

Introduction to

# Blockchain Science & Engineering

An informatics Master's level course

Aggelos Kiayias

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



(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” ?



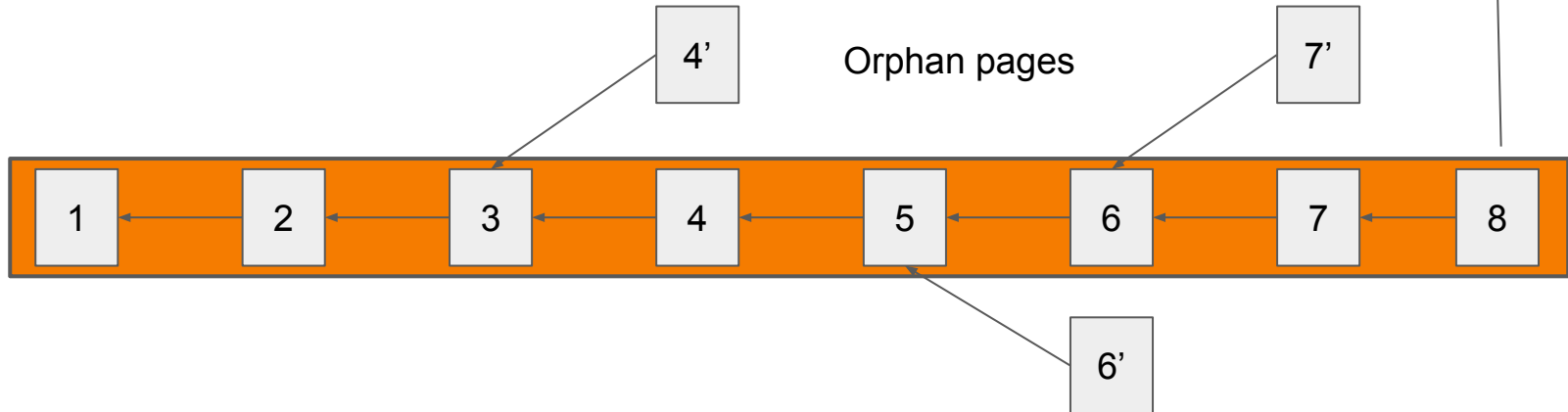
# Choosing the correct book ?



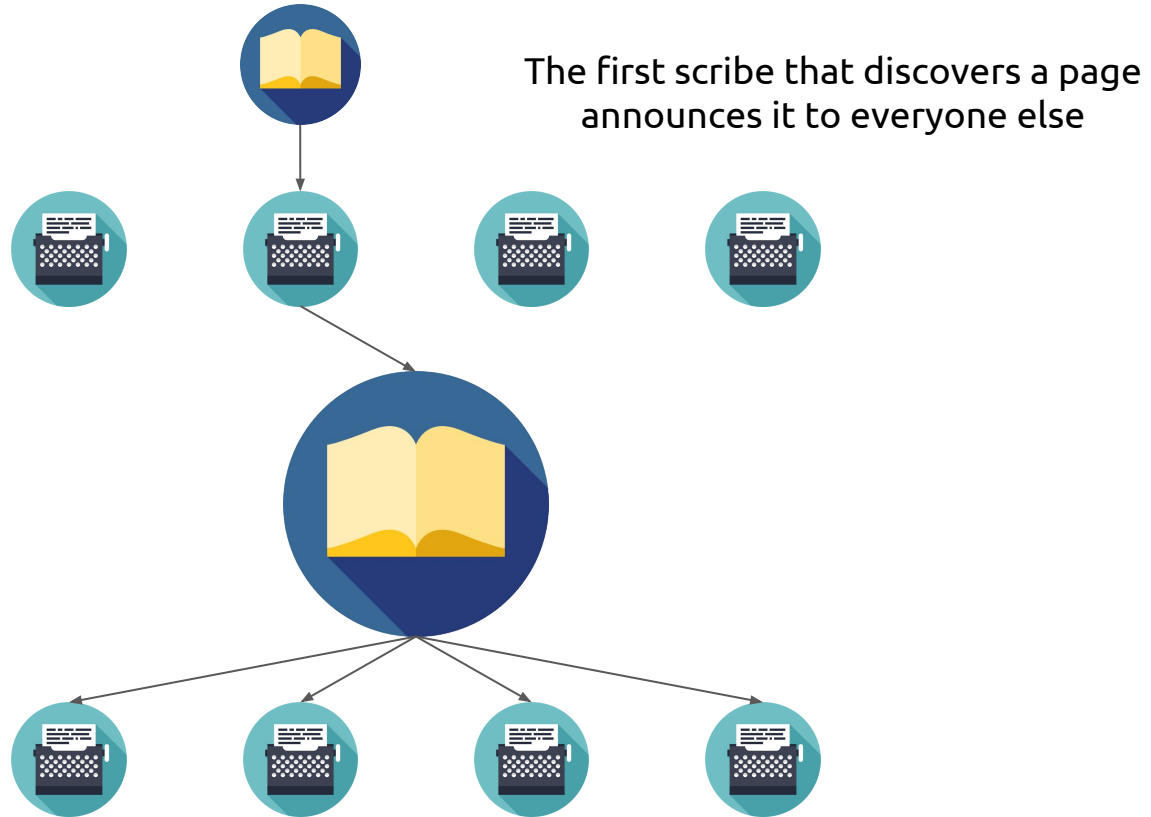
The **correct book** to work on & refer to is the book with the most pages. If multiple exist, just pick one at random.

