Gentle Introduction to Blockchains

Orfeas Stefanos Thyfronitis Litos
PhD in Cryptography and Blockchains
University of Edinburgh

11/10/2019

Outline

- Why it works
- Smart contracts
- Types, ideas and the future

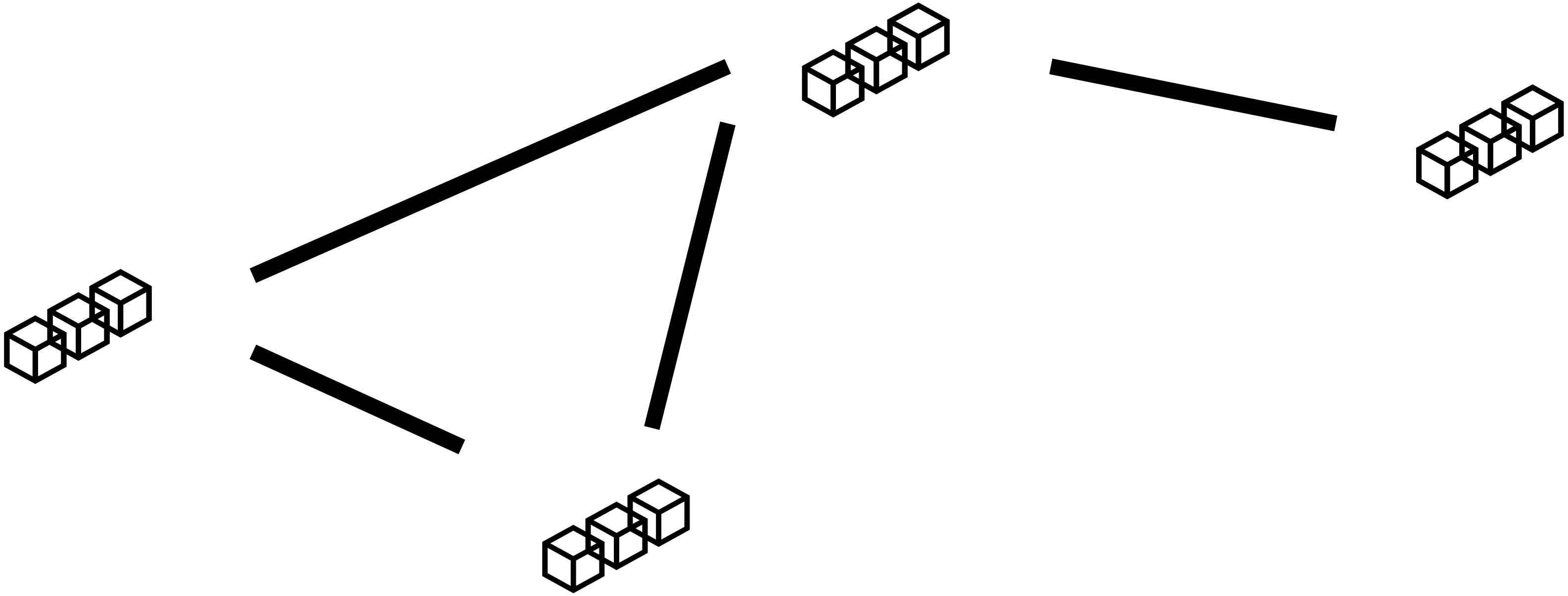
Part I

Why it works, or a Bitcoin primer

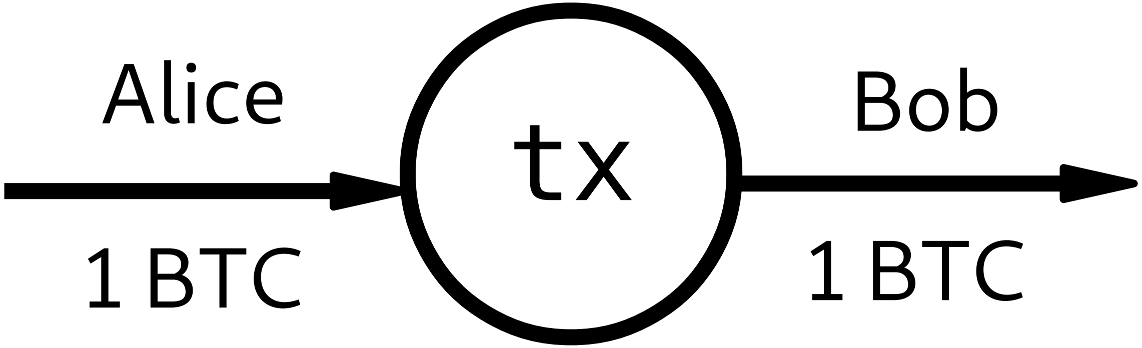
What is a Blockchain?

- distributed,
- append-only,
- transaction ledger

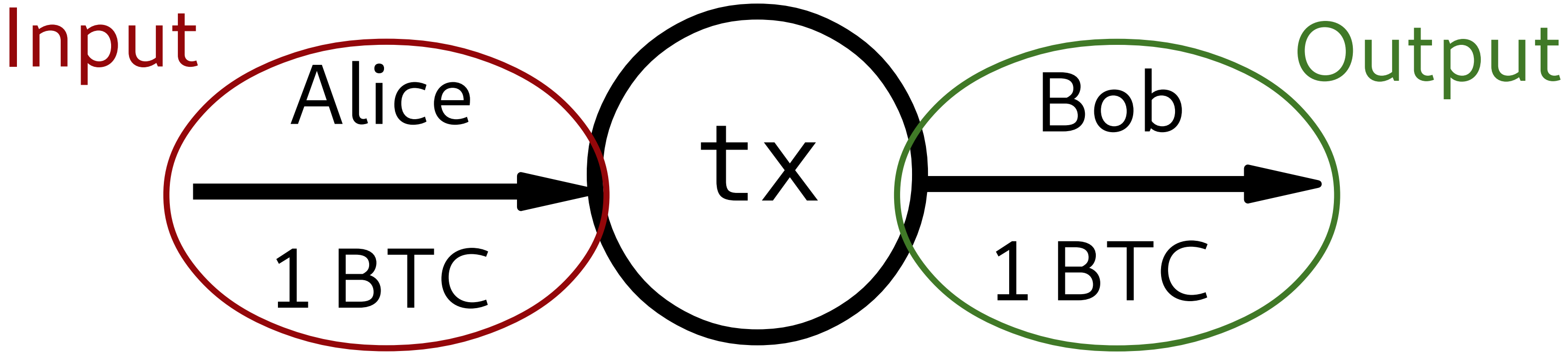
What is a Blockchain?



