Blockchains & Distributed Ledgers

Lecture 01

Aggelos Kiayias

Slide credits: AK, Dionysis Zindros, Christos Nasikas

Introduction

- Introduction to Blockchain
- What is money ?
- The never-ending book parable
- Cryptocurrencies from a user’s perspective

Why study Blockchains?

Why study Blockchains?

- Provide good foundations for exploring the security of information systems in general.
- Highlight the importance of decentralisation, a property of increasing importance in the design of modern information systems.
- Facilitate a solid understanding of many security critical components, incl.
  - Key management.
  - Software security.
  - Privacy preserving technologies.
  - Public Key Infrastructure.
- They have an increasing impact on various aspects of societal organisation.
- It’s fun!

What is a blockchain ?

What is a blockchain ?

- A blockchain is a distributed database that satisfies a unique set of safety and liveness properties.
- Distributed ledgers use blockchain protocol as one means of implementation.
- To understand it, we can focus to its first (and so far most successful) application.

Case study: Money

WEEKLY BUGLE.
HARPERS WEE
CHURCH

THE COUNTRY EDITOR—PAYING THE YEARLY SUBSCRIPTION.—[Drawn by F. S. Church.]

(1874) A man offering chicken for a yearly newspaper subscription

Properties of Money

- **A medium of exchange:** Can be used as medium for the exchange of goods - no bartering
- **A unit of account:** Can be used for pricing of all goods and services, for accounting purposes and debt recording
- **A store of value:** Storing and retrieving it at a point in the future maintains its value.

Money 1.0: Using a trusted object

Analysis of Money 1.0

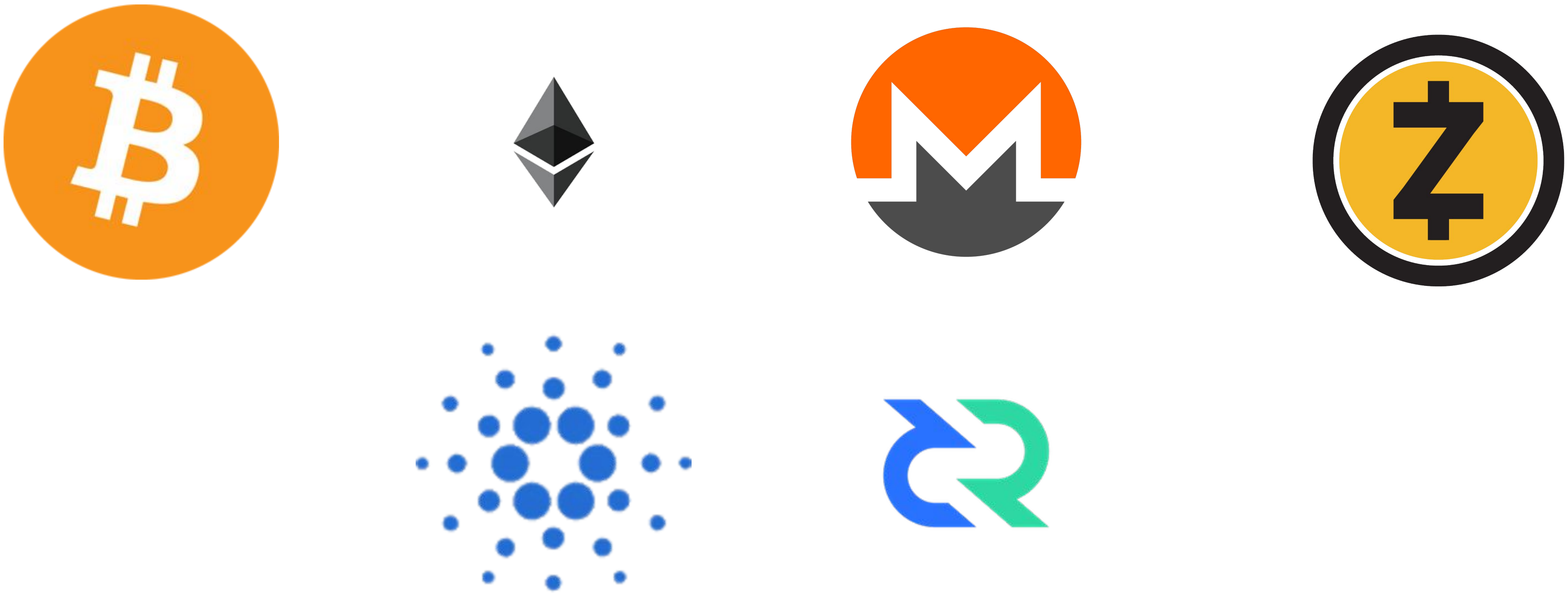
- A medium of exchange: Medium
  - Ok to face to face transactions
- A unit of account: Mediocre
  - Fungible, but not divisible well
  - Typically forgeable
- A store of value: Bad
  - Some objects may deteriorate.
  - May have unknown hidden quantities.

Money 2.0: Using a trusted entity

Analysis of Money 2.0

- A medium of exchange: good
  - For transactions within the domain of the trusted entity
- A unit of account: great
  - Fungible & divisible
- A store of value: Mediocre
  - Tied to the availability & reputation of the issuing entity

Money 3.0: Using cryptocurrencies



The never-ending book parable

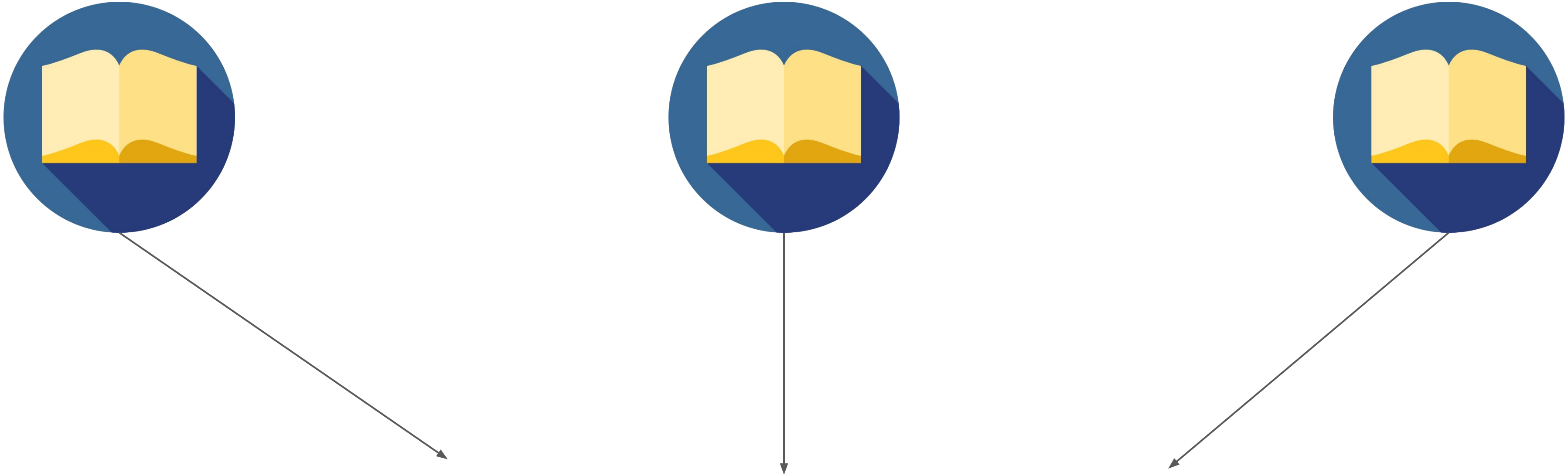
A book of transactions

- Anyone can be a scribe and produce a page.
- New pages are produced indefinitely as long as scribes are interested in doing so.
- Each new page requires some effort to produce.

Importance of consensus

- If multiple conflicting books exist, which is the “right one” ?

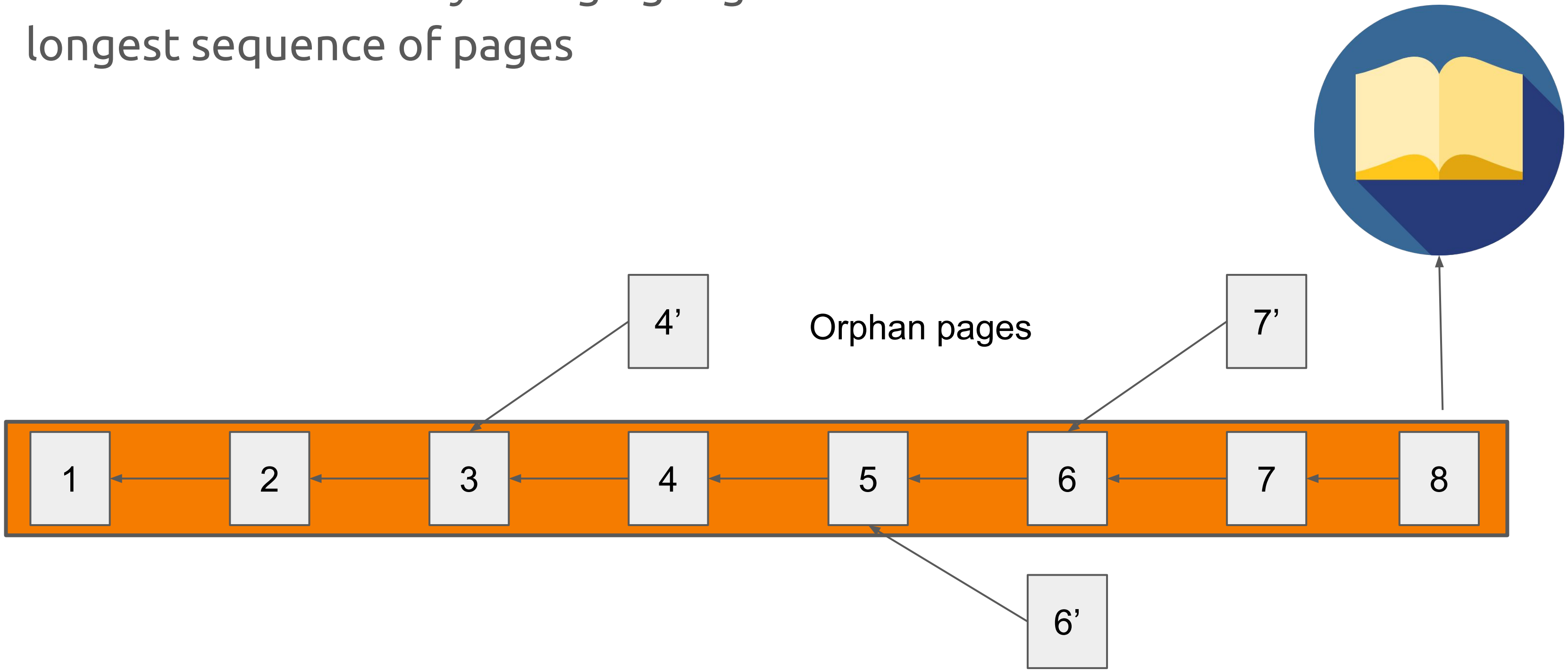
Choosing the correct book ?



The correct book to work on & refer to is the book with the most pages. If multiple exist, just pick one at random.

