Blockchain, bitcoins and decentralized finance

Pierre-O. Goffard

UNISTRA
goffard@unistra.fr

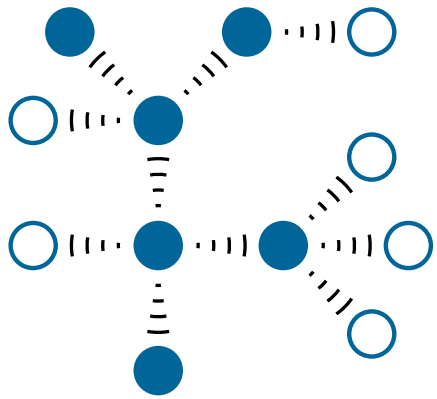
18 octobre 2023

Outline

Blockchain

A data ledger made of a sequence of blocks maintained by a achieving consensus in a Peer-To-Peer network.

- Decentralized
- Public/private
- Permissionned/permissionless
- Immutable
- Incentive compatible



We will focus on public blockchain and their associated consensus protocol.

Blocks

A block contains

- block height/ID
- Time stamp
- hash of the block
- hash of the previous block
- Set of transactions (data stored in the blockchain)

```
Block Height: 0
Block Hash: a52bea61a9f4131588cc101e8e1c731fa9f69f16934c5ab3a05a2134a42c13e0
Time:2021-07-12 10:03:04.812744
Block data: [{'sender': 'Coinbase', 'recipient': 'Satoshi', 'amount': 100, 'fee': 1}]
Mined: False
Previous block hash: 0
--------------
```

`https://www.blockchain.com/`

Consensus protocols

The mechanism to make all the nodes agree on a common data history.

The three dimensions of blockchain systems analysis

1. Efficiency
   - Throughputs
   - Transaction confirmation time
2. Decentralization
   - Fair distribution of the accounting right
3. Security
   - Resistance to attacks

X. Fu, H. Wang, and P. Shi, "A survey of blockchain consensus algorithms : mechanism, design and applications," *Science China Information Sciences*, vol. 64, nov 2020.

Applications of blockchain : Cryptocurrency

S. Nakamoto, "Bitcoin : A peer-to-peer electronic cash system." Available at https://bitcoin.org/bitcoin.pdf, 2008.

A. Antonopoulos, *Mastering Bitcoin*. O'Reilly UK Ltd., July 2017.

- Transaction anonymity
- Banking and reliable currency in certain regions of the world
- Money Transfer worldwide (at low fare)
- No need for a thrusted third party

Consensus protocol

Definition

Algorithm to allows the full nodes to agree on a common data history

It must rely on the scarce resources of the network

- bandwidth
- computational power
- storage (disk space)

Types of consensus protocols

Consensus protocol

1. Voting based

L. Lamport, R. Shostak, and M. Pease, "The byzantine generals problem," *ACM Transactions on Programming Languages and Systems*, pp. 382–401, July 1982.

⚠ Communication overhead

⚠ Denial of service

2. Leader based
   - Proof-of-Work (computational power)
   - Proof-of-Capacity and Proof-of-Spacetime (storage)
   - Proof-of-Interaction (bandwidth)
   - Proof-of-Stake (tokens)

Conflict resolution in blockchain

Consensus protocol

Fork

A fork arises when there is a disagreement between the nodes resulting in several branches in the blockchain.

LCR

The *Longest Chain Rule* states that if there exist several branches of the blockchain then the longest should be trusted.

In practice

- A branch can be considered legitimate if it is $k \in \mathbb{N}$ blocks ahead of its pursuers.
- Fork can be avoided when

$$\text{block appending time} > \text{propagation delay}$$

Proof-of-Work

Consensus protocol

Objective

Elect a leader based on computational effort to append the next block.

What's inside a block ?

A block consists of

- a header
- a list of "transactions" that represents the information recorded through the blockchain.

The header usually includes

- the date and time of creation of the block,
- the block height which is the index inside the blockchain,
- the hash of the block
- the hash of the previous block.

Question

What is the hash of a block ?

Cryptographic Hash function

Consensus protocol

A function that maps data of arbitratry size (message) to a bit array of fixed size (hash value)

$$h : \{0,1\}^* \mapsto \{0,1\}^d.$$

A good hash function is

- deterministic
- quick to compute
- One way
  - ↪ For a given hash value $\overline{h}$ it is hard to find a message m such that

$$h(m) = \overline{h}$$

- Colision resistant
  - ↪ Impossible to find m_1 and m_2 such that

$$h(m_1) = h(m_2)$$

- Chaotic

$$m_1 \approx m_2 \Rightarrow h(m_1) \neq h(m_2)$$

SHA-256

Consensus protocol

The SHA-256 function which converts any message into a hash value of 256 bits.