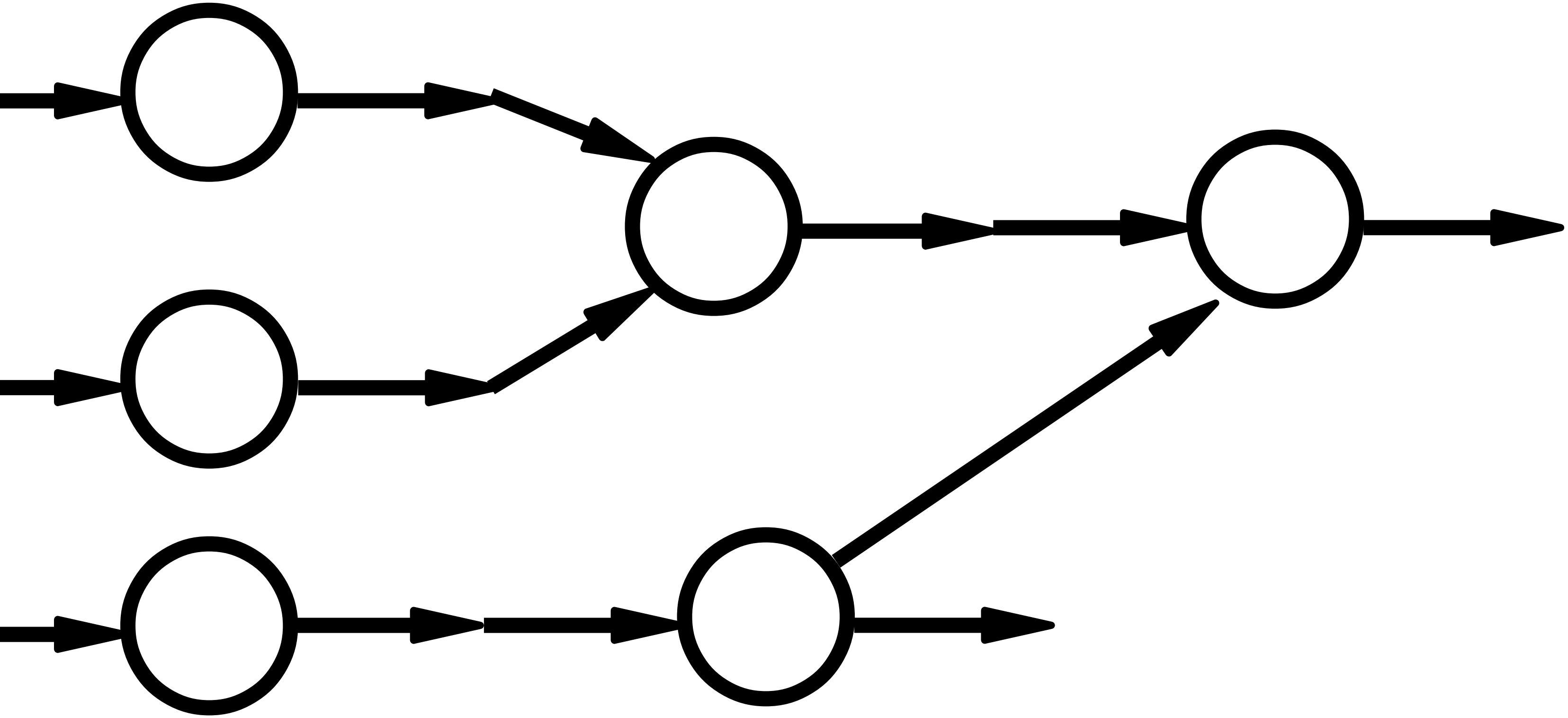
Transactions



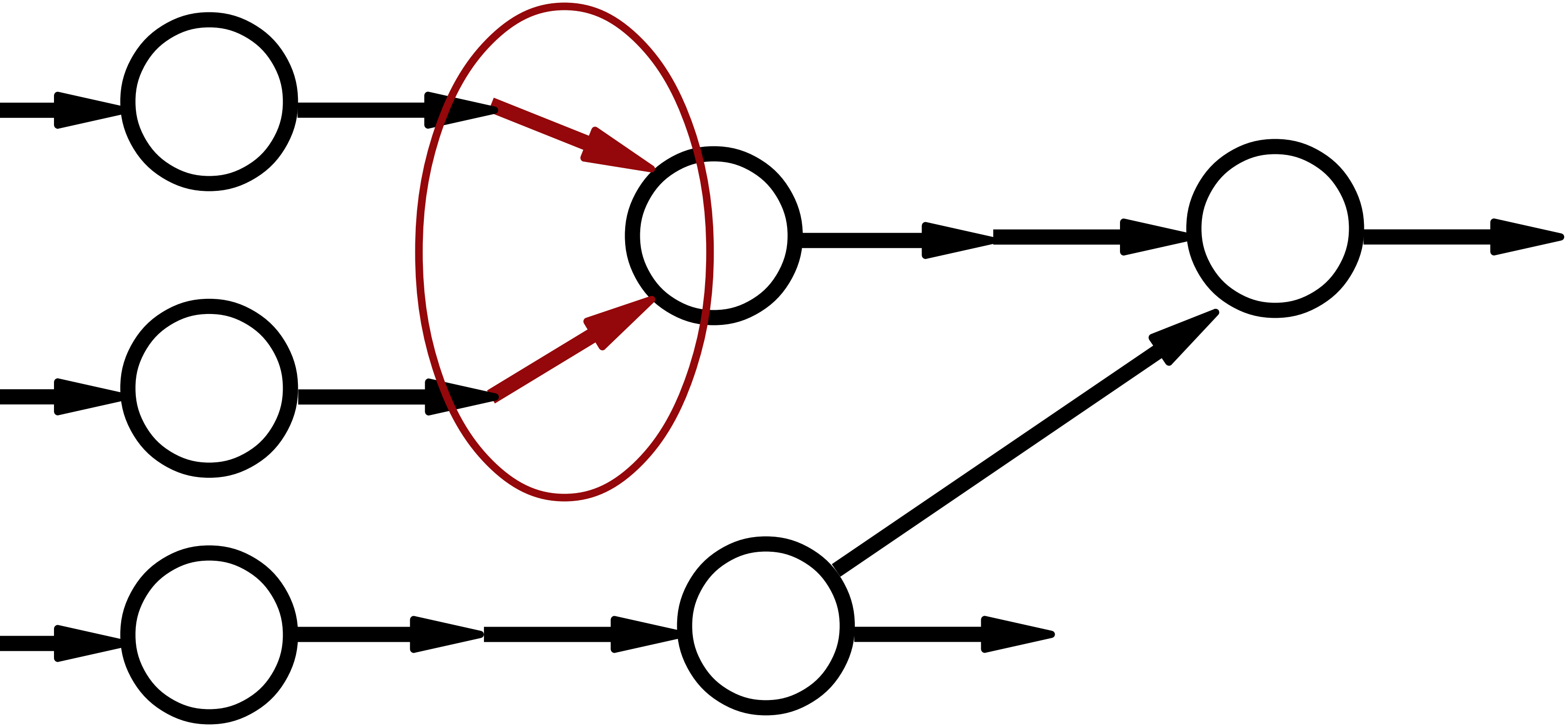
Transactions



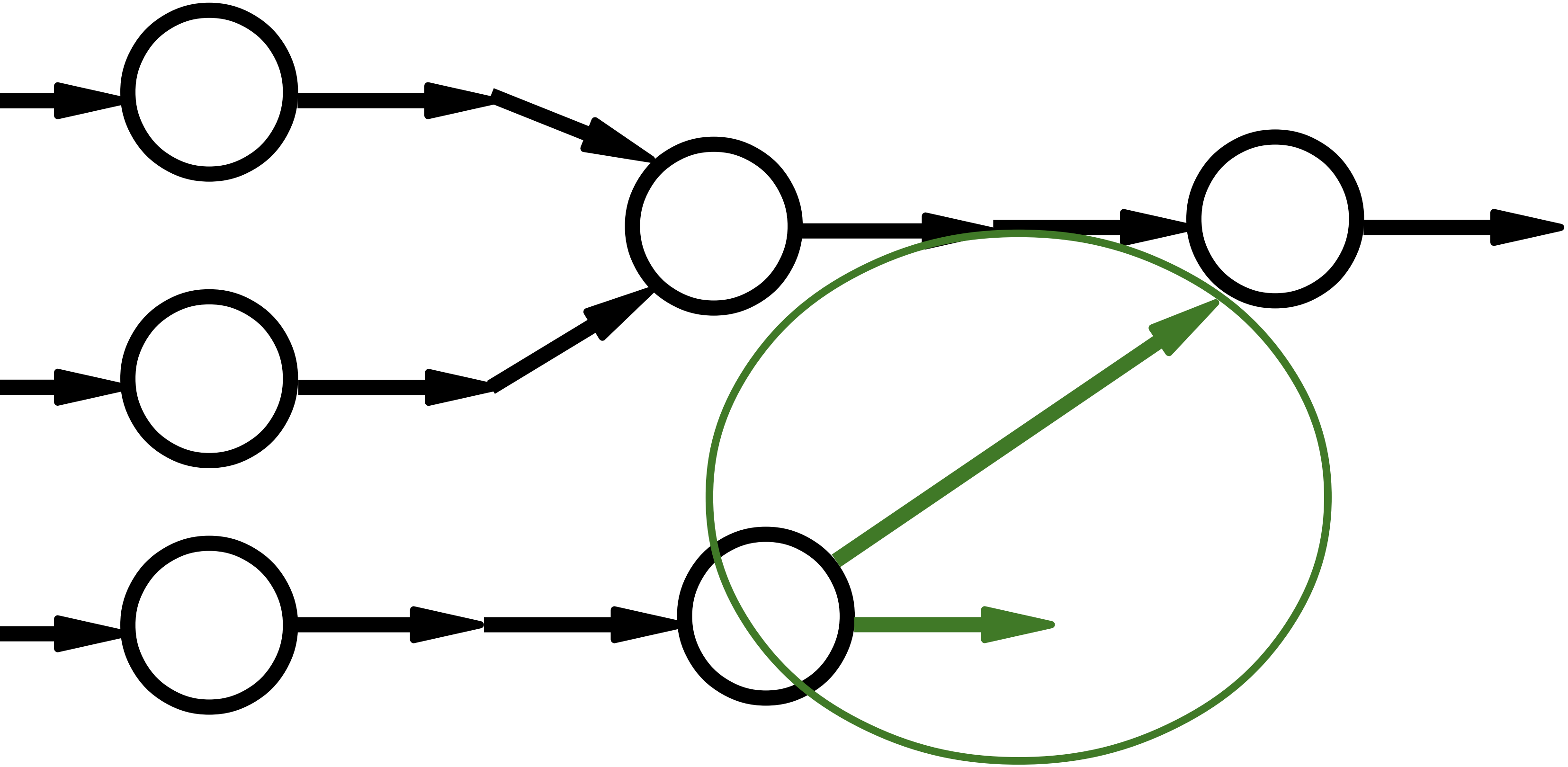
Transaction Graph



