

# THE BITCOIN TRANSACTION NETWORK

# BITCOIN IN A NUTSHELL

# HISTORY

- Invented by Satoshi Nakamoto (person or group of person), started in 2009
- The protocol is still evolving, the official *bitcoin core* is a GitHub repository, controlled by 5-10 individuals, on which anyone can propose contributions
  - Objectives: More efficient, faster, more secure, more anonymous,...

<https://github.com/bitcoin/bitcoin>

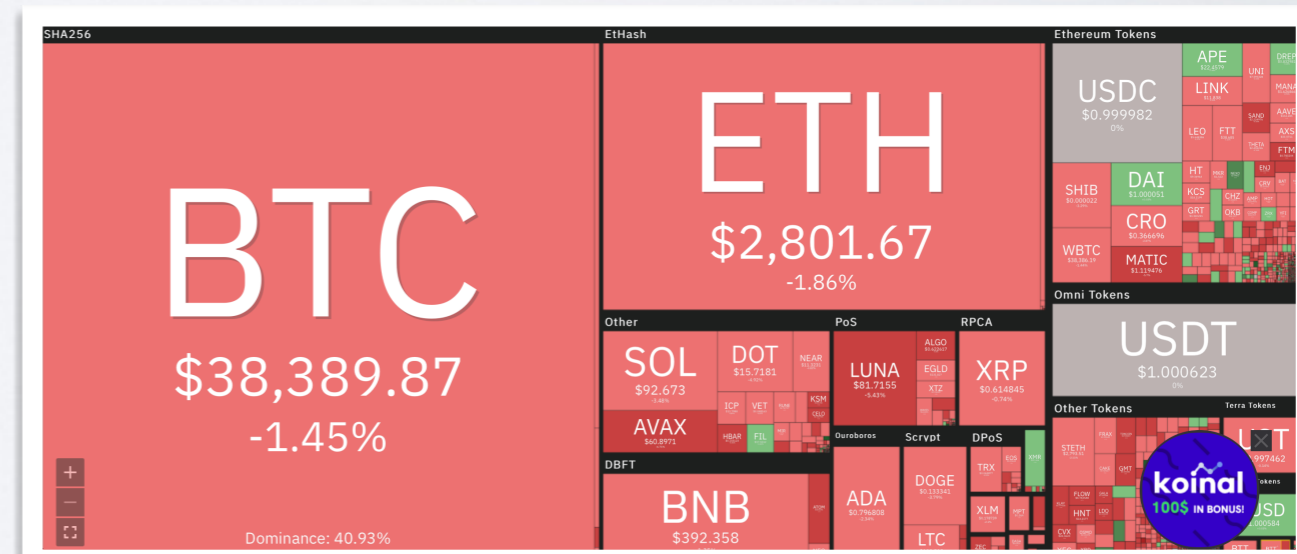
# WHAT IS IT?

- A cryptocurrency
- A decentralized digital currency
  - No central authority (no central bank or state issue or guarantee the currency)
  - Cryptographic methods guarantee that no-one is cheating:
    - Issuing their own coins
    - Stealing coins
    - Etc.



<https://coin360.com> (January 2024)

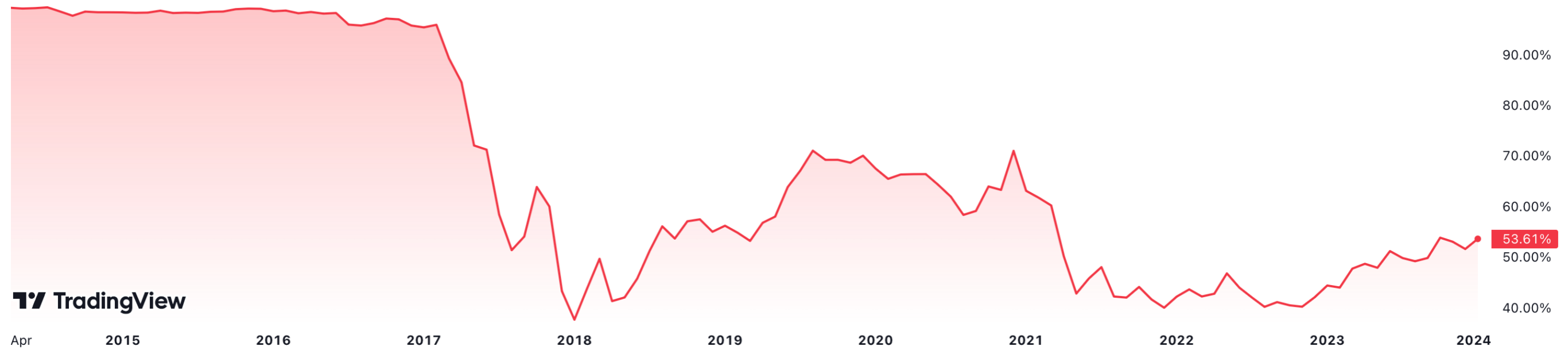
April 2022



# MARKET CAP DOMINANCE

📈 BTC.D 53.61% +0.07 +0.13%

[See on Supercharts](#)



