Life and Times of a BitShares Operation

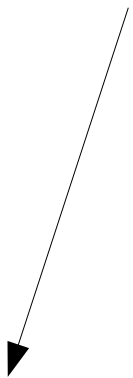
Michel Santos
BitFest Amsterdam
September 22, 2018

Context

Technical introduction to the mechanics of BitShares operations

Familiarity with
- public-private key cryptography
- blockchain fundamentals

Bonus material available online



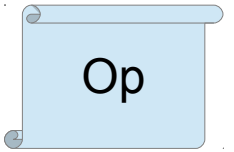
Bonus
Blockchain Fundamentals

Smart Contracts and Operations

BitShares platform contains various smart contracts

- Asset Issuance
- Transfers
- Decentralized Exchange (DEX)
- Governance

Events in these contracts can be triggered with valid operations



Bonus
BitShares Whitepapers
dev.bitshares.works

Case Study
Alice's Limit Order

Alice has an account on BitShares that holds 200 bitEUR

Alice wants to place an order on the BitShares decentralized exchange

Offering up to 11.5 bitEUR for 100 bitCNY (0.115 bitEUR per bitCNY)

What are the mechanics?

Step 0: Account on BitShares

Alice having an account on the blockchain means

(a) her account name (“alice”) was registered on the blockchain

(b) her account is associated with a set of keys: owner, active, memo

Public Key Private Key

Bonus
Genesis accounts
Registrars
Accounts have three keys
Complex multi-signature accounts

Step 1: Wallet Software

Alice will use her wallet software of choice

- Web browser wallet
- Desktop wallet software
- Mobile phone software

Alice should evaluate the trust of the developers and the trust of the software source

Alice will be loading her account's private keys into the wallet software!

- If the software is malicious or hacked, then her private keys are exposed

Bonus
Beet

Step 2: Create and Sign the Transaction

Alice will use her wallet software to create the operation and sign It with her account's private side of the active keys

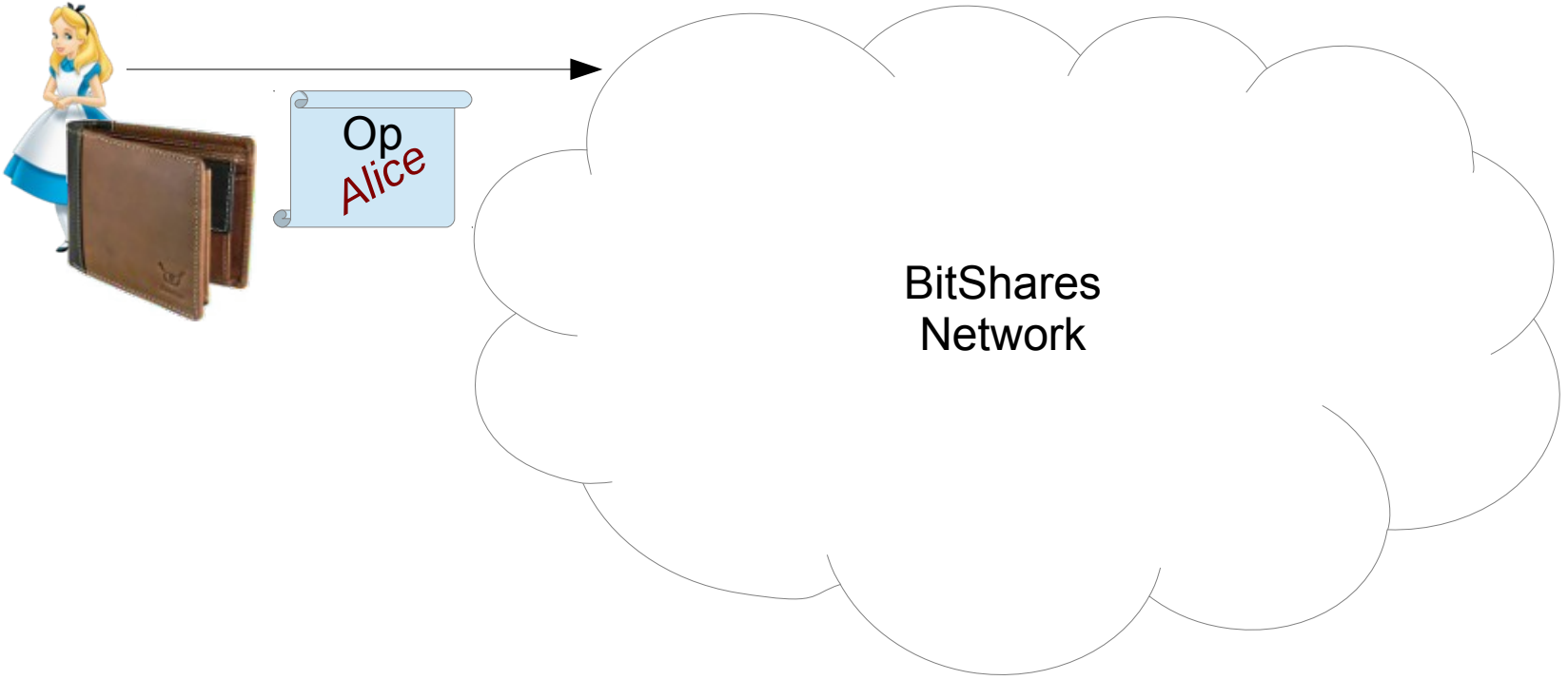
Alice actually signs <u>the transaction containing the operation</u>