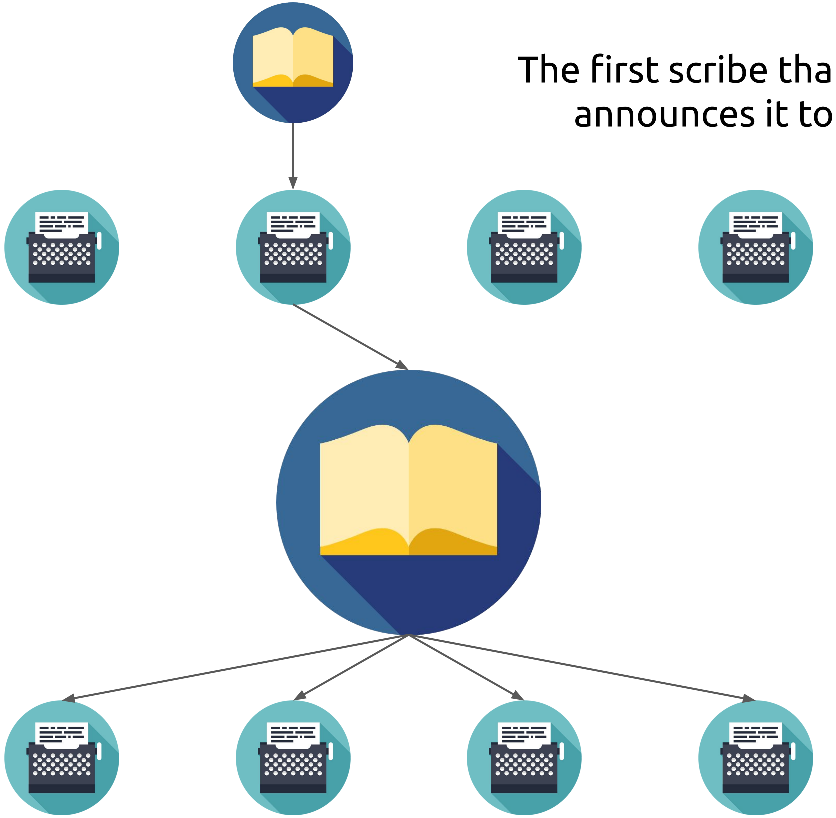
Assembling the current book

- Each page refers only to the previous one
- Current assembled by stringing together the longest sequence of pages



Orphan pages

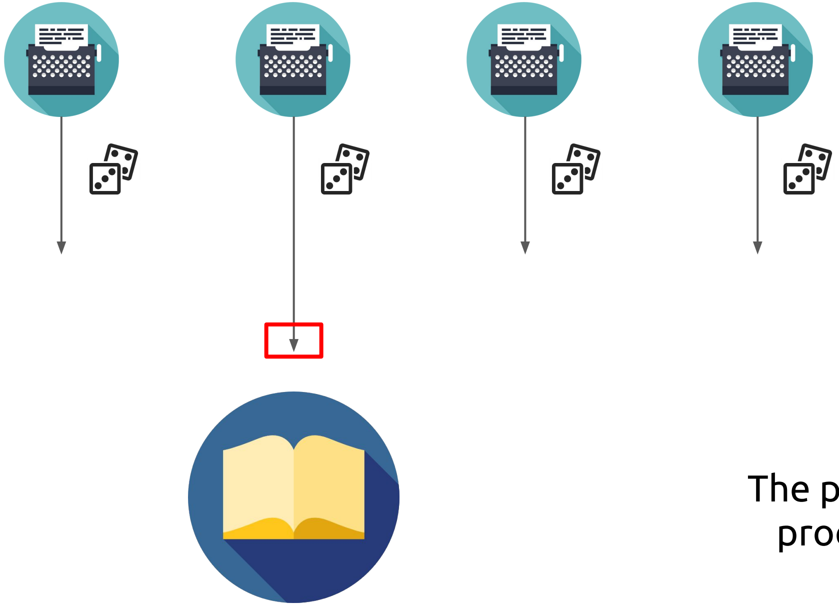
Rules of extending the book



The first scribe that discovers a page announces it to everyone else

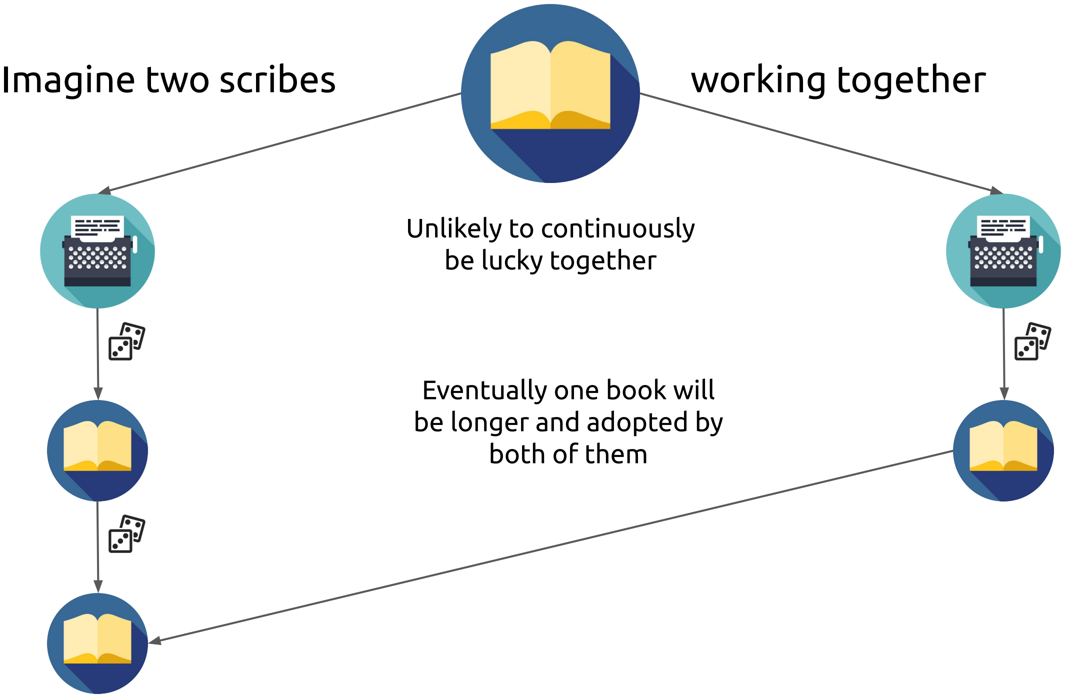
Effort is needed to produce a page

Equivalent to: each page needs a special combination from a set of dice to be rolled.



The probabilistic nature of the process is paramount to its security

The benefits of randomness



Imagine two scribes

working together

Unlikely to continuously be lucky together

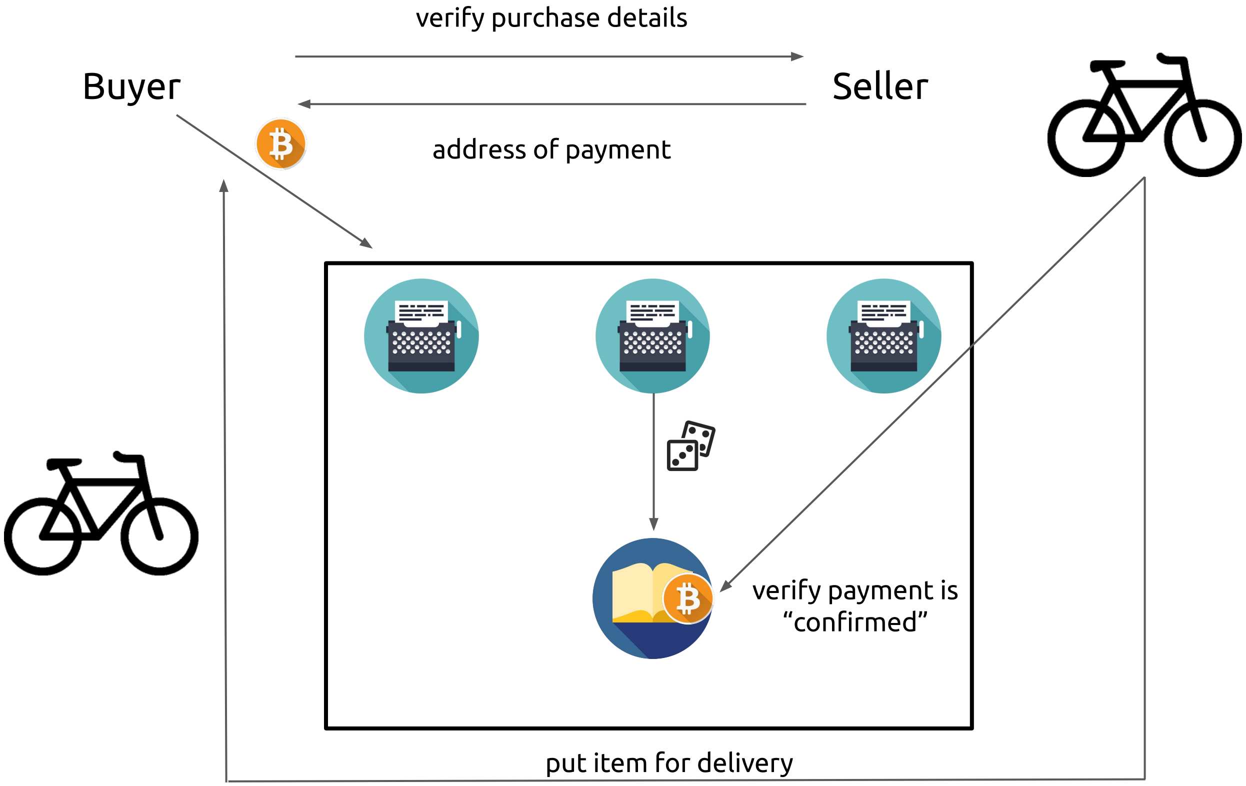
Eventually one book will be longer and adopted by both of them

Symmetry Breaking

Being a scribe

- Anyone can be a scribe for the book.
- As long as one has a set of dice.
- The more dice one has, the higher the likelihood to produce the winning combination to make a page.

Using the book



Parable & Reality

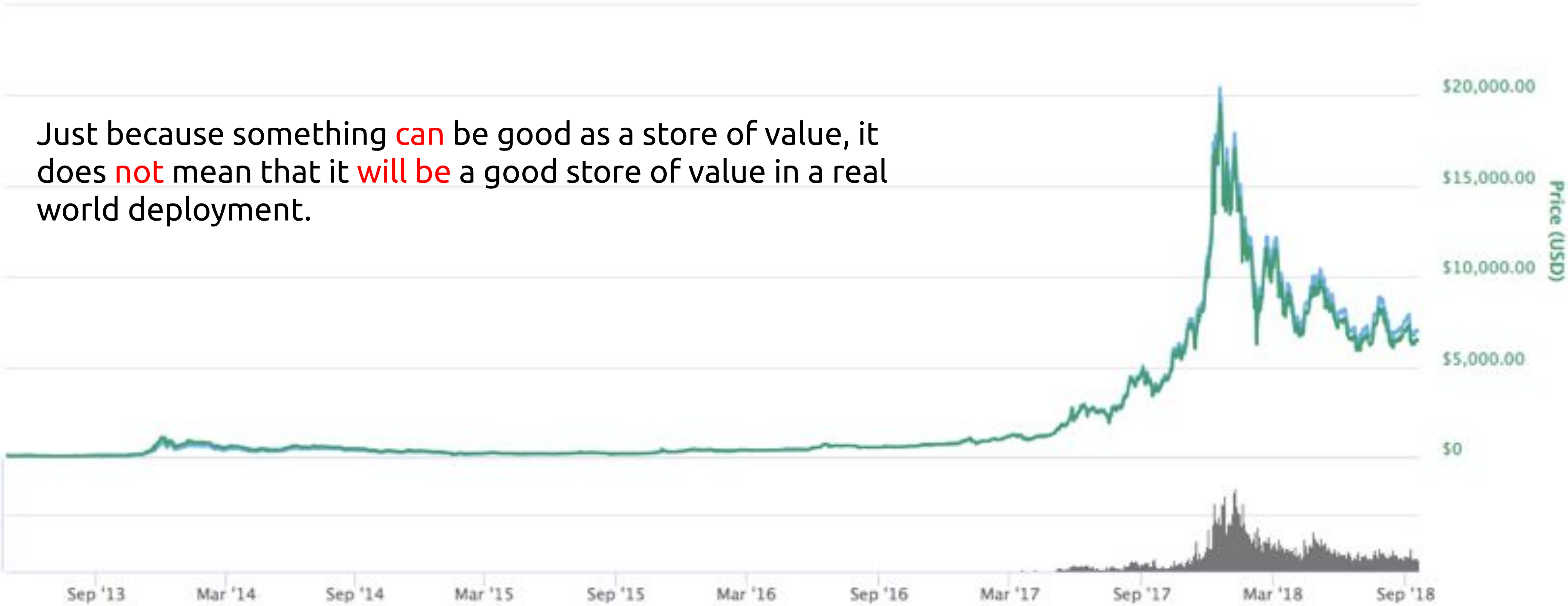
	The “blockchain”
	“Miners” / Computer systems that organize transactions in blocks
	Solving a cryptographic puzzle that is moderate hard to solve
	Using a computer to test for a solution from a large space of candidate solutions

Analysis of Money 3.0

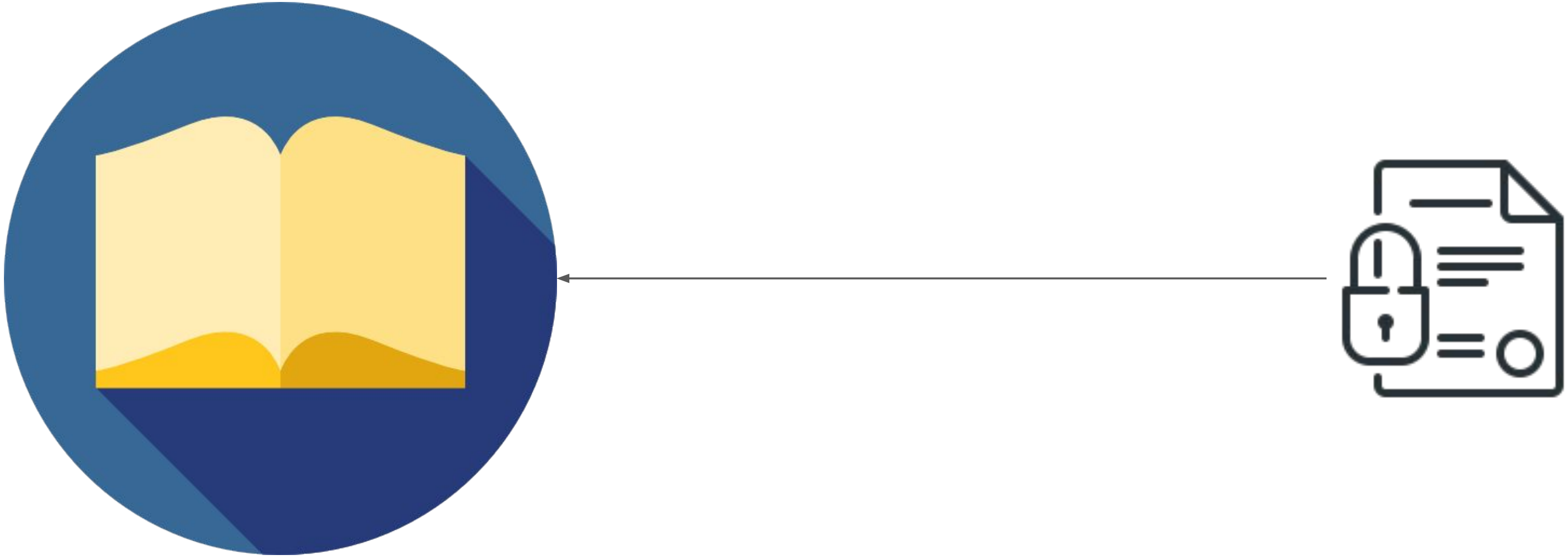
- A medium of exchange: improving
  - assuming internet connectivity / adoption
- A unit of account: good
  - Fungible* & divisible
- A store of value: good
  - No trusted parties
  - No natural deterioration

Word of caution

Just because something can be good as a store of value, it does not mean that it will be a good store of value in a real world deployment.



