FTEC 4004

E-payment Systems and Cryptocurrency Technologies

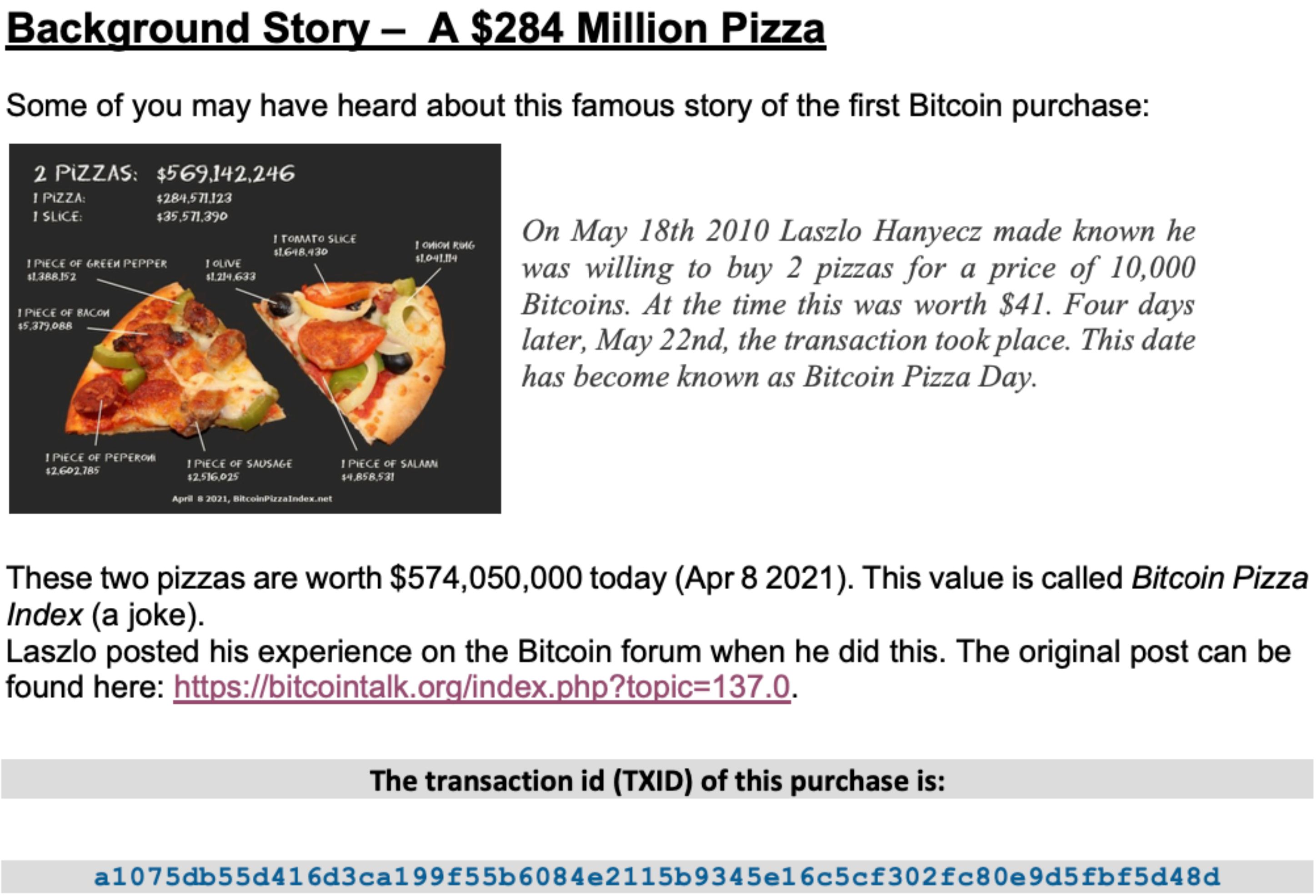
Tutorial 9

Get a taste of Bitcoin

WANG Xianbo

xianbo@ie.cuhk.edu.hk

Homework 4 was just released! It is about Bitcoin.



Background Story – A $284 Million Pizza

Some of you may have heard about this famous story of the first Bitcoin purchase:

2 PiZZAS: $569,142,246
1 PiZZA: $284,571,123
1 SLiCE: $35,571,390
1 TOMATO SLICE $1,648,430
1 ONION RING $1,041,114
1 PIECE OF GREEN PEPPER $1,388,152
1 OLIVE $1,214,633
1 PIECE OF BACON $5,379,088
1 PIECE OF PEPERONI $2,602,785
1 PIECE OF SAUSAGE $2,516,025
1 PIECE OF SALAMI $4,858,531
April 8 2021, BitcoinPizzaIndex.net

On May 18th 2010 Laszlo Hanyecz made known he was willing to buy 2 pizzas for a price of 10,000 Bitcoins. At the time this was worth $41. Four days later, May 22nd, the transaction took place. This date has become known as Bitcoin Pizza Day.

These two pizzas are worth $574,050,000 today (Apr 8 2021). This value is called *Bitcoin Pizza Index* (a joke).
Laszlo posted his experience on the Bitcoin forum when he did this. The original post can be found here: https://bitcointalk.org/index.php?topic=137.0.

The transaction id (TXID) of this purchase is:

`a1075db55d416d3ca199f55b6084e2115b9345e16c5cf302fc80e9d5fbf5d48d`

Overview of today’s topic

- Show you how to become an average Bitcoin user

What can you learn?

- Bitcoin knowledge that everybody knows
    - History of Bitcoin
    - Why’s Bitcoin special
    - Basic concepts: units, wallet, etc.
- Get started with Bitcoin
    - Setup a wallet
    - How to buy Bitcoin
    - How to send/receive Bitcoin
- How to explore Bitcoin data
    - Inspect Bitcoin transaction data online
    - Observe details of blocks and transactions

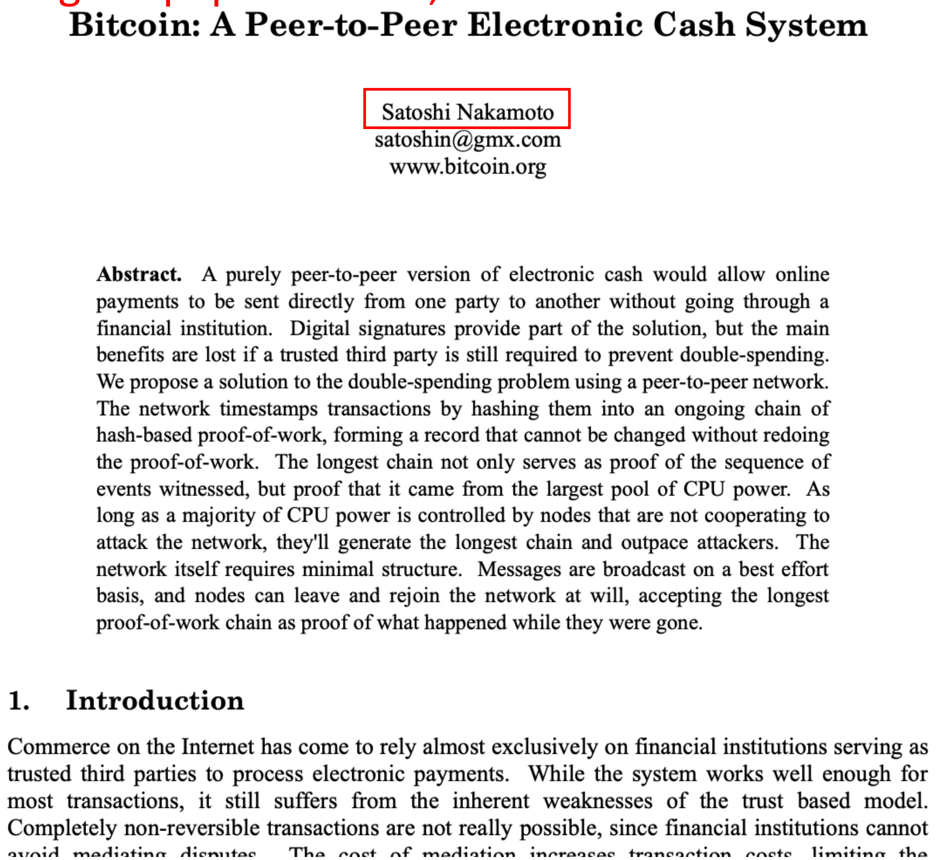
Before we start …

- Short discussion on HW 3

- If you have no question, start creating your (first) Bitcoin wallet (you may refer to https://bitcoin.org/).
- ~~I will send the first student who paste his/her wallet address in Zoom chat some **real** Bitcoin (0.5 mBTC, or 0.0005 BTC).~~

Bitcoin is 12 years old!