Example

The hexadecimal digest of the message

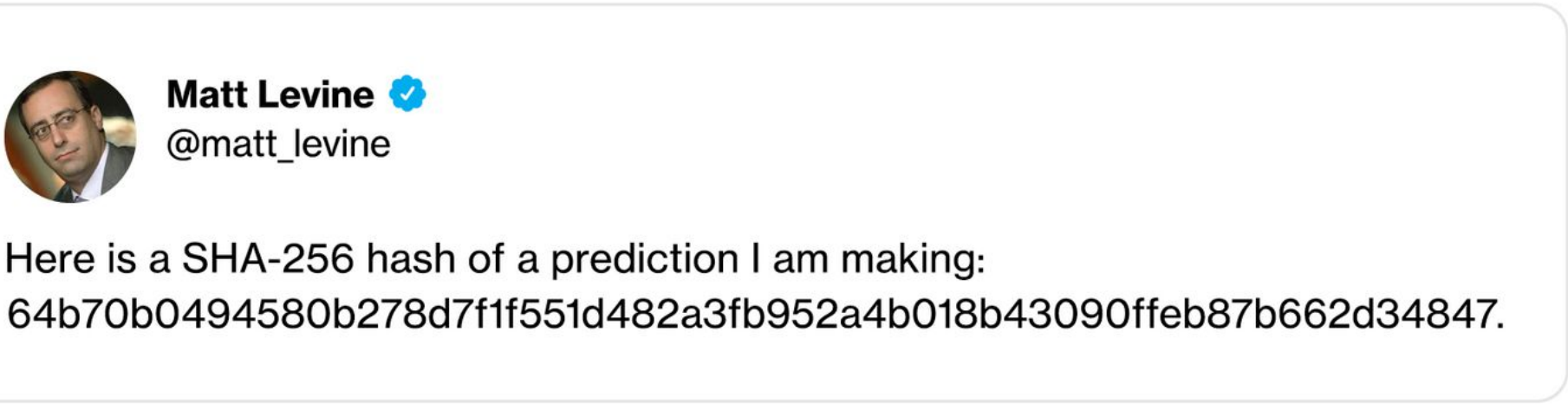
```
BLOCKASTICS is fantastic!
```

is

```
60a147c28568dc925c347bce20c910ef90f3774e2501ac63344f3411b6a6bf79
```

Hidden prediction

Consensus protocol



M. Levine, "The crypto story." Bloomberg business week, Oct. 2022.

Mining a block

Consensus protocol

```
Block Hash: 1fc23a429aa5aaf04d17e9057e03371f59ac8823b1441798940837fa2e318aaa
Block Height: 0
Time:2022-02-25 12:42:04.560217
Nonce:0
Block data: [{'sender': 'Coinbase', 'recipient': 'Satoshi', 'amount': 100, 'fee': 0}, {'sen
der': 'Satoshi', 'recipient': 'Pierre-O', 'amount': 5, 'fee': 2}]
Previous block hash: 0
Mined: False
--------------
```

Figure – A block that has not been mined yet.

Mining a block

Consensus protocol

The maximum value for a 256 bits number is

$$T_{\max} = 2^{256} - 1 \approx 1.16e^{77}.$$

Mining consists in drawing at random a nonce

$$\text{Nonce} \sim \text{Unif}(\{0, \ldots, 2^{32} - 1\}),$$

until

$$h(\text{Nonce}|\text{Block info}) < T,$$

where T is referred to as the target.

Difficulty of the cryptopuzzle

$$D = \frac{T_{\max}}{T}.$$

Mining a block

Consensus protocol

If we set the difficulty to $D = 2^4$ then the hexadecimal digest must start with at least 1 leading 0

```
Block Hash: 0869032ad6b3e5b86a53f9dded5f7b09ab93b24cd5a79c1d8c81b0b3e748d226
Block Height: 0
Time:2022-02-25 13:41:48.039980
Nonce:2931734429
Block data: [{'sender': 'Coinbase', 'recipient': 'Satoshi', 'amount': 100, 'fee': 0}, {'sen
der': 'Satoshi', 'recipient': 'Pierre-O', 'amount': 5, 'fee': 2}]
Previous block hash: 0
Mined: True
--------------
```

Figure – A mined block with a hash value having on leading zero.

The number of trial is geometrically distributed

- Exponential inter-block times
- Lenght of the blockchain = Poisson process

Bitcoin protocol

Consensus protocol

- One block every 10 minutes on average
- Depends on the hashrate of the network
- Difficulty adjustment every 2,016 blocks ($\approx$ two weeks)
- Reward halving every 210,000 blocks

Check out `https://www.bitcoinblockhalf.com/`

Mining equipments

How it started

- CPU, GPU

How it is going

- Application Specific Integrated Chip (ASIC)
  - Increase of the network electricity consumption `https://digiconomist.net/bitcoin-energy-consumption`
  - E-Waste
  - Centralization issue `https://www.bitmain.com/`
    - Mining pool ranking at `https://btc.com/`
    - Mining equipment profitability at `https://v3.antpool.com/minerIncomeRank`

Proof of Stake

Consensus protocol

PoW is slow and ressource consuming. Let $\{1,\dots,N\}$ be a set of miners and $\{\pi_1,\dots,\pi_N\}$ be their share of cryptocoins.