TradingView

# Is this the end of crypto?

The collapse of FTX has dealt a catastrophic blow to crypto's reputation and aspirations



Nov 17th 2022

[Share](#)

15,875.32 EUR

+ Follow

-35,318.26 (68.99%) ↓ past year

Nov 23, 14:47 UTC · [Disclaimer](#)

1D | 5D | 1M | 6M | YTD | 1Y | 5Y | Max



Bitcoin



15,875.32 EUR

+ Follow

-35,318.26 (68.99%) ↓ past year

Nov 23, 14:47 UTC · Disclaimer

1D | 5D | 1M | 6M | YTD | 1Y | 5Y | Max



Market Summary > Meta Platforms Inc

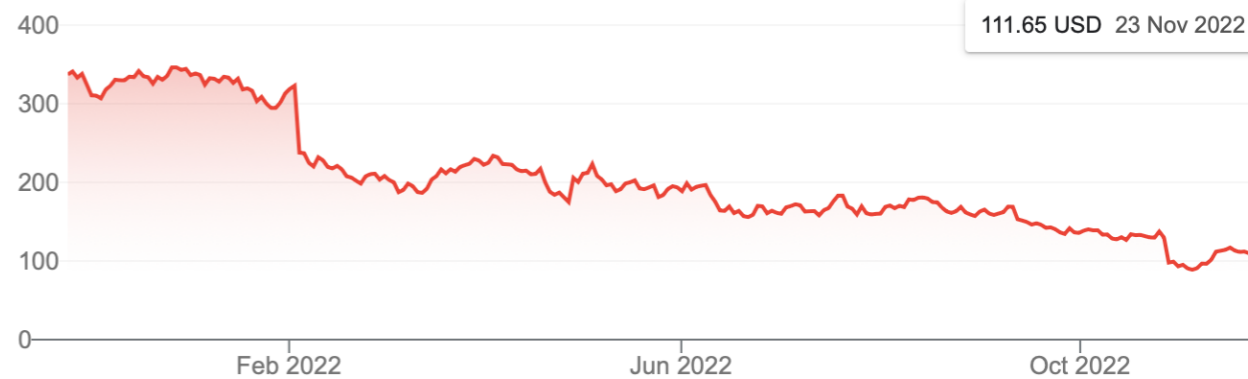
111.84 USD

+ Follow

-225.59 (-66.89%) ↓ past year

Nov 23, 09:51 EST · Disclaimer

1D | 5D | 1M | 6M | YTD | 1Y | 5Y | Max



Amazon

176.76 USD

+ Follow

-192.99 (-52.20%) ↓ past year

Nov 23, 09:52 EST · Disclaimer

1D | 5D | 1M | 6M | YTD | 1Y | 5Y | Max



Netflix

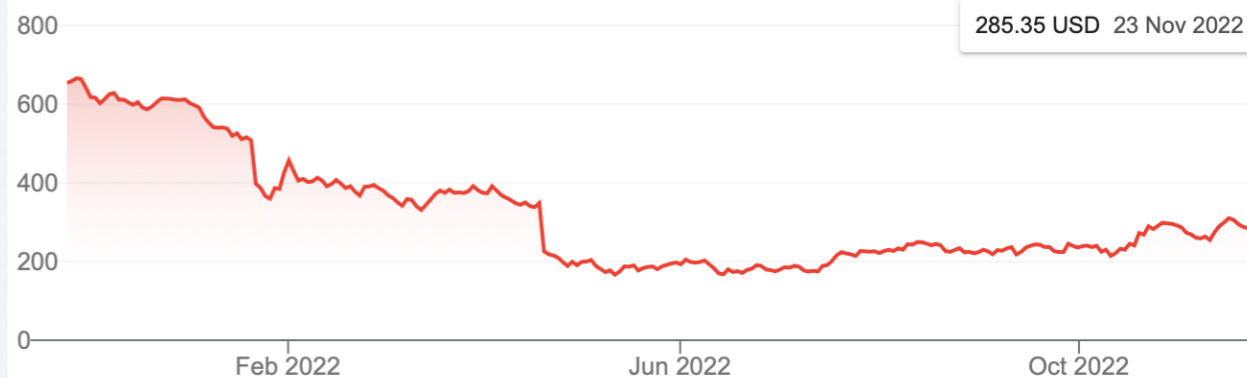
285.35 USD

+ Follow

-368.71 (-56.37%) ↓ past year

Nov 23, 09:52 EST · Disclaimer

1D | 5D | 1M | 6M | YTD | 1Y | 5Y | Max



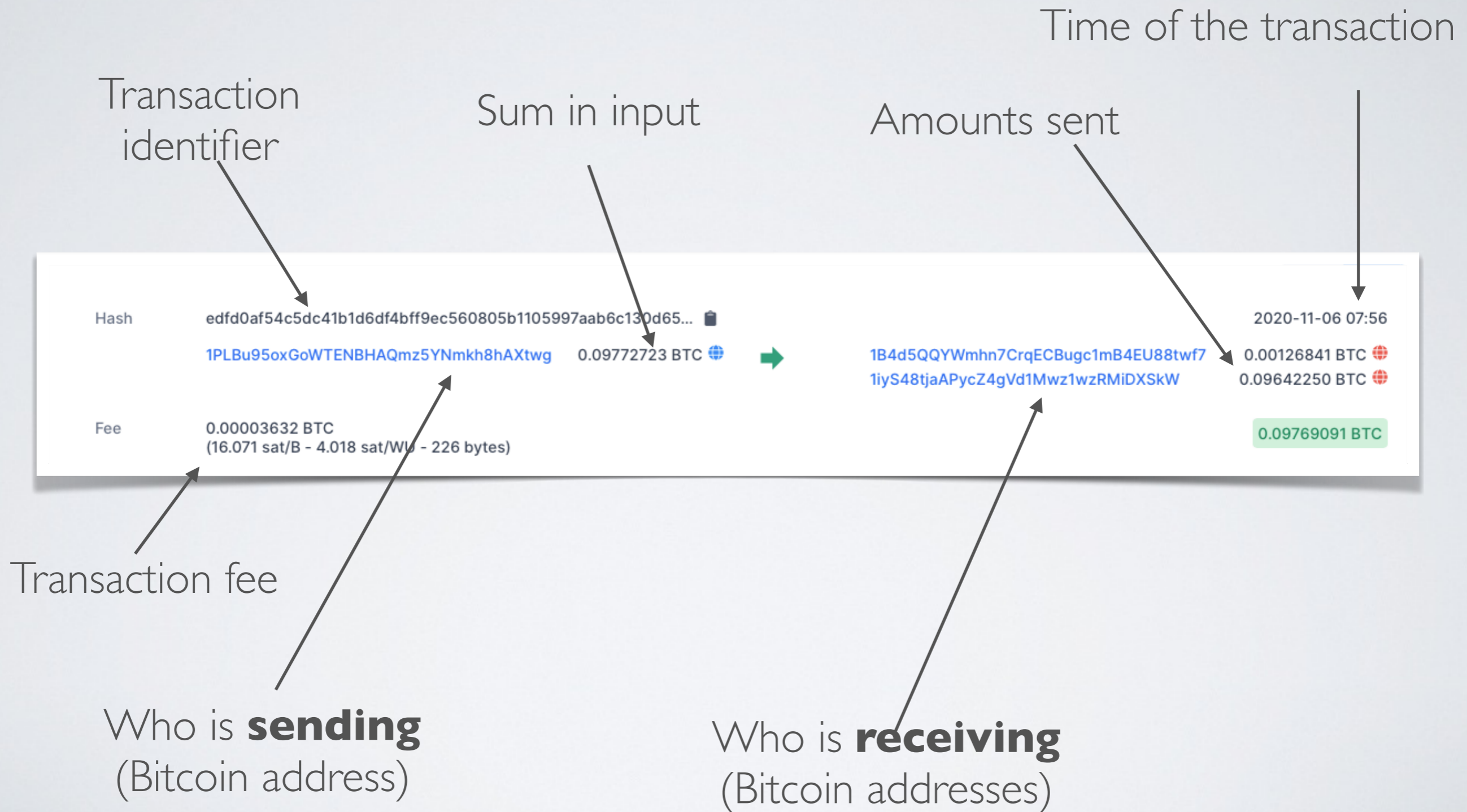
# SOME NUMBERS (2023)

- Bitcoins in existence(market cap) > \$300 Billions
  - > Samsung, intel, mastercard, visa, LVMH
- Transactions per day > 300,000 (+L2, lightning etc.)
  - VISA: 150 million.
- Median transaction fee = \$0,7
- Total value sent per day(without change) > \$5 Billion
- Trading volume per day > Between \$0.5 - 5 Billion
- Median transaction value = \$600

# DIGITAL LEDGER

- Bitcoin is based on a **blockchain**
  - ▶ Every transaction is stored in a *sequential database* (chain), a digital ledger.
    - Each new transaction is added at the end of the chain (in blocks)
    - Anyone can read everything in this chain
    - No-one can modify the older blocks in the chain
    - Adding a new element to the chain requires to solve a cryptographic problem

# TYPICAL RECORD



# TRADING VS BLOCKCHAIN

- False intuition : transactions in the blockchain mainly correspond to trading activities
- Changing BTC $\leftrightarrow$ \$/€  $\Rightarrow$  Exchange platforms
  - Nothing written in the Blockchain
- Volumes exchanged
  - Blockchain (day) > \$5 Billions
  - Estimated trading : About \$0.5 - 5 Billions

# BITCOIN ANONYMITY

- Anyone can see all transactions=>We can study in details aggregated statistics
  - Evolution of numbers, amount of transactions, fees, etc.
- So can we track user's activity?
  - Pseudonymity=>no way to link **bitcoin address** to **identity**
  - Users can create multiple addresses easily
  - Multiple addresses of a same person can sometimes be associated
  - In practice:
    - Large actors (companies, ...) are not anonymous
    - Individual users can hide what they are doing