Original paper: Oct 31, 2008



Bitcoin: A Peer-to-Peer Electronic Cash System

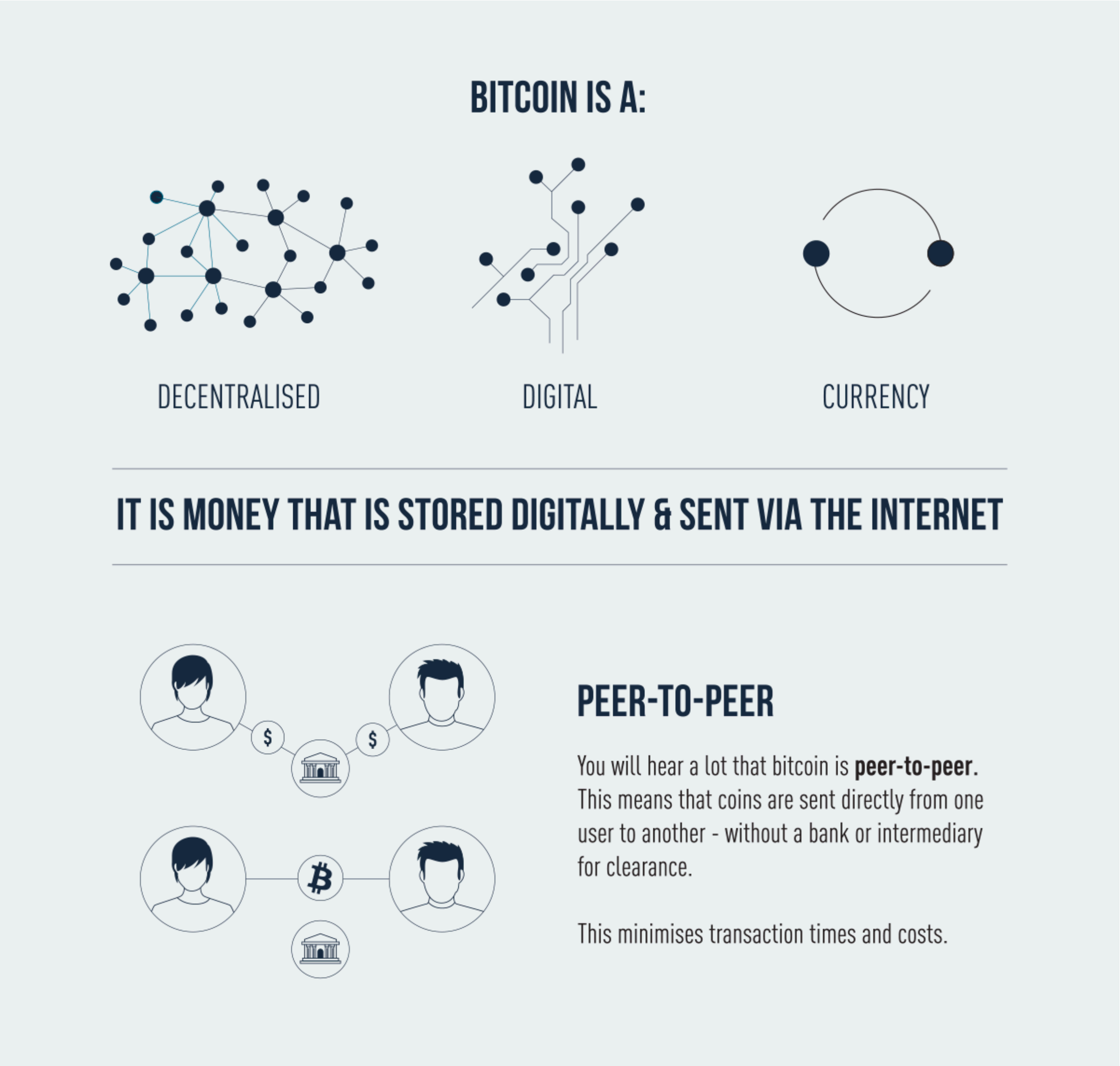
Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

1. Introduction

Commerce on the Internet has come to rely almost exclusively on financial institutions serving as trusted third parties to process electronic payments. While the system works well enough for most transactions, it still suffers from the inherent weaknesses of the trust based model. Completely non-reversible transactions are not really possible, since financial institutions cannot avoid mediating disputes. The cost of mediation increases transaction costs, limiting the

https://bitcoin.org/bitcoin.pdf



IT IS MONEY THAT IS STORED DIGITALLY & SENT VIA THE INTERNET

PEER-TO-PEER

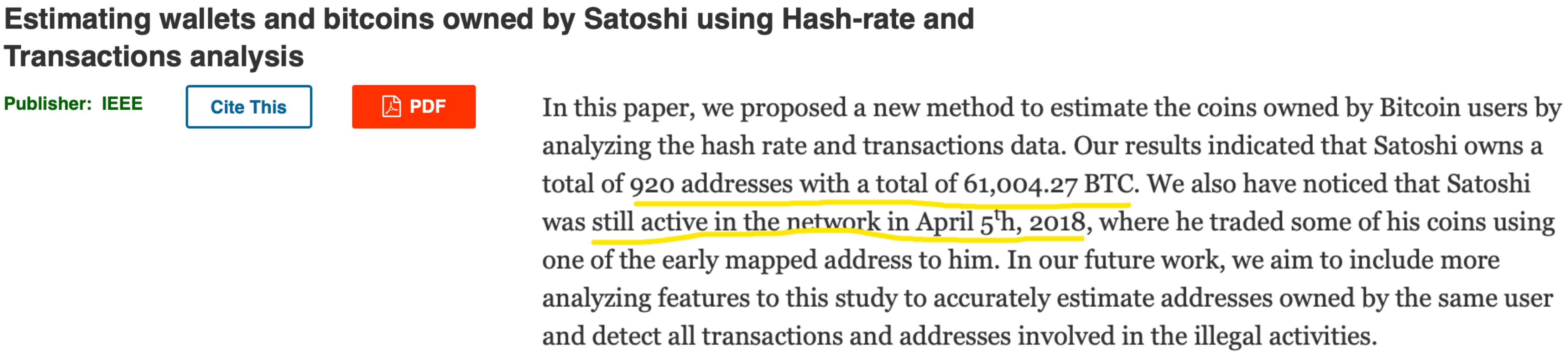
You will hear a lot that bitcoin is **peer-to-peer**. This means that coins are sent directly from one user to another - without a bank or intermediary for clearance.

This minimises transaction times and costs.

https://www.genesis-mining.com/infographic/what-is-bitcoin

More about the history

- Besides authoring the paper, Satoshi also wrote code for the initial version of Bitcoin. (version 0.1 released on Sourceforge)
- Control was handed over to Bitcoin community in late 2010, coins he owned was never touched (*maybe*) until now, which once (Dec 2017) valued over US$19 billion.

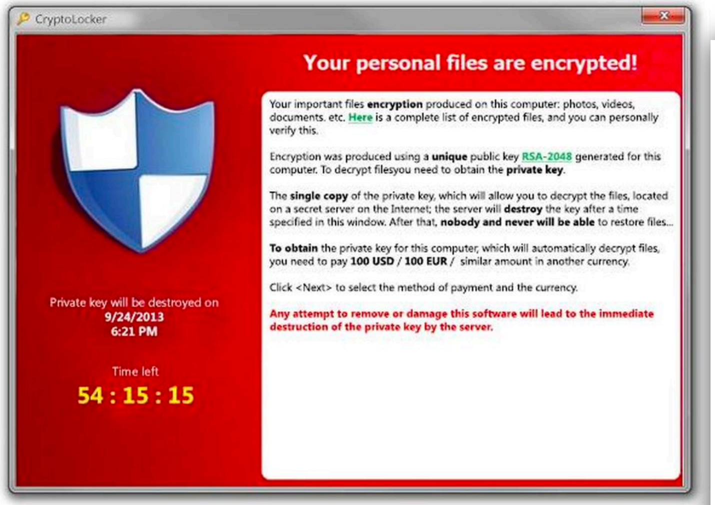


Estimating wallets and bitcoins owned by Satoshi using Hash-rate and Transactions analysis

Publisher: IEEE

In this paper, we proposed a new method to estimate the coins owned by Bitcoin users by analyzing the hash rate and transactions data. Our results indicated that Satoshi owns a total of 920 addresses with a total of 61,004.27 BTC. We also have noticed that Satoshi was still active in the network in April 5th, 2018, where he traded some of his coins using one of the early mapped address to him. In our future work, we aim to include more analyzing features to this study to accurately estimate addresses owned by the same user and detect all transactions and addresses involved in the illegal activities.

Do you still remember the first time you heard about Bitcoin? Did you ever owned some?



Your personal files are encrypted!

Your important files **encryption** produced on this computer: photos, videos, documents. etc. Here is a complete list of encrypted files, and you can personally verify this.

Encryption was produced using a **unique** public key RSA-2048 generated for this computer. To decrypt filesyou need to obtain the **private key**.

The **single copy** of the private key, which will allow you to decrypt the files, located on a secret server on the Internet; the server will **destroy** the key after a time specified in this window. After that, **nobody and never will be able** to restore files...