# Assembling the current book

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

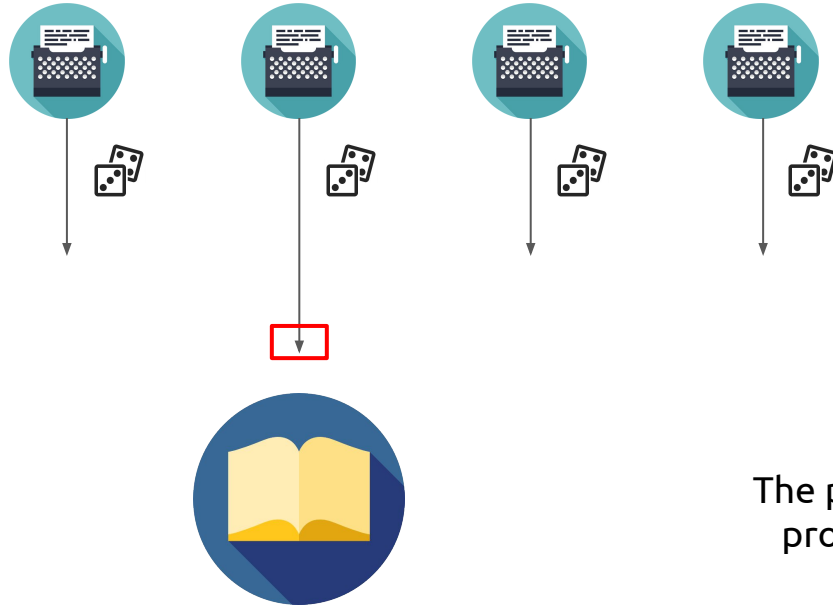


# Rules of extending the book



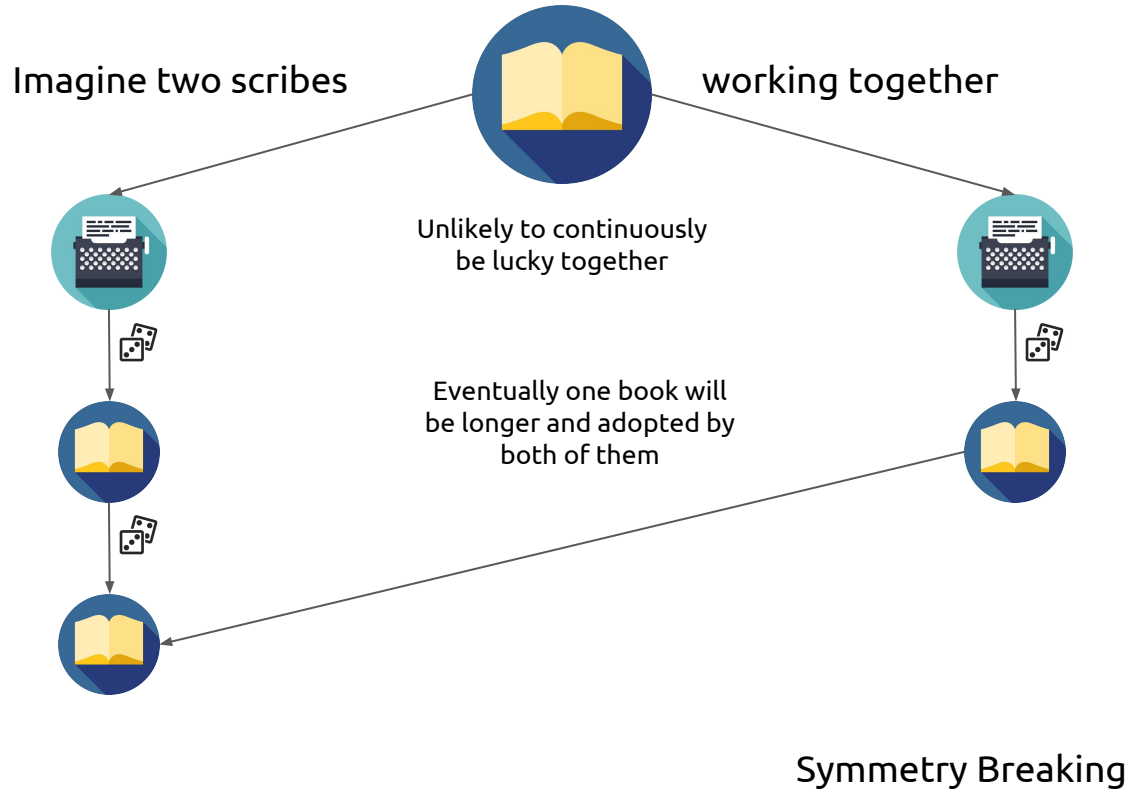
# Effort is needed to produce a page

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

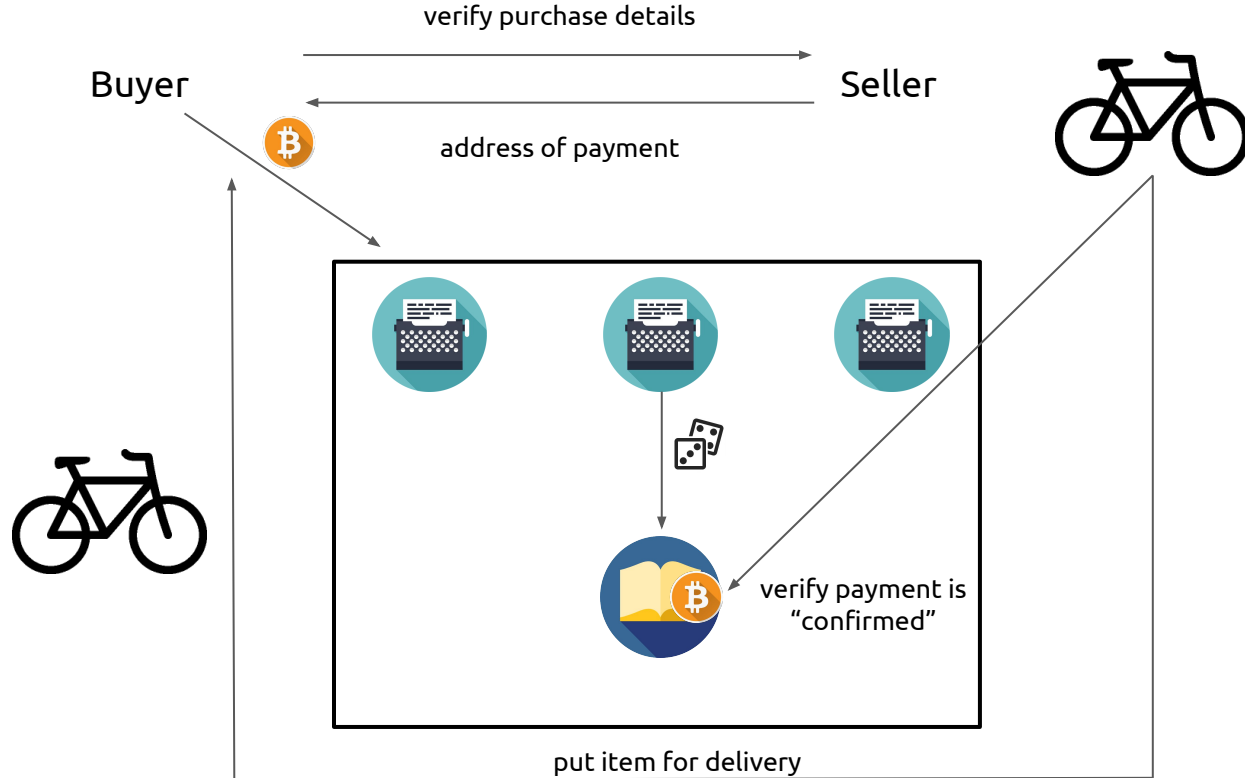
# The benefits of randomness







# 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 <b>cryptographic puzzle</b> that