# BITCOIN MARKETS

- Bitcoin value in \$ is fixed based on exchange markets
  - Trading, much as any other currency
  - Trade operations are usually not written in the blockchain, the bank virtually exchange between counts of its customers
- Transaction fees are decided based on another market
  - **Miners** use computation power to solve cryptographic problems to include transactions in the blockchain
    - They are paid by 1) newly created coins 2) transaction fee
  - Anyone is free to propose any transaction fee
    - Miners choose in priority transactions with higher fees

# CRYPTOCURRENCY OR CRYPTO-ASSET ?

- What is a currency ?
  - A priori definition: created by Central Bank, guaranteed by state, monetary policy... => Boring no
  - Definition based on functions:
    - 1) Medium of exchange, 2) unit of account, 3) Store of value => ?
- But how to evaluate ?
  - What fraction of actual exchange ?
  - What fraction of trading ?



# BITCOIN MARKETS

- What are bitcoin transactions?
  - ▶ Mining
  - ▶ Exchange between users?
  - ▶ Users buying services/products?
  - ▶ Trading?
    - No, not directly. Trading is done on exchange platforms and mostly handled internally
  - ▶ Gambling?
  - ▶ Exchange between “banks”, i.e., wallet managers?
  - ▶ Money laundering?
  - ▶ L2 transactions ? (Tether, Lightning, NFT, etc.)
- Detail is not known(yet) with precision

# ROLE PLAYED BY EXCHANGE PLATFORMS

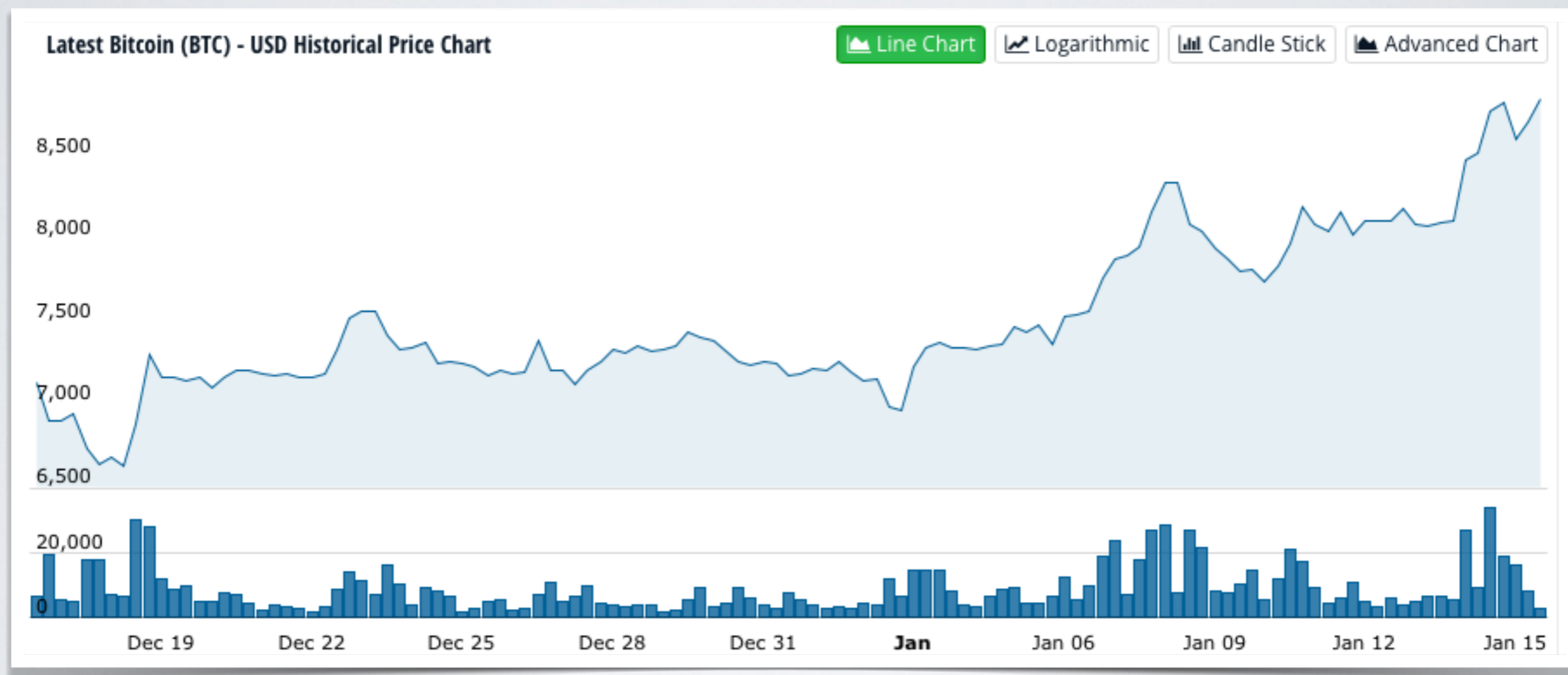
- Exchange behave as (centralized) banks
  - Exchange \$/€=>BTC
  - Gestion of “public accounts”
    - Transfer from/to accounts, internals and externals
    - => Payments
- 3 levels of usage of Bitcoin
  - Manual hand-made transactions (full control)
  - Using a Wallet application (trusting the wallet)
  - Account in an Exchange/centralized walled (full trust, centralized)
- Natural evolution of usage ?
  - Fear of errors, theft, loss (of secret codes...), insurance, ... ?