Smart contract



From Money to Smart Contracts

- Since we have created the book, why stop at recording monetary transactions?
- We can encode in the book’s pages arbitrary relations between persons.
- Furthermore, scribes, can perform tasks such as verifying that stakeholders comply to contractual obligations … and take action if they do not.

Questions to Consider

- How are pages created? Since the book is empty at the beginning, where do the money come from?
- How is it possible to sign something digitally?
- How does a page properly refer to the previous page?

Questions to Consider

- How are pages created? Since the book is empty at the beginning, where do the money come from? - Proof-of-Work
- How is it possible to sign something digitally? - Digital signatures
- How does a page properly refer to the previous page? - Hash functions

Hash Functions

- An algorithm that produces a fingerprint of a file.
- what are the required properties (traditionally):
  a. Efficiency
  b. A good spread for various input distributions.
- What are Security/Cryptographic considerations

$$\mathcal{H} : \{0,1\}^* \to \{0,1\}^\lambda$$

Collision resistance

Collision attack

Find $x, y : \mathcal{H}(x) = \mathcal{H}(y)$

Second pre-image attack

Find $y : \mathcal{H}(x) = \mathcal{H}(y)$

For given x

Birthday paradox

- How many people should be in a room so that the probability that two of them share a birthday becomes larger than 50% ?

Paradox explained

n possible dates $\qquad$ k people

$$\Pr[\neg Col] =$$

$$\frac{n}{n}\frac{n-1}{n}\frac{n-2}{n}\dots\frac{n-k+1}{n} = \prod_{\ell=1}^{k}(1-\frac{\ell}{n})$$

$$\leq \exp(-\frac{1}{n}\sum_{\ell=1}^{k}\ell) = \exp(-k(k+1)/2n)$$

$$\Pr[Col] = \frac{1}{2} \Rightarrow k \approx 1.177\sqrt{n}$$

What do we learn about collision finding?

Describe an algorithm that finds collisions taking advantage of the Birthday paradox.

Pre-image attack

Given $\mathcal{H}(m)$ $m \in \{0,1\}^t$

Find an element of $\mathcal{H}^{-1}(\mathcal{H}(m))$

Generic algorithm tries all possible candidates
Complexity: ?

One-way functions

$$f : X \to Y$$

easy : $\text{given } x \text{ find } f(x)$

hard : $\text{given } f(x) \text{ sample } f^{-1}(f(x))$

Do one-way functions exist?

Relates to most important open question in computer science right now:

$$P \neq NP$$

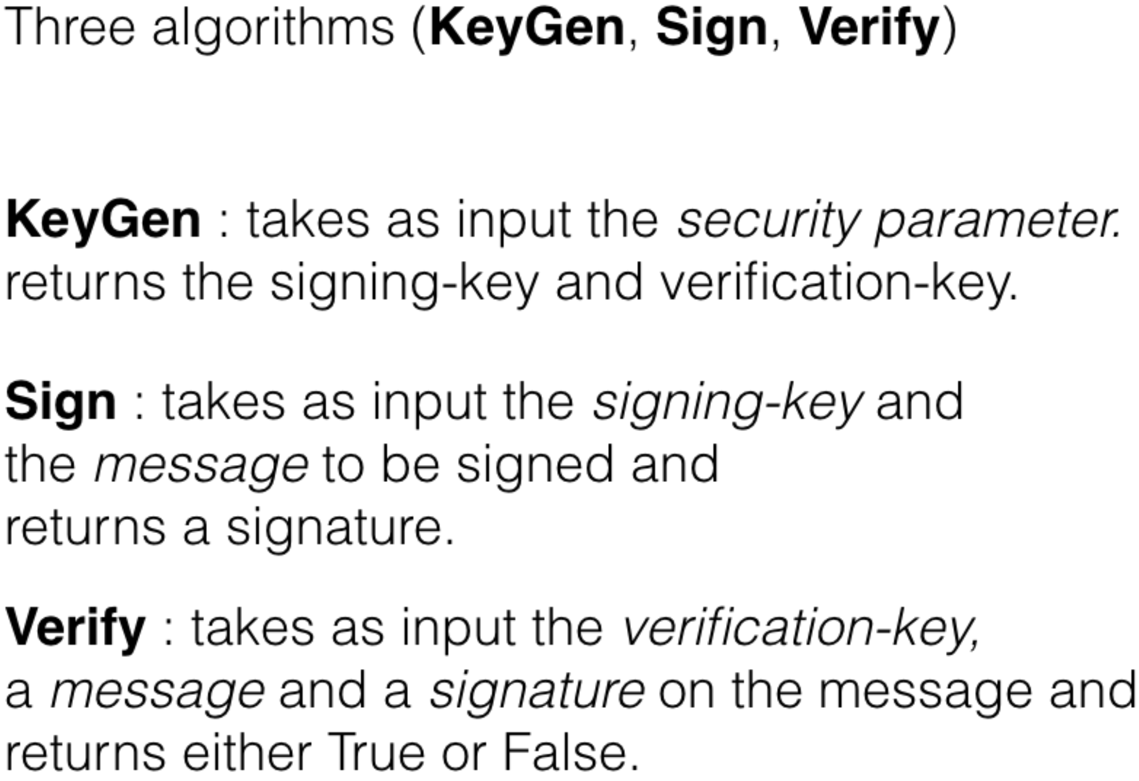
Hash function instantiations

- **Retired.** MD5, SHA1.
- **Current.** SHA2, SHA3, available for 224,256,384,512 bits fingerprints.
- **Bitcoin.** Uses SHA2 with 256 bits output, SHA-256.

Digital Signatures

- Can be produced by one specified entity.
- Can be verified by anyone (that is suitably “equipped" and “initialised”).
- Cannot be forged on a new message even if multiple signatures have been transmitted.

Digital Signatures



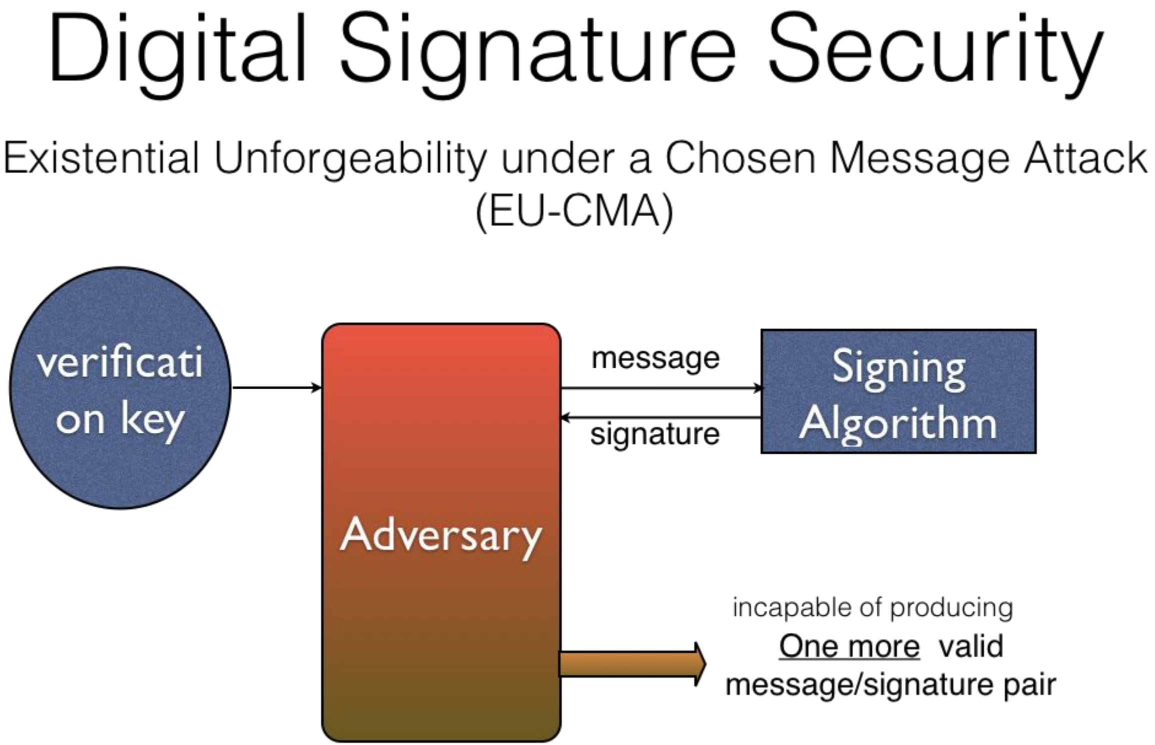
Three algorithms (**KeyGen**, **Sign**, **Verify**)

KeyGen : takes as input the *security parameter.*
returns the signing-key and verification-key.

Sign : takes as input the *signing-key* and
the *message* to be signed and
returns a signature.

Verify : takes as input the *verification-key,*
a *message* and a *signature* on the message and
returns either True or False.

Digital Signature Security



Digital Signature Security

Existential Unforgeability under a Chosen Message Attack (EU-CMA)

incapable of producing <u>One more</u> valid message/signature pair

Constructing Digital Signatures

- Major challenge:
  - what prevents the adversary from learning how to *sign* messages by analyzing the *verification-key?*
- Exercise: construct a digital signature based on a hash-function that is one-time secure (i.e., it is secure for signing only a single message)

Digital Signature Implementations

- Based on the RSA (Rivest Shamir Adleman), one way trapdoor function (with hardness that relates to the factoring problem).
  - The RSA algorithm
- Based on the discrete-logarithm problem.
  - the DSA algorithm
- Bitcoin. Uses ECDSA, a DSA variant over elliptic curve groups.

Proof of Work

Objective: given some *data* ensure that some amount of work has been invested for them.

```
int counter;
counter = 0
while Hash(data, counter) > Target
    increment counter
return counter
```

In this case: proof-of-work of *data* equals to a value *w* with the property Hash(*data*, *w*) <= Target

(Informal) Properties: efficient verification, no computational shortcuts (i.e., independent of algorithm that computes it complexity is proportional to Target), independence for symmetry-breaking.