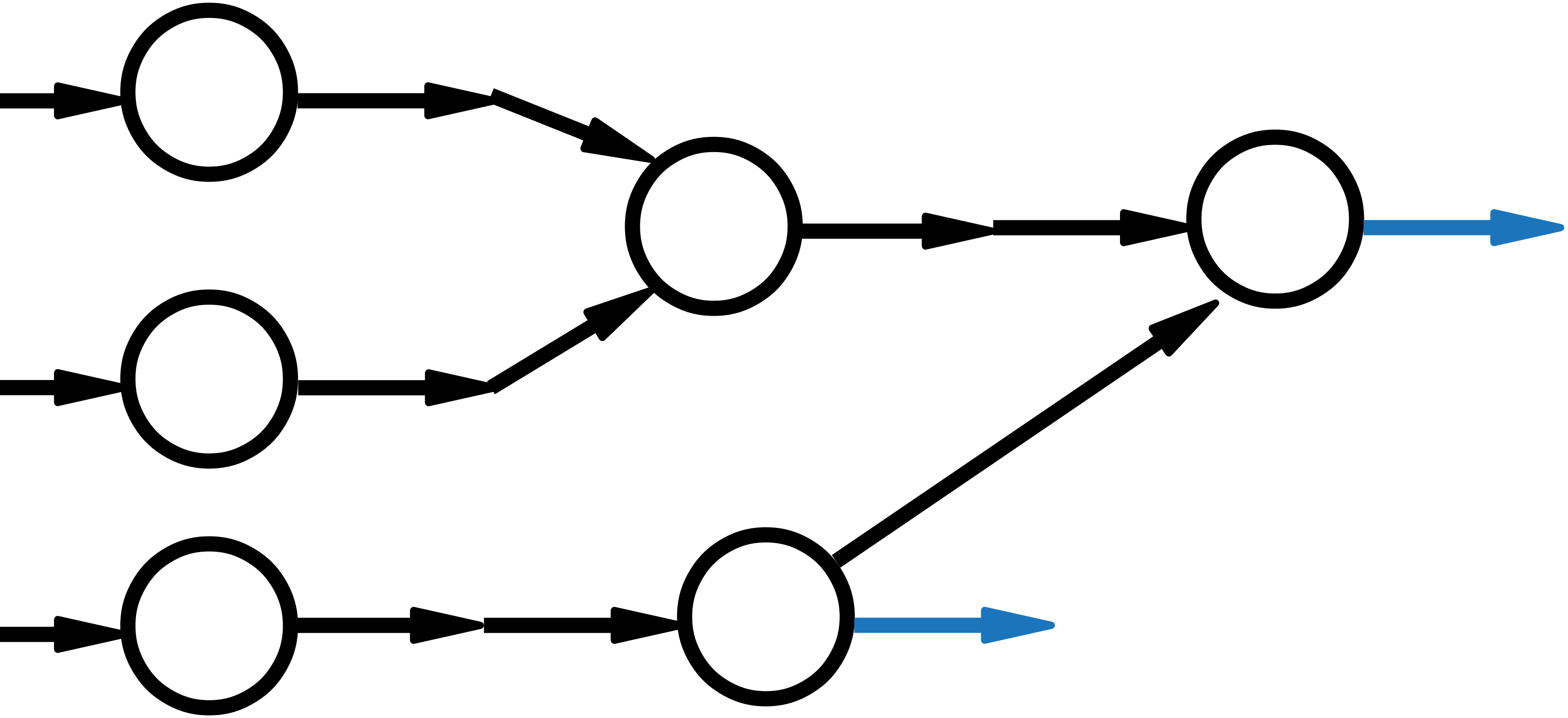
Many inputs



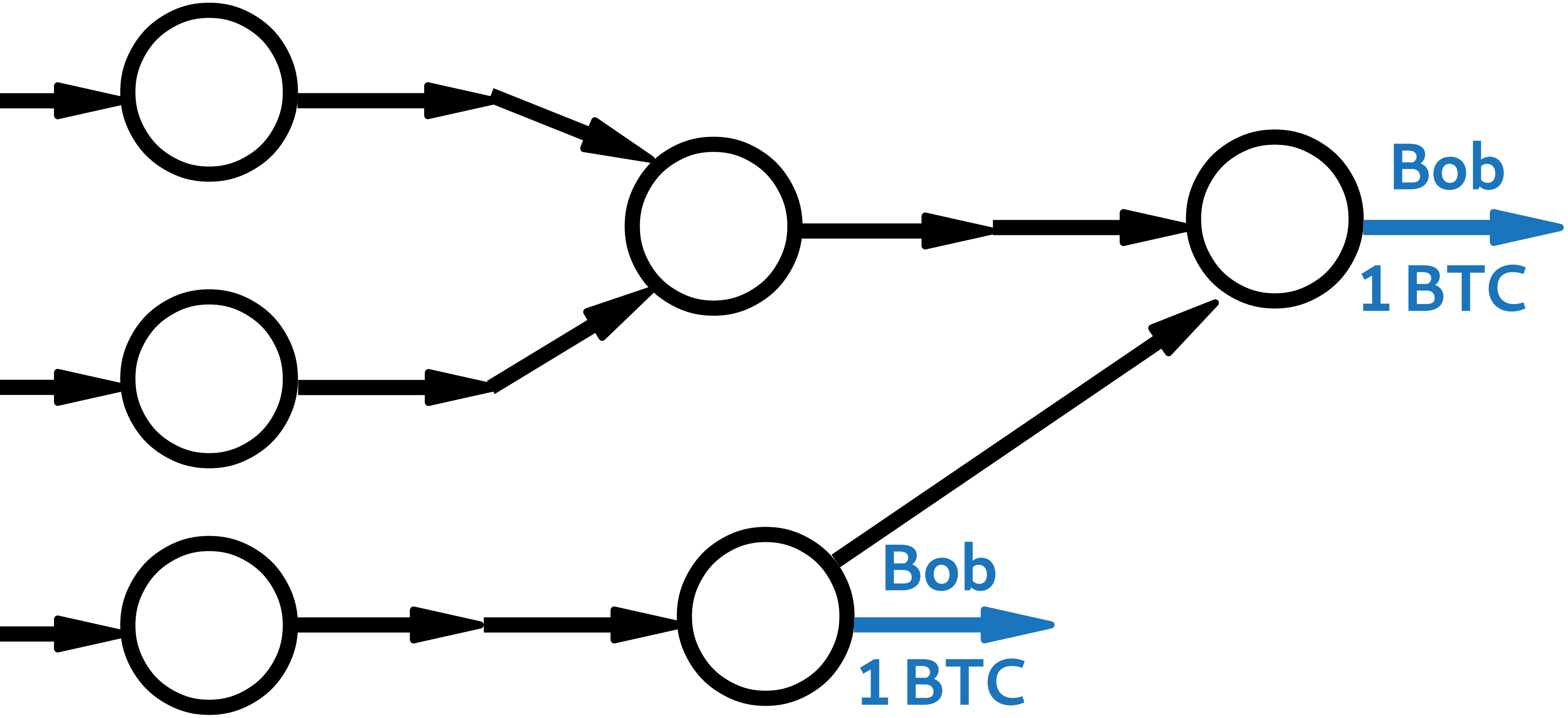
Many outputs



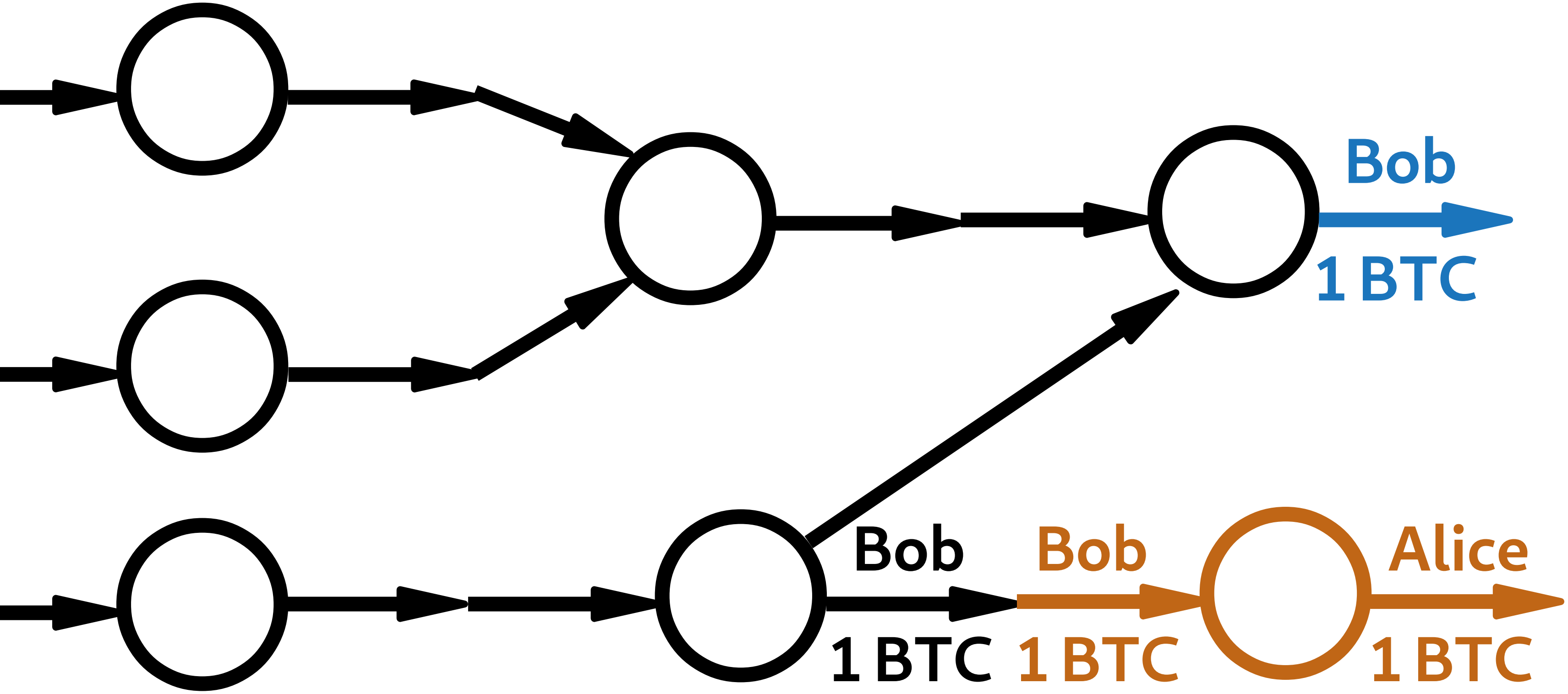
Unspent Transaction Outputs (UTXO)