PoS

1. Node $i \in \{1,\dots,N\}$ is selected with probability π_i to append the next block

Nodes are chosen according to what they own.

- Nothing at stake problem
- Rich gets richer ?
- `https://www.peercoin.net/`

F. Saleh, "Blockchain without waste : Proof-of-stake," *The Review of Financial Studies*, vol. 34, pp. 1156–1190, jul 2020.

Incentive mechanism

Participation to the network is costly to the nodes.

Native cryptocurrency

The nodes must be retributed for their hard work.

Applications of blockchain : Cryptocurrency

Cryptocurrencies and decentralized finance

S. Nakamoto, "Bitcoin : A peer-to-peer electronic cash system." Available at https://bitcoin.org/bitcoin.pdf, 2008.

- Transaction anonymity
- Banking and reliable currency in certain regions of the world
- Money Transfer worldwide (at low fare)
- No need for a thrusted third party

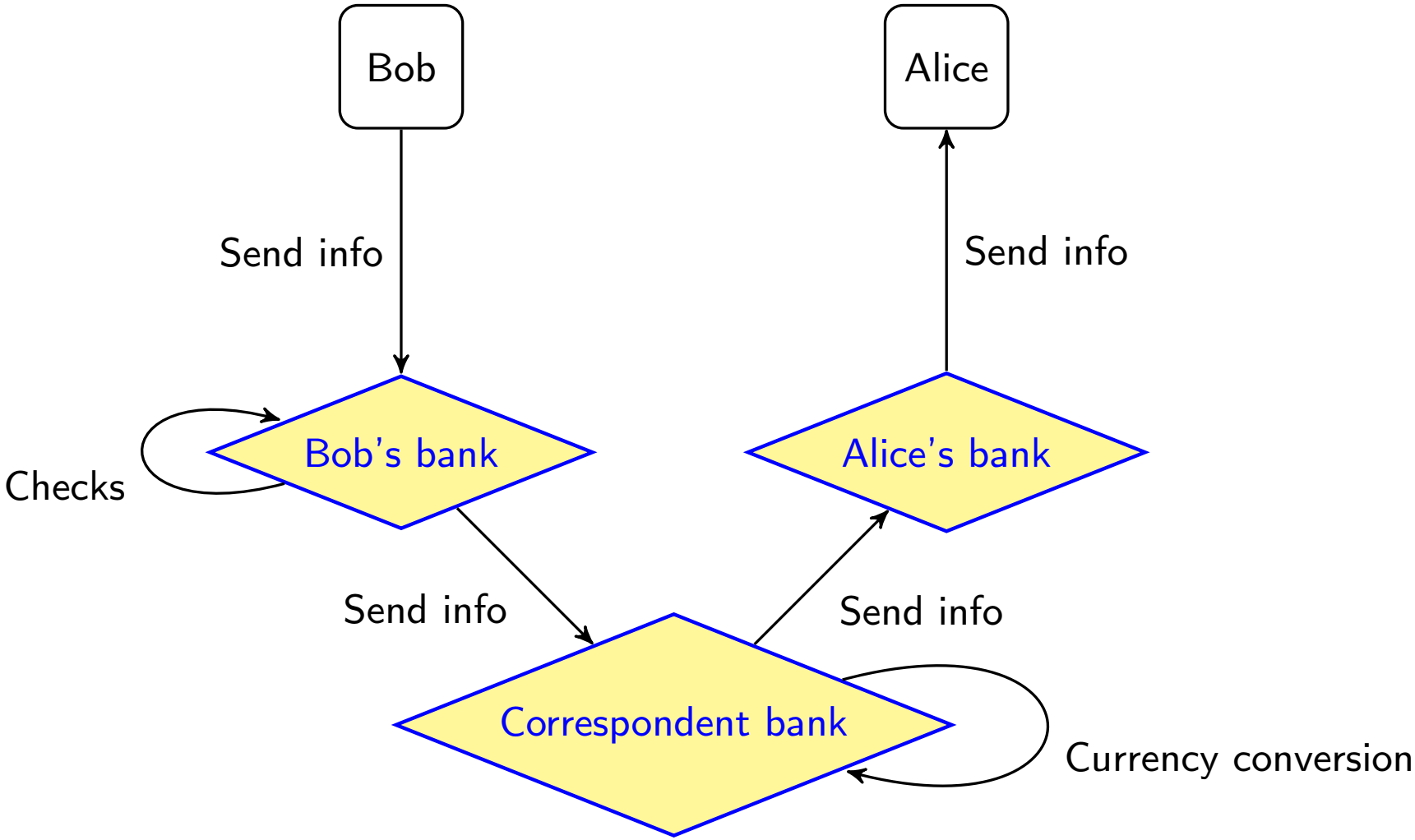
Why cryptocurrencies ?