# BITCOIN TRANSACTION NETWORK ANALYSIS

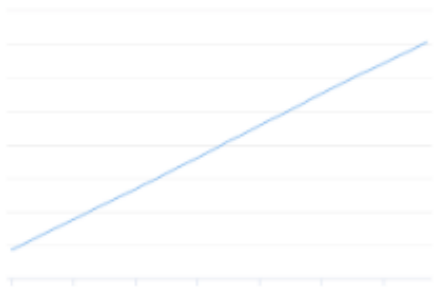
# BITCOIN

- In this class (today), we are **not** interested in:
  - Cryptographic aspects
  - How the blockchain works
  - Governance of cryptocurrencies
  - Smart Contracts
  - NFT
  - Defi
  - CBDC
- What we are interested in:
  - Observing and understanding what is happening at the micro-level in one cryptocurrency (for this class, the largest one, Bitcoin) => **Look under the hood !**
  - How what is happening at the micro-level can be connected to what we observe at the macro-level (crisis, price fluctuation, macro-indicators...)

# BITCOIN - MACRO LEVEL

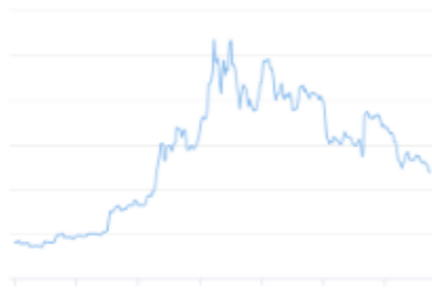


**Bitcoins in circulation**



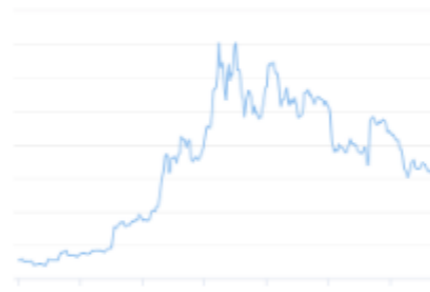
The total number of bitcoins that have already been mined.

**Market Price (USD)**



Average USD market price across major bitcoin exchanges.

**Market Capitalization**



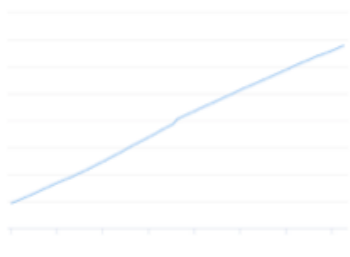
The total USD value of bitcoin supply in circulation.

**USD Exchange Trade Volume**



The total USD value of trading volume on major bitcoin exchanges.

**Blockchain Size**



The total size of all block headers and transactions.

**Average Block Size**



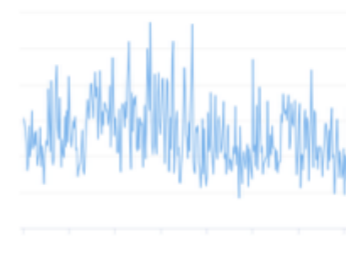
The average block size in MB.

**Transactions per Block**



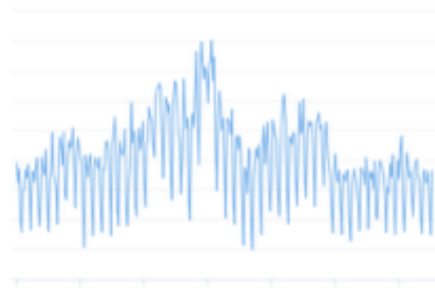
The average number of transactions per block.

**Median Transaction Confirmation Time (with fee)**



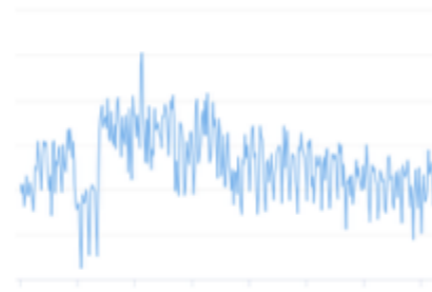
The median time for a transaction to be accepted into a mined block.

**Unique Addresses**



The total number of unique addresses used on the Bitcoin blockchain.

**Total Number of Transactions Per Day**



The number of daily confirmed Bitcoin transactions.

**Total Number of Transactions**



Total number of transactions.

**Transactions Rate**



The number of Bitcoin transactions added to the mempool per second.