A single Graphene transaction can contain thousands of operations

Bonus
Blocktivity.info
Transaction signing

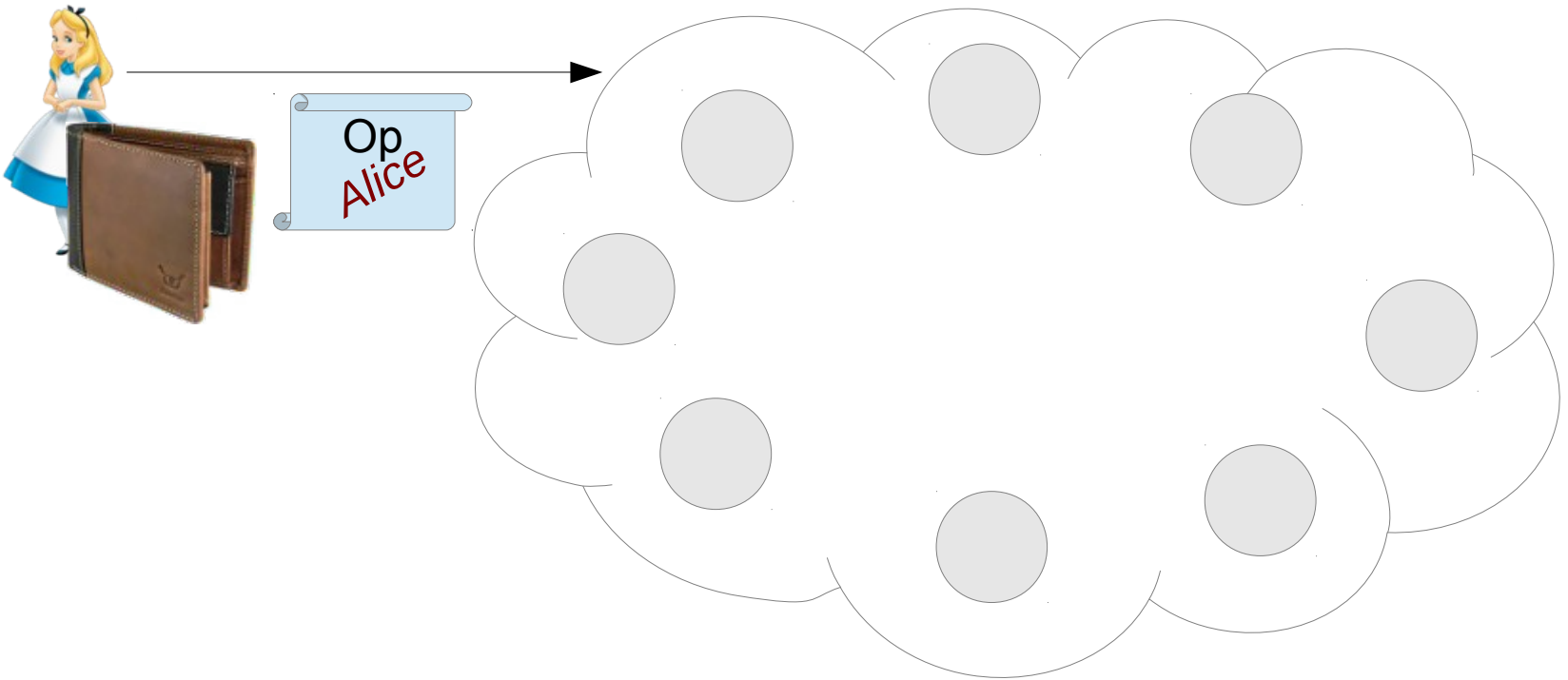
Step 3: Submit Transaction to Network

Alice will use her wallet software to submit the transaction to the network