What is wrong with the current financial system ?

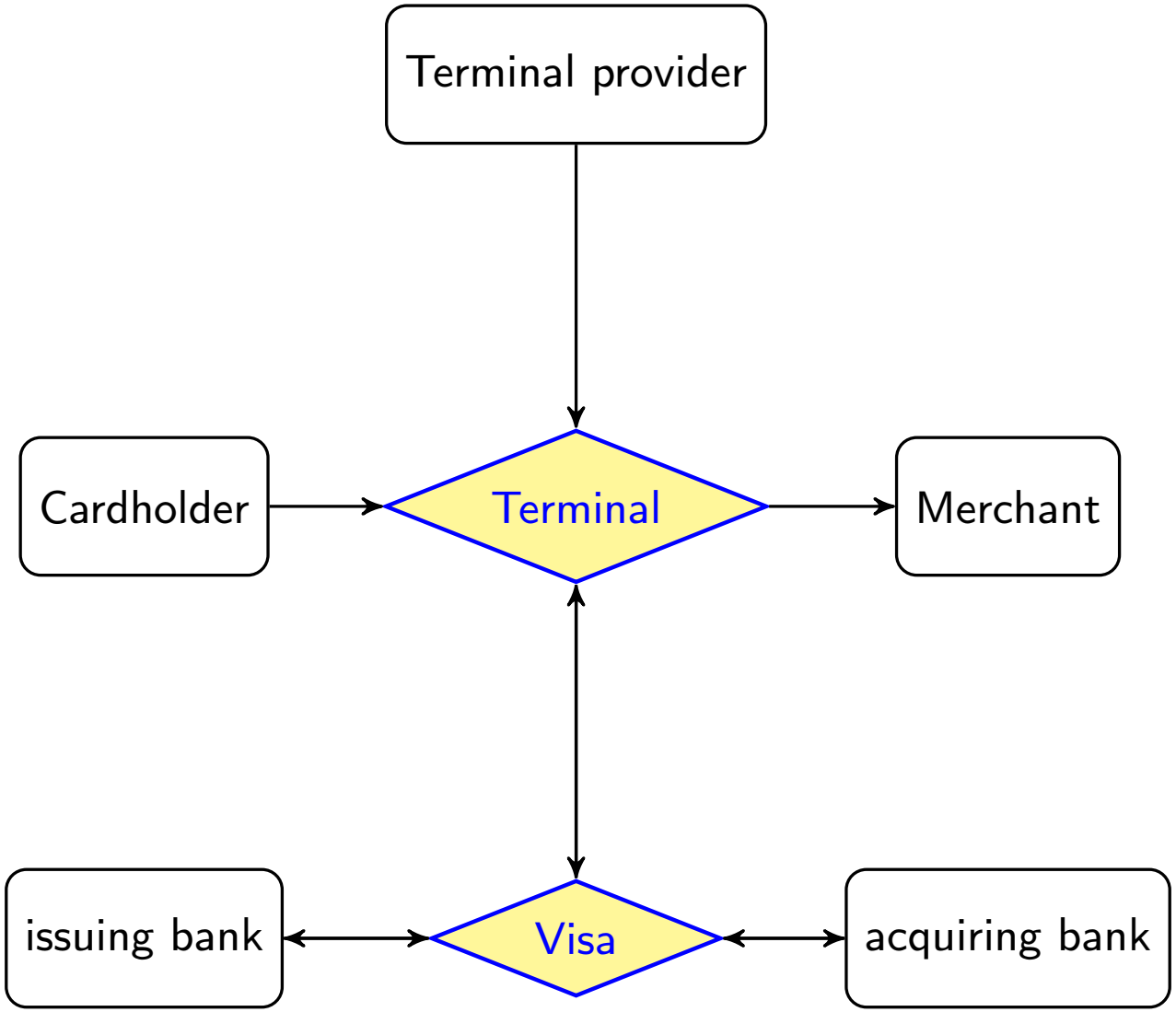
- No data privacy
- No real ownership
- Outdated technology to transfer ownersip
- Huge middlemen costs