Proof-of-Work Algorithms

Hashcash (as in previous slide)

Memory hardness

- ASIC resistance (ASIC = application specific integrated circuit).
- A number of algorithms proposed: scrypt, argon, progpow

Cryptocurrencies from a user’s perspective

Bitcoin

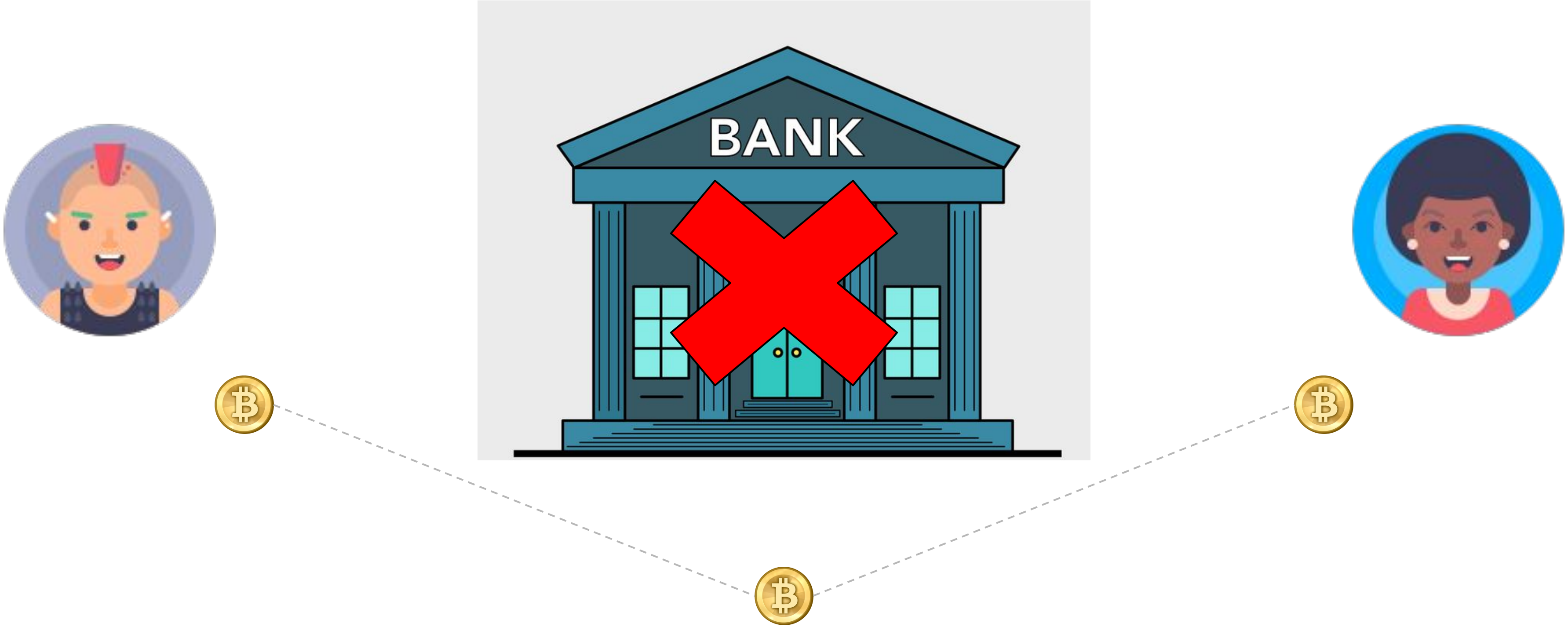
What is bitcoin ?

Bitcoin /ˈbɪtkɔɪn/

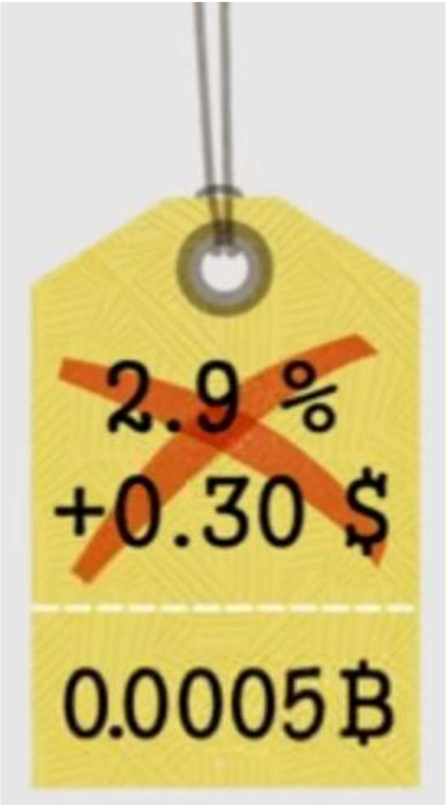
- First decentralized digital currency.
- Digital coins you can send through the Internet.

Advantages

Person to person



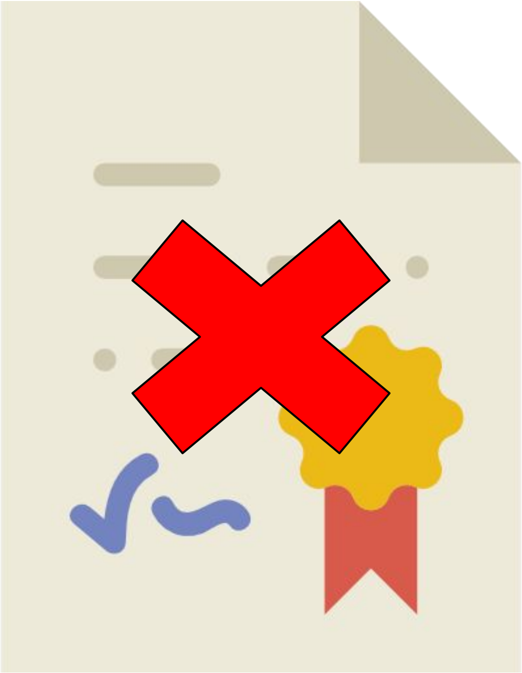
Fees determined by free market



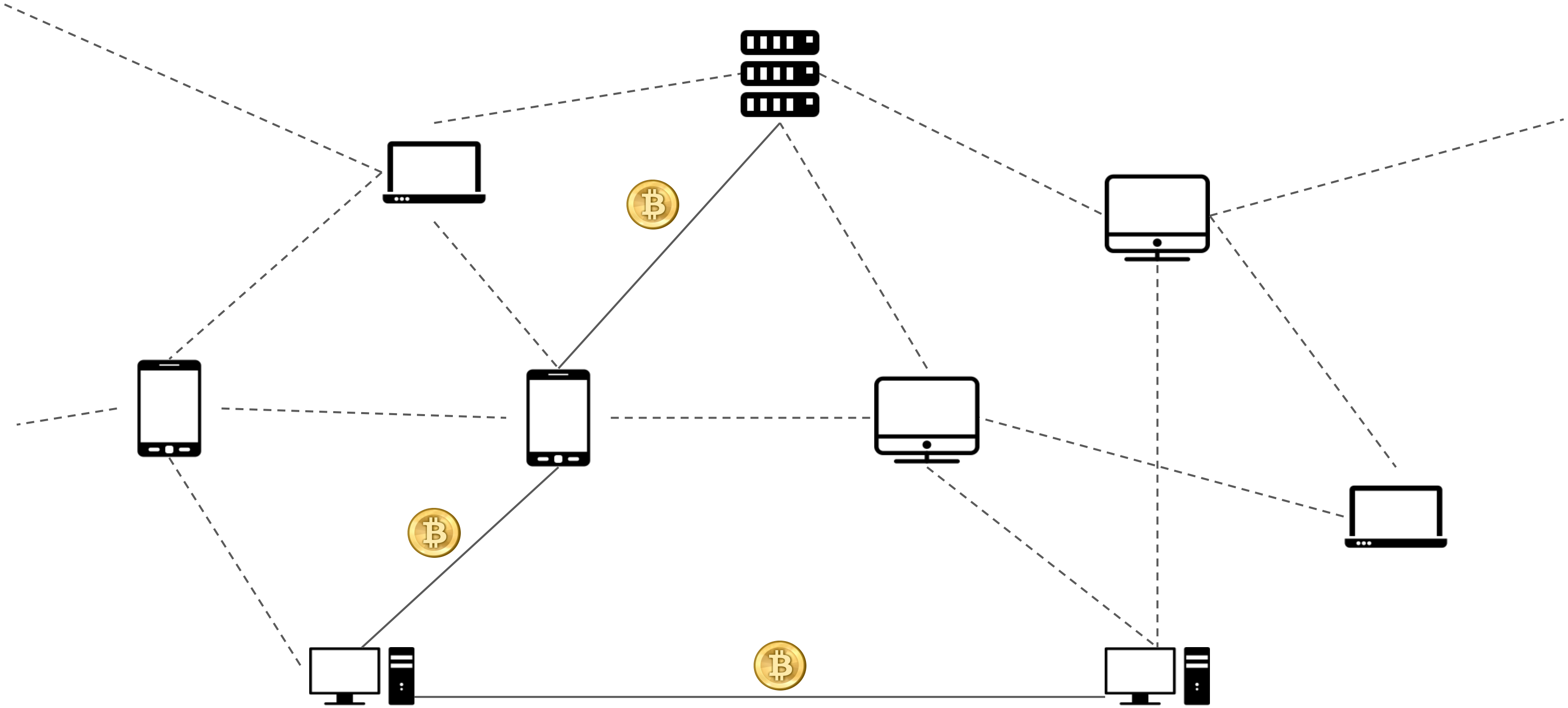
Available to the whole world

You own your account

No prerequisites or arbitrary limits



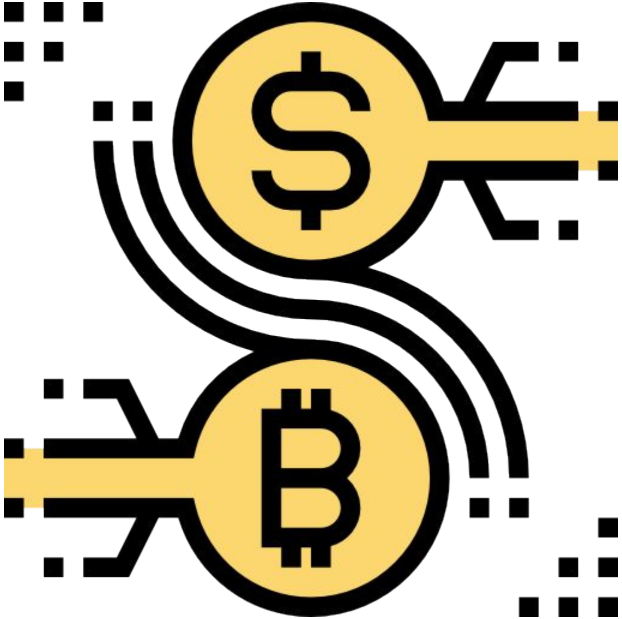
Trust to third party is not a requirement



Open source: Anyone can review the code

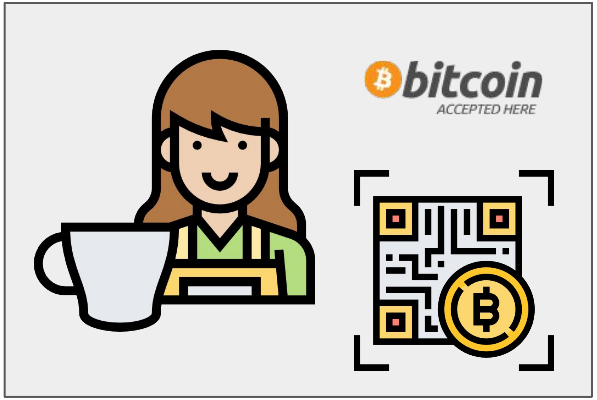
Great! But… how can I use it ?

Exchange: Buy or sell bitcoin for various currencies

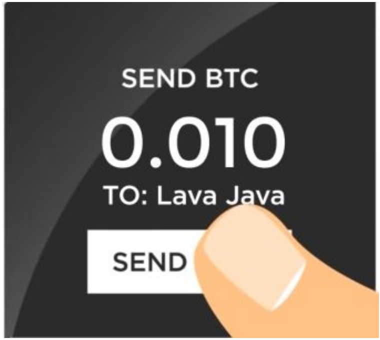


Digital wallet: Bitcoins are kept in your computer or mobile device

Transactions: Bob wants to buy a coffee from Alice



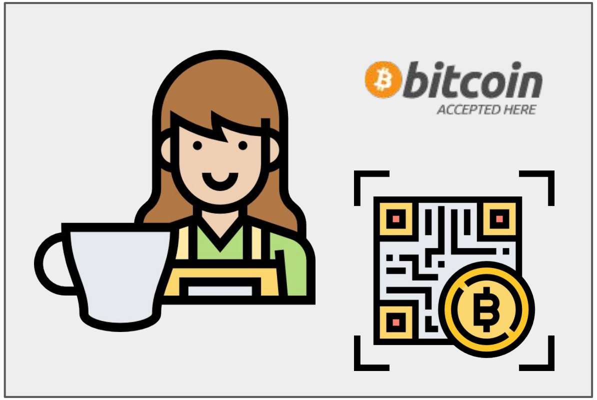
Transactions: Bob pays Alice by sending the proper amount to Alice's bitcoin address