is <b>moderate hard</b> 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.



# 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.

# Smart contract



# 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**

# Cryptocurrencies from a user's perspective

# Bitcoin

What is bitcoin ?





# Bitcoin /'bitkɔɪn/

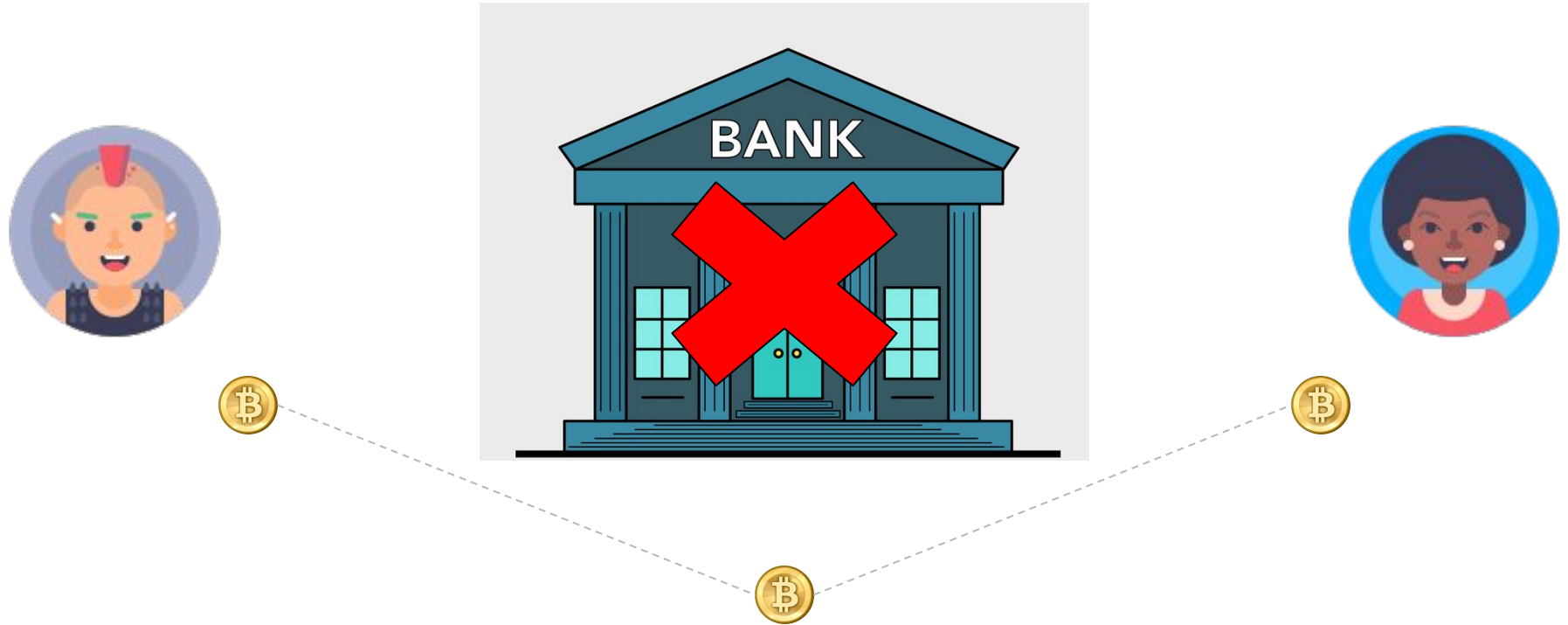
- First decentralized digital currency.
- Digital coins you can send through the Internet.