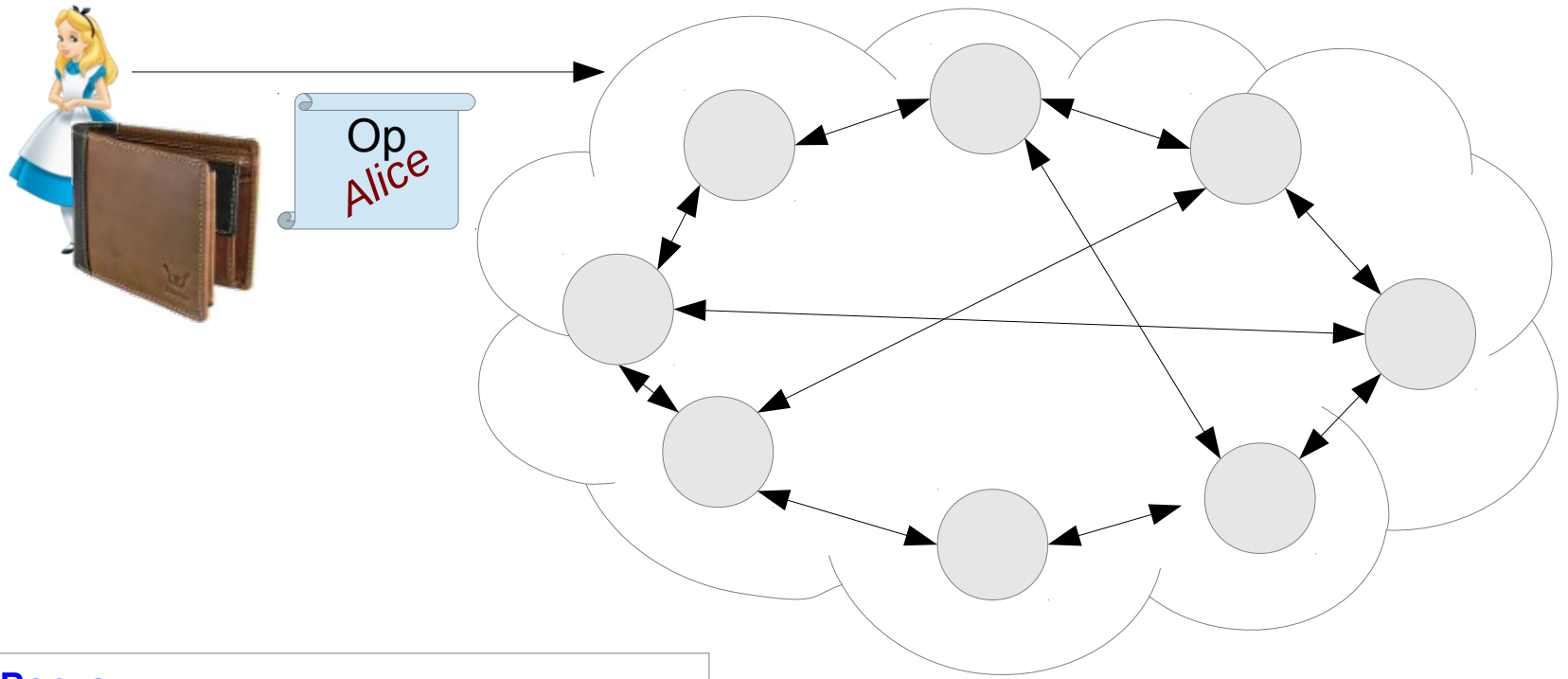
Step 3: Submit Transaction to Network

Network consists of distinct nodes



Step 3: Submit Operation to Network

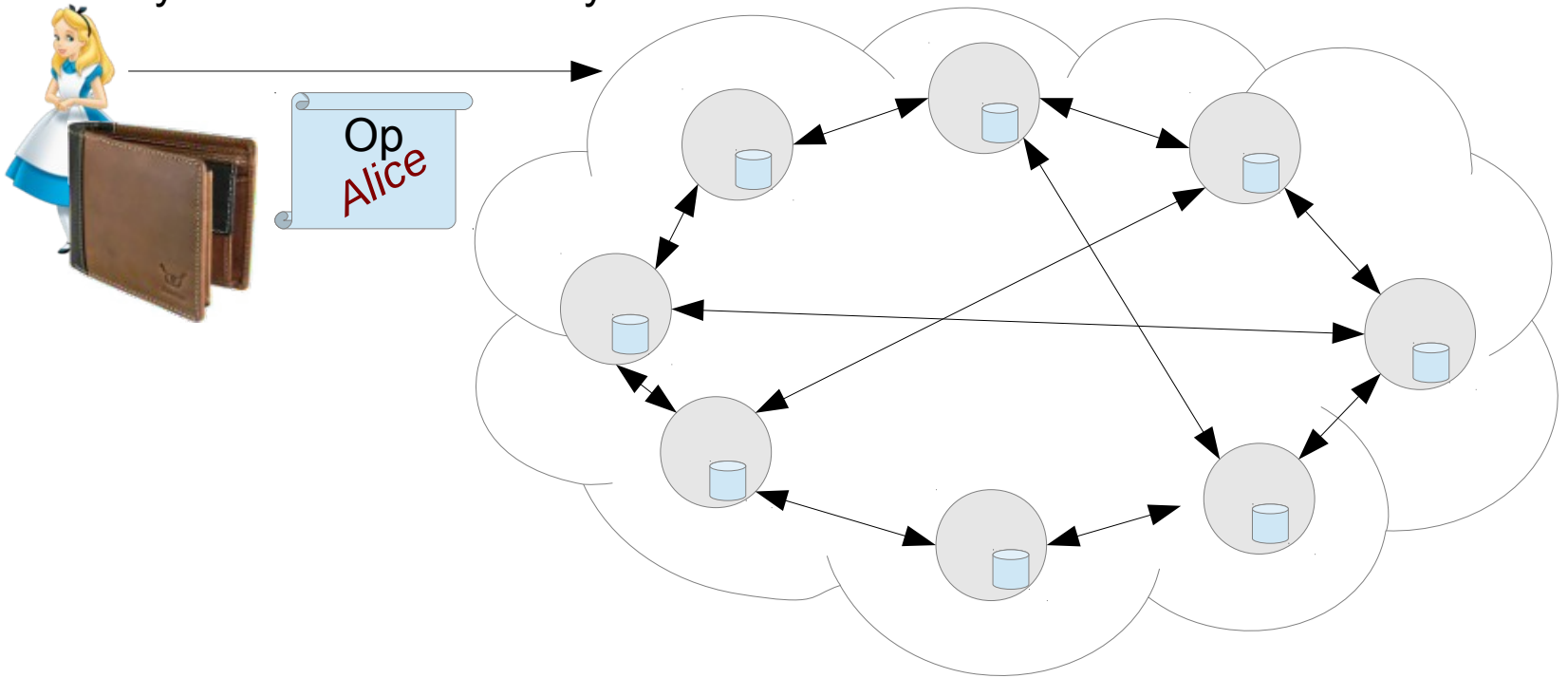
Every node is connected to some other nodes through the peer-to-peer network (P2P)