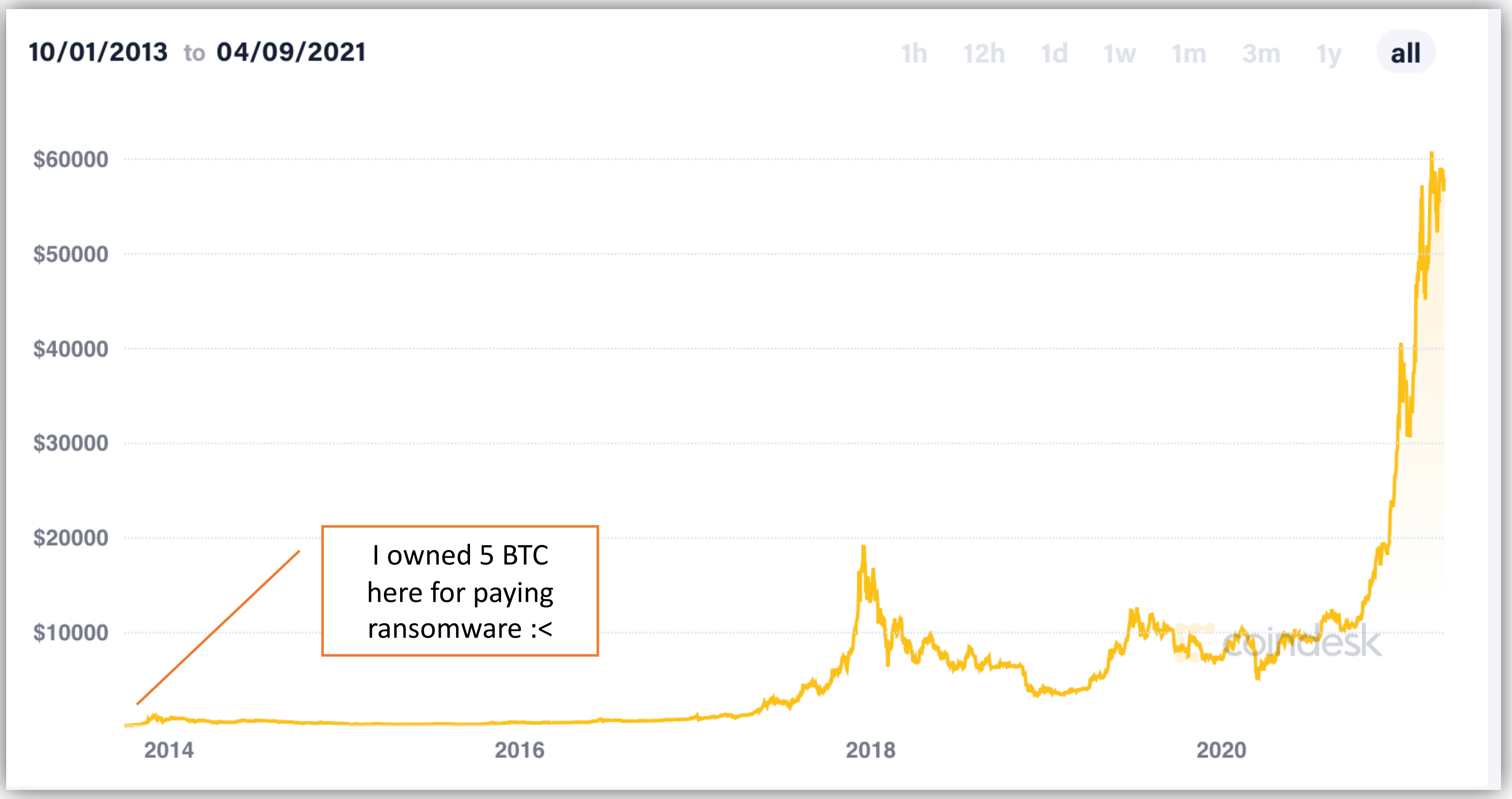
To obtain the private key for this computer, which will automatically decrypt files, you need to pay **100 USD / 100 EUR /** similar amount in another currency.

Click <Next> to select the method of payment and the currency.

Any attempt to remove or damage this software will lead to the immediate destruction of the private key by the server.

Private key will be destroyed on
9/24/2013
6:21 PM

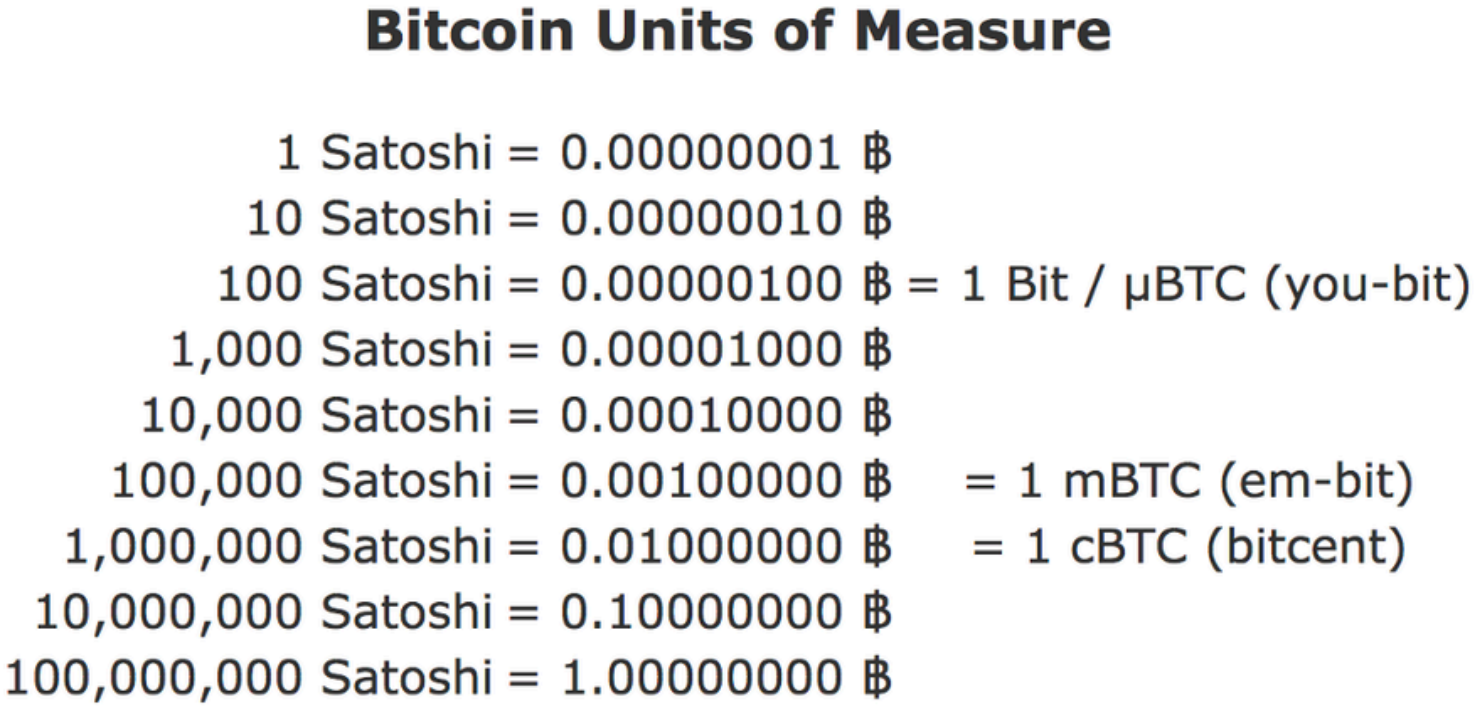
Time left
54 : 15 : 15



I owned 5 BTC here for paying ransomware :<

Bitcoin Units

The smallest unit is Satoshi (proposed by Ribuck in 2010)



Bitcoin Units of Measure

1 Satoshi = 0.00000001 ฿

10 Satoshi = 0.00000010 ฿

100 Satoshi = 0.00000100 ฿ = 1 Bit / μBTC (you-bit)

1,000 Satoshi = 0.00001000 ฿

10,000 Satoshi = 0.00010000 ฿

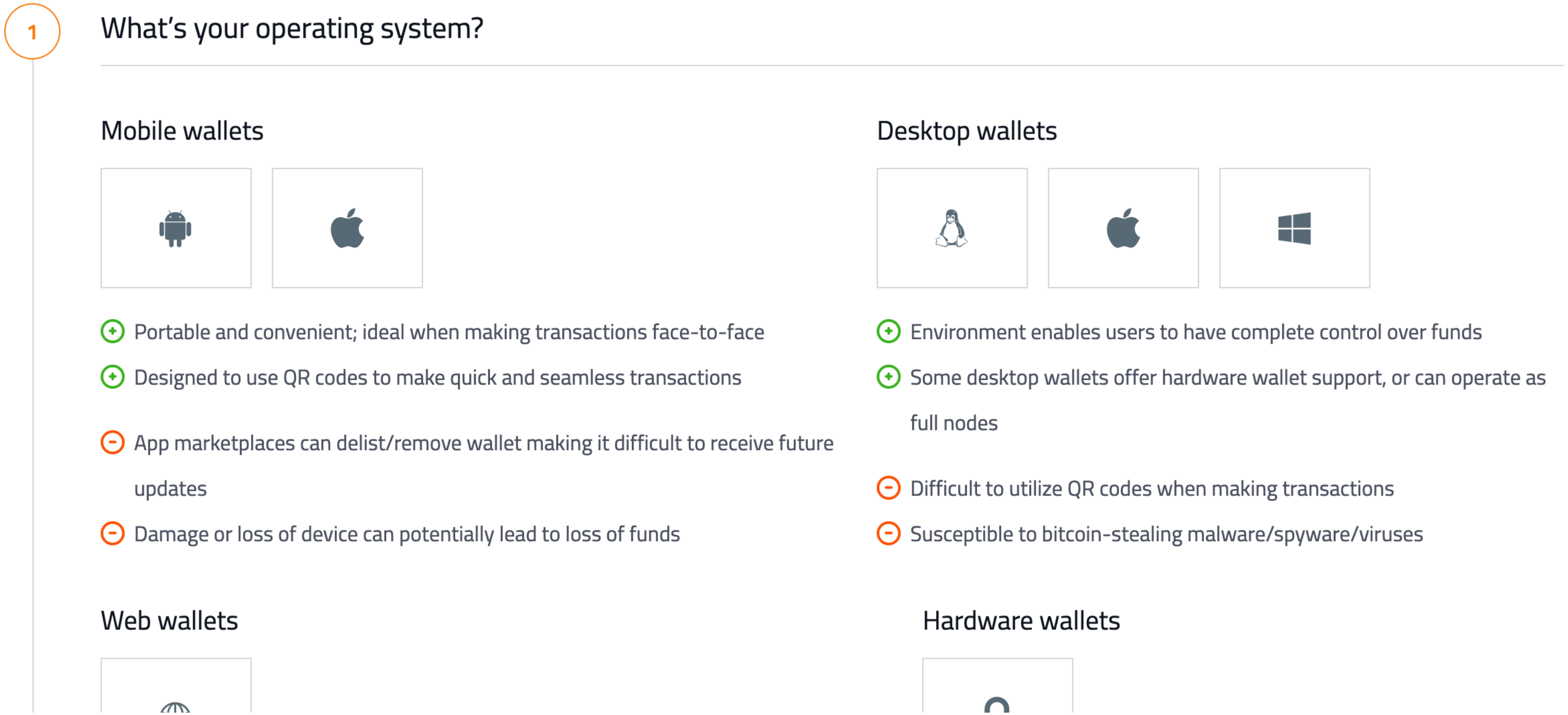
100,000 Satoshi = 0.00100000 ฿ = 1 mBTC (em-bit)