# BITCOIN - MACRO LEVEL

- This type of aggregated data is mostly identical to data you are used to in finance/economy
- Can be studied with time series analysis (ARIMA, ...)
- What is unique about Bitcoin:
  - We have all data about all transactions done using a given currency
  - We can use this information in relation with macro-level statistics
  - We can use it for new types of analysis

# BITCOIN - DATA

- The data we use: Content of the bitcoin blockchain
  - Seen as a simple list of transactions

| Transaction | From | To  | Value |
|-------------|------|-----|-------|
| t0          | @1   | @2  | 5     |
| t1          | @1   | @3  | 2     |
| ...         | ...  | ... | ...   |

- Bitcoin transactions are a little bit more complicated than that



# BITCOIN - DATA

- You can explore it using tools such as a blockchain explorer
  - E.g.: <https://www.blockchain.com/explorer>

| Transactions       |  |                                      |                                      |                |
|--------------------|--|--------------------------------------|--------------------------------------|----------------|
| 1 2 3 4 5 Next +10 |  |                                      |                                      |                |
| Hash               | 4f8d922cb55ef80bd272ea0caa816d220789cbcc8d8435415a6f7f5...     |                                      | 2020-01-16 10:56                     |                |
|                    | COINBASE (Newly Generated Coins)                               | → 1KFHE7w8BhaENAswwryaoccDb6qcT6DbYY | 12.57483993 BTC                      |                |
|                    |  | OP_RETURN                            | 0.00000000 BTC                       |                |
|                    |  | OP_RETURN                            | 0.00000000 BTC                       |                |
|                    |  | OP_RETURN                            | 0.00000000 BTC                       |                |
| Fee                | 0.00000000 BTC<br>(0.000 sat/B - 0.000 sat/WU - 377 bytes)     |                                      | 12.57483993 BTC                      |                |
|                    |  |                                      | 1 Confirmations                      |                |
| Hash               | 7f1b409d20899c72698ae94e21541828256c7b5109f2ff6b4982316...     |                                      | 2020-01-16 10:55                     |                |
|                    | 1FLEdjadaP9Zih2Vu4fbkY5SbyNcfu85n2                             | 0.00029891 BTC                       | → 16S7Dfb7oD9Cy3RNFkqKSQMMNjxYdhcqQ7 | 0.00895513 BTC |
|                    | 1NDWrpHZouTFnB8uoRzEtXpHLZ6SLb2WQ                              | 0.00450559 BTC                       | → 3JoNoM1NxbvYCvsbZW8jib2K5F4cpdAwWr | 0.01408432 BTC |
|                    | 199RNd2JH9snPJFYoyayuy9MiAZcu36ftjB                            | 0.01928015 BTC                       |                                      |                |
| Fee                | 0.00104520 BTC<br>(201.776 sat/B - 50.444 sat/WU - 518 bytes)  |                                      | 0.02303945 BTC                       |                |
|                    |  |                                      | 1 Confirmations                      |                |
| Hash               | e04d42b758f43c93c09adcf08250e00d9c646118c2be167854c13d...      |                                      | 2020-01-16 10:56                     |                |
|                    | 34UExmBatmg8HccyFn1Zi93XpkwLAeyNtb                             | 0.00369290 BTC                       | → 346jtLokRPBUwaQPM1TZkC8kxyrc1iuavi | 4.79133982 BTC |
|                    | 3MGTiY83SatUbxDexxi3yDziCg6eH7Zd1v                             | 0.01280760 BTC                       |                                      |                |
|                    | 3LTjJ7n5sf8vhLqVDFKLNyo486dmsRjo4N                             | 0.00257434 BTC                       |                                      |                |
|                    | 3MRbeCXA1ZTA73NGZSjhiS9bTB2if42Qux                             | 0.02100000 BTC                       |                                      |                |
|                    | 3F5HeK5iNNNHAQqVfo2CKGy53xomaUocN9                             | 0.00245706 BTC                       |                                      |                |
|                    | 3PvLyDHFkuiPgTD6QjAD98p61FQqkDpUHP                             | 0.00200000 BTC                       |                                      |                |
|                    | 3JFxmAqzCkCnSwJdXootcDywpBUHBUyVzi                             | 0.04191421 BTC                       |                                      |                |
|                    | 3HzE43w3gb5sx1VQKKJTmVCyzRKtRbaMf                              | 0.00239492 BTC                       |                                      |                |
|                    | 3Lou9V7CqvGvAk9B6qVfV9VNMEMB7myPfi                             | 0.00200000 BTC                       |                                      |                |
|                    | 3EN1io5CbKdKRDDod3YJGwoaiFD4dbZXmq                             | 0.06100000 BTC                       |                                      |                |
|                    | Load more inputs... (63 remaining)                             |                                      |                                      |                |
| Fee                | 0.01069765 BTC<br>(85.404 sat/B - 40.114 sat/WU - 12526 bytes) |                                      | 4.79133982 BTC                       |                |
|                    |  |                                      | 1 Confirmations                      |                |