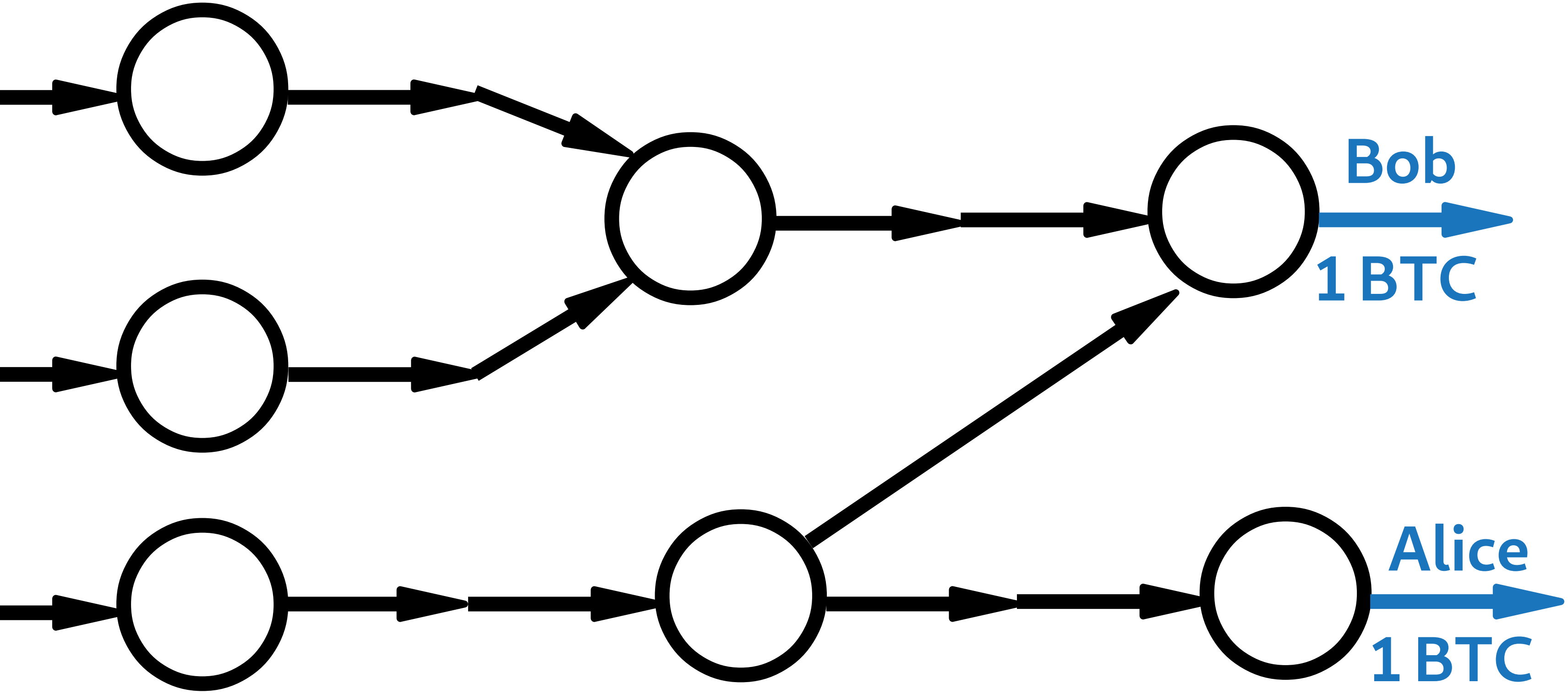
Bob has 2 BTC



Bob pays 1 BTC to Alice



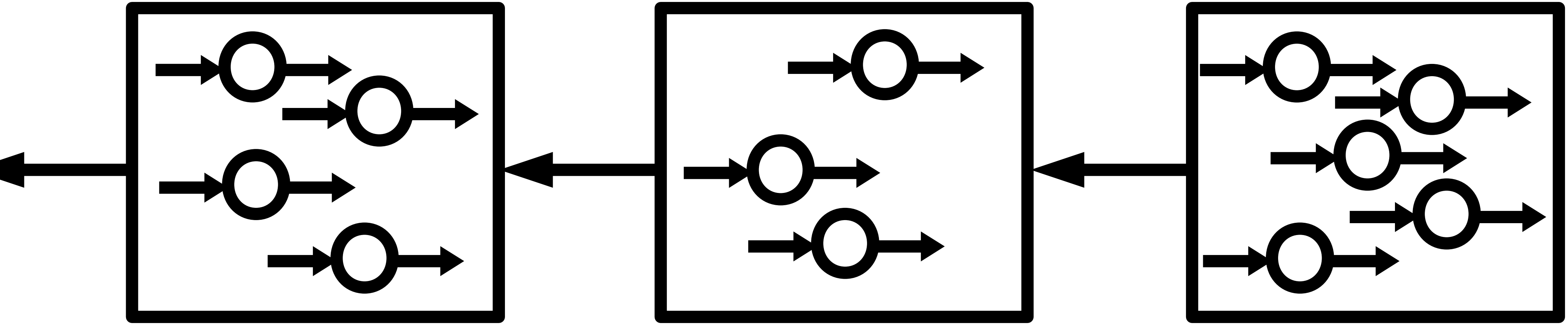
New UTXO



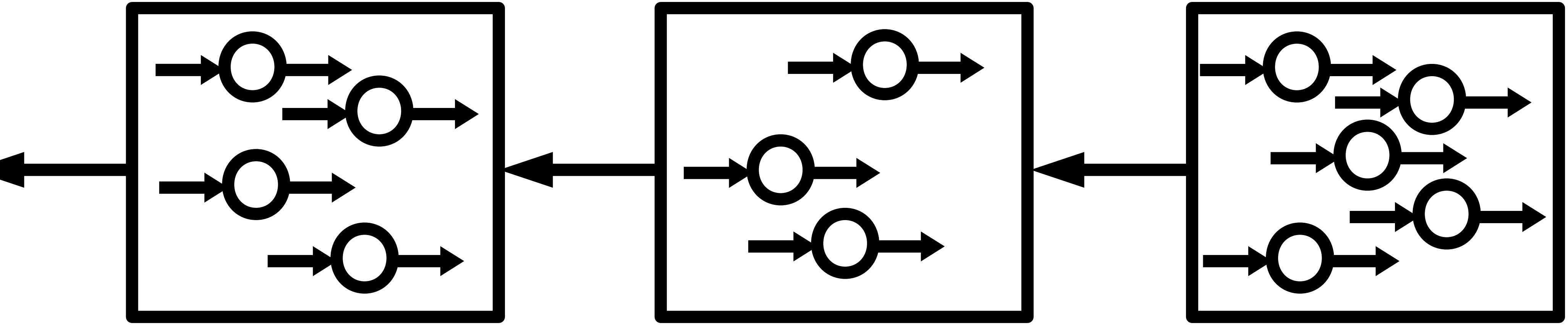
Block

- Contains
  - ▪ transactions
  - ▪ metadata
- Has unique parent

Blockchain

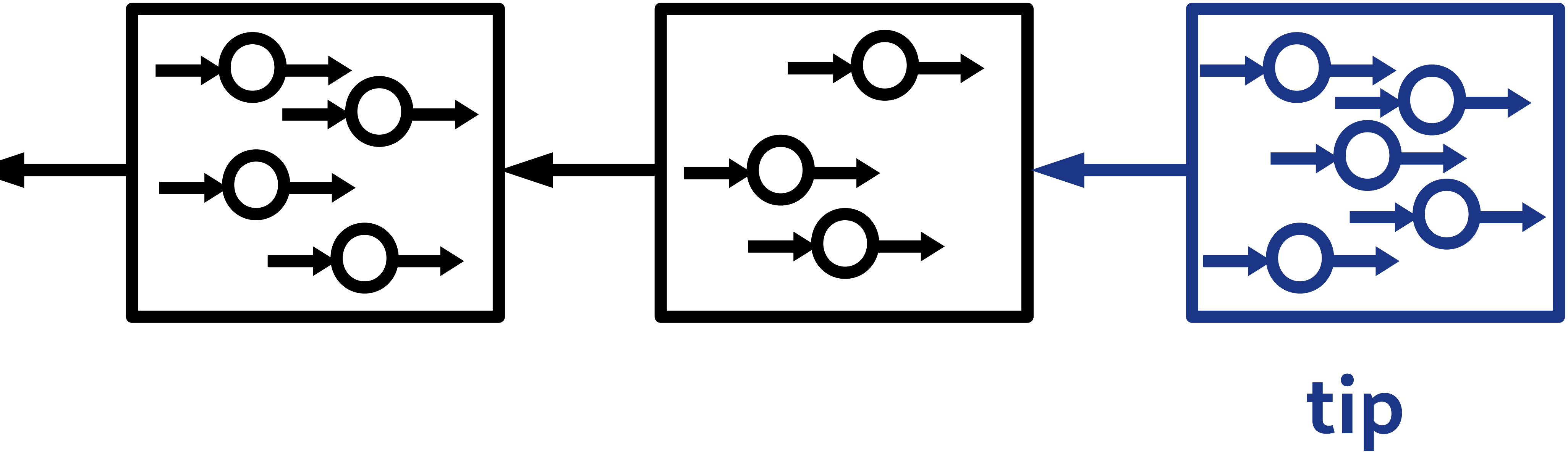