Bonus
Bootstrapping the known seed nodes

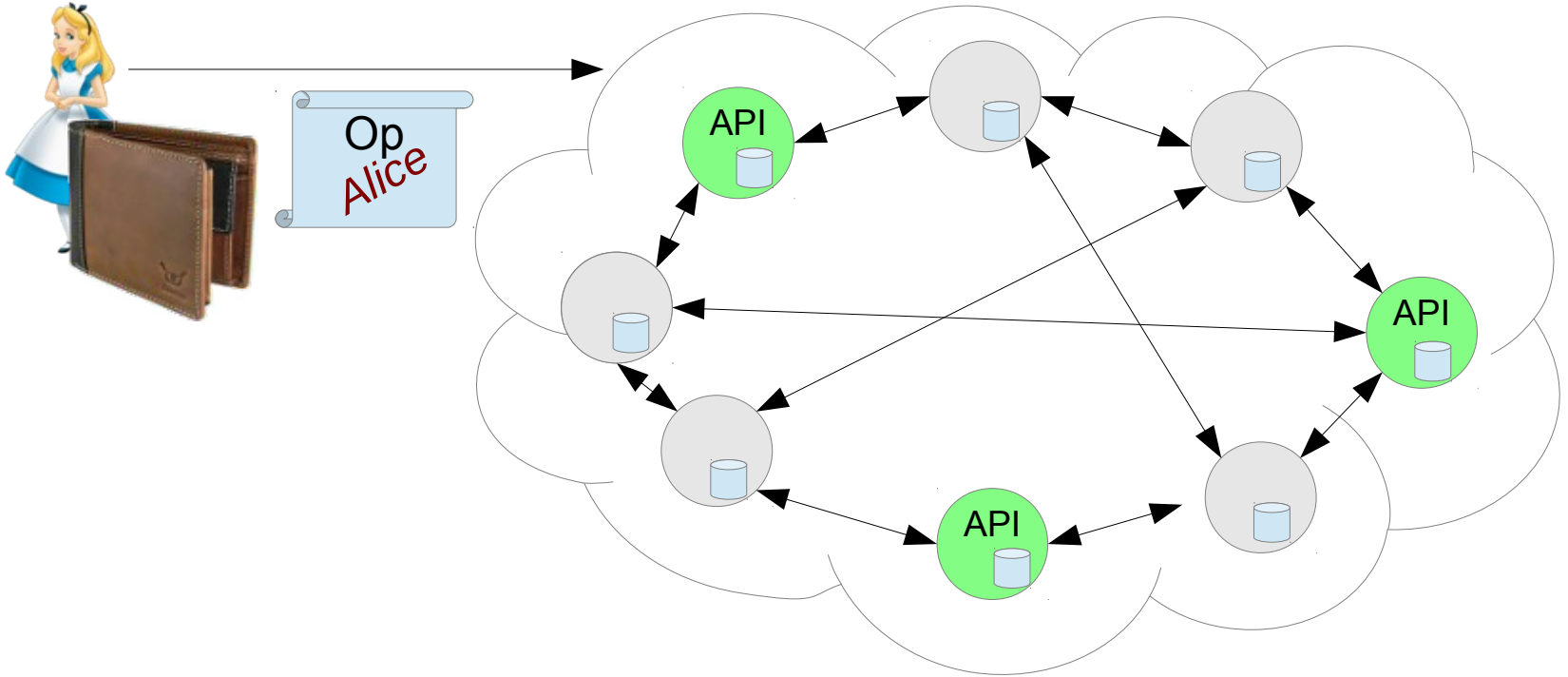
Step 3: Submit Operation to Network

Every node maintains its own record the entire blockchain history and current state
Every node validates every transaction