A. Lipton and A. Treccani, *Blockchain and Distributed Ledgers*. WORLD SCIENTIFIC, apr 2021.

Wire transfer



Credit card payments

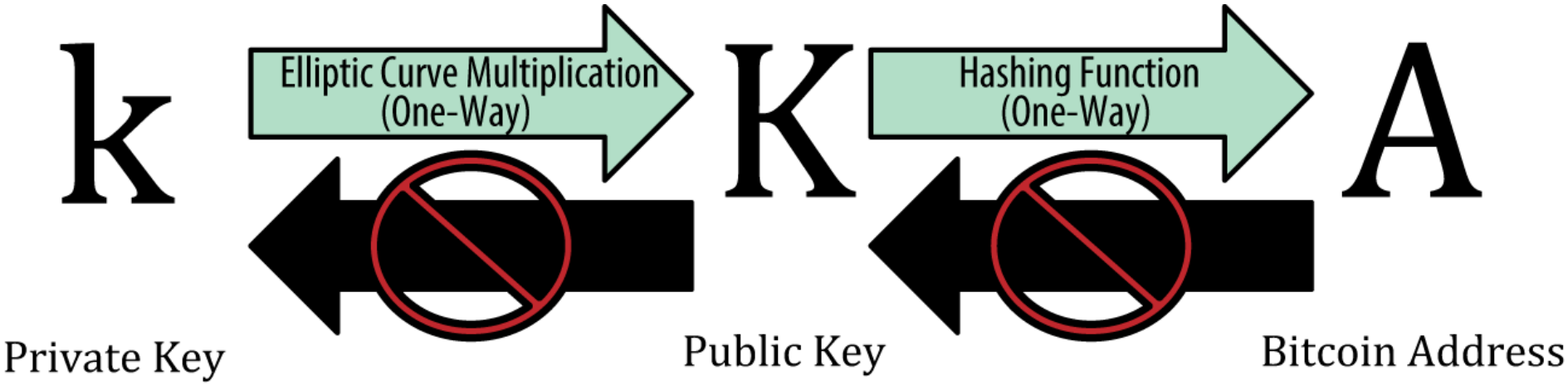


How does it work ?

1. No central authority (Decentralized network)
2. Ledger to record all the transactions and coin ownership (blockchain)
3. A coin generation process (block finding reward)
   - ↪ Incentive to the full nodes
4. Ownership can be proved cryptographically (wallet associated to a public/private key)
5. Transactions can be issued by an entity proving ownership of the cryptographic unit (through the private key)
6. The system cannot process more than one transaction associated to the same cryptographic unit (double spending)

J. Lansky, "Possible state approaches to cryptocurrencies," *Journal of Systems Integration*, vol. 9, pp. 19–31, jan 2018.

Public and private keys



- Private key = Pin number
  - ↪ Generate the public key
  - ↪ Sign transaction
- Public key = Bank acccount information
  - ↪ Verify transaction

Unspent transaction

Transaction View information about a bitcoin transaction

0627052b6f28912f2703066a912ea577f2ce4da4caa5a5fbd8a57286c345c2f2

1Cdid9KFAaatwczBwBttQcwXYCpvK8h7FK (0.1 BTC - Output)

1GdK9UzpHBzqzX2A9JFP3Di4weBwqgmoQA - (Unspent) 0.015 BTC

1Cdid9KFAaatwczBwBttQcwXYCpvK8h7FK - (Unspent) 0.0845 BTC

97 Confirmations | 0.0995 BTC

Summary	
Size	258 (bytes)
Received Time	2013-12-27 23:03:05
Included In Blocks	277316 (2013-12-27 23:11:54 +9 minutes)

Inputs and Outputs	
Total Input	0.1 BTC
Total Output	0.0995 BTC
Fees	0.0005 BTC
Estimated BTC Transacted	0.015 BTC