Blockchain

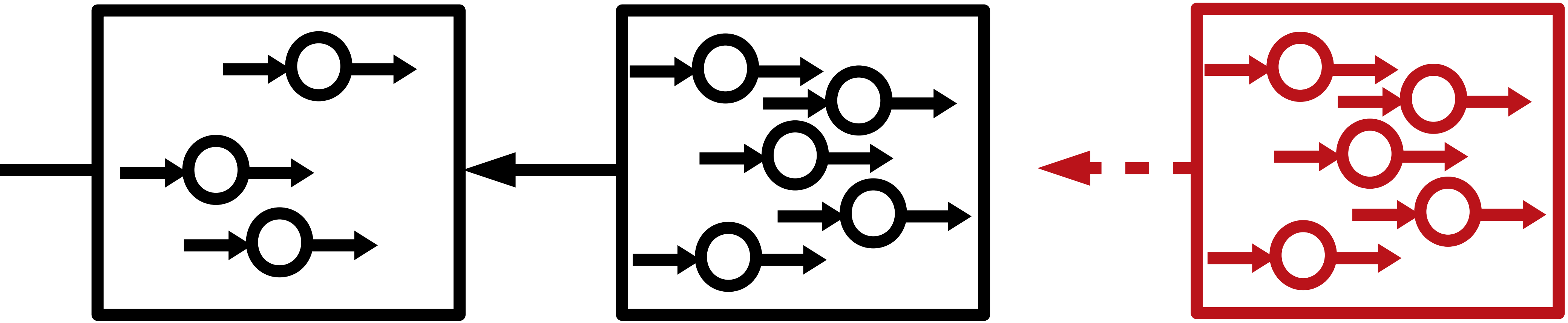


History of all transactions

Blockchain

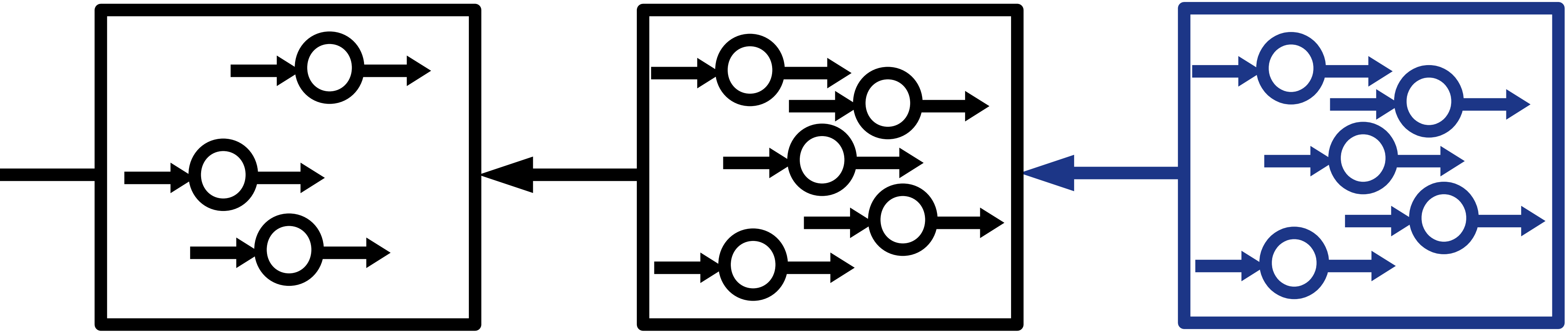


Mining (a.k.a. writing history)



- Only valid transactions?
- Proof of Work?

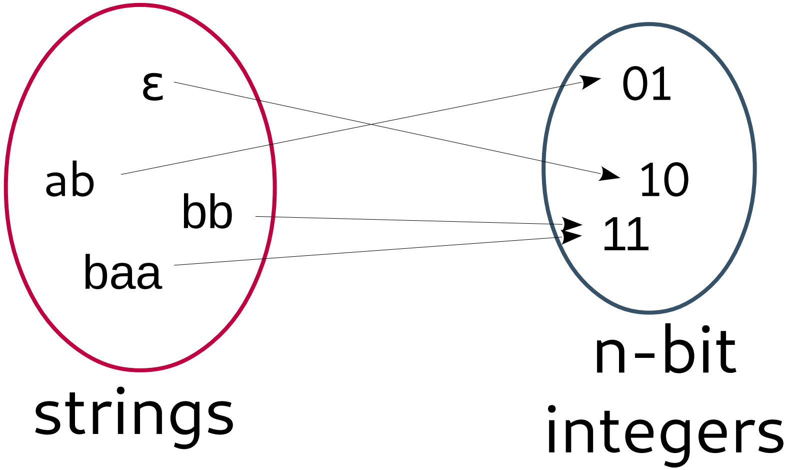
Mining (a.k.a. writing history)