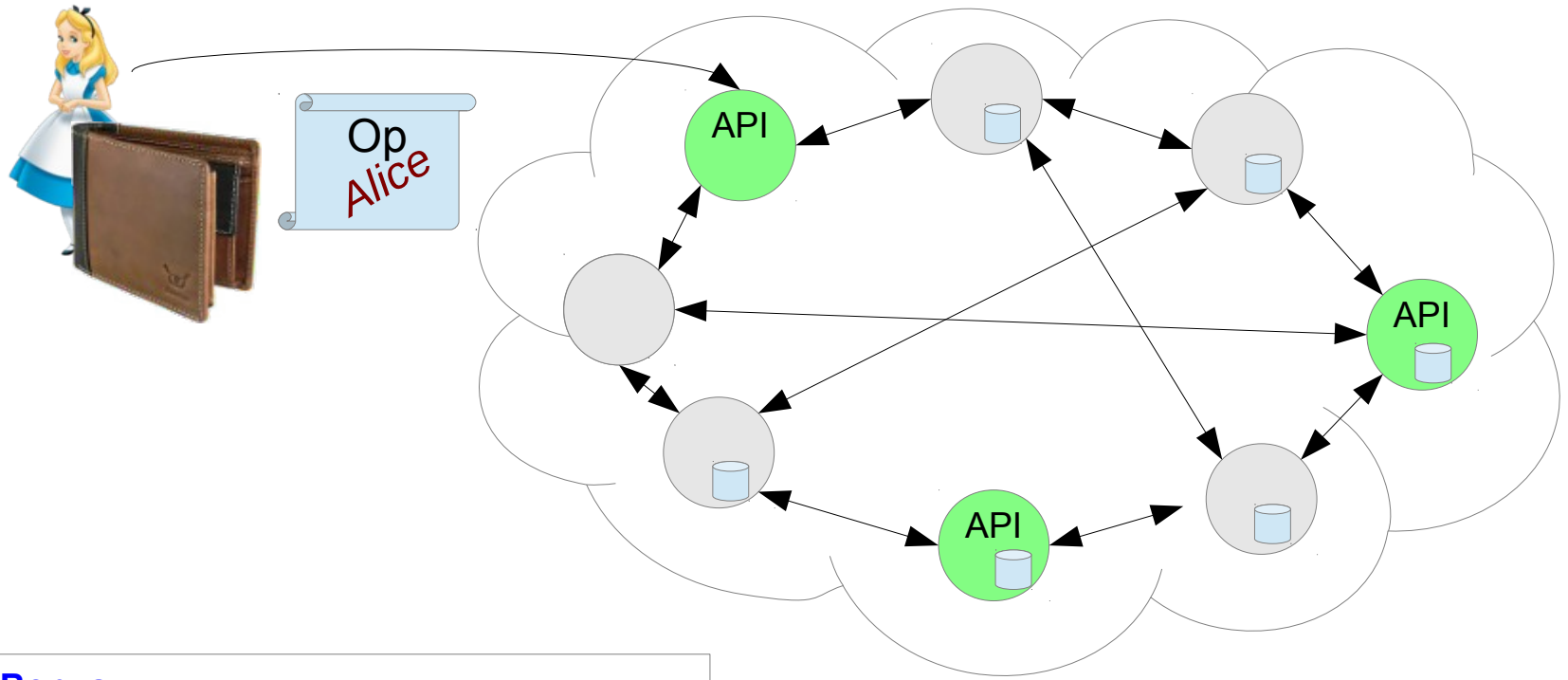
Step 3: Submit Transaction to Network

Only some of the nodes are open to accepting new transactions



Step 3: Submit Transaction to Network

Alice actually submits her transaction to a specific API node

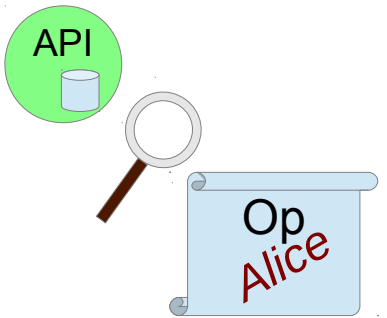


Bonus
Bootstrapping the known API nodes

Step 4: Node Pre-Validates the Transaction

The API Node validates the transaction

Is the transaction signature valid?
Is operation consistent with itself?
Is operation consistent with blockchain?



Even if valid, the transaction is is not yet officially embedded into the blockchain!

Bonus
Definition of pre-validation

DPOS

DPOS
Delegated Proof of Stake

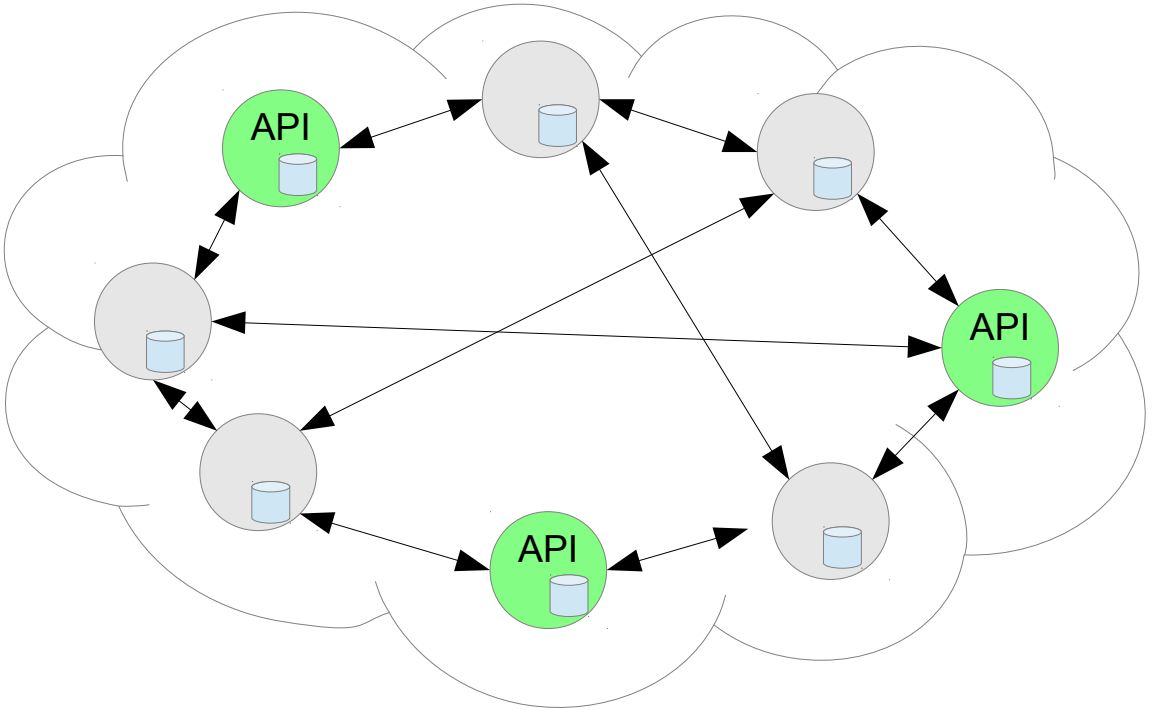
BitShares is a DPOS blockchain

Holders of the core token (BTS) vote on
- who can certify new data (produce new blocks)
- who can set blockchain parameters (Committee member)
- which endeavors should be funded from the Reserves (Worker Proposals)