# Advantages



# Person to person



# Low fees



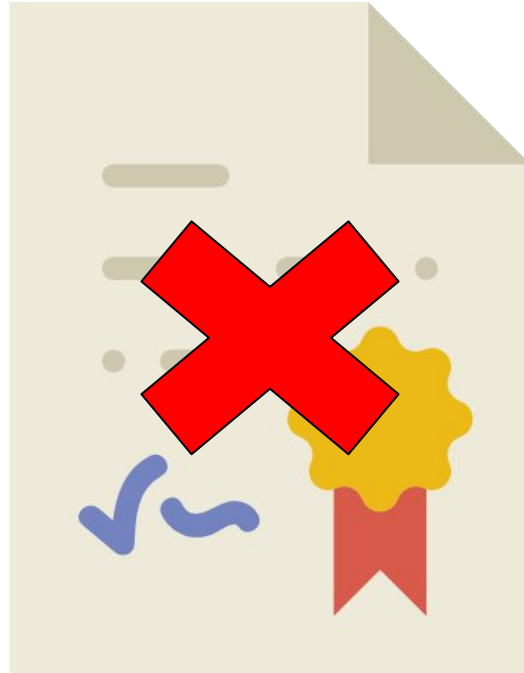
Available to the whole world



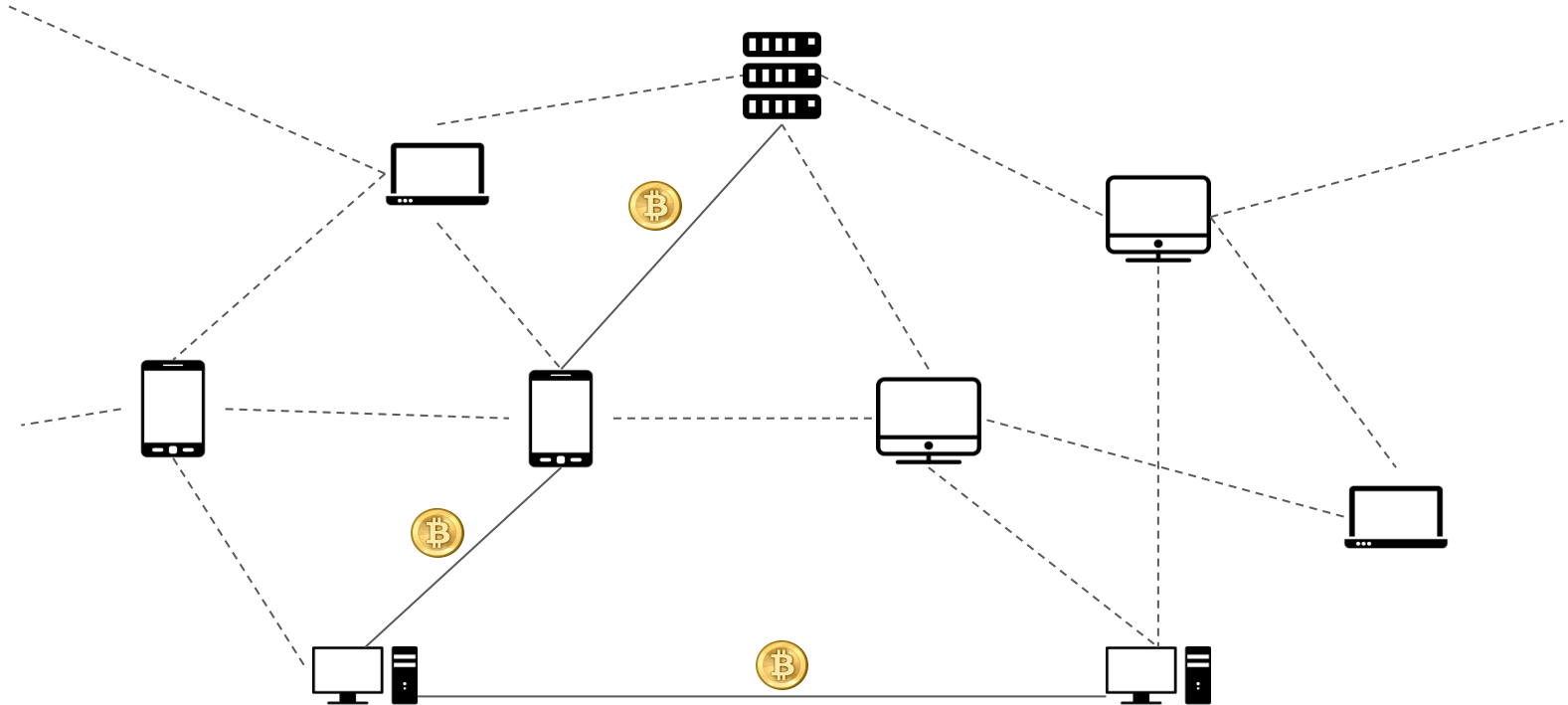
# You own your account



# No prerequisites or arbitrary limits



# Trust to third party is not a requirement



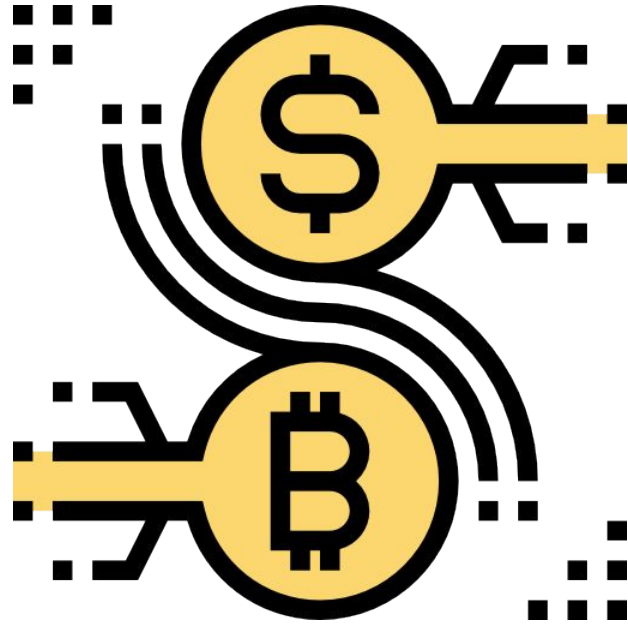


Open source: Anyone can review the code



Great! But... how can I use  
it?

Exchange: Buy or sell bitcoin for various currencies



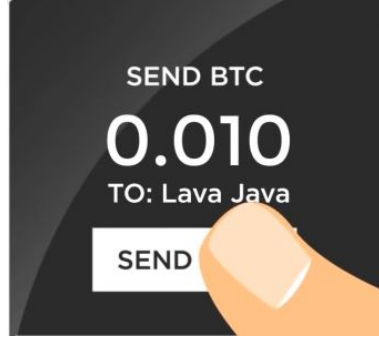
Digital wallet: Bitcoins are kept in your computer or mobile device



# Transactions: Bob want to buy a coffee from Alice



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



# Exchanges

# Exchanges

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



# Kraken

ETH/EUR

Last	High	Low	24 Hour Volume	Weighted Avg
€119.96	€144.41	€115.56	235,264.51	€124.53

Trade

Funding

Security

Settings

History

Get Verified

Current time: 02-25-19 11:28:54 +00:00  
Last Updated: 50 seconds ago

Overview

New Order

Orders

Positions

Trades

0.16 / 0.26%  
Current Fee

\$0.0000 / \$50,000 (0.00%)

0.14 / 0.24%  
Next Fee

Simple

Intermediate

Advanced

New Charting & Trading Tools

BETA

Buy

Sell

Amount

ETH

×

120.01

EUR

Market

Limit

=

Total

EUR

Amount of ETH to buy.