1,000,000 Satoshi = 0.01000000 ฿ = 1 cBTC (bitcent)

10,000,000 Satoshi = 0.10000000 ฿

100,000,000 Satoshi = 1.00000000 ฿

Get started – Setup your wallet



1 What's your operating system?

Mobile wallets

- ⊕ Portable and convenient; ideal when making transactions face-to-face
- ⊕ Designed to use QR codes to make quick and seamless transactions
- ⊖ App marketplaces can delist/remove wallet making it difficult to receive future updates
- ⊖ Damage or loss of device can potentially lead to loss of funds

Desktop wallets

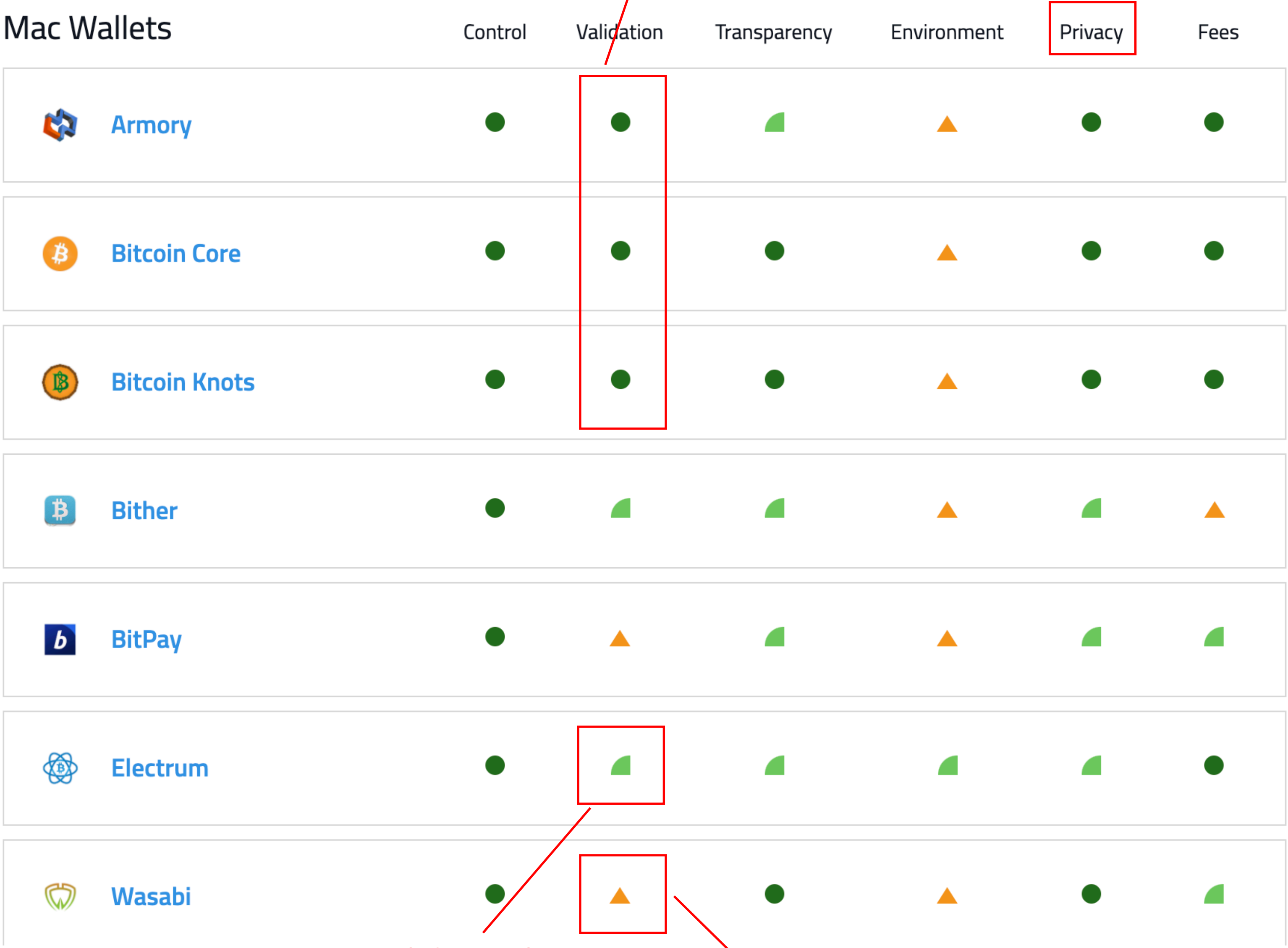
- ⊕ Environment enables users to have complete control over funds
- ⊕ Some desktop wallets offer hardware wallet support, or can operate as full nodes
- ⊖ Difficult to utilize QR codes when making transactions
- ⊖ Susceptible to bitcoin-stealing malware/spyware/viruses

Web wallets

Hardware wallets

Run a full node
(~ 250 GB)

Rotating wallet
address, etc.



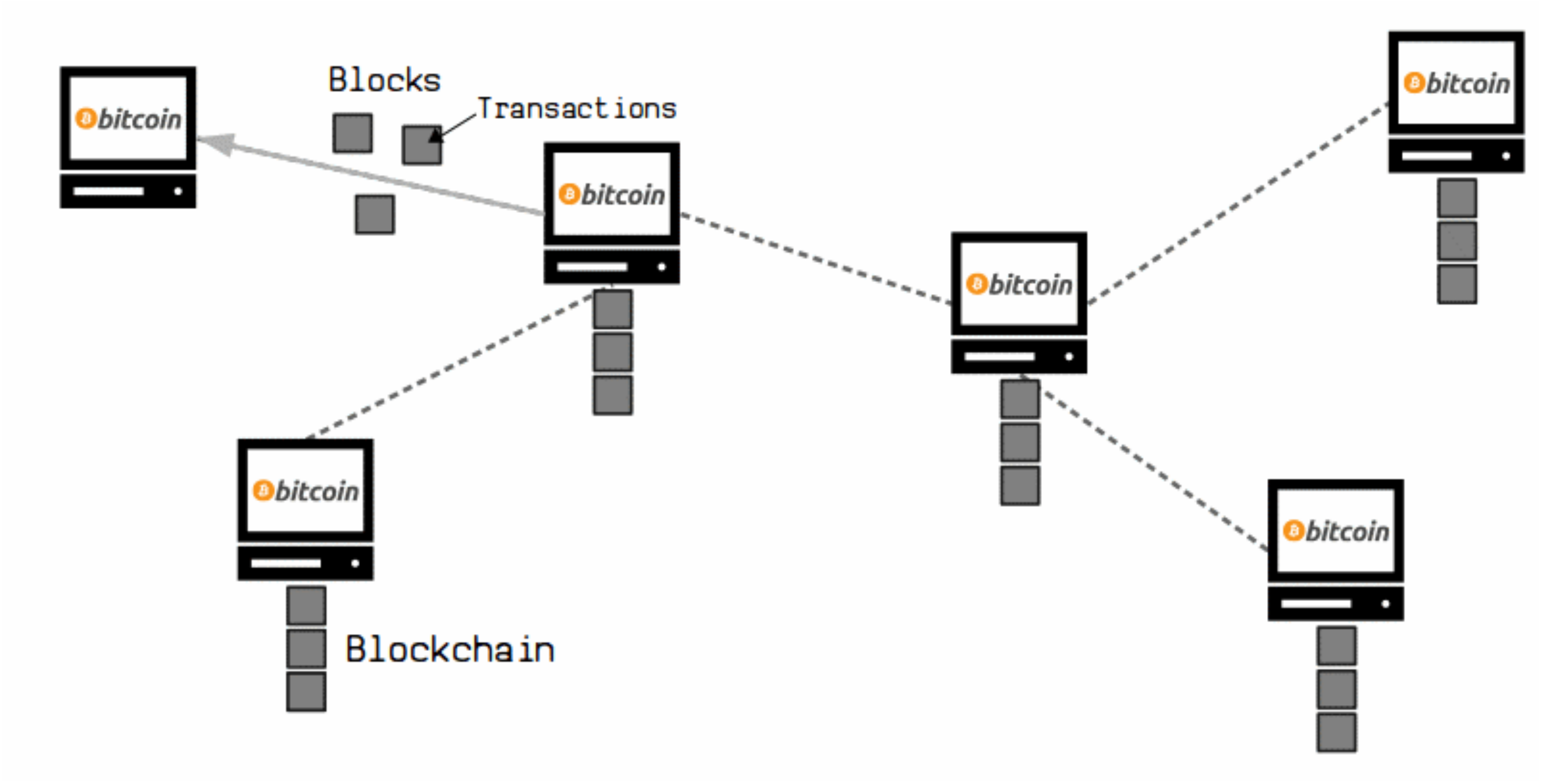
Mac Wallets	Control	Validation	Transparency	Environment	Privacy	Fees
Armory	●	●	◔	▲	●	●
Bitcoin Core	●	●	●	▲	●	●
Bitcoin Knots	●	●	●	▲	●	●
Bither	●	◔	◔	▲	◔	▲
BitPay	●	▲	◔	▲	◔	◔
Electrum	●	◔	◔	◔	◔	●
Wasabi	●	▲	●	▲	●	◔