Account votes are multiplied by the core tokens held by an account

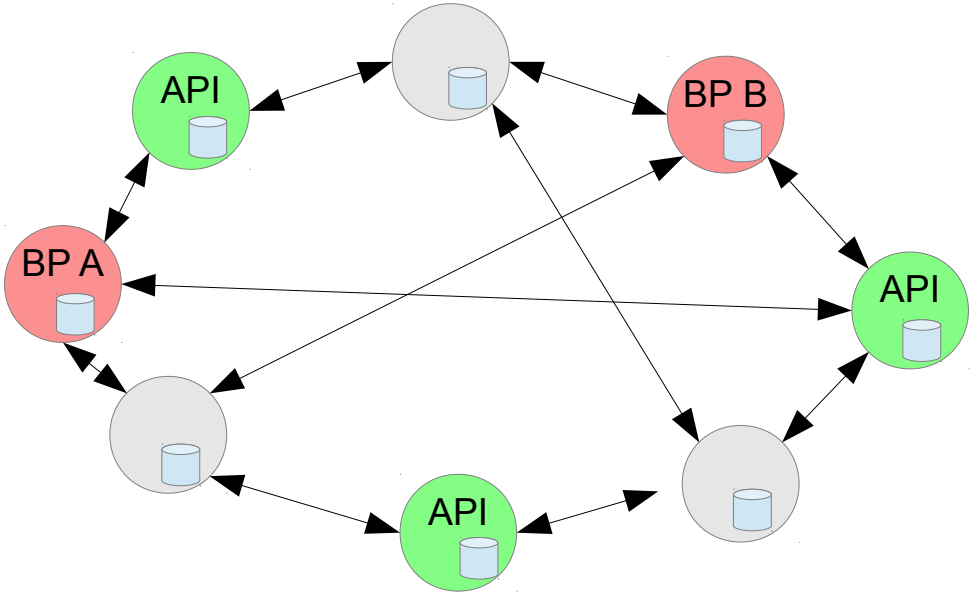
DPOS

API Nodes cannot certify new data



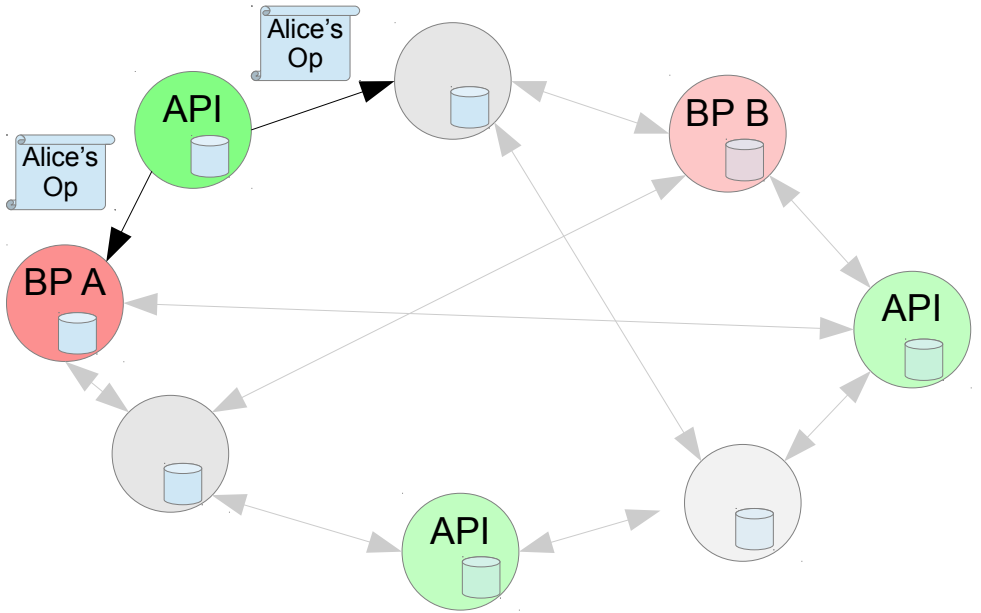
DPOS

Only block producer nodes can certify new data into the blockchain



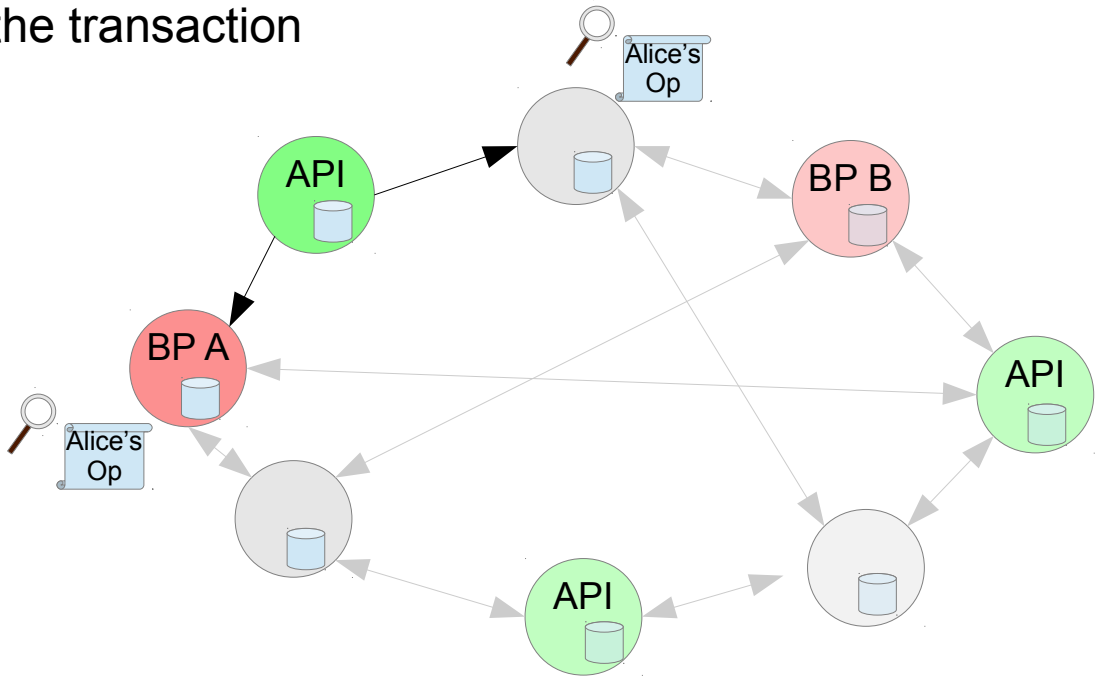
Step 5: Node Transmits the New Transaction to Its Peers