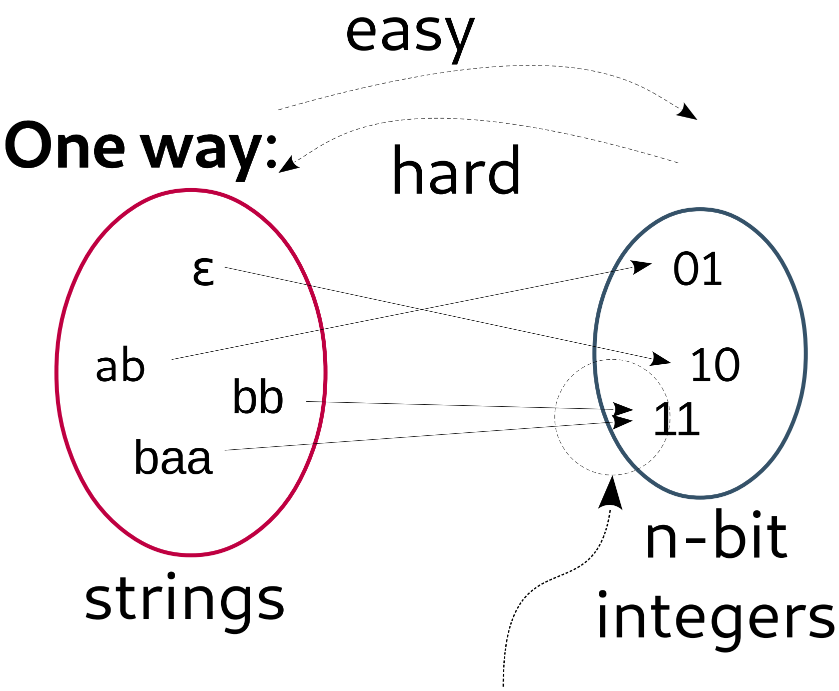
- Only valid transactions!
- Proof of Work!

new tip

Hash function



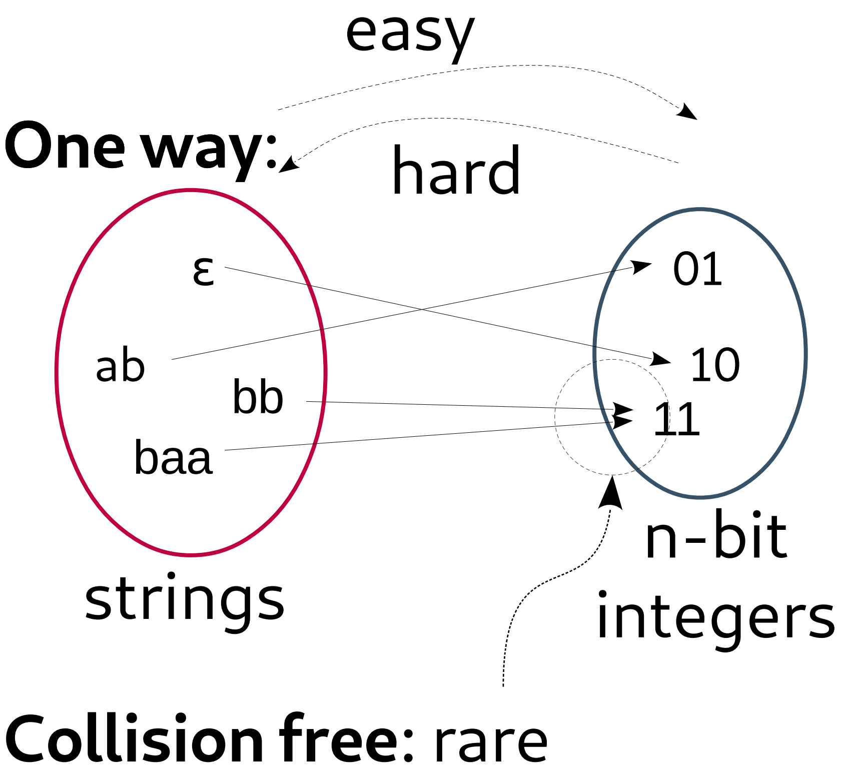
Hash function



One way:

Collision free: rare

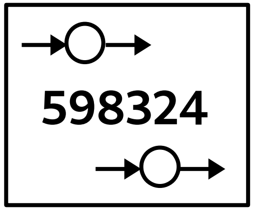
Hash function



One way:

Collision free: rare

Bitcoin uses SHA256, e.g.:

SHA256() =

0000000000000000000
d7819fc59c65ca6f3e8f73c
6eeadf538aa874a31341fb

Proof of work

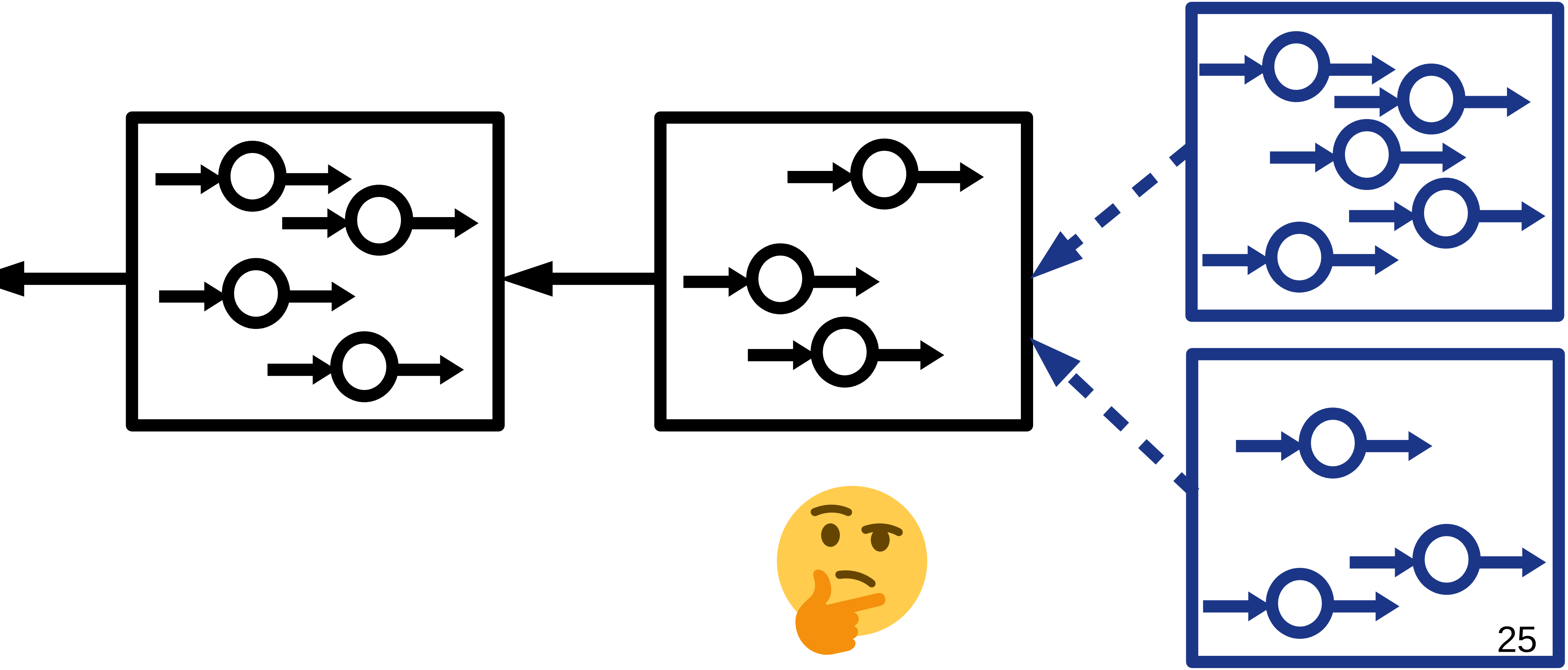
```
def hasProofOfWork(block):
  if hasManyLeadingZeroes(SHA256(block)):
    return True
  return False
```