Buy at a fixed price per ETH.

Estimated amount of EUR to spend.

Buy ETH with EUR »

☐ Skip order confirmations.


New & Open Orders

Positions

Order Book

Order	Order Type	Pair	Price	Volume Rem.	Cost Rem.	Status	Opened
No orders currently available.							


# Bittrex


 Connected

MarketsOrdersWalletsSettingsLogout


## Ethereum (ETH)

Last Price: 0.03604990 BTC  
24hr Volume: 1526.77 BTC







Top Volume  
Ethereum (ETH)  
**1526.77 BTC**  
-8.7 ↓



Top Volume  
XRP (XRP)  
**439.98 BTC**  
-2.8 ↓



Biggest % Gain  
Enjin (ENJ)  
**65.96 BTC**  
29.0 ↑



Biggest % Gain  
AidCoin (AID)  
**18.31 BTC**  
21.3 ↑

### USD MARKETS

Total Volume = \$ 15513980.266

Find...

MARKET	CURRENCY	VOLUME ↓	% CHANGE	LAST PRICE	24HR HIGH	24HR LOW	% SPREAD	ADDED
USD-BTC	Bitcoin	9428628.26	-8.7 ↓	3780.47300000	4141.91800000	3700.00000000	0.2	05/31/2018
USD-ETH	Ethereum	3149860.66	-16.4 ↓	136.40000000	163.90000000	131.56300000	0.2	06/20/2018
USD-XRP	XRP	1218627.27	-10.7 ↓	0.29900000	0.33700000	0.29500000	0.3	08/21/2018
USD-USDT	Tether	638958.94	-0.3 ↓	0.99500000	1.00100000	0.99100000	0.3	05/31/2018
USD-LTC	Litecoin	374067.00	-15.8 ↓	44.00000000	52.32200000	42.43600000	0.7	09/18/2018
USD-BCH	Bitcoin Cash (ABC)	269744.25	-15.6 ↓	130.53800000	154.73500000	127.50000000	0.3	10/03/2018
USD-TRX	TRON	86680.05	-11.1 ↓	0.02400000	0.02700000	0.02200000	4.2	09/18/2018
USD-TUSD	TrueUSD	83556.56	0.2 ↑	1.00200000	1.00500000	0.99800000	0.3	05/31/2018
USD-ADA	Cardano	71890.67	-16.0 ↓	0.04200000	0.05000000	0.04100000	2.3	09/06/2018
USD-ETC	Ethereum Classic	62838.77	-15.9 ↓	4.10000000	4.87900000	4.07000000	0.4	08/21/2018
USD-BSV	Bitcoin SV	35569.05	-4.0 ↓	65.05300000	67.71900000	60.00000000	5.3	12/27/2018
USD-PAX	Paxos Standard	31726.58	-0.1 ↓	0.99900000	1.00700000	0.99500000	0.7	01/10/2019
USD-ZEC	ZCash	24799.88	-12.3 ↓	50.32800000	58.47000000	49.51700000	1.5	09/06/2018
USD-DGB	DigiByte	17617.27	-8.3 ↓	0.01100000	0.01200000	0.01000000	9.1	01/17/2019
USD-ZRX	0x Protocol	9385.29	-10.8 ↓	0.23100000	0.25800000	0.22600000	1.3	12/11/2018
USD-BAT	Basic Attention Token	3281.96	-10.5 ↓	0.12800000	0.14000000	0.12700000	1.5	12/27/2018
USD-EDR	Endor	2605.07	-12.5 ↓	0.02800000	0.03100000	0.02800000	18.8	01/24/2019
USD-ZEN	Horizen	2141.57	-10.0 ↓	5.03000000	5.39400000	4.97000000	12.3	01/31/2019
USD-KMD	Komodo	640.65	-18.1 ↓	0.63800000	0.63700000	0.63000000	0.3	03/03/2019

# Candlesticks



# 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

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

Order Book

10

25

50

100

BUY

SELL

ORDER TYPE

Limit (Default)

QUANTITY

0

ETH

BID PRICE

0

BTC

TOTAL

0

BTC

TIME IN FORCE

Good 'Til Cancelled (Default)

Buy Ethereum

Available Balance

0.00000013 BTC

0.00000000 ETH

MAX BUY

ETH can be traded by both

International and US customers.