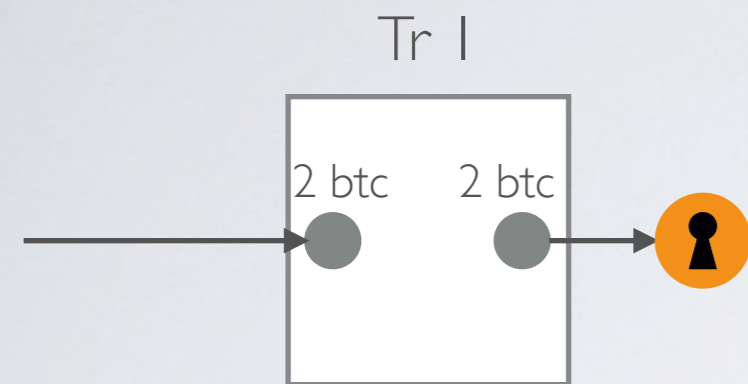
# UNDERSTANDING BITCOIN TRANSACTIONS

- Transactions are between  $m$  “inputs” and  $n$  “outputs”
- Each *input* (resp. *output*) is a pair (value, bitcoin address)
- *inputs* are necessarily *outputs* of previous transactions
  - Unlocked by the private key of the payer

# UNDERSTANDING BITCOIN TRANSACTIONS

- A user possess one (or several) **private keys**
- A user has a **public key** (bitcoin addresses) corresponding to each of these private keys
  - Instantaneously
  - At no cost
  - As often as wanted
- Public key  $\approx$  lock that can be opened only by an associated private key

# ILLUSTRATION



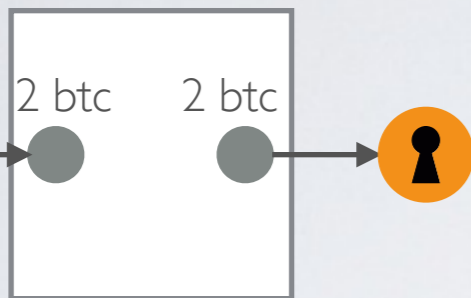
Public keys of user U1 :



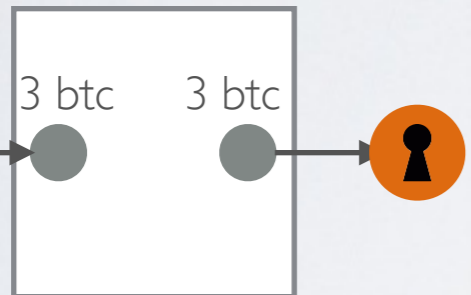
I BusVkYQvbbGbSDZNo5DfhrFeQdgKIYIVY

# ILLUSTRATION

Tr 1



Tr 2



Public keys of user U1 :