SEND BTC

0.010

TO: Lava Java

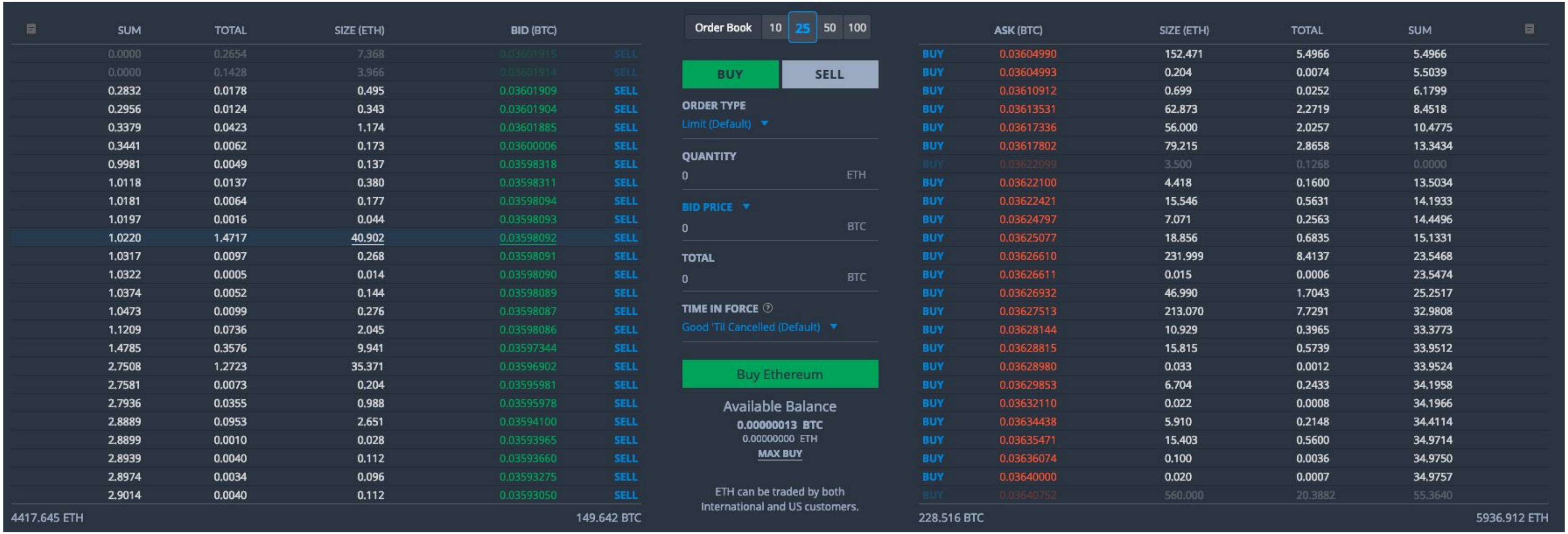


Exchanges

Exchanges

- Bittrex
- Kraken
- Coinbase
- CoinMama
- SpectroCoin
- BitPanda
- LocalBitcoins (Buy / Sell from people near you)
- Bisq (Decentralized)
- Friends!!

Order book



SUM	TOTAL	SIZE (ETH)	BID (BTC)	
0.0000	0.2654	7.368	0.03601915	SELL
0.0000	0.1428	3.966	0.03601914	SELL
0.2832	0.0178	0.495	0.03601909	SELL
0.2956	0.0124	0.343	0.03601904	SELL
0.3379	0.0423	1.174	0.03601885	SELL
0.3441	0.0062	0.173	0.03600006	SELL
0.9981	0.0049	0.137	0.03598318	SELL
1.0118	0.0137	0.380	0.03598311	SELL
1.0181	0.0064	0.177	0.03598094	SELL
1.0197	0.0016	0.044	0.03598093	SELL
1.0220	1.4717	40.902	0.03598092	SELL
1.0317	0.0097	0.268	0.03598091	SELL
1.0322	0.0005	0.014	0.03598090	SELL
1.0374	0.0052	0.144	0.03598089	SELL
1.0473	0.0099	0.276	0.03598087	SELL
1.1209	0.0736	2.045	0.03598086	SELL
1.4785	0.3576	9.941	0.03597344	SELL
2.7508	1.2723	35.371	0.03596902	SELL
2.7581	0.0073	0.204	0.03595981	SELL
2.7936	0.0355	0.988	0.03595978	SELL
2.8889	0.0953	2.651	0.03594100	SELL
2.8899	0.0010	0.028	0.03593965	SELL
2.8939	0.0040	0.112	0.03593660	SELL
2.8974	0.0034	0.096	0.03593275	SELL
2.9014	0.0040	0.112	0.03593050	SELL

4417.645 ETH

149.642 BTC

ORDER TYPE
Limit (Default)

QUANTITY
0 ETH

BID PRICE
0 BTC

TOTAL
0 BTC

TIME IN FORCE
Good 'Til Cancelled (Default)

Available Balance
0.00000013 BTC
0.00000000 ETH
MAX BUY

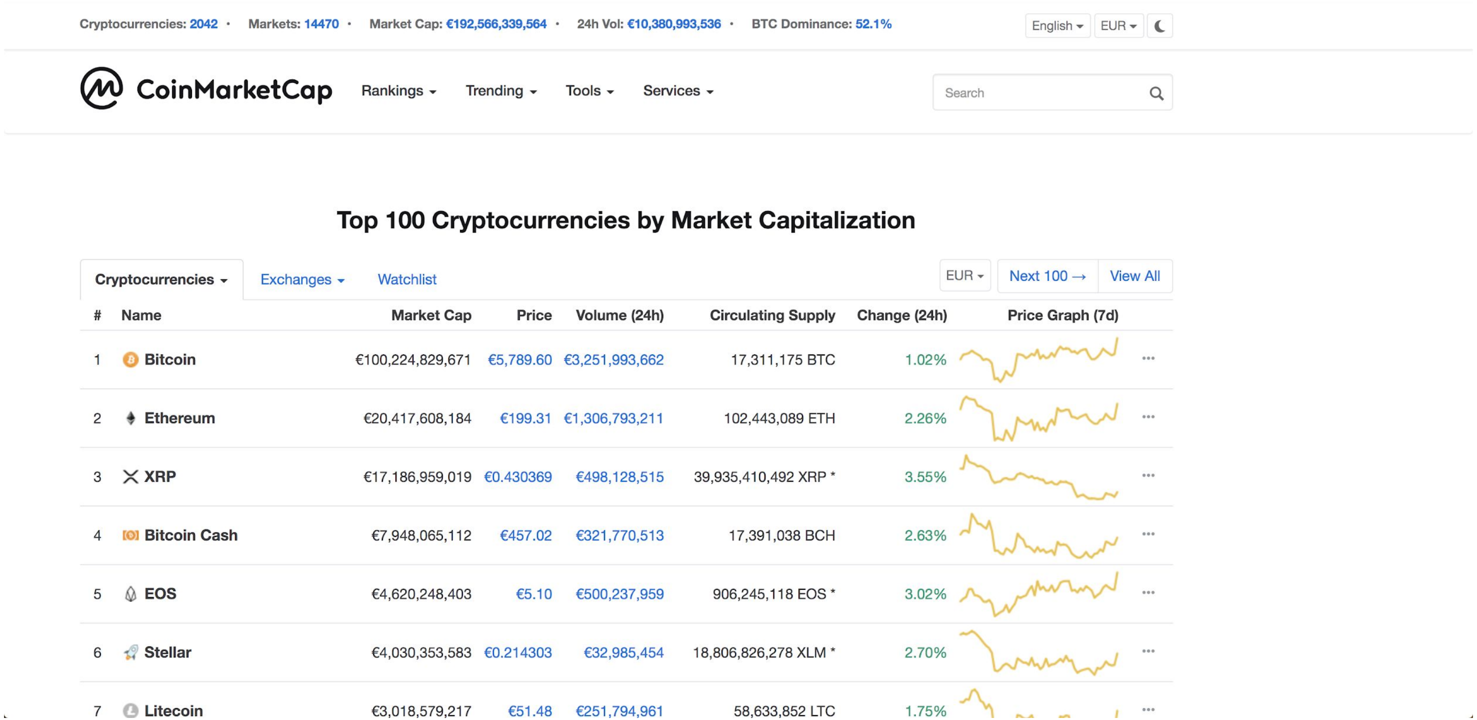
ETH can be traded by both International and US customers.

	ASK (BTC)	SIZE (ETH)	TOTAL	SUM
BUY	0.03604990	152.471	5.4966	5.4966
BUY	0.03604993	0.204	0.0074	5.5039
BUY	0.03610912	0.699	0.0252	6.1799
BUY	0.03613531	62.873	2.2719	8.4518
BUY	0.03617336	56.000	2.0257	10.4775
BUY	0.03617802	79.215	2.8658	13.3434
BUY	0.03622099	3.500	0.1268	0.0000
BUY	0.03622100	4.418	0.1600	13.5034
BUY	0.03622421	15.546	0.5631	14.1933
BUY	0.03624797	7.071	0.2563	14.4496
BUY	0.03625077	18.856	0.6835	15.1331
BUY	0.03626610	231.999	8.4137	23.5468
BUY	0.03626611	0.015	0.0006	23.5474
BUY	0.03626932	46.990	1.7043	25.2517
BUY	0.03627513	213.070	7.7291	32.9808
BUY	0.03628144	10.929	0.3965	33.3773
BUY	0.03628815	15.815	0.5739	33.9512
BUY	0.03628980	0.033	0.0012	33.9524
BUY	0.03629853	6.704	0.2433	34.1958
BUY	0.03632110	0.022	0.0008	34.1966
BUY	0.03634438	5.910	0.2148	34.4114
BUY	0.03635471	15.403	0.5600	34.9714
BUY	0.03636074	0.100	0.0036	34.9750
BUY	0.03640000	0.020	0.0007	34.9757
BUY	0.03640752	560.000	20.3882	55.3640

228.516 BTC

5936.912 ETH

Coinmarketcap



Cryptocurrencies: 2042 • Markets: 14470 • Market Cap: €192,566,339,564 • 24h Vol: €10,380,993,536 • BTC Dominance: 52.1%

Top 100 Cryptocurrencies by Market Capitalization

#	Name	Market Cap	Price	Volume (24h)	Circulating Supply	Change (24h)	Price Graph (7d)
1	Bitcoin	€100,224,829,671	€5,789.60	€3,251,993,662	17,311,175 BTC	1.02%	
2	Ethereum	€20,417,608,184	€199.31	€1,306,793,211	102,443,089 ETH	2.26%	
3	XRP	€17,186,959,019	€0.430369	€498,128,515	39,935,410,492 XRP *	3.55%	
4	Bitcoin Cash	€7,948,065,112	€457.02	€321,770,513	17,391,038 BCH	2.63%	
5	EOS	€4,620,248,403	€5.10	€500,237,959	906,245,118 EOS *	3.02%	
6	Stellar	€4,030,353,583	€0.214303	€32,985,454	18,806,826,278 XLM *	2.70%	
7	Litecoin	€3,018,579,217	€51.48	€251,794,961	58,633,852 LTC	1.75%	

Addresses

Addresses

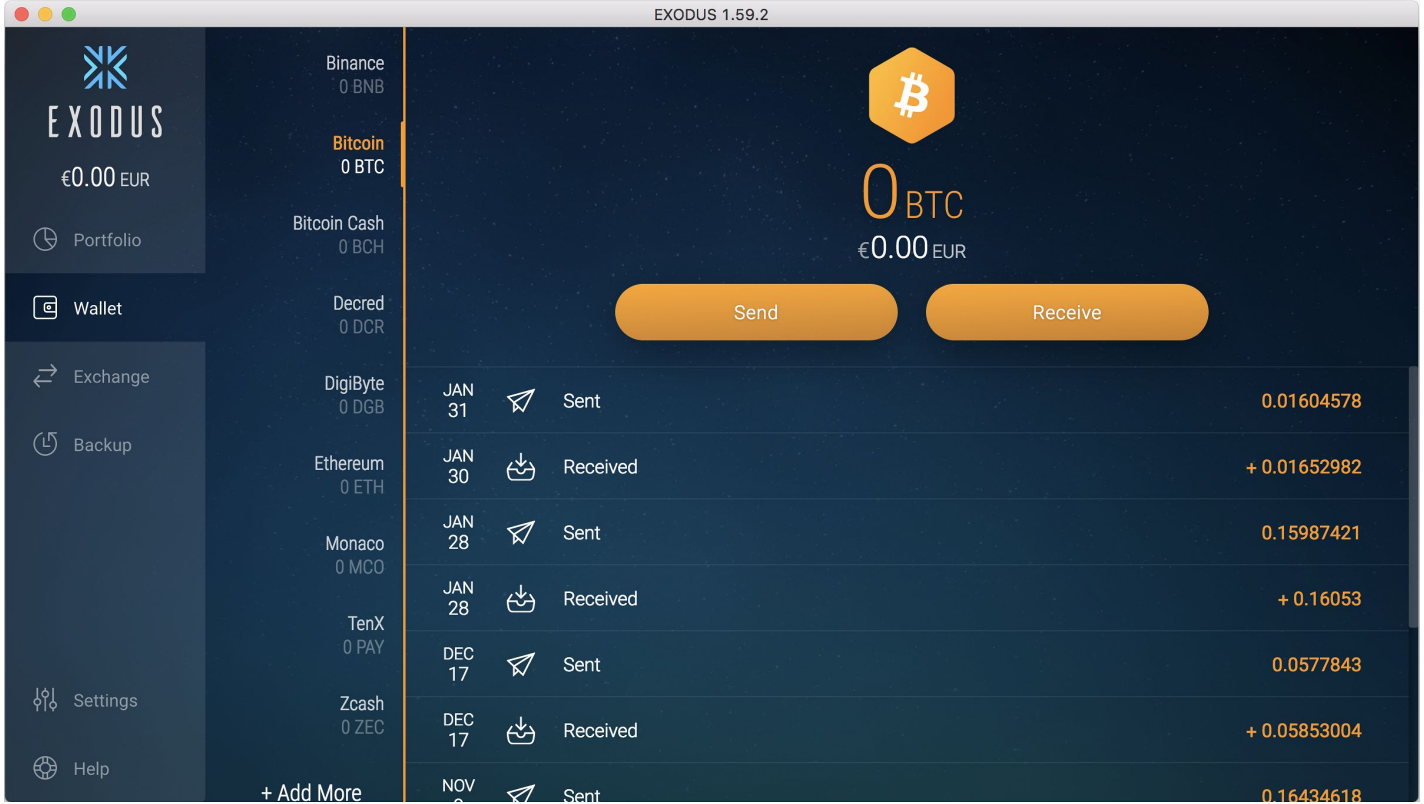
- Like an email address.
- You send bitcoins to a person by sending bitcoins to one of their addresses.
- You can have as many addresses as you want.
- No need to be online to create an address.
- Pseudonymous: A unique address should be used for each transaction.
- Most wallets do it automatically.