The API Node transmits the new transaction to its peers



Step 6: Node Receives the New Transaction From Its Peers

The connected nodes receive the new transactions from its peers
And pre-validates the transaction

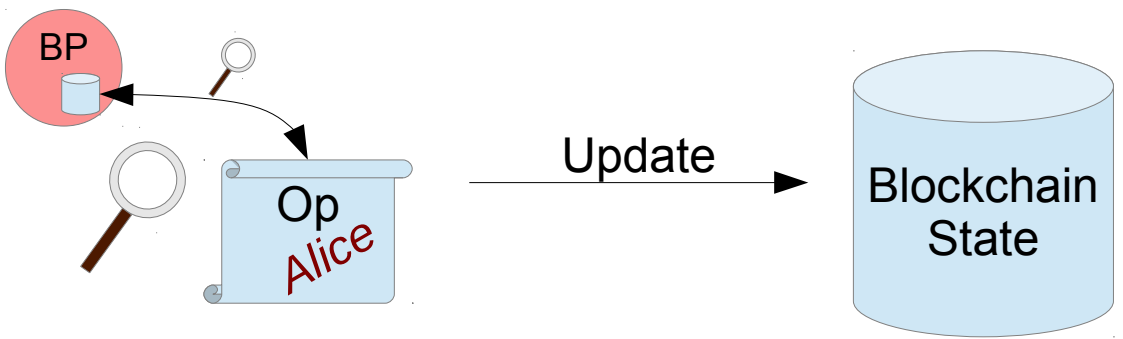


Step 7: BP Triggers the Relevant Smart Contract

Transaction is fully validated

Operation now triggers the relevant smart contract

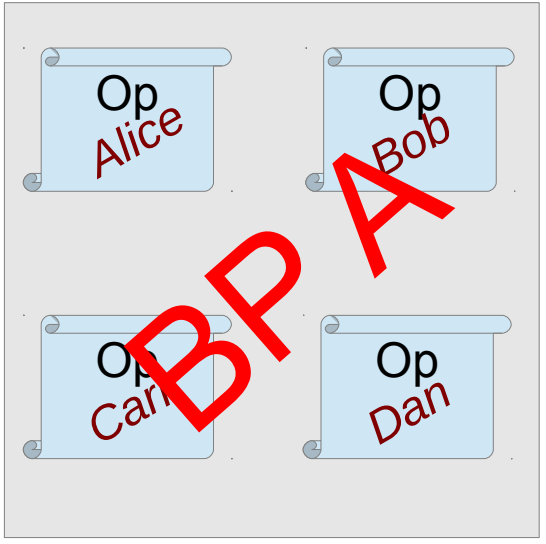
State of the blockchain changes according to the smart contract rules



Step 8: BP Certifies New Block Block

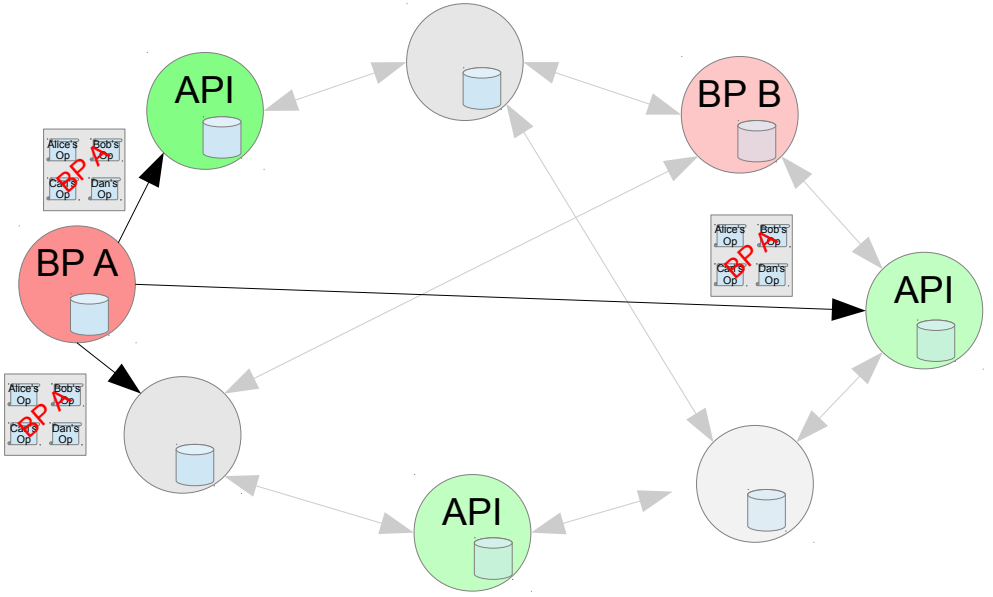
Transaction is now included into the next block