Valid blocks need energy

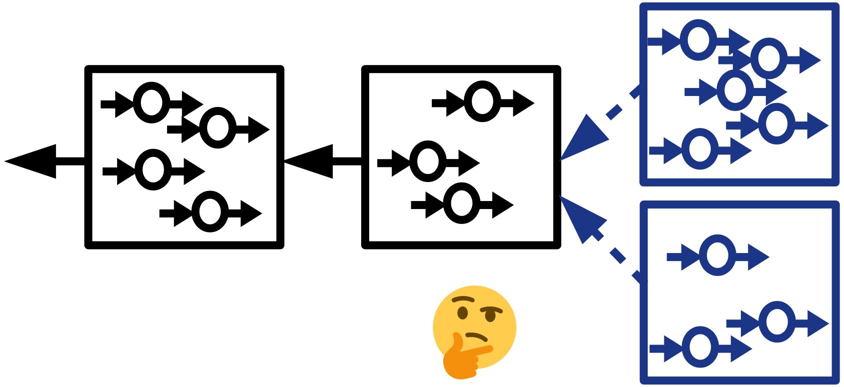
→

can’t spam blocks

Forks



Forks



Protocol says:

- Choose longest fork
- If equal, choose random

Nice properties

if *honest* mining power > 50%,

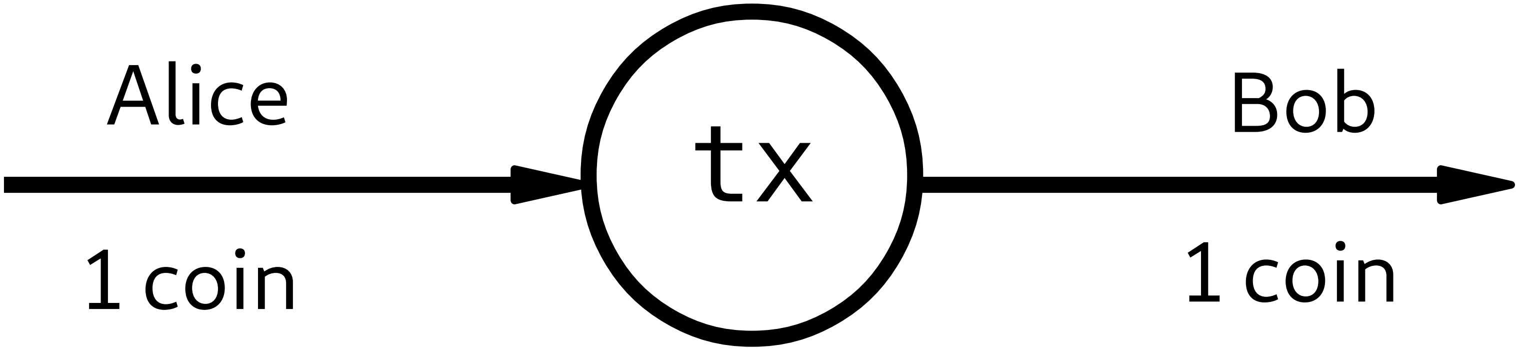
- **Liveness**: a new tx *will enter* the chain
- **Persistence**: Old blocks *won't change*

Garay, Kiayias, Leonardos. "The bitcoin backbone protocol: Analysis and applications." Annual International Conference on the Theory and Applications of Cryptographic Techniques. Springer, Berlin, Heidelberg, 2015.

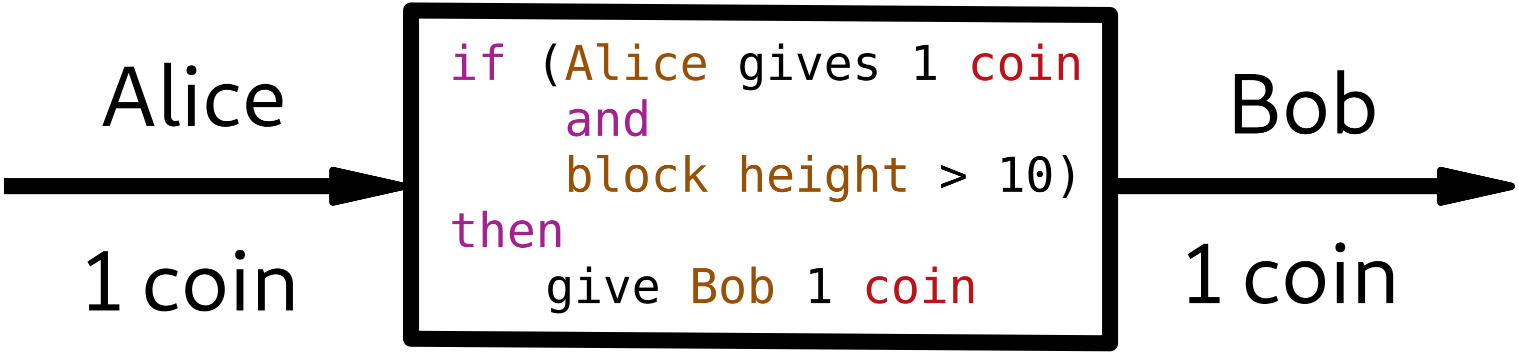
Part II

Smart Contracts: Programmable money

Remember transactions?



Now add some code!



Alice

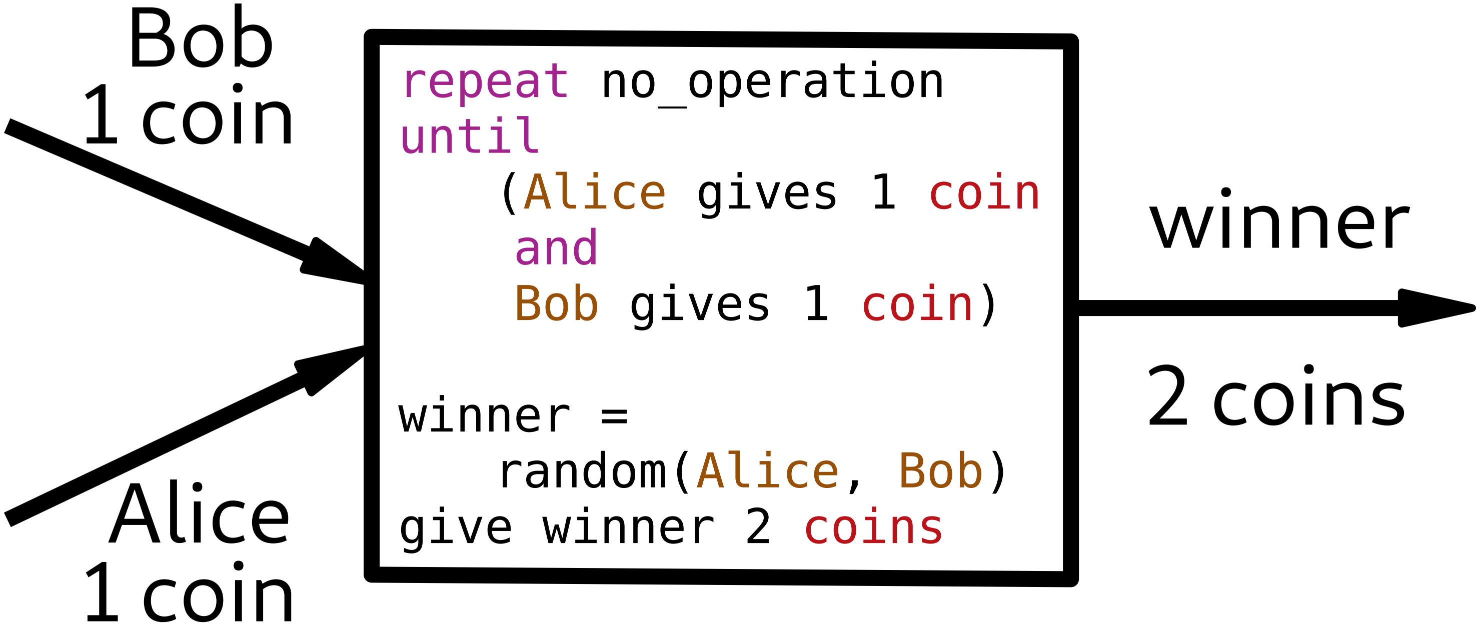
1 coin

```
if (Alice gives 1 coin
    and
    block height > 10)
then
   give Bob 1 coin
```