Addresses

1BvBMSEYstWetqTFn5Au4m4GFg7xJaNVN2

Wallets

Desktop Wallet - Exodus



€0.00 EUR

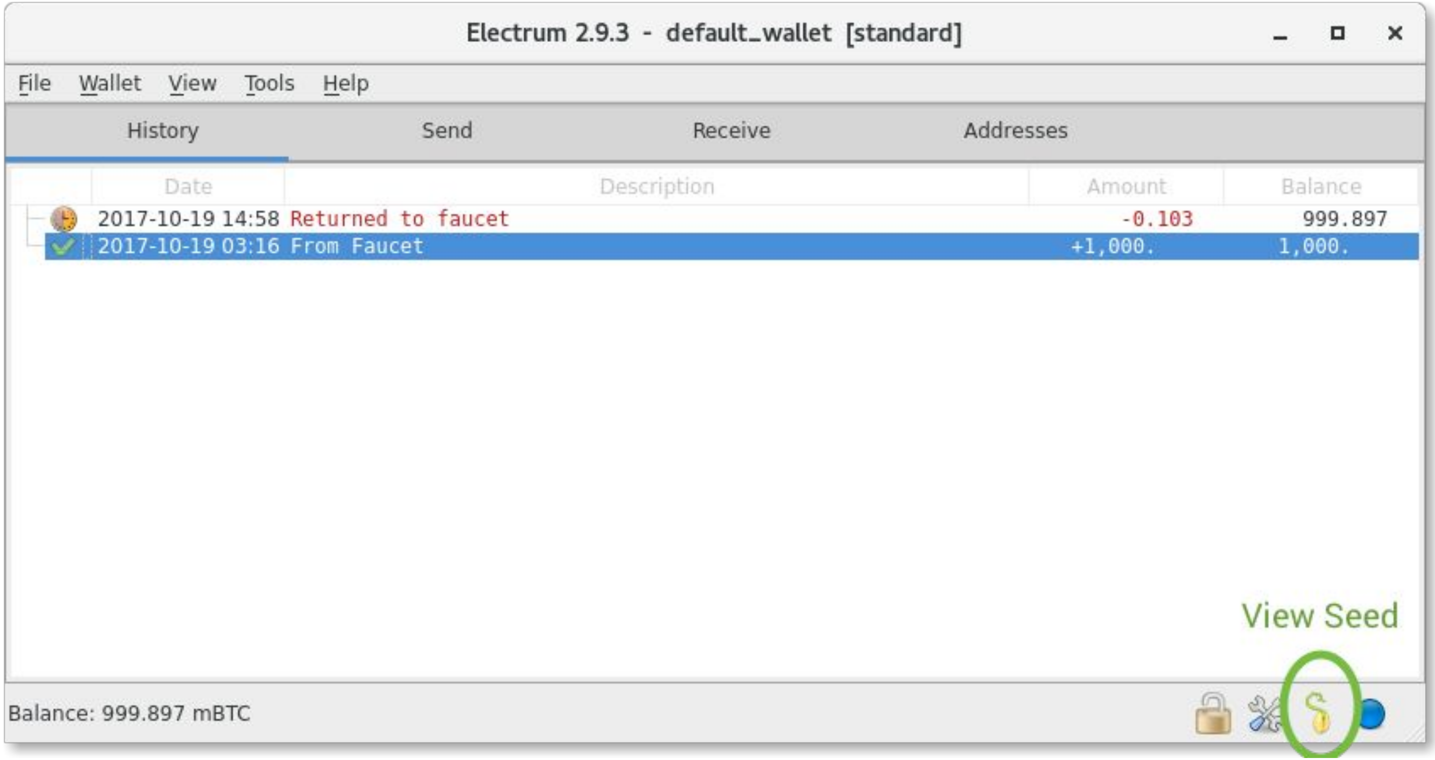
Binance	0 BNB
Bitcoin	0 BTC
Bitcoin Cash	0 BCH
Decred	0 DCR
DigiByte	0 DGB
Ethereum	0 ETH
Monaco	0 MCO
TenX	0 PAY
Zcash	0 ZEC

0 BTC

€0.00 EUR

JAN 31	Sent	0.01604578
JAN 30	Received	+ 0.01652982
JAN 28	Sent	0.15987421
JAN 28	Received	+ 0.16053
DEC 17	Sent	0.0577843
DEC 17	Received	+ 0.05853004
NOV	Sent	0.16434618

Desktop Bitcoin Wallet - Electrum (open source)

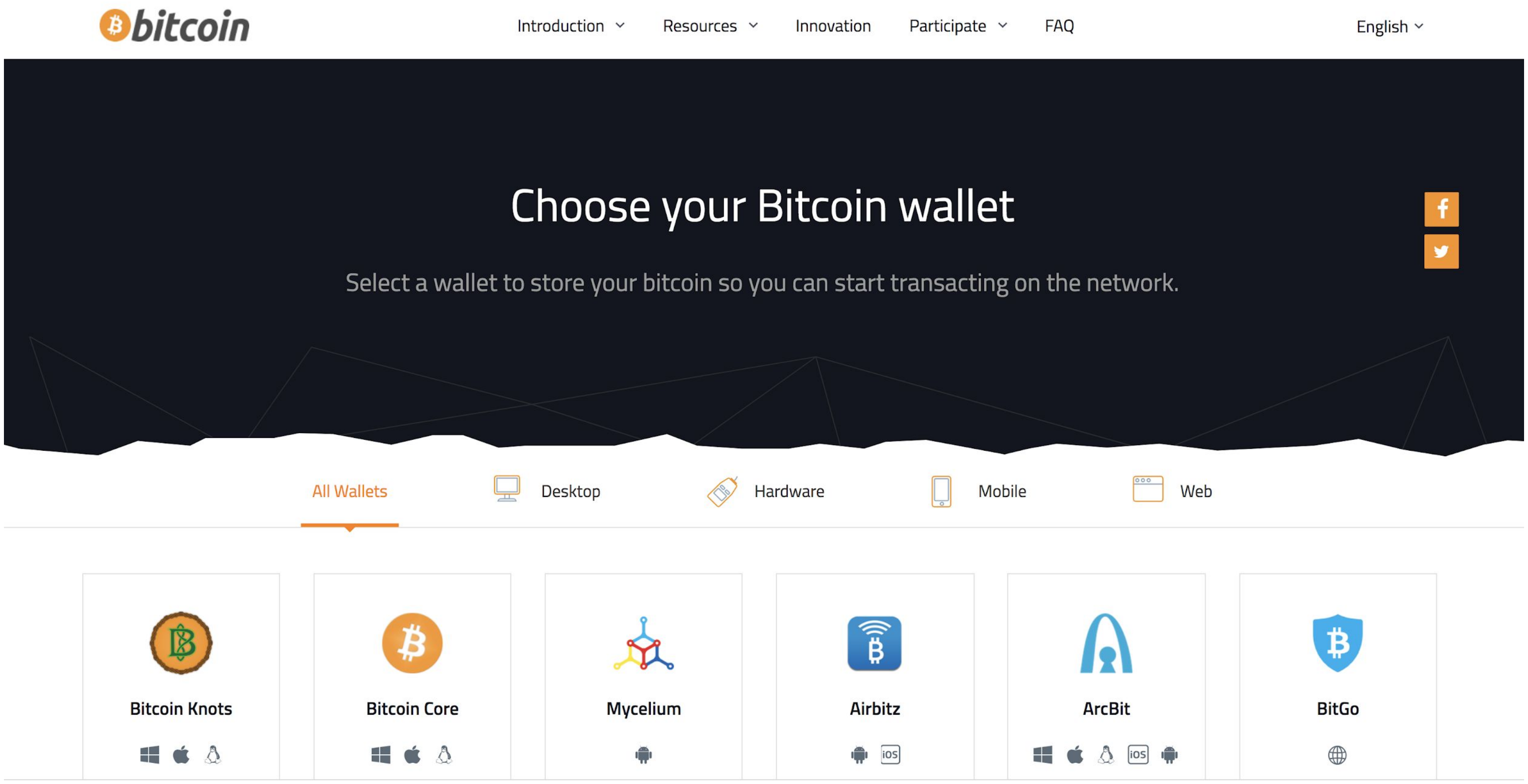


Date	Description	Amount	Balance
2017-10-19 14:58	Returned to faucet	-0.103	999.897
2017-10-19 03:16	From Faucet	+1,000.	1,000.

Balance: 999.897 mBTC

View Seed

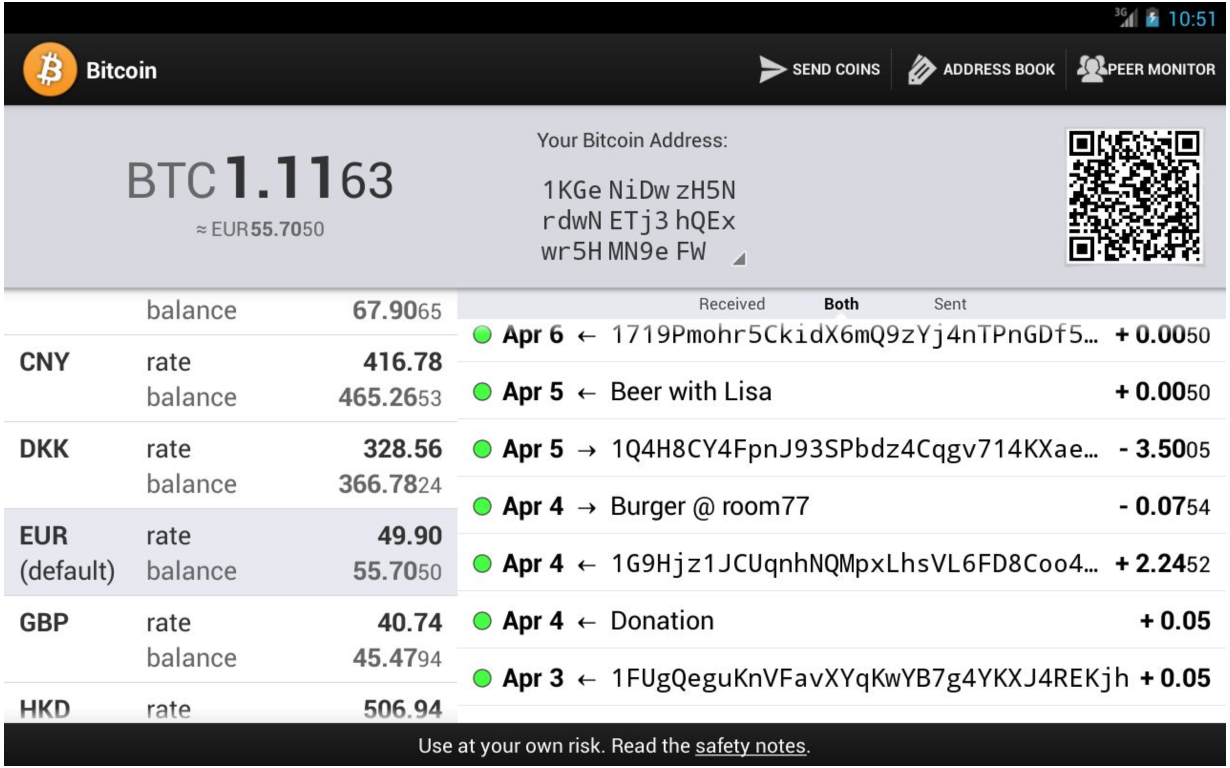
More Bitcoin wallets … (mobile)



Choose your Bitcoin wallet

Select a wallet to store your bitcoin so you can start transacting on the network.