Signed/certified by the BP



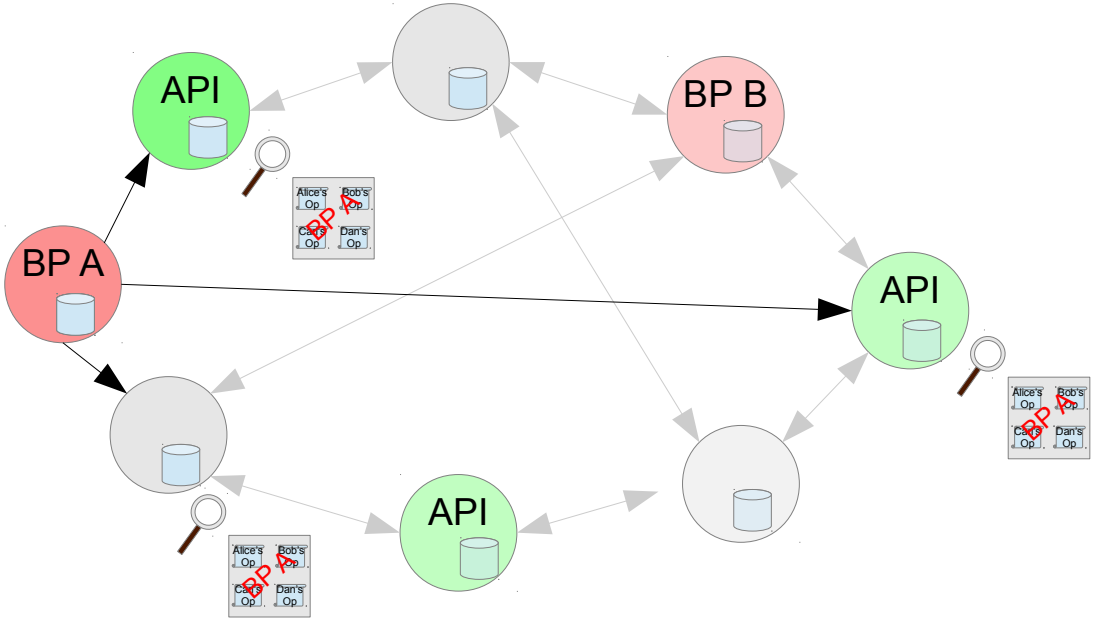
Step 9: BP Transmits New Block

BP now transmits the new block to its connected peers



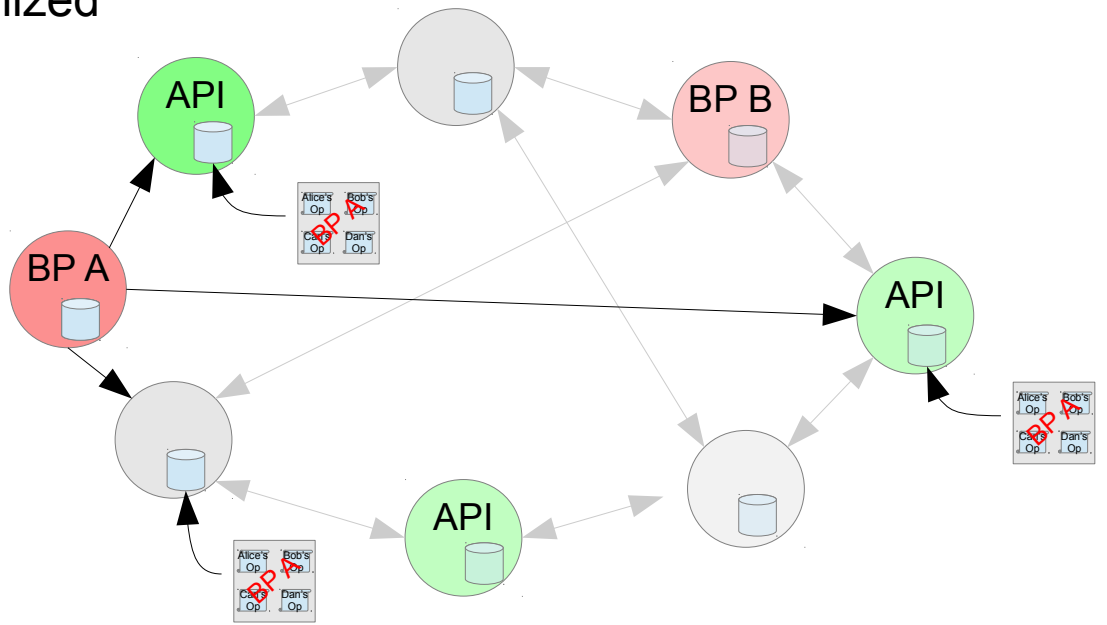
Step 10: Nodes Receive New Block

Other nodes receive the block
Inspect authenticity of the block



Step 11: Other Nodes Trigger Their Smart Contracts

Block is added to each node's blockchain
Relevant smart contracts are triggered
Nodes are now synchronized



Bonus
State Representation versus Consensus

Operation Endures in the Network

Effects of the operation now persist on the blockchain and affect the current and future state of the blockchain forever