Trust validation by
(random) servers

Rely on centralized service

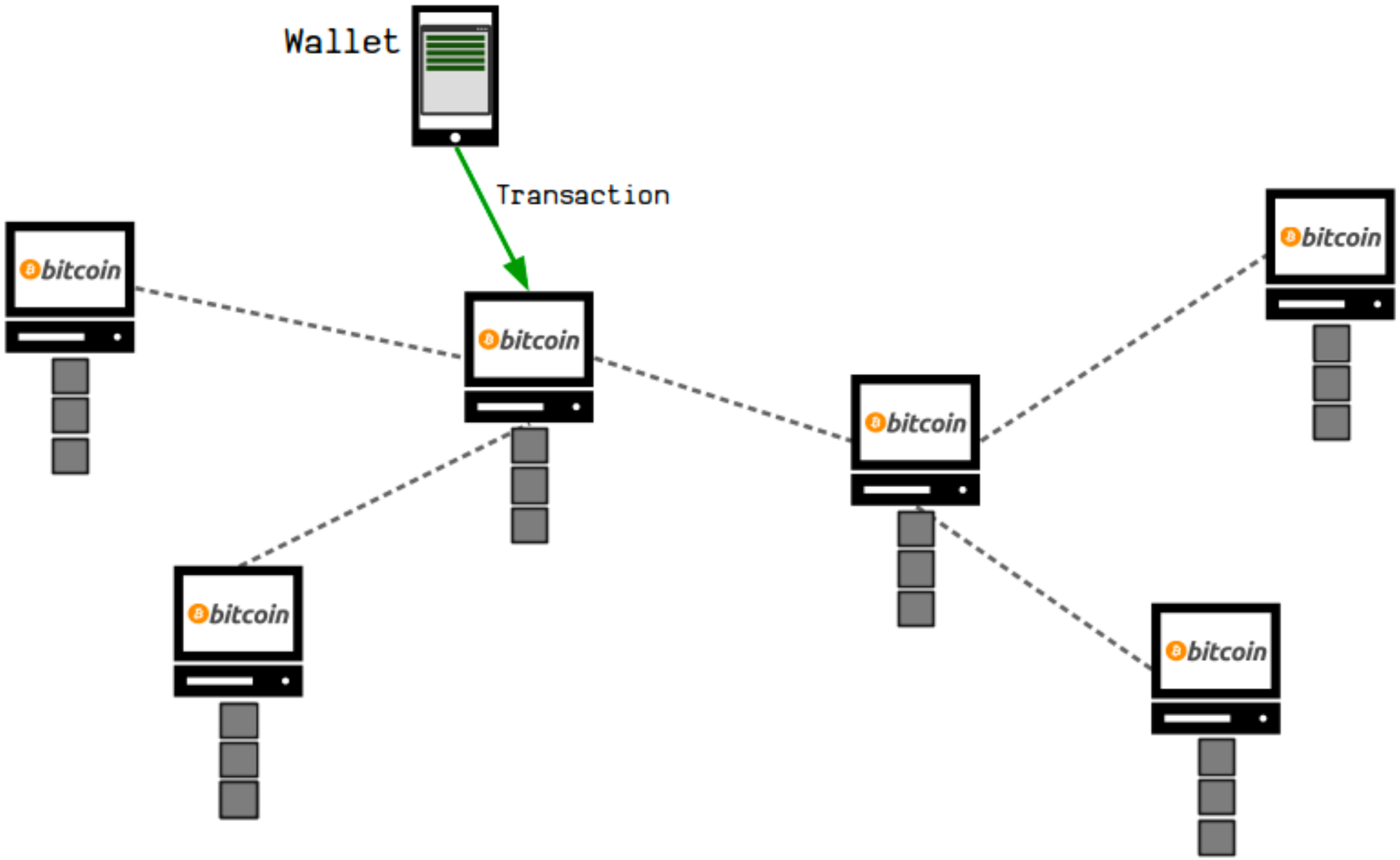
Full node mode

You need to download the full blockchain (over 250 GB) and do verfication, then you can start making transactions



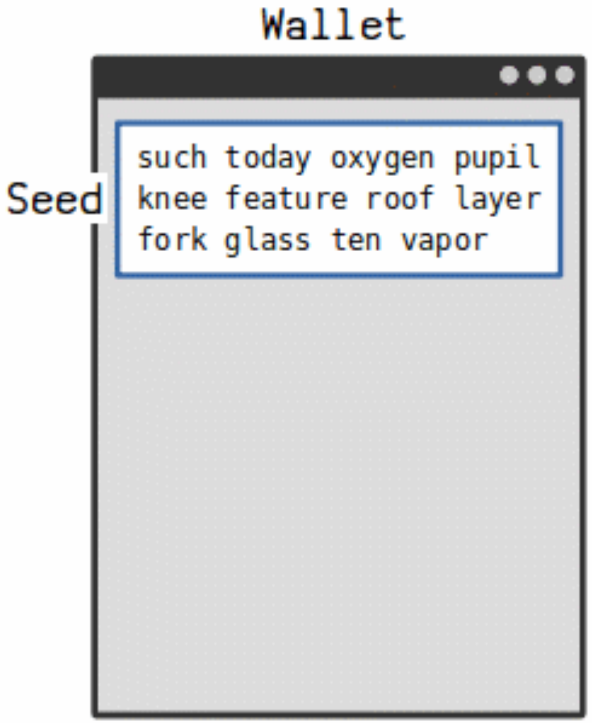
Light wallet

Need to trust other machines with full nodes, but save you a lot of disk space.



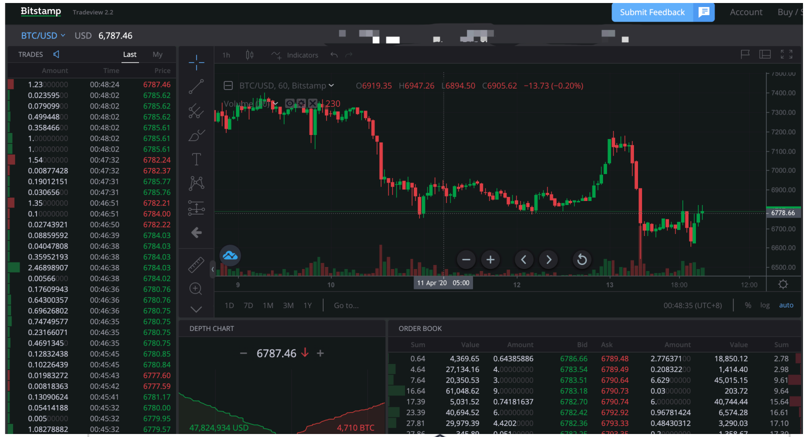
Seed

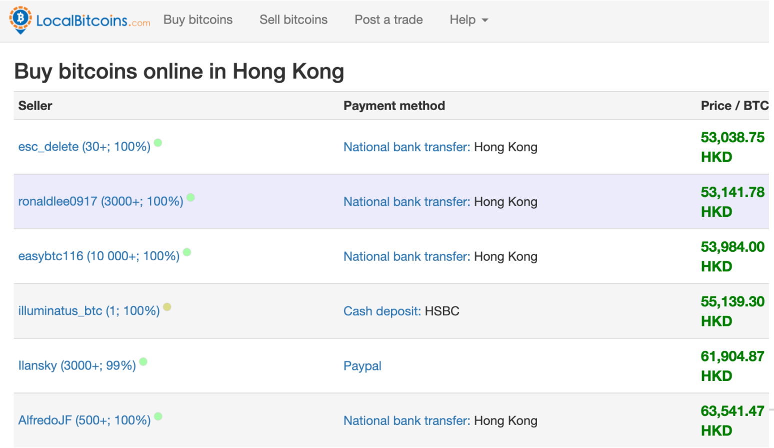
Random generated words (your secret) used to generate rotating wallet addresses.



such today oxygen pupil
knee feature roof layer
fork glass ten vapor

Buy Bitcoin





Buy bitcoins online in Hong Kong

Seller	Payment method	Price / BTC
esc_delete (30+; 100%)	National bank transfer: Hong Kong	53,038.75 HKD
ronaldlee0917 (3000+; 100%)	National bank transfer: Hong Kong	53,141.78 HKD
easybtc116 (10 000+; 100%)	National bank transfer: Hong Kong	53,984.00 HKD
illuminatus_btc (1; 100%)	Cash deposit: HSBC	55,139.30 HKD
Ilansky (3000+; 99%)	Paypal	61,904.87 HKD
AlfredoJF (500+; 100%)	National bank transfer: Hong Kong	63,541.47 HKD

Use a Bitcoin Exchange

Our Bitcoin Exchange page, lists many different businesses that can help you buy bitcoin using your bank account.