Mobile wallet - Android



BTC 1.1163

≈ EUR 55.7050

Your Bitcoin Address:

1KGe NiDw zH5N
rdwN ETj3 hQEx
wr5H MN9e FW

	balance	67.9065
CNY	rate balance	416.78 465.2653
DKK	rate balance	328.56 366.7824
EUR (default)	rate balance	49.90 55.7050
GBP	rate balance	40.74 45.4794
HKD	rate	506.94

●	Apr 6	←	1719Pmohr5CkidX6mQ9zYj4nTPnGDf5…	+ 0.0050
●	Apr 5	←	Beer with Lisa	+ 0.0050
●	Apr 5	→	1Q4H8CY4FpnJ93SPbdz4Cqgv714KXae…	- 3.5005
●	Apr 4	→	Burger @ room77	- 0.0754
●	Apr 4	←	1G9Hjz1JCUqnhNQMpxLhsVL6FD8Coo4…	+ 2.2452
●	Apr 4	←	Donation	+ 0.05
●	Apr 3	←	1FUgQeguKnVFavXYqKwYB7g4YKXJ4REKjh	+ 0.05

Use at your own risk. Read the safety notes.

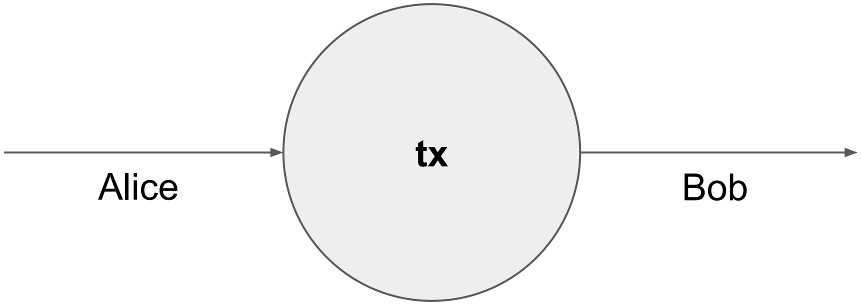
Hardware wallets

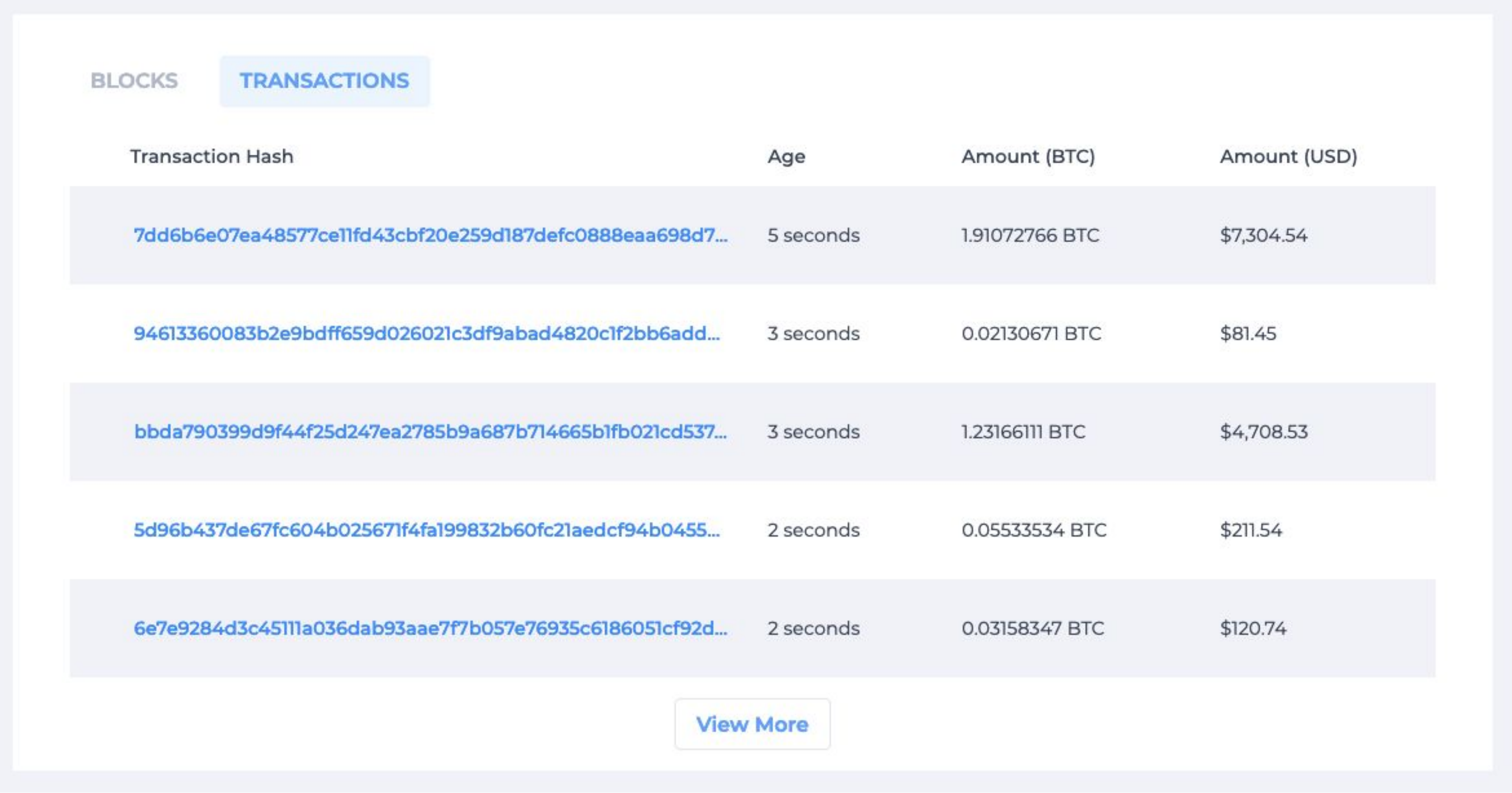
Explorers

Explorers

- An online blockchain browser.
- Displays the contents of individual blocks and transactions
- Displays the transaction histories and balances of addresses.
- Quick way to see if your transactions are confirmed.
- Bitcoin:
  - https://www.blockchain.com/explorer (Mainnet)
  - https://testnet.blockexplorer.com/ (Testnet)
- Ethereum:
  - https://etherscan.io/ (Mainnet)
  - https://ropsten.etherscan.io/ (Testnet)
  - https://rinkeby.etherscan.io/ (Testnet)

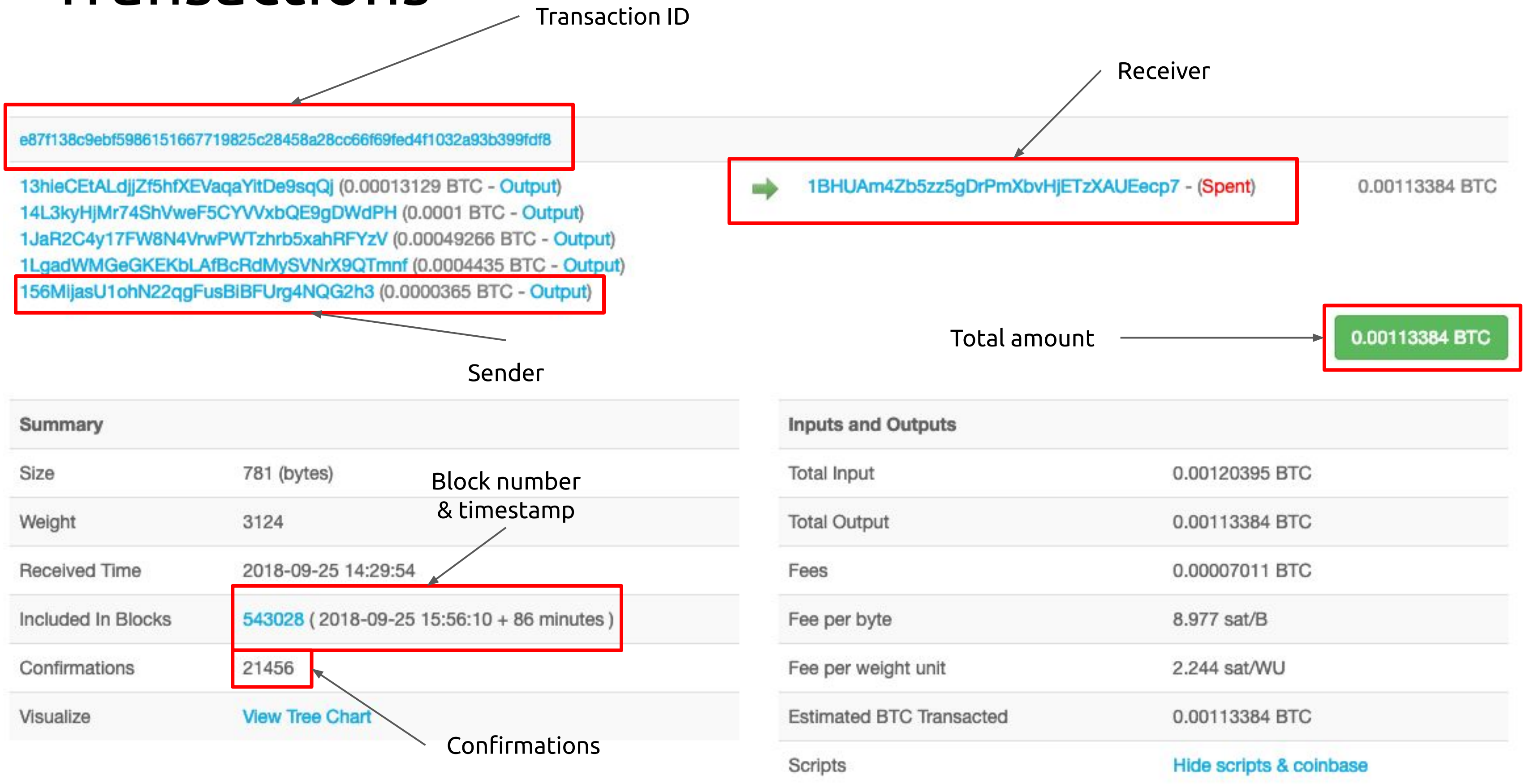
Transactions





Transaction Hash	Age	Amount (BTC)	Amount (USD)
7dd6b6e07ea48577ce11fd43cbf20e259d187defc0888eaa698d7...	5 seconds	1.91072766 BTC	$7,304.54
94613360083b2e9bdff659d026021c3df9abad4820c1f2bb6add...	3 seconds	0.02130671 BTC	$81.45
bbda790399d9f44f25d247ea2785b9a687b714665b1fb021cd537...	3 seconds	1.23166111 BTC	$4,708.53
5d96b437de67fc604b025671f4fa199832b60fc21aedcf94b0455...	2 seconds	0.05533534 BTC	$211.54
6e7e9284d3c45111a036dab93aae7f7b057e76935c6186051cf92d...	2 seconds	0.03158347 BTC	$120.74

Transactions



e87f138c9ebf5986151667719825c28458a28cc66f69fed4f1032a93b399fdf8

13hieCEtALdjjZf5hfXEVaqaYitDe9sqQj (0.00013129 BTC - Output)
14L3kyHjMr74ShVweF5CYVVxbQE9gDWdPH (0.0001 BTC - Output)
1JaR2C4y17FW8N4VrwPWTzhrb5xahRFYzV (0.00049266 BTC - Output)
1LgadWMGeGKEKbLAfBcRdMySVNrX9QTmnf (0.0004435 BTC - Output)
156MijasU1ohN22qgFusBiBFUrg4NQG2h3 (0.0000365 BTC - Output)

➡ 1BHUAm4Zb5zz5gDrPmXbvHjETzXAUEecp7 - (Spent) 0.00113384 BTC

0.00113384 BTC

Summary	
Size	781 (bytes)
Weight	3124
Received Time	2018-09-25 14:29:54
Included In Blocks	543028 (2018-09-25 15:56:10 + 86 minutes)
Confirmations	21456
Visualize	View Tree Chart

Inputs and Outputs	
Total Input	0.00120395 BTC
Total Output	0.00113384 BTC
Fees	0.00007011 BTC
Fee per byte	8.977 sat/B
Fee per weight unit	2.244 sat/WU
Estimated BTC Transacted	0.00113384 BTC
Scripts	Hide scripts & coinbase