Bob

1 coin

Example 1: Flip a coin



Bob
1 coin

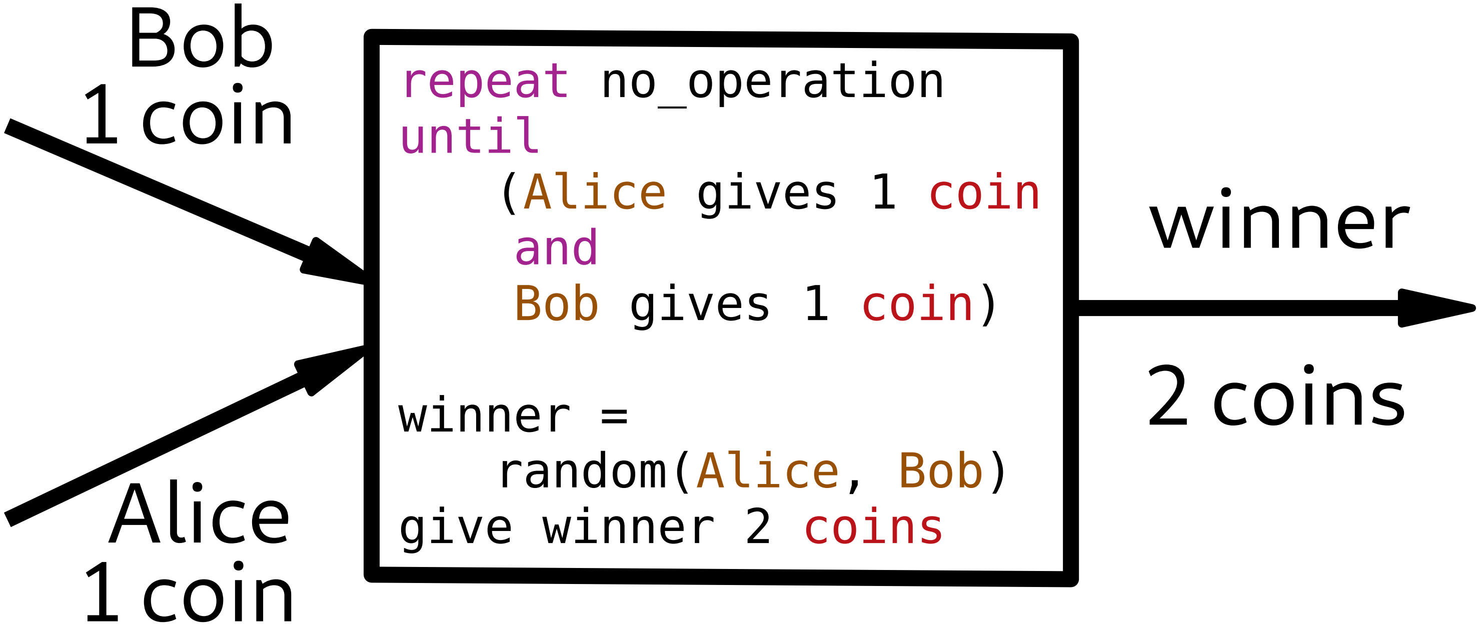
```
repeat no_operation
until
    (Alice gives 1 coin
     and
     Bob gives 1 coin)

winner =
    random(Alice, Bob)
give winner 2 coins
```

Alice
1 coin

winner

2 coins

Example 1: Flip a coin



Bob
1 coin

Alice
1 coin

```
repeat no_operation
until
    (Alice gives 1 coin
     and
     Bob gives 1 coin)

winner =
    random(Alice, Bob)
give winner 2 coins
```

winner

2 coins

Don’t use this contract in real life!

Example 2: King of the Hill

```
top = 0
king = null
while (true)
  if (user gives x coins
      and
      x > top)
     give king top coins
     king = user
     top = x
```

Don’t use this contract in real life!

Still too hard

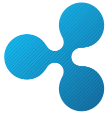
A fast way to lose your (and others')

Smart Contracts: ~~Programmable~~ money

- Very easy to make mistakes
  - TheDAO
  - Parity wallet
- Smart contract languages not (yet) safe

Part III

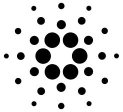
LND

 v

Types of blockchains, applications and the future

DASH

v

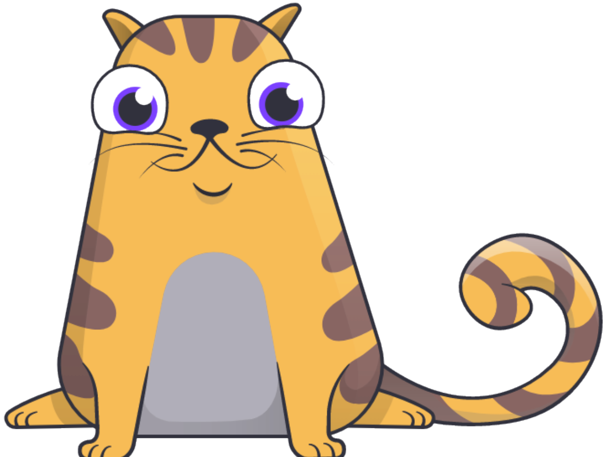


Xchain

v

Cryptokitties

Cute kitties that live on Ethereum!



MakerDao

- Decentralised stablecoin
  - On Ethereum
- 1 Dai = 1 USD
- Overcollateralised by floating “Maker”

Types of blockchains

- Permissioned vs Permissionless

v

- Proof of Work vs Proof of Stake

DASH

v

- Private vs Transparent

v

Scalability issue

₿: 7 txs/sec

VISA: 20,000 txs/sec

Problem: too much redundancy

Candidate Solution

Payment Channels! (e.g. Lightning, LND)

- 1 tx on-chain to open channel
- Unlimited off-chain txs
- 1 tx on-chain to close channel

Crosschain transactions

Move coins to another chain

E.g. use bitcoins in Ethereum contracts

Interconnected blockchains

Specialised blockchains

Separation of duties

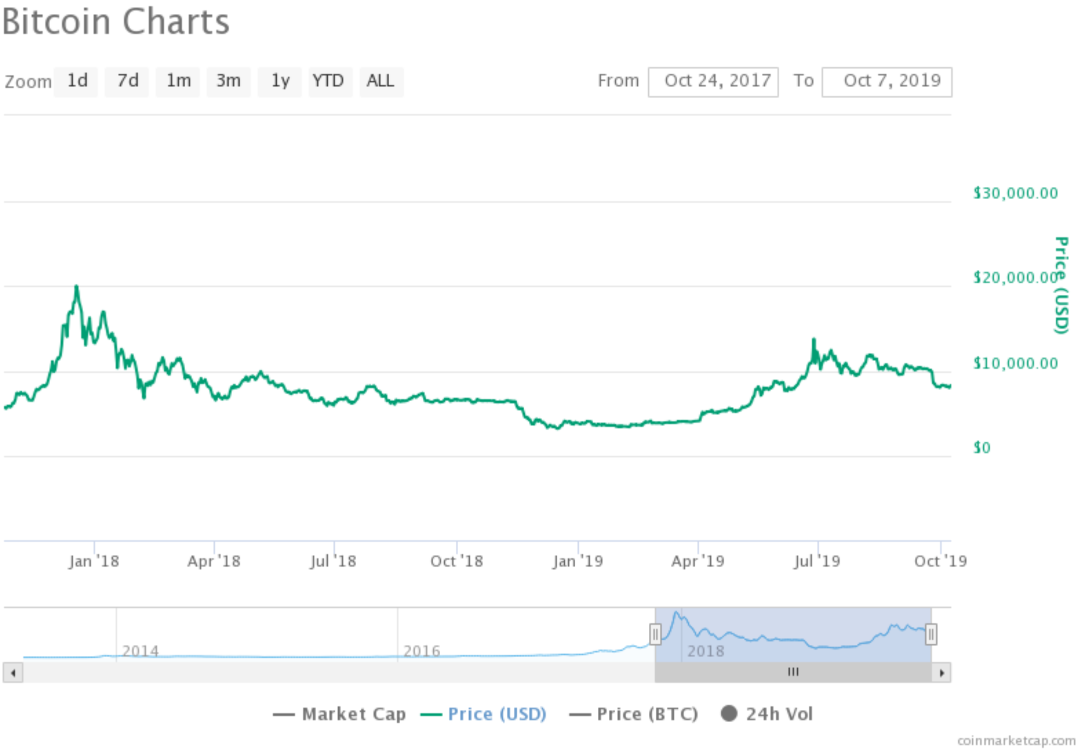
Related: Sharding

Questions?

Credits:

- Blockchain by Pablo Rozenberg from the Noun Project

THE TIMES
Eat Out from £5
More than 900 great restaurants, including four Gordon Ramsay favourites from £15
Israel prepares to send tanks and troops into Gaza
Michael Sheen Frost, Nixon and me
Working mums So that's how she does it
Detox in style The best spas on the planet
Salman Rushdie I won't marry again
Chancellor on brink of second bailout for banks
99p
Giant killing? Guide to the FA Cup third round


Bitcoin Charts

Zoom 1d 7d 1m 3m 1y YTD ALL

From Oct 24, 2017 To Oct 7, 2019