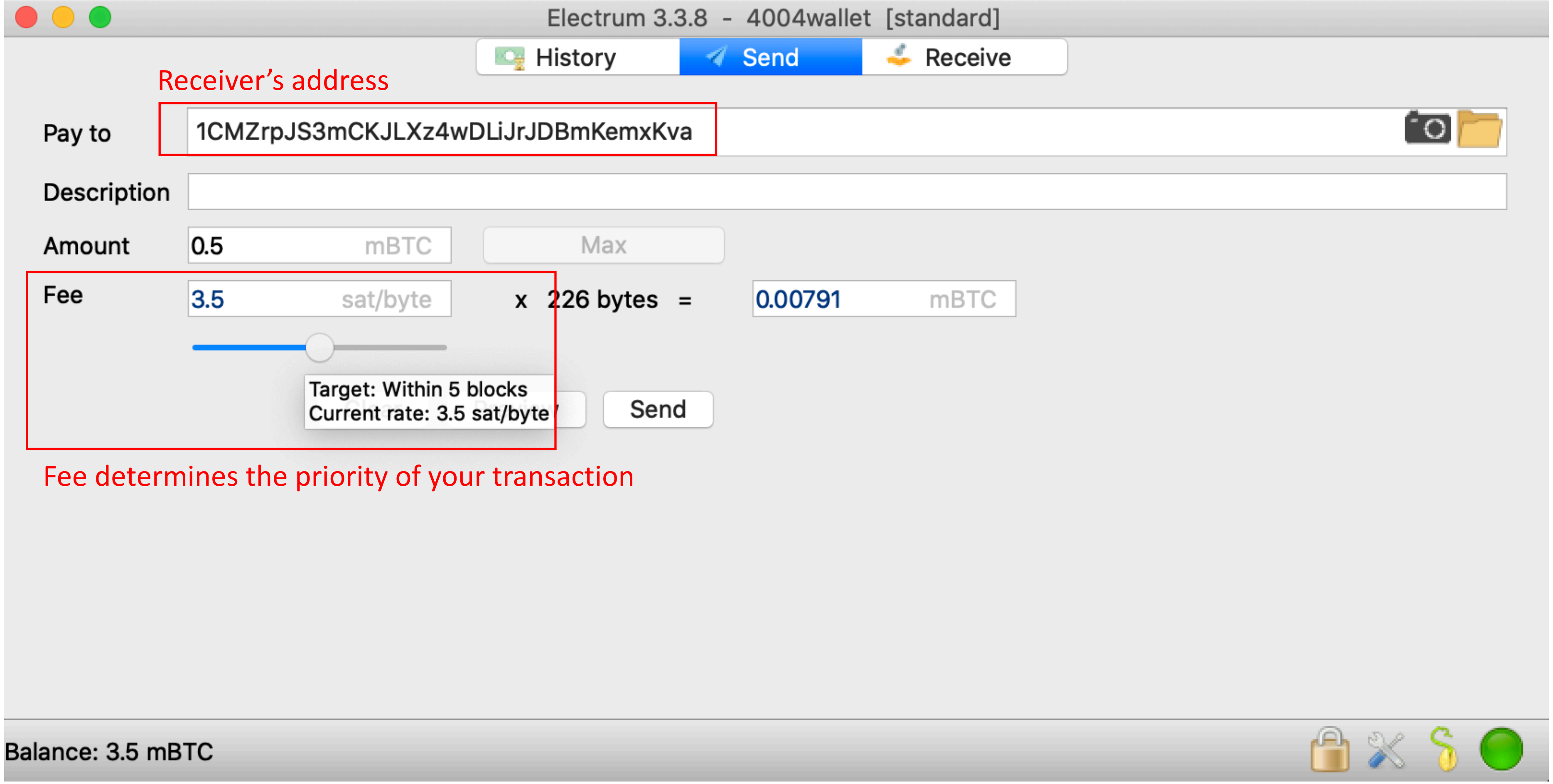
Browse a P2P Directory

Using an exchange based off of a peer-to-peer directory lets you search and browse through various sellers of bitcoin. Sellers have reviews and feedback scores to help you choose.

Use a Bitcoin ATM

Bitcoin ATMs work like a regular ATM, except they allow you to deposit and withdrawal money so that you can buy and sell bitcoin. Coin ATM Radar has an interactive map to help you find the closest bitcoin ATM near you.

Send Bitcoin



Electrum 3.3.8 - 4004wallet [standard]

Receiver's address

Pay to: 1CMZrpJS3mCKJLXz4wDLiJrJDBmKemxKva

Description:

Amount: 0.5 mBTC

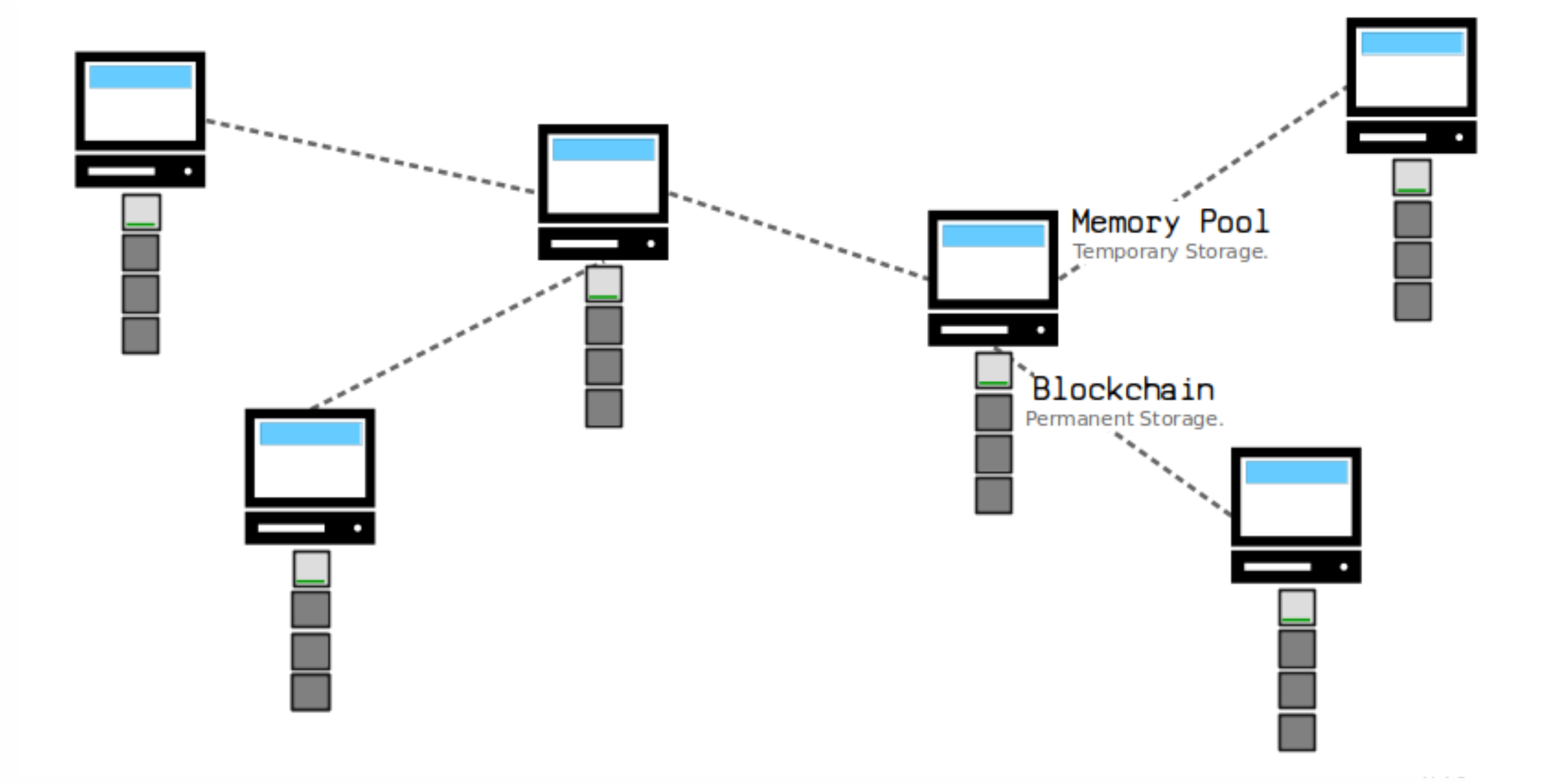
Fee: 3.5 sat/byte x 226 bytes = 0.00791 mBTC

Target: Within 5 blocks
Current rate: 3.5 sat/byte

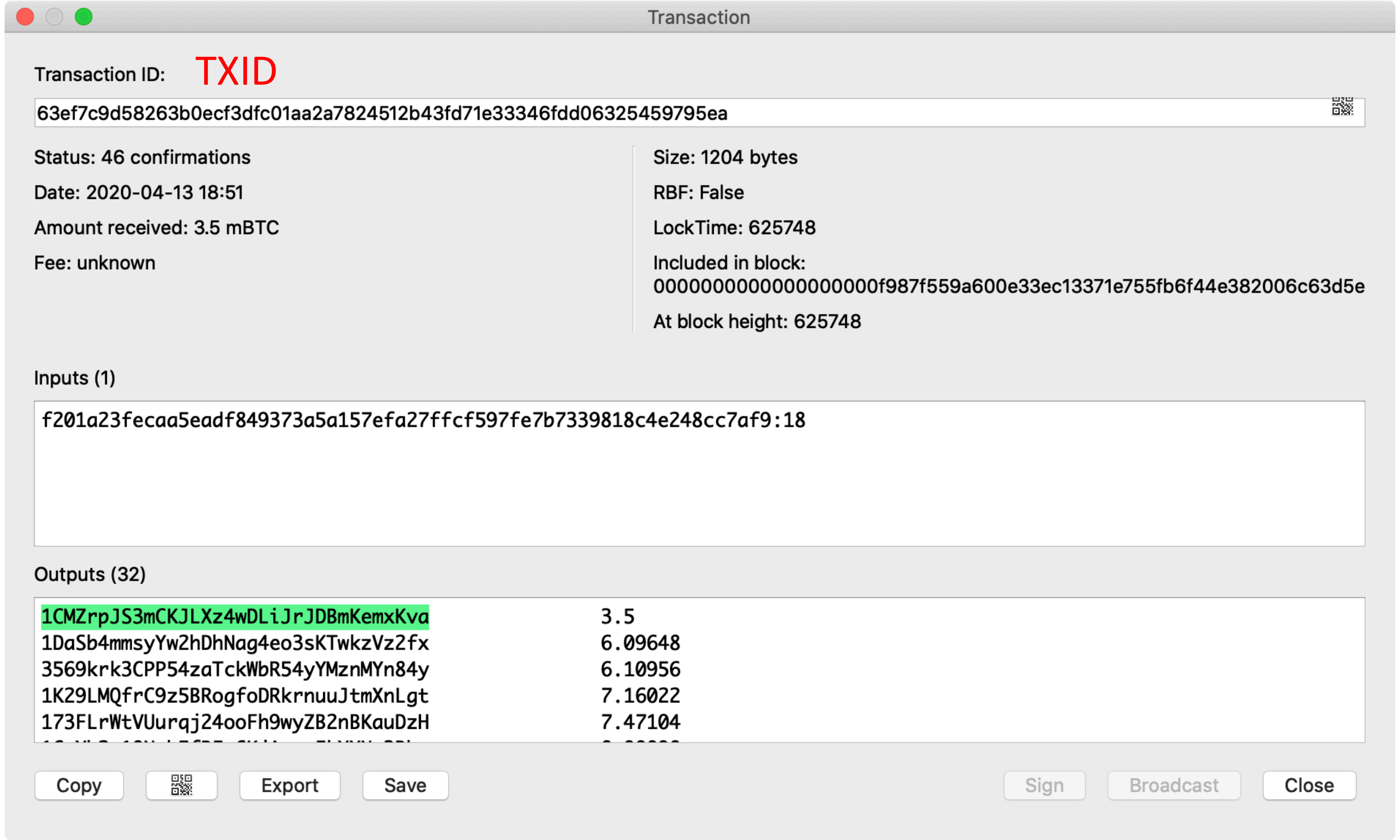
Fee determines the priority of your transaction