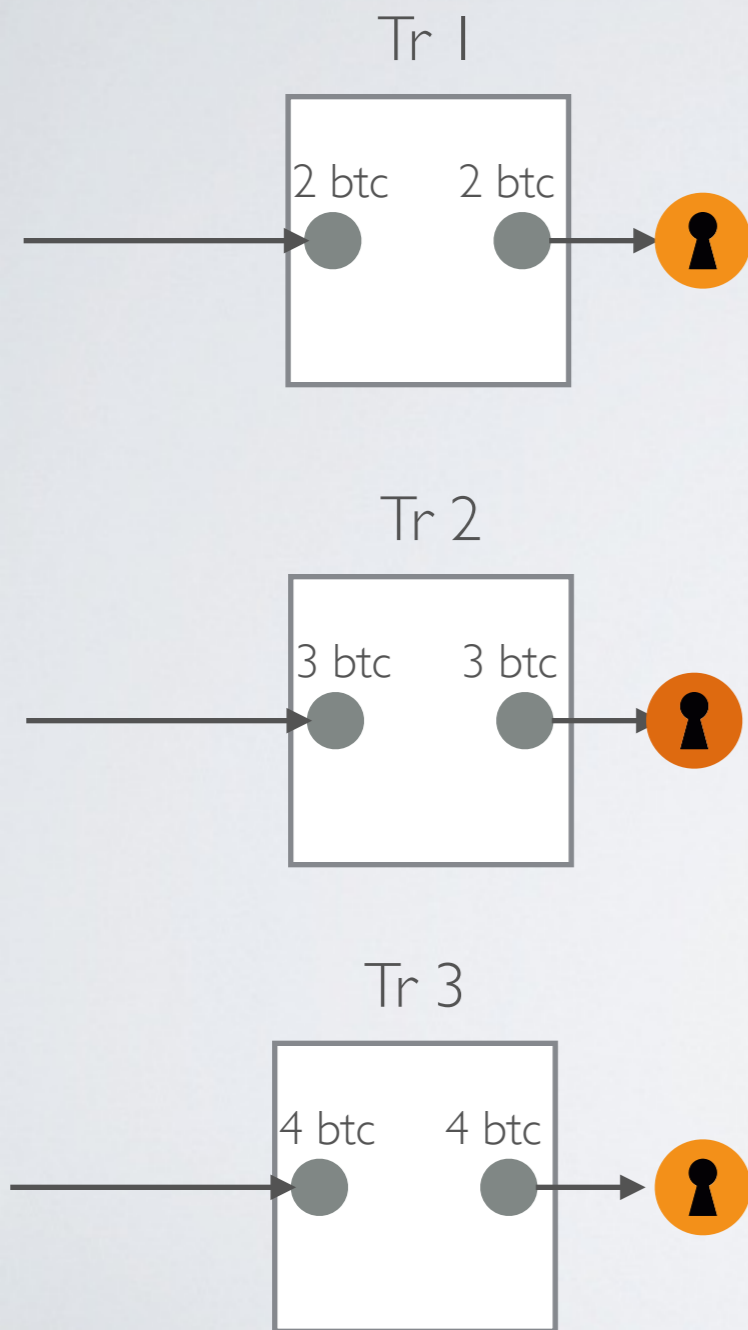


I BusVkYQvbbGbSDZNo5DfhrFeQdgKIYIVY



I QFdbGkhiCDFF45mBHgzWUdiqv55NJbd4u

# ILLUSTRATION



Public keys of user U1 :



I BusVkYQvbbGbSDZNo5DfhrFeQdgKIYIVY



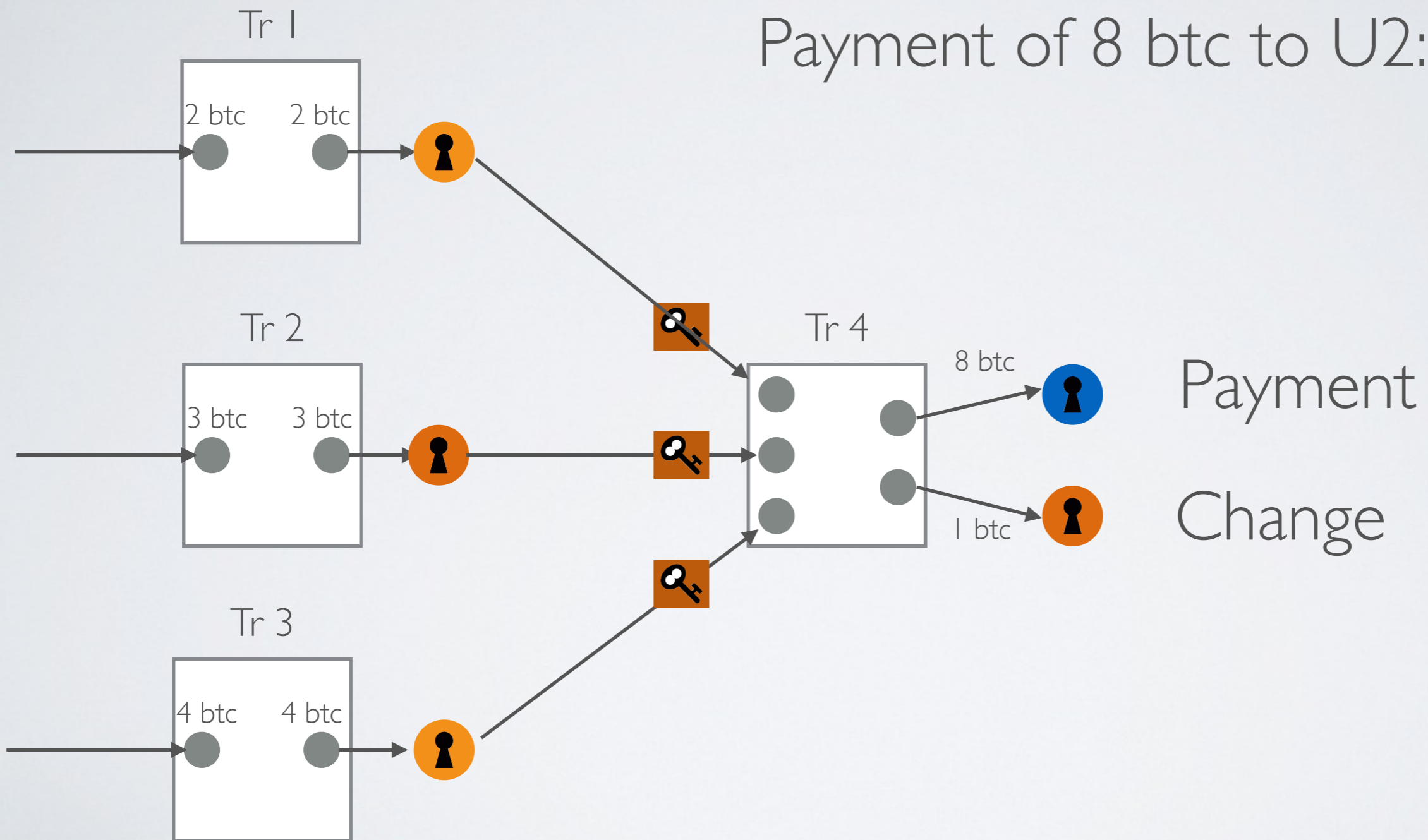
I QFdbGkhiCDFF45mBHgzWUdiqv55NJbd4u

**“Wallet” of U1:**

- 9 btc
- Divided in 3 “output”
- Locked by 2 different public keys

# ILLUSTRATION

Payment of 8 btc to U2:

