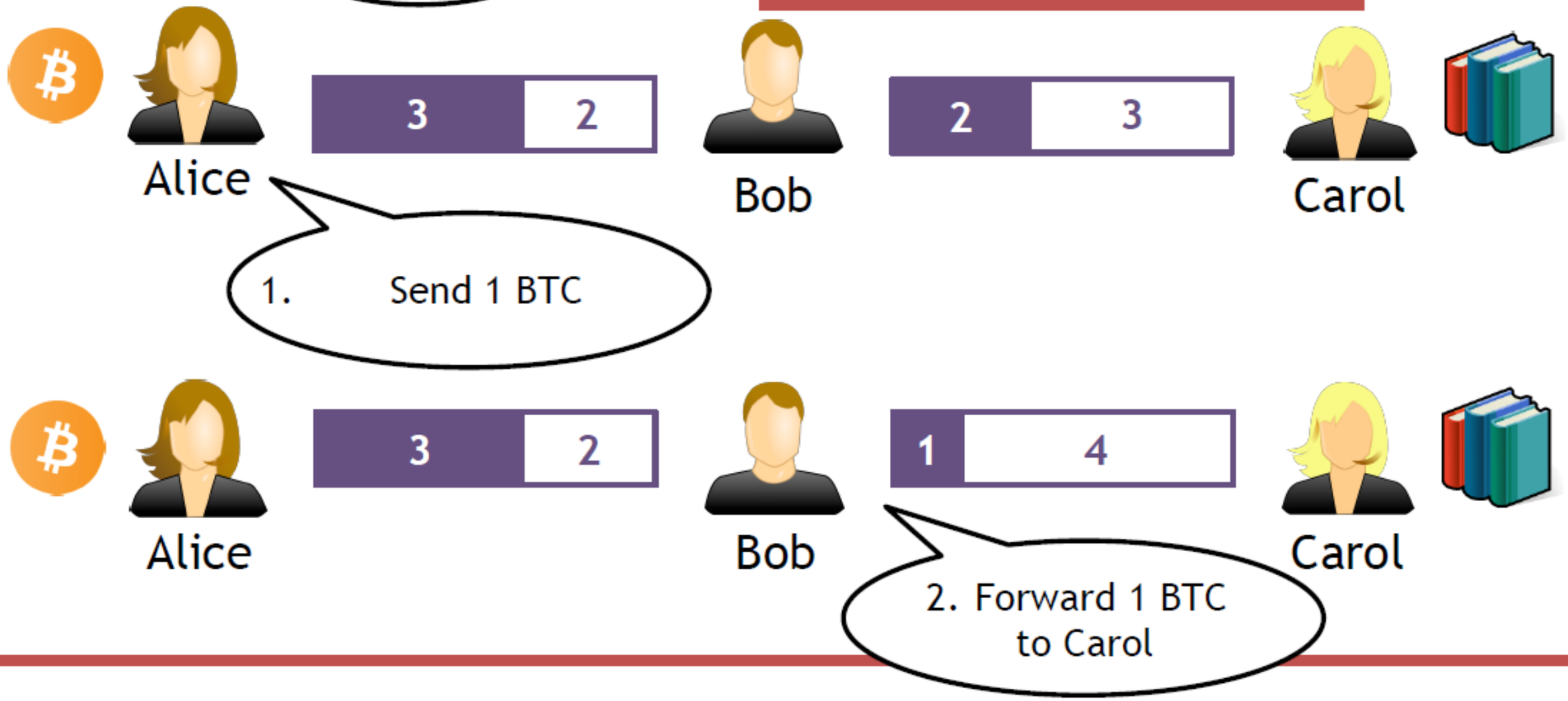


Payment Channel Networks



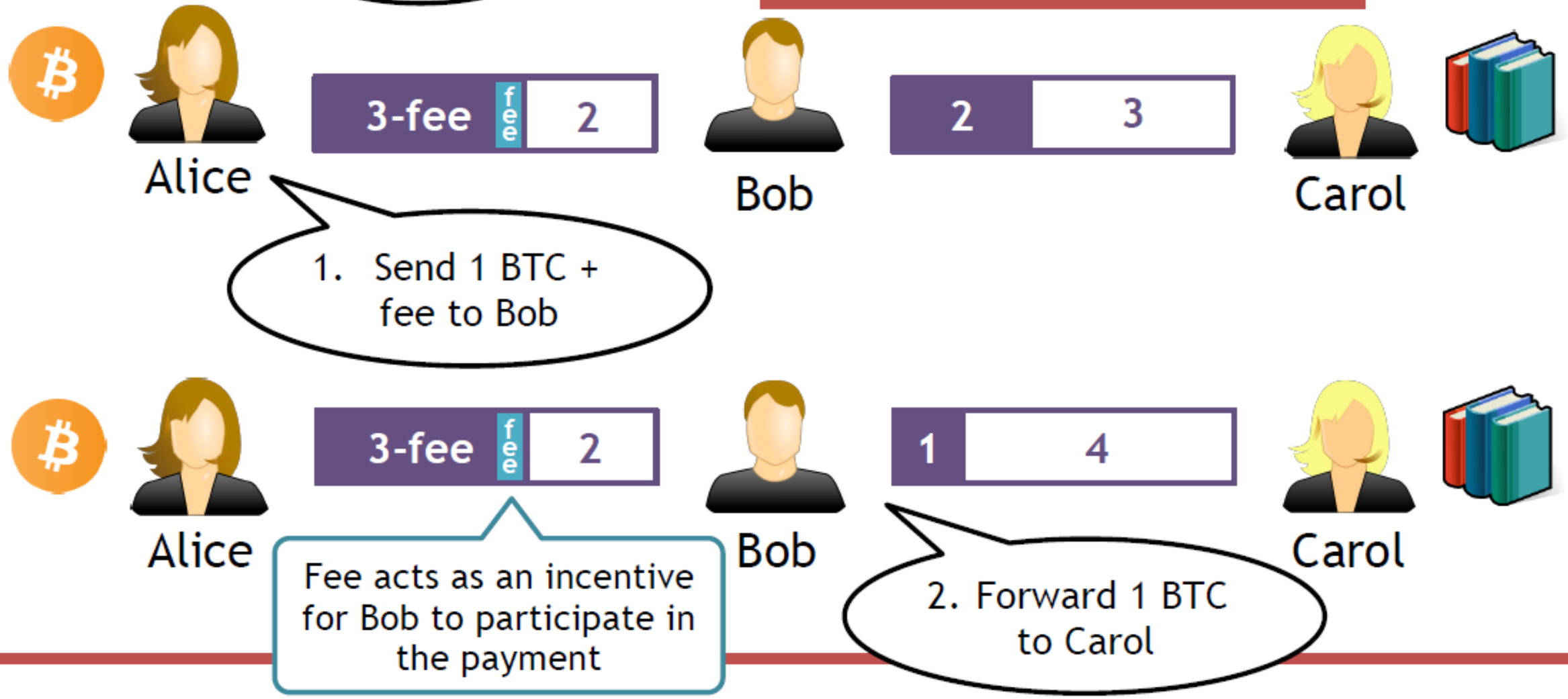
Payment Channel Networks

Should happen atomically

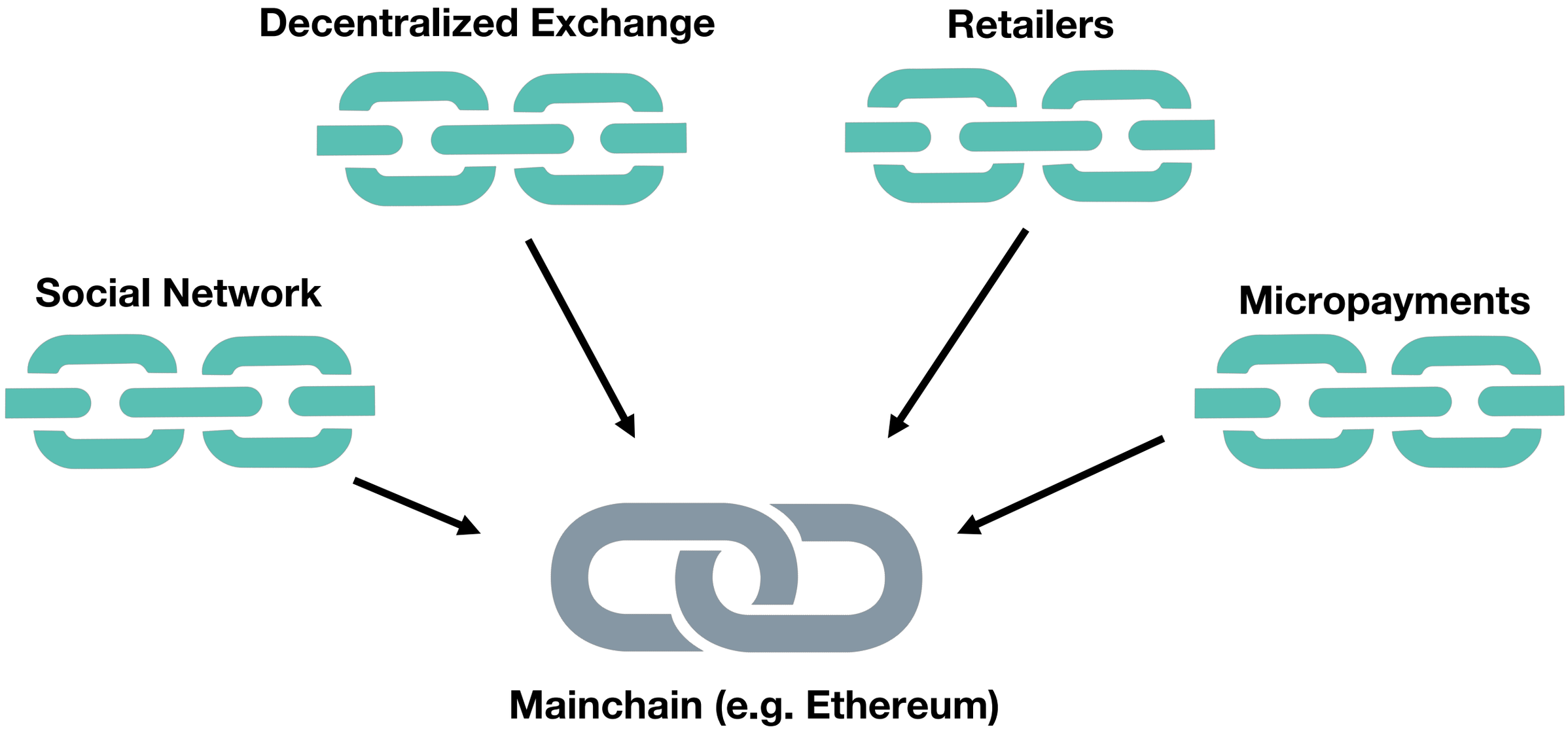


Payment Channel Networks