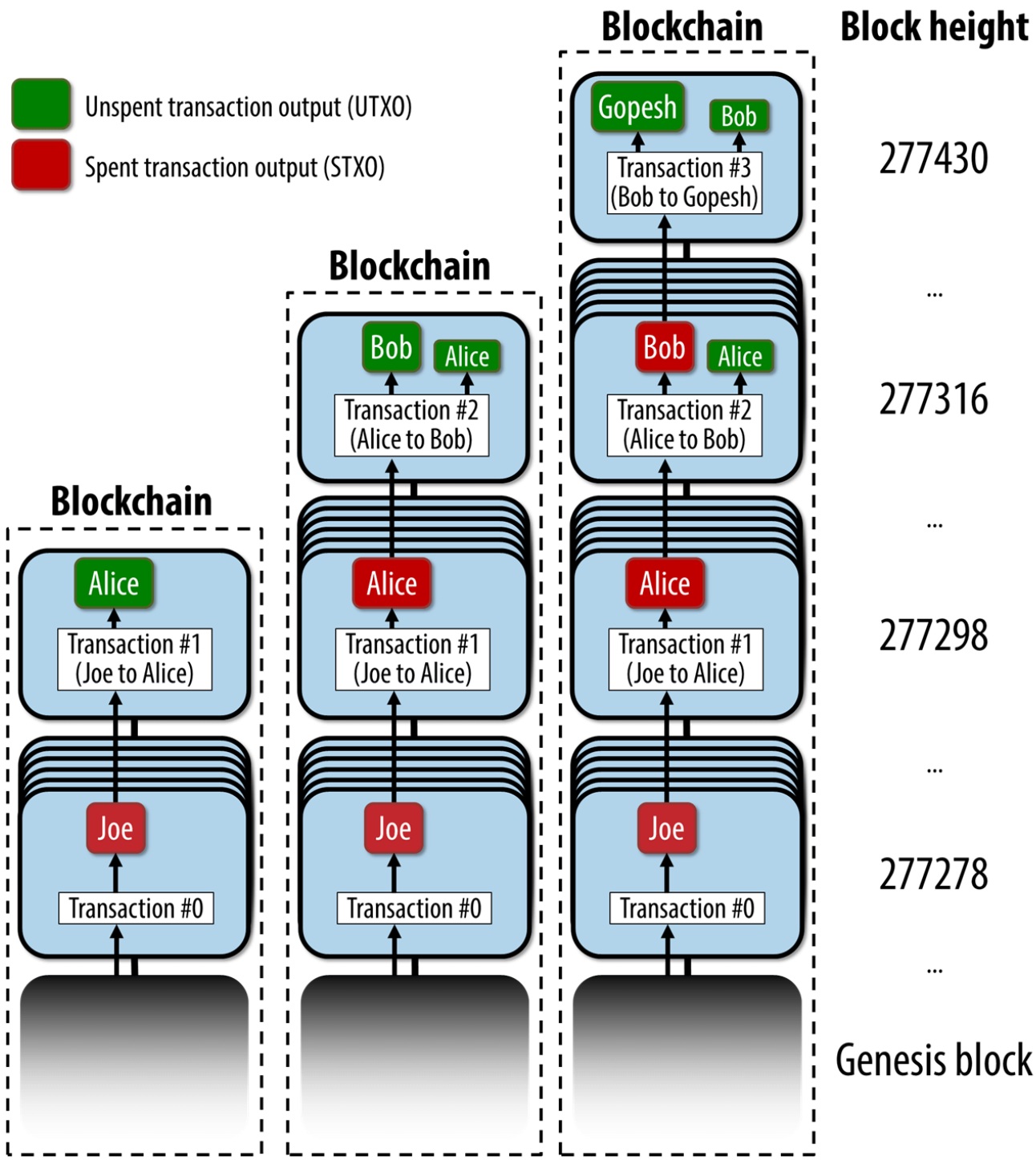
User's balance

UTXO

Unspent transaction outputs.

The balance of a bitcoin user is the sum of all the UTXO associated to the BTC addresses she controls.

A. Antonopoulos, *Mastering Bitcoin*.
O'Reilly UK Ltd., July 2017.


Blockchain
Block height
Unspent transaction output (UTXO)
Spent transaction output (STXO)
Gopesh
Bob
Transaction #3
(Bob to Gopesh)
277430
...
Bob
Alice
Transaction #2
(Alice to Bob)
277316
...
Alice
Transaction #1
(Joe to Alice)
277298
...
Joe
Transaction #0
277278
...
Genesis block

Cryptocurrency implementation

Cryptocurrencies and decentralized finance

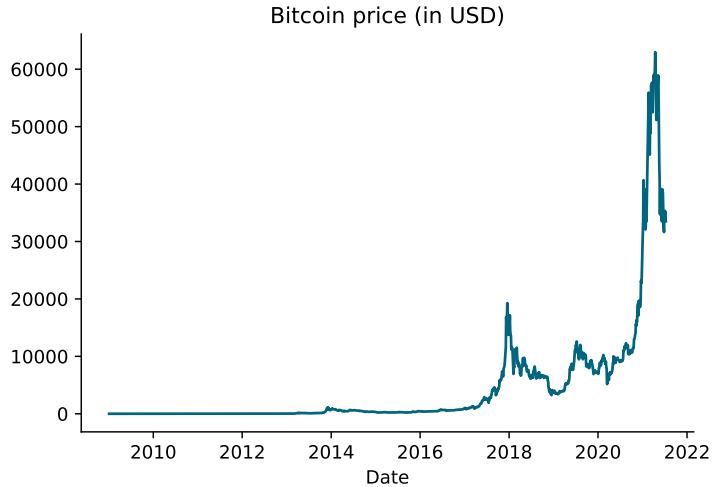
Blockchain parameters

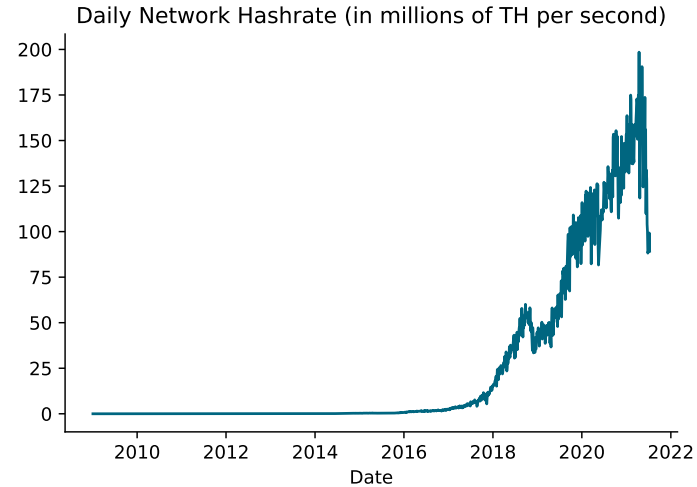
- Consensus protocol (PoW or PoS)
  - ↪ Hash function (SHA-256 for Bitcoin and scrypt for LiteCoin)
  - ↪ Hybrid PoW/PoS (PeerCoin)
- Block generation time
  - ↪ every 10 minutes for Bitcoin
  - ↪ every 12 sec for Ethereum
- Block finding reward
  - ↪ Halved every 210,000 blocks in Bitcoin. It started at 50 BTC, is now 6.25 BTC `https://www.bitcoinblockhalf.com/`
- Total coin supply
  - ↪ 21,000,000 in total for Bitcoin
- Transaction fees
  - ↪ GAS in Ethereum