Balance: 3.5 mBTC

What happends to transactions



Inspect transaction data



Transaction ID: TXID

63ef7c9d58263b0ecf3dfc01aa2a7824512b43fd71e33346fdd06325459795ea

Status: 46 confirmations

Date: 2020-04-13 18:51

Amount received: 3.5 mBTC

Fee: unknown

Size: 1204 bytes

RBF: False

LockTime: 625748

Included in block:
0000000000000000000f987f559a600e33ec13371e755fb6f44e382006c63d5e

At block height: 625748

Inputs (1)

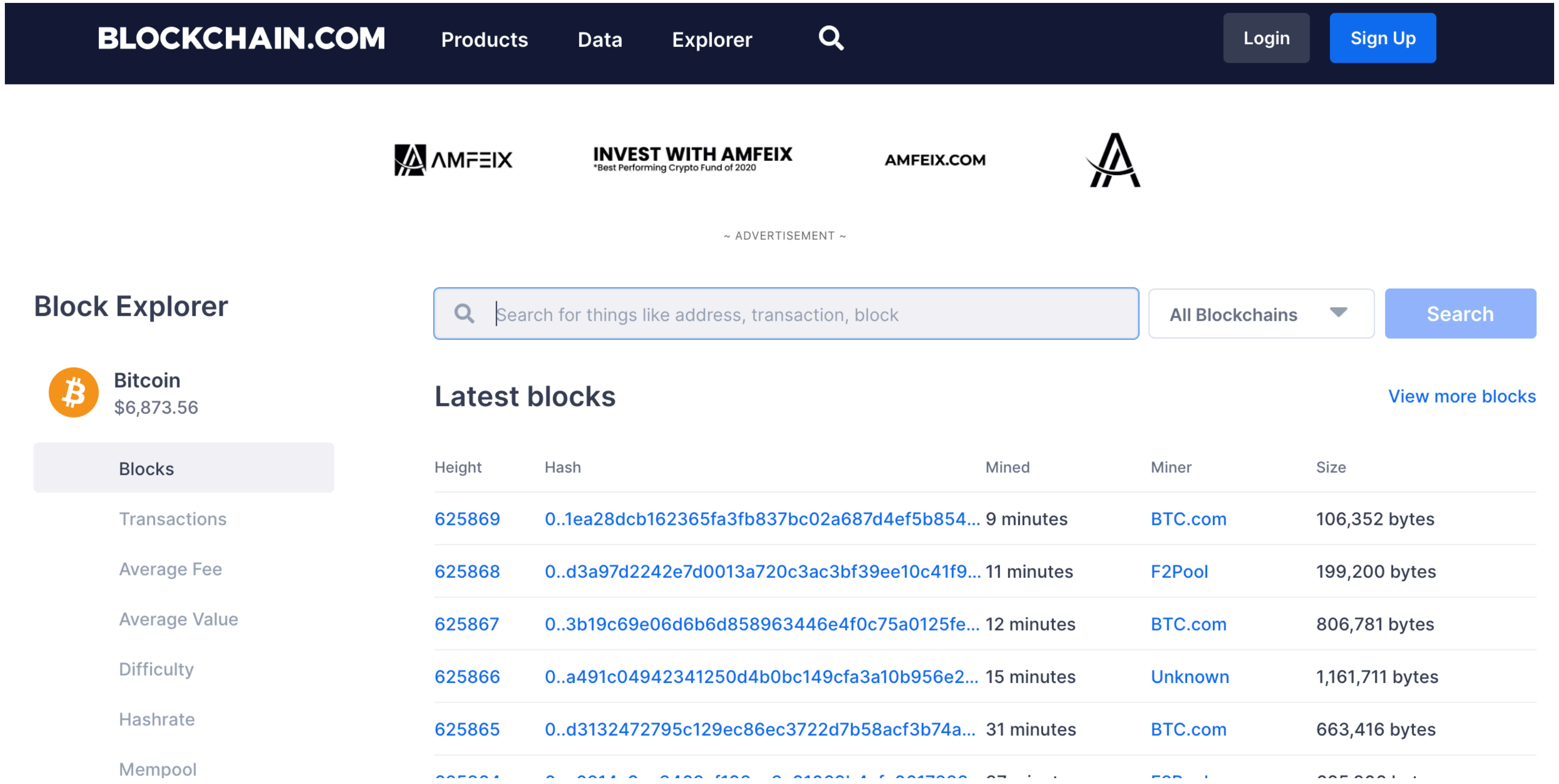
```
f201a23fecaa5eadf849373a5a157efa27ffcf597fe7b7339818c4e248cc7af9:18
```

Outputs (32)

```
1CMZrpJS3mCKJLXz4wDLiJrJDBmKemxKva          3.5
1DaSb4mmsyYw2hDhNag4eo3sKTwkzVz2fx          6.09648
3569krk3CPP54zaTckWbR54yYMznMYn84y          6.10956
1K29LMQfrC9z5BRogfoDRkrnuuJtmXnLgt          7.16022
173FLrWtVUurqj24ooFh9wyZB2nBKauDzH          7.47104
```

Explore public blockchain data

There are some website for searching/browsing (Bitcoin) blockchain data



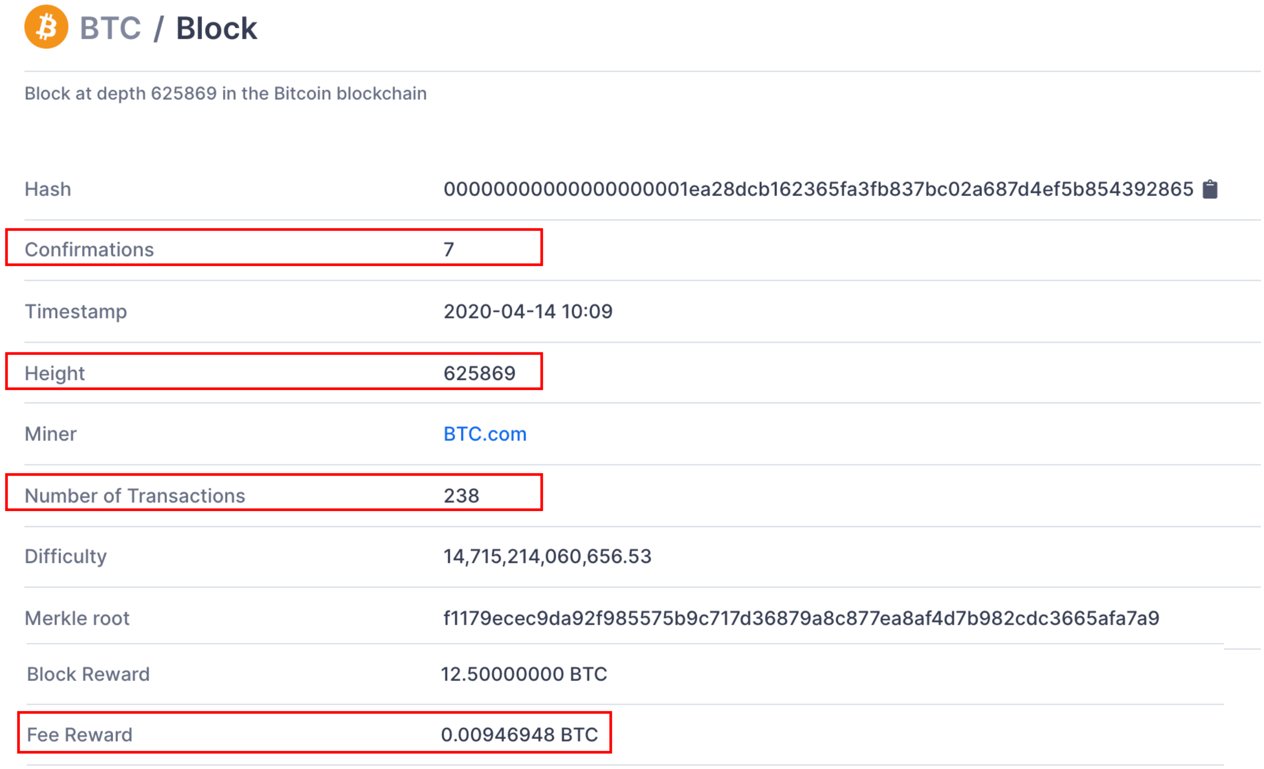
Block Explorer

Latest blocks

Height	Hash	Mined	Miner	Size
625869	0..1ea28dcb162365fa3fb837bc02a687d4ef5b854...	9 minutes	BTC.com	106,352 bytes
625868	0..d3a97d2242e7d0013a720c3ac3bf39ee10c41f9...	11 minutes	F2Pool	199,200 bytes
625867	0..3b19c69e06d6b6d858963446e4f0c75a0125fe...	12 minutes	BTC.com	806,781 bytes
625866	0..a491c04942341250d4b0bc149cfa3a10b956e2...	15 minutes	Unknown	1,161,711 bytes
625865	0..d3132472795c129ec86ec3722d7b58acf3b74a...	31 minutes	BTC.com	663,416 bytes