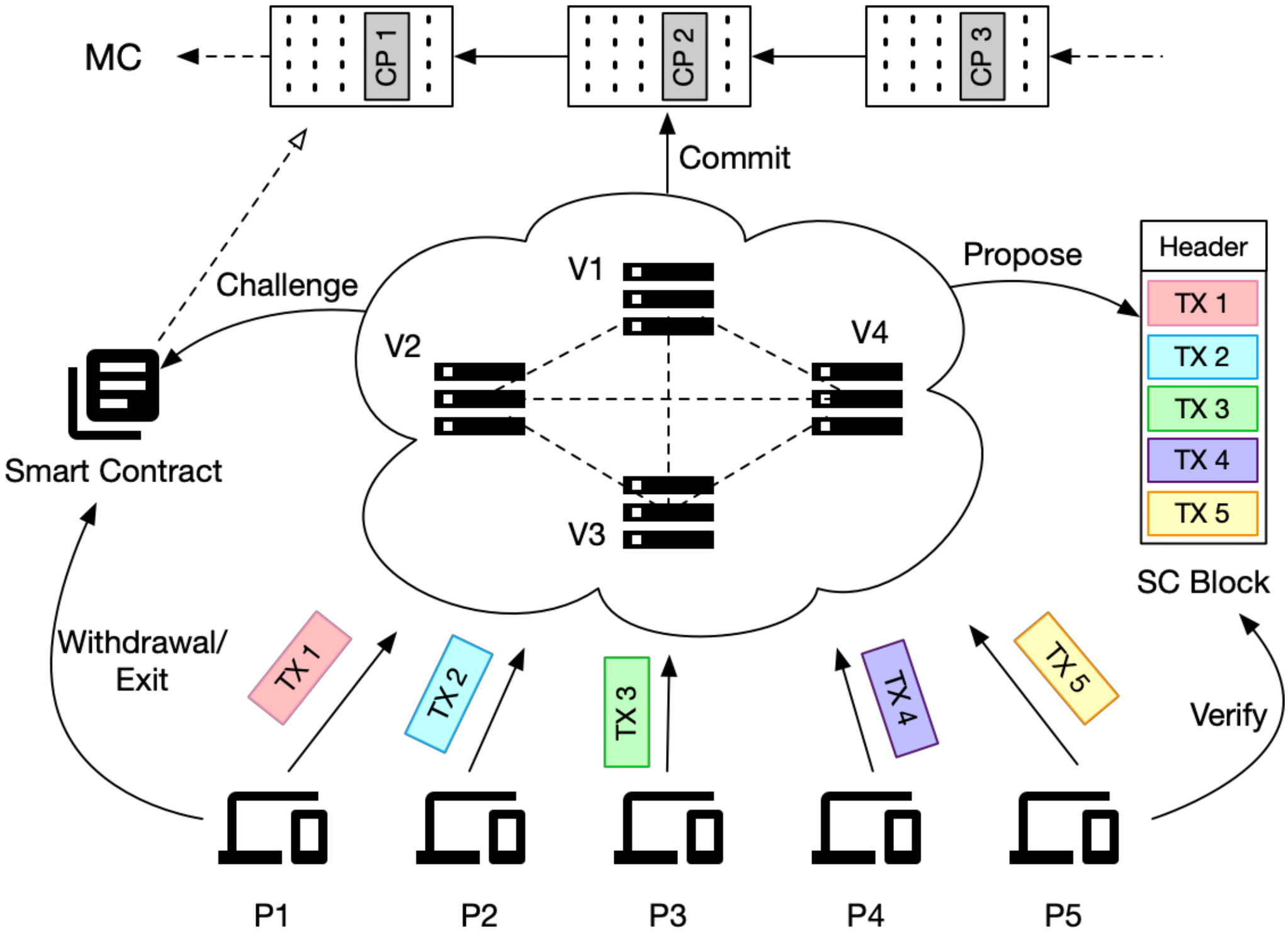
Should happen atomically



Sidechain


Decentralized Exchange
Retailers
Social Network
Micropayments
Mainchain (e.g. Ethereum)

Sidechain


MC
CP 1
CP 2
CP 3
Commit
Challenge
Propose
Header
TX 1
TX 2
TX 3
TX 4
TX 5
SC Block
V1
V2
V3
V4
Smart Contract
Withdrawal/
Exit
Verify
P1
P2
P3
P4
P5

Summary

Open challenges for off-chain protocols

- Online Watchdog Requirements
- Long withdrawal/exit time
- Withholding attack
- Locked and Fragmented Collateral
- Introduce new attack plane

Thanks!

Scale-Out Blockchains
Off-Chain Scaling
Q&A

Fangyu Gai, Ph.D. student, supervised by Dr. Chen Feng

University of British Columbia – Okanagan Campus

April 23, 2019

https://medium.com/coinmonks/blockchain-101-4acc9902b3a4