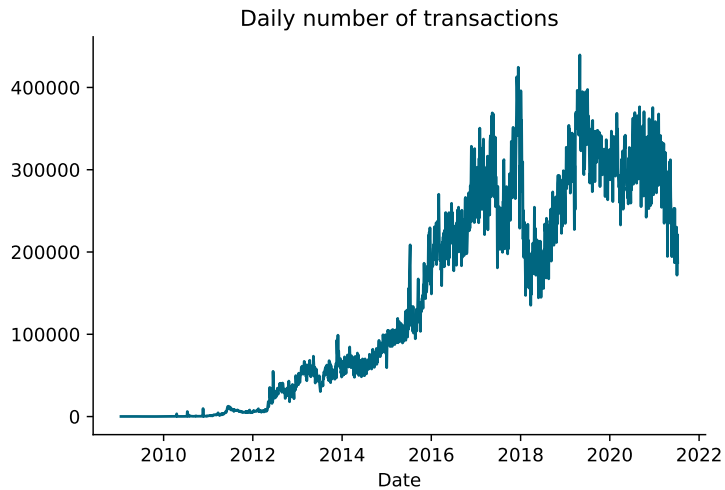
These choices lead to the creation of multiple cryptocurrencies

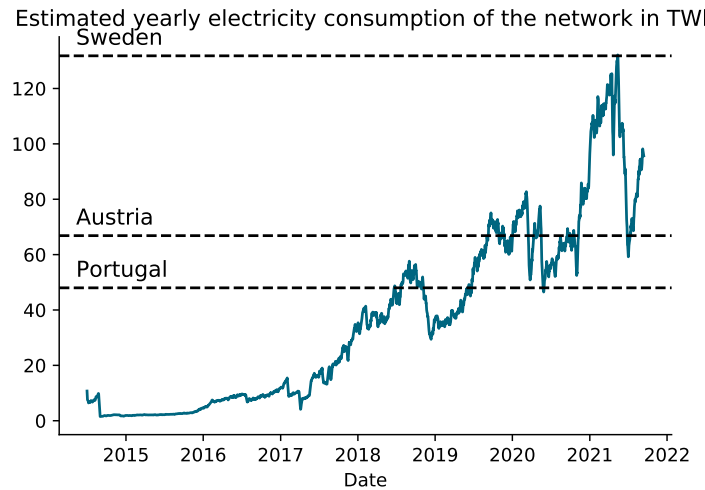
Examples

Bitcoin and AltCoins (Ethereum, LiteCoin, DogeCoin, Ripple...), see `https://en.wikipedia.org/wiki/List_of_cryptocurrencies`









. **Sources** : `https://www.blockchain.com/` & `https://cbeci.org/`

Decentralized application

The network provide ressources such as

- storage
- computing power

through a smart contract on the ethereum blockchain.

GOLEM (`https://www.golem.network/`)

Build a network of idle computers to do paralell computing.

Utility tokens are used to access the service and provision the network ressources.

Equation of Exchange (Fisher 1911)

$$MV = PQ$$

Decentralized finance

DEFI creates new financial architecture

+ Non custodial
+ Anonymous
+ Permisionless
+ openly auditable

- Unregulated
- Tax evasion
- Fraud
- Money laundering

Extends the Bitcoin promises to more complex financial operations

- Collateralized lending
- Decentralized Exchange Platform
- Tokenized assets
- Fundraising vehicle (ICO, STO, ...)

S. M. Werner, D. Perez, L. Gudgeon, A. Klages-Mundt, D. Harz, and W. J. Knottenbelt, "Sok : Decentralized finance (defi)," 2021.

Tokenized real-world assets

Tokenized version of a real-world, physical asset

- Increases the liquidity of certain type of assets
- Make certain classes of assets available to the many
- Can be used as store of value or collateral

These token can be backed by

- fiat currency ⇒ stablecoin
- commodities like gold `https://ekon.gold/`
- stocks (security token) that includes voting right and profit sharing mechanism
- Art
- Digital art (Non Fungible tokens on the Ethereum blockchain)

Central authority

This requires a custodian to ensure that the tokens are actually backed by these off-chain assets (except for NFTs).