Block

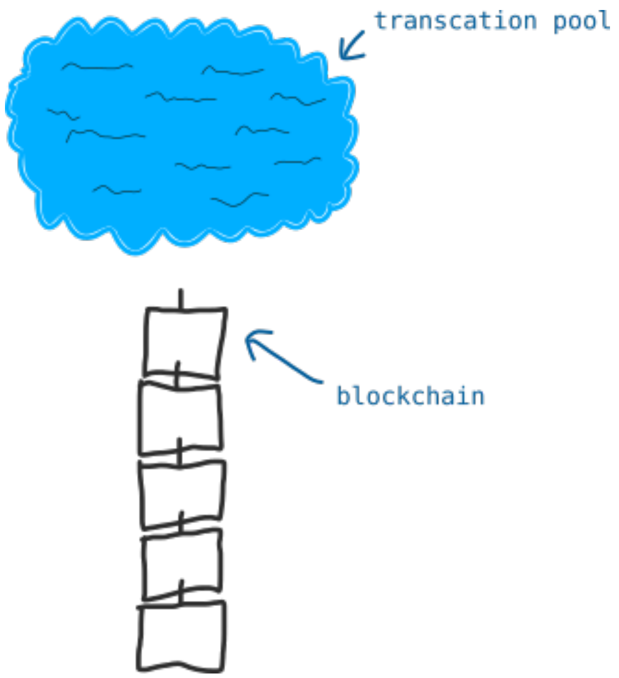
A **block** is a bunch of **transactions** that have been added to the **blockchain**.



BTC / Block

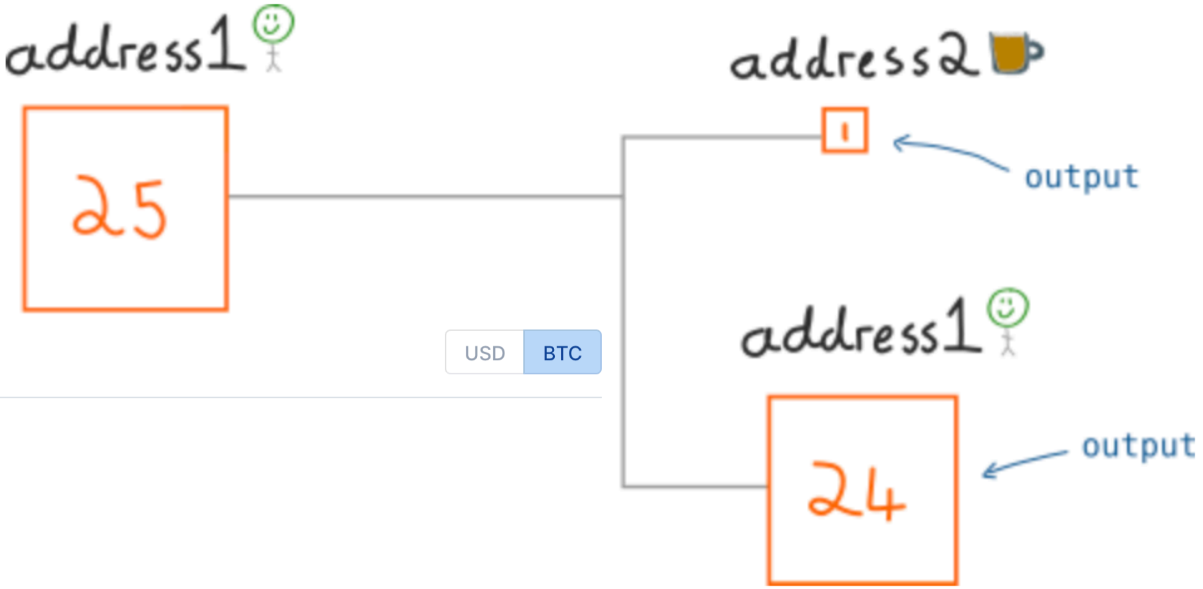
Block at depth 625869 in the Bitcoin blockchain

Hash	00000000000000000001ea28dcb162365fa3fb837bc02a687d4ef5b854392865
Confirmations	7
Timestamp	2020-04-14 10:09
Height	625869
Miner	BTC.com
Number of Transactions	238
Difficulty	14,715,214,060,656.53
Merkle root	f1179ecec9da92f985575b9c717d36879a8c877ea8af4d7b982cdc3665afa7a9
Block Reward	12.50000000 BTC
Fee Reward	0.00946948 BTC



Transactions

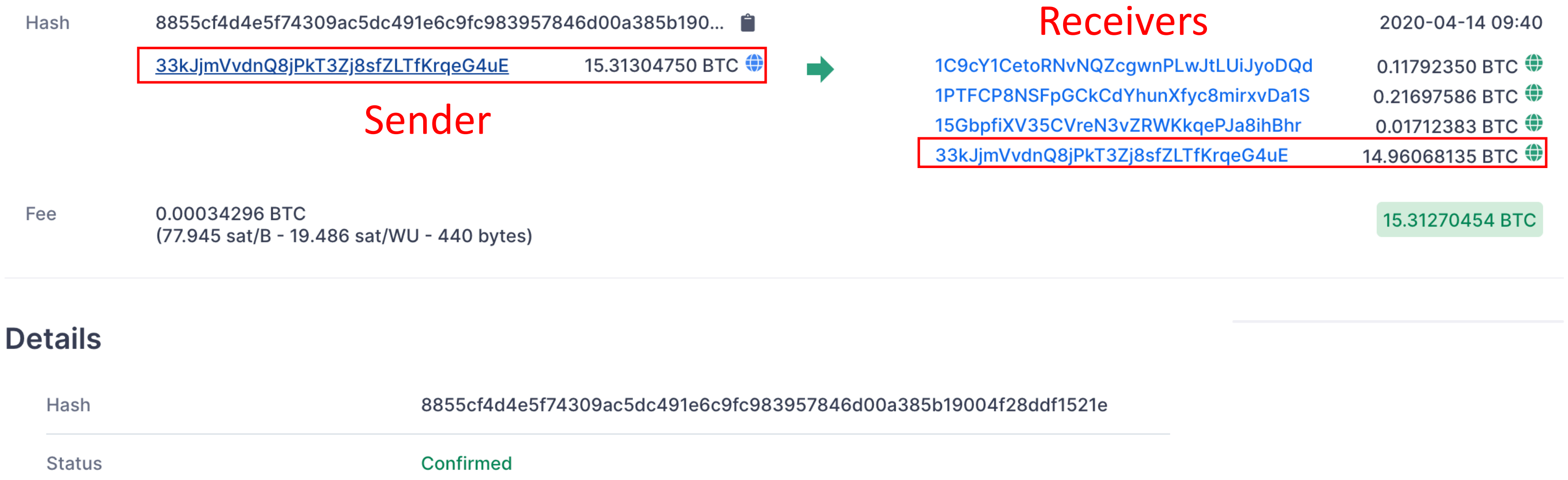
“Send the change to yourself”



BTC / Transaction

USD BTC

View information about a Bitcoin transaction



Summary

Hash 8855cf4d4e5f74309ac5dc491e6c9fc983957846d00a385b190...

33kJjmVvdnQ8jPkT3Zj8sfZLTfKrqeG4uE 15.31304750 BTC

Sender

Receivers

2020-04-14 09:40

1C9cY1CetoRNvNQZcgwnPLwJtLUiJyoDQd	0.11792350 BTC
1PTFCP8NSFpGCkCdYhunXfyc8mirxvDa1S	0.21697586 BTC
15GbpfiXV35CVreN3vZRWKkqePJa8ihBhr	0.01712383 BTC
33kJjmVvdnQ8jPkT3Zj8sfZLTfKrqeG4uE	14.96068135 BTC

Fee 0.00034296 BTC
(77.945 sat/B - 19.486 sat/WU - 440 bytes)

15.31270454 BTC

Details

Hash	8855cf4d4e5f74309ac5dc491e6c9fc983957846d00a385b19004f28ddf1521e
Status	Confirmed

Demo Time

Recommended Readings & References

- Lean me a Bitcoin, https://learnmeabitcoin.com/, where most animations in my slides come from.
- Bitcoin Wiki, https://en.bitcoin.it/wiki/, a comprehensive wiki for Bitcoin
- *"But how does bitcoin actually work?"* by 3Blue1Brown, https://www.youtube.com/watch?v=bBC-nXj3Ng4&t=198s, the best video explaining how Bitcoin works I've seen.
- The original Bitcoin paper, https://bitcoin.org/bitcoin.pdf
- *"A beginners' guide to using the Bitcoin testnet"*, https://www.armedia.com/blog/bitcoin-testnet-beginners-guide/, if you want to play with Bitcoin without paying any real money.