Transaction ID

Receiver

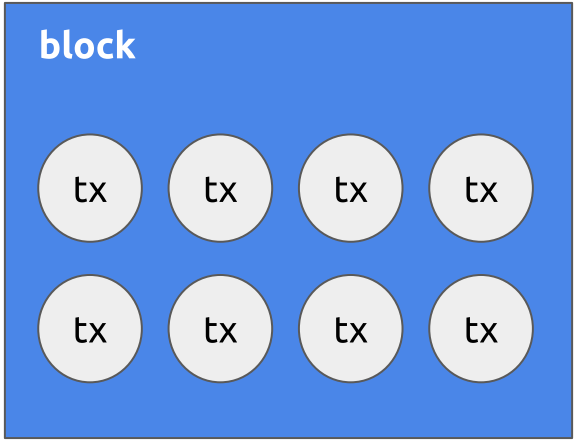
Sender

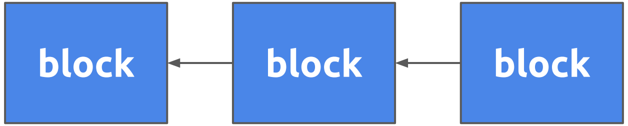
Total amount

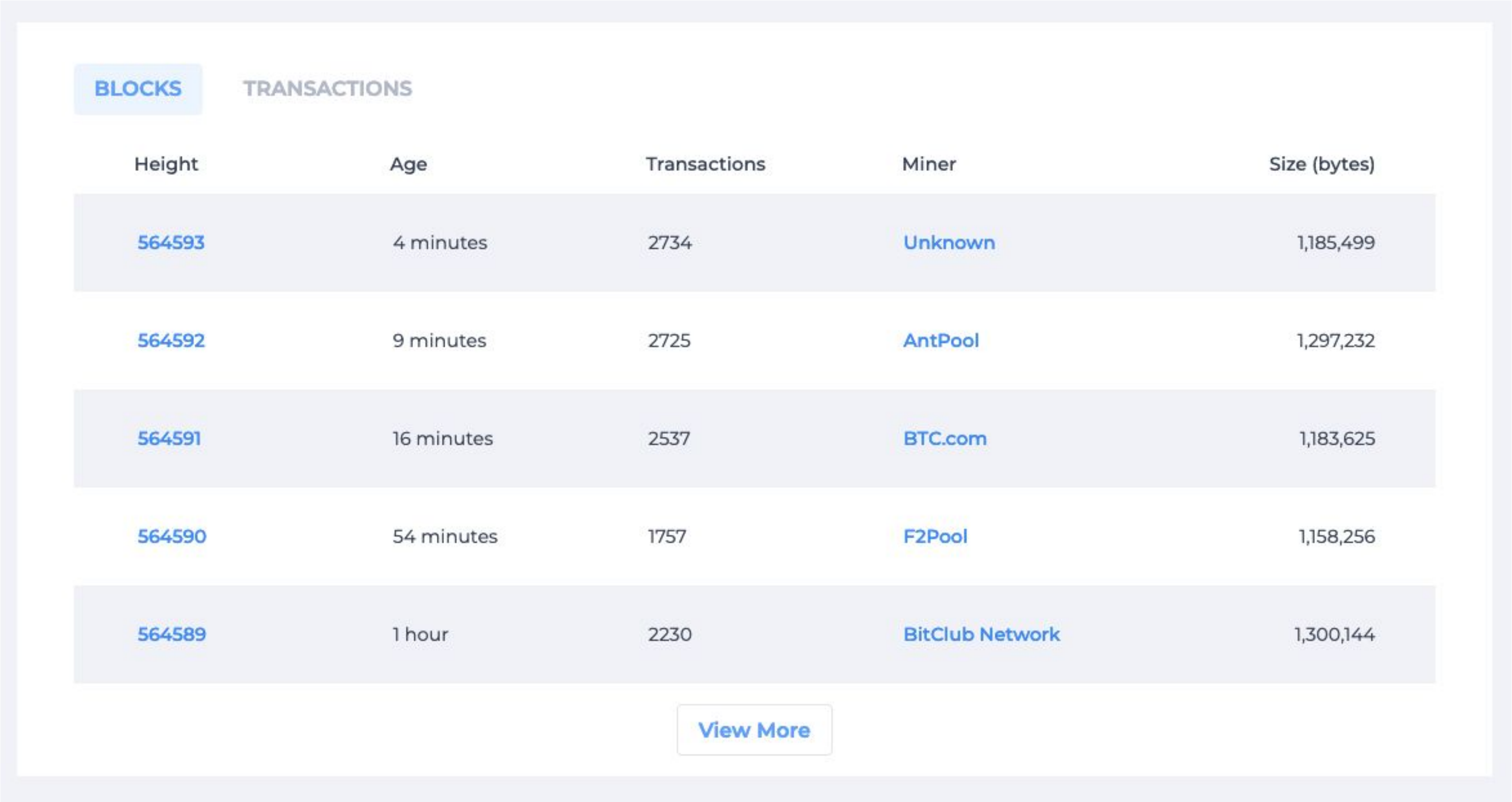
Block number
& timestamp

Confirmations

Blocks

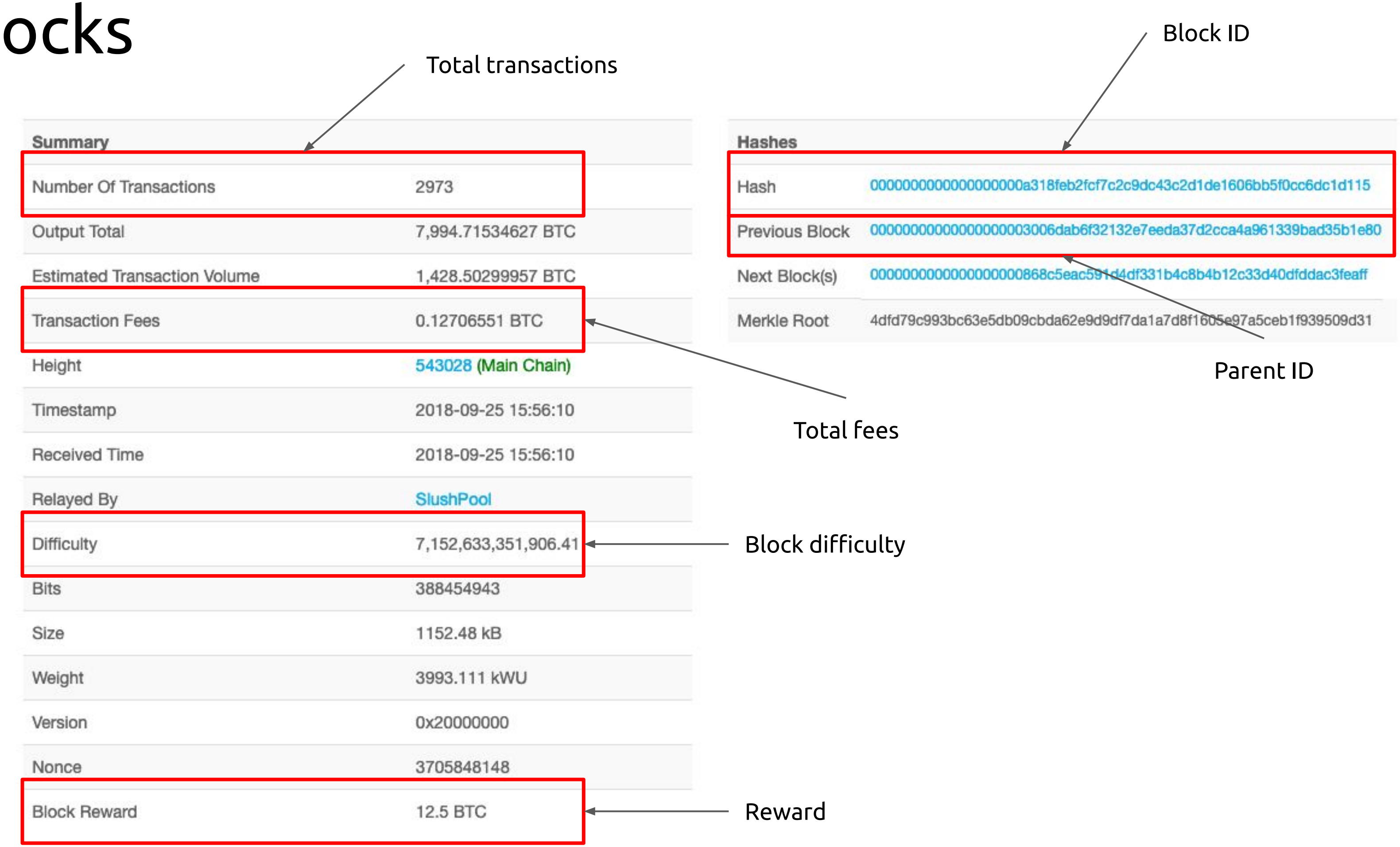






Height	Age	Transactions	Miner	Size (bytes)
564593	4 minutes	2734	Unknown	1,185,499
564592	9 minutes	2725	AntPool	1,297,232
564591	16 minutes	2537	BTC.com	1,183,625
564590	54 minutes	1757	F2Pool	1,158,256
564589	1 hour	2230	BitClub Network	1,300,144

Blocks



Summary	
Number Of Transactions	2973
Output Total	7,994.71534627 BTC
Estimated Transaction Volume	1,428.50299957 BTC
Transaction Fees	0.12706551 BTC
Height	543028 (Main Chain)
Timestamp	2018-09-25 15:56:10
Received Time	2018-09-25 15:56:10
Relayed By	SlushPool
Difficulty	7,152,633,351,906.41
Bits	388454943
Size	1152.48 kB
Weight	3993.111 kWU
Version	0x20000000
Nonce	3705848148
Block Reward	12.5 BTC

Hashes	
Hash	0000000000000000000a318feb2fcf7c2c9dc43c2d1de1606bb5f0cc6dc1d115
Previous Block	00000000000000000003006dab6f32132e7eeda37d2cca4a961339bad35b1e80
Next Block(s)	0000000000000000000868c5eac591d4df331b4c8b4b12c33d40dfddac3feaff
Merkle Root	4dfd79c993bc63e5db09cbda62e9d9df7da1a7d8f1605e97a5ceb1f939509d31

Total transactions

Block ID

Total fees

Parent ID

Block difficulty

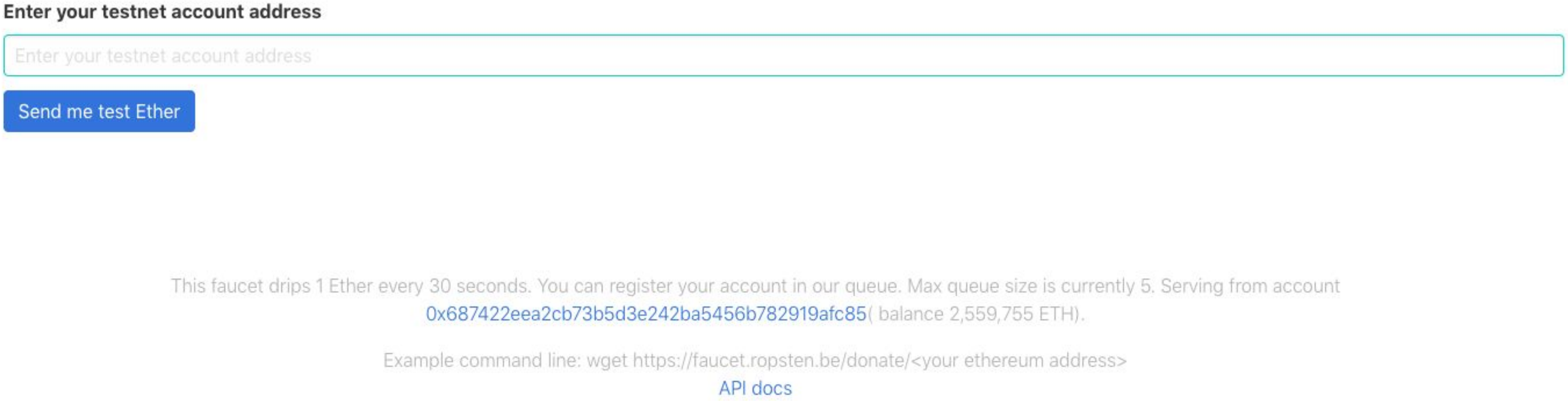
Reward

Development

- Local blockchains: e.g., ganache
    - Used for local development.
    - Instant mining.
    - Very small in size.
  - In class we will use our own ETH deployment.
- Testnets:
    - Used for testing and experiment. Very useful specifically for smart contract development.
    - Different blockchain and different genesis block.
    - Coins are separated and and distinct from actual coins (with no real value).
    - Different ports and DNS seeds.
    - Bitcoin: Testnet3 (Run bitcoin or bitcoind with the -testnet flag)
    - Ethereum: Rinkeby, Ropsten, Kovan
- Main net (production):
    - Blockchains are immutable and irrevertible.
    - You cannot simply update your code once deployed!

Faucet

- A way to get test coins necessary for any testing.
- Ethereum:
    - https://faucet.rinkeby.io/
    - https://faucet.metamask.io/
    - https://faucet.ropsten.be/
- Bitcoin:
    - http://tbtc.bitaps.com/
    - https://bitcoinfaucet.uo1.net/
    - https://testnet-faucet.mempool.co/
    - https://block.io/ (Online testnet wallet)



Enter your testnet account address
Enter your testnet account address
Send me test Ether

This faucet drips 1 Ether every 30 seconds. You can register your account in our queue. Max queue size is currently 5. Serving from account 0x687422eea2cb73b5d3e242ba5456b782919afc85(balance 2,559,755 ETH).

Example command line: wget https://faucet.ropsten.be/donate/<your ethereum address>

API docs