OECD, "The tokenisation of assets and potential implications for financial markets," tech. rep., 2020.

Valuation models

- Cryptocurrencies are medium of exchange and may be priced via transaction cost model (Beaumol-Tobin and such)


W. J. Baumol, "The transactions demand for cash : An inventory theoretic approach," *The Quarterly Journal of Economics*, vol. 66, p. 545, nov 1952.


L. Schilling and H. Uhlig, "Some simple bitcoin economics," *Journal of Monetary Economics*, vol. 106, pp. 16–26, oct 2019.

- Tokenized asset depends on the real asset that backs the token


J. Hargrave, N. Sahdev, and O. Feldmeier, "How value is created in tokenized assets," in *Blockchain Economics : Implications of Distributed Ledgers*, pp. 125–143, WORLD SCIENTIFIC (EUROPE), jan 2019.

- Utility tokens


J. R. Gan, G. Tsoukalas, and S. Netessine, "Initial coin offerings, speculation, and asset tokenization," *Management Science*, vol. 67, pp. 914–931, feb 2021.


L. W. Cong, Y. Li, and N. Wang, "Tokenomics : Dynamic adoption and valuation," *The Review of Financial Studies*, vol. 34, pp. 1105–1155, aug 2020.

ICO tuning and timeline

1 ICO period

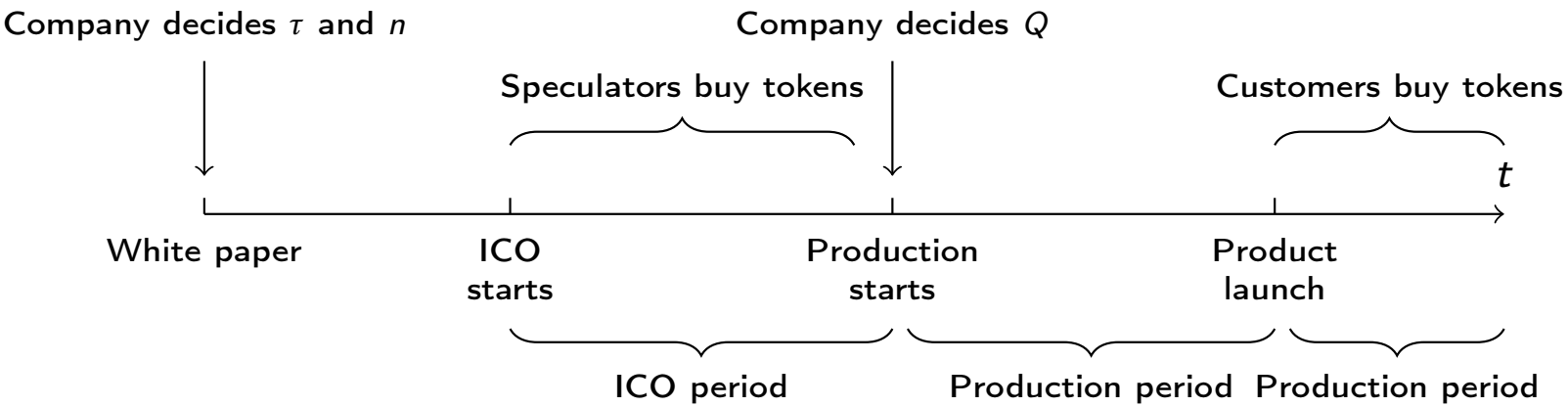
- The firm publishes a white paper and set
  - The token price τ
  - The total number of token m
  - The number of token issued to the investors during the ICO $n \leq m$.
- s among $z >> m$ investors buy token

2 Production period

- The firm uses the funds raised $s\tau$ to finance the production of Q units of goods

3 Market period

- Customers purchase token to meet their needs $D \sim F(.)$



J. R. Gan, G. Tsoukalas, and S. Netessine, "Initial coin offerings, speculation, and asset tokenization," *Management Science*, vol. 67, pp. 914–931, feb 2021.

Decentralized insurance

Parametric insurance

Compensation if a measurable quantity reaches a threshold

- Example : Flight delay insurance
  - `https://etherscan.io/address/0xdc3d8fc2c41781b0259175bdc19516f7da11cba7`
- Use smart contract and off-chain data through oracles
- Transparent and automatic

Blockchain as a research topic

Cryptocurrencies and decentralized finance

- Computer science
  - Peer-to-peer networks and consensus algorithm
  - Cryptography and security
- Economics
  - Game theory to study the incentive mechanism at play
  - Nature of the cryptoassets
- Operations research
  - Optimization of complex system
- Financial math
  - Valuation models for cryptoassets
- Machine learning and statistics
  - Open data
  - Interaction between blockchain users
  - (Social) network analysis
  - Clustering of public keys and addresses in the bitcoin blockchain.