4417.645 ETH

149.642 BTC

# Coinmarketcap

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

English ▼ EUR ▼ 🌙



CoinMarketCap

Rankings ▼

Trending ▼

Tools ▼

Services ▼

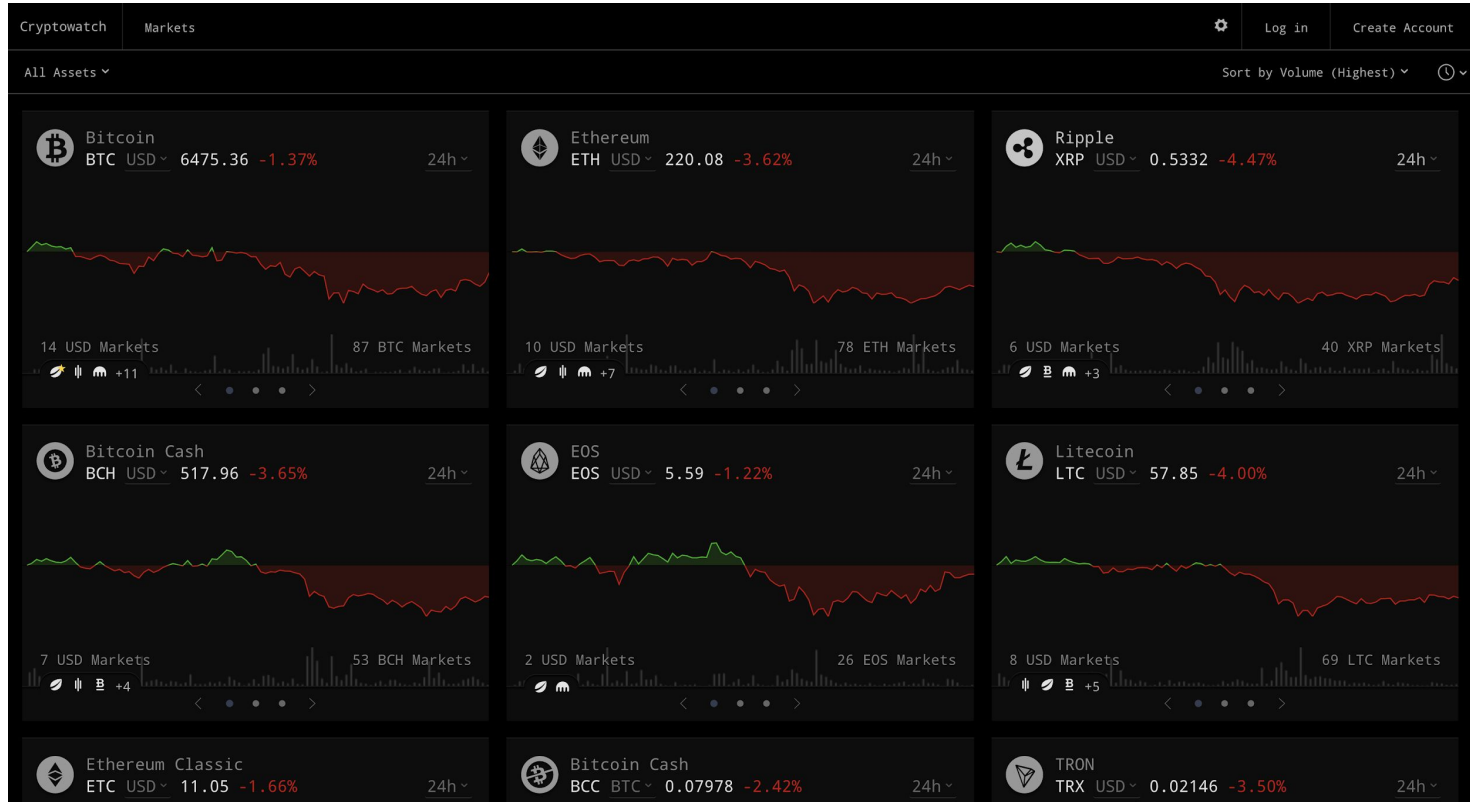
Search



## Top 100 Cryptocurrencies by Market Capitalization

Cryptocurrencies ▼		Exchanges ▼		Watchlist		EUR ▼		Next 100 →	View All
#	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%		***	

# Cryptowatch



# 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.
- Pseudo-anonymous: A unique address should be used for each transaction.
- Most wallets do it automatically.



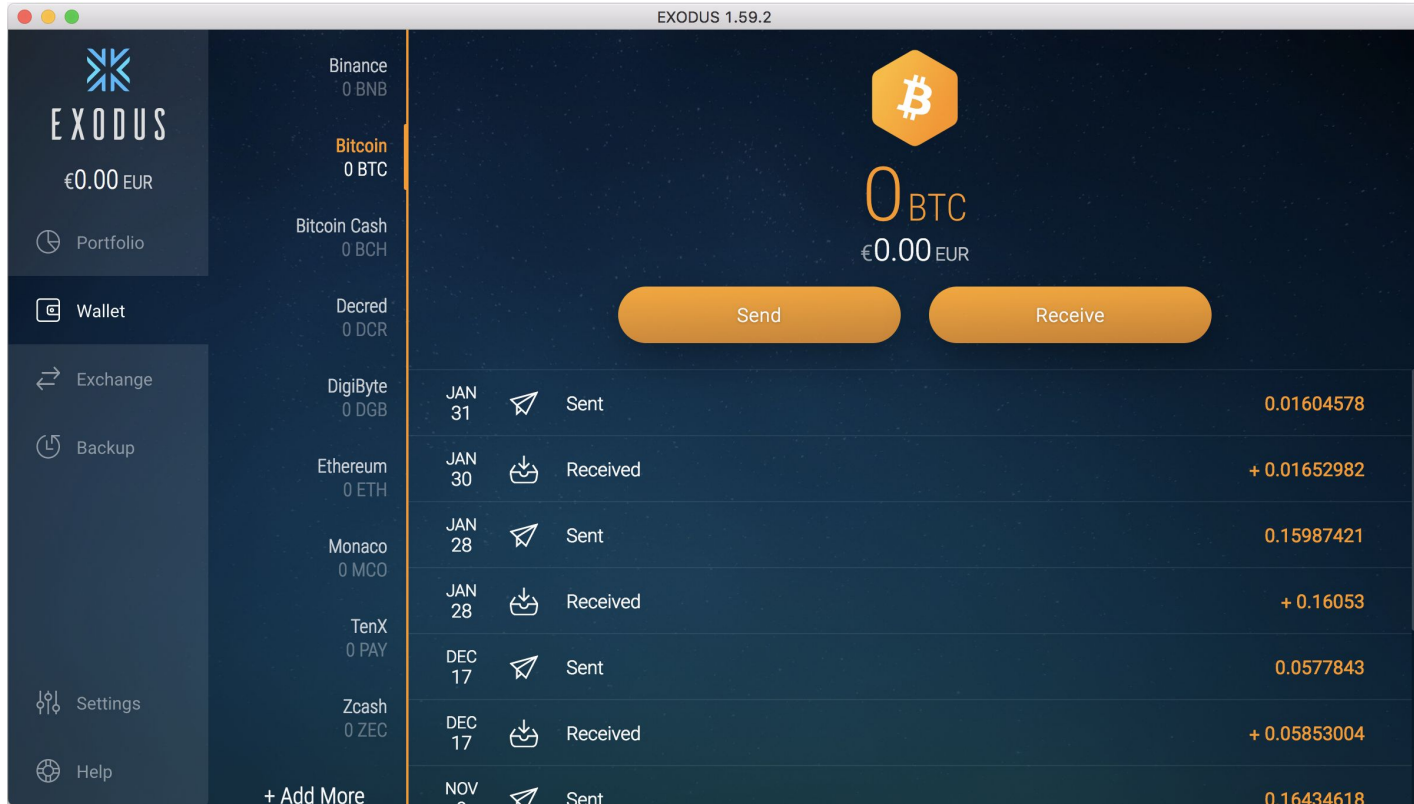
# Addresses



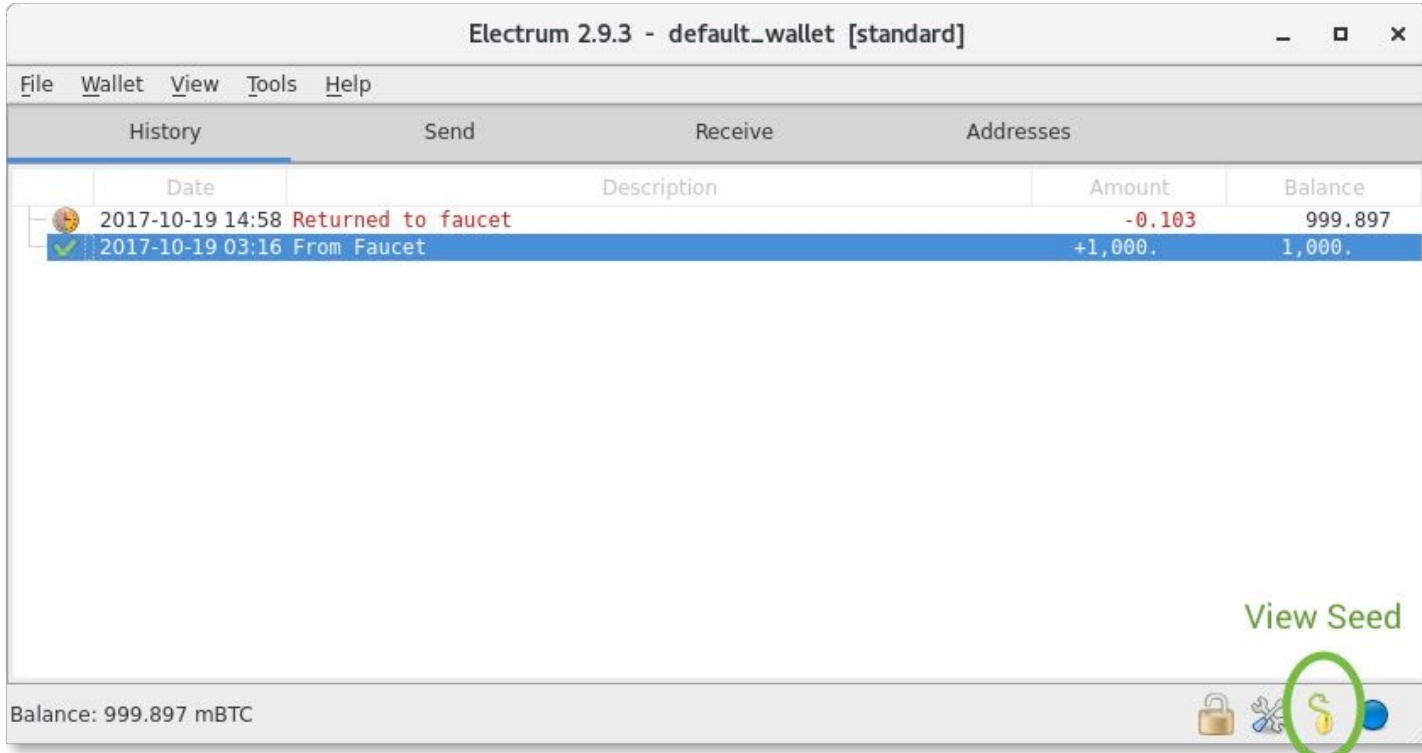
1BvBMSEYstWetqTFn5Au4m4GFg7xJaNVN2

# Wallets


# Desktop Wallet - Exodus



# Desktop Bitcoin Wallet - Electrum (open source)





# More Bitcoin wallets ... (mobile)


 [Introduction](#) [Resources](#) [Innovation](#) [Participate](#) [FAQ](#) [English](#)

## Choose your Bitcoin wallet


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




[All Wallets](#) [Desktop](#) [Hardware](#) [Mobile](#) [Web](#)





Bitcoin Knots







Bitcoin Core







Mycelium







Airbitz






ArcBit






BitGo



# Mobile wallet - Android


 **Bitcoin**

3G 10:51

SEND COINS ADDRESS BOOK PEER MONITOR

**BTC 1.1163**  
≈ EUR 55.7050

Your Bitcoin Address:  
1KGe NiDw zH5N  
rdwN ETj3 hQEx  
wr5H MN9e FW



	balance	67.9065	Received	Both	Sent
CNY	rate	416.78	● Apr 6 ← 1719Pmohr5CkidX6mQ9zYj4nTPnGDf5... + 0.0050		
	balance	465.2653	● Apr 5 ← Beer with Lisa + 0.0050		
DKK	rate	328.56	● Apr 5 → 1Q4H8CY4FpnJ93SPbdz4Cqgv714KXae... - 3.5005		
	balance	366.7824	● Apr 4 → Burger @ room77 - 0.0754		
EUR (default)	rate	49.90	● Apr 4 ← 1G9Hjz1JCUqnhNQmpxLhsVL6FD8Coo4... + 2.2452		
	balance	55.7050	● Apr 4 ← Donation + 0.05		
GBP	rate	40.74	● Apr 3 ← 1FugQeguKnVFavXYqKwYB7g4YKXJ4REKjh + 0.05		
	balance	45.4794			
HKD	rate	506.94			

Use at your own risk. Read the [safety notes](#).

# Hardware wallets



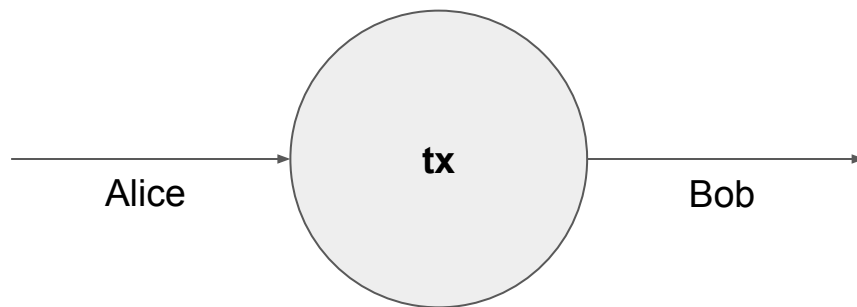
# Explorers



# 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



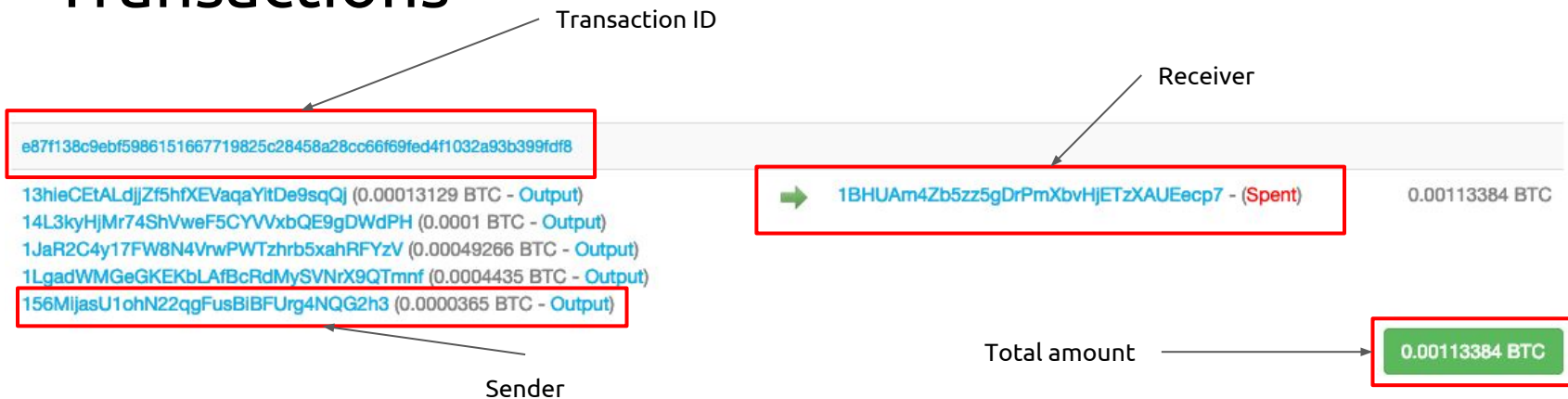
## BLOCKS

## TRANSACTIONS

Transaction Hash	Age	Amount (BTC)	Amount (USD)
<a href="#">7dd6b6e07ea48577ce11fd43cbf20e259d187defc0888eaa698d7...</a>	5 seconds	1.91072766 BTC	\$7,304.54
<a href="#">94613360083b2e9bdff659d026021c3df9abad4820cf2bb6add...</a>	3 seconds	0.02130671 BTC	\$81.45
<a href="#">bbda790399d9f44f25d247ea2785b9a687b714665b1fb021cd537...</a>	3 seconds	1.23166111 BTC	\$4,708.53
<a href="#">5d96b437de67fc604b025671f4fa199832b60fc21aedcf94b0455...</a>	2 seconds	0.05533534 BTC	\$211.54
<a href="#">6e7e9284d3c45111a036dab93aae7f7b057e76935c6186051cf92d...</a>	2 seconds	0.03158347 BTC	\$120.74

[View More](#)

# Transactions



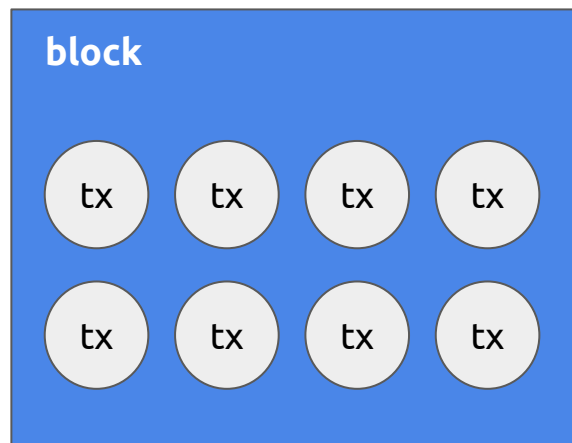
Summary	
Size	781 (bytes)
Weight	3124
Received Time	2018-09-25 14:29:54
Included In Blocks	543028 ( 2018-09-25 15:56:10 + 86 minutes )
Confirmations	21456
Visualize	<a href="#">View Tree Chart</a>

Block number  
& timestamp

Confirmations

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	<a href="#">Hide scripts &amp; coinbase</a>

# Blocks



**BLOCKS****TRANSACTIONS**

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

[View More](#)

# 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	0000000000000000000a318feb2fc7c2c9dc43c2d1de1606bb5f0cc6dc1d115
Previous Block	00000000000000000003006dab6f32132e7eeda37d2cca4a961339bad35b1e80
Next Block(s)	0000000000000000000868c5eac591d4df331b4c8b4b12c33d40dfddac3feaff
Merkle Root	4dfd79c993bc63e5db09cbda62e9d9df7da1a7d8f1605e97a5ceb1f939509d31

Total transactions

Block ID

Total fees

Block difficulty

Parent ID

Reward

# Development

- Local blockchain: ganache
  - Used for local development.
  - Instant mining.
  - Very small in size.
- Testnets:
  - Used for testing and experiment. Very useful specifically for smart contract development.
  - Different blockchain and different genesis block.
  - Coins are separated and distinct from actual coins (fake, no 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 irreversible.
  - You can delete or 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://bitcoinafaucet.uo1.net/>
  - <https://testnet-faucet.mempool.co/>
  - <https://block.io/> (Online testnet wallet)

**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](#)

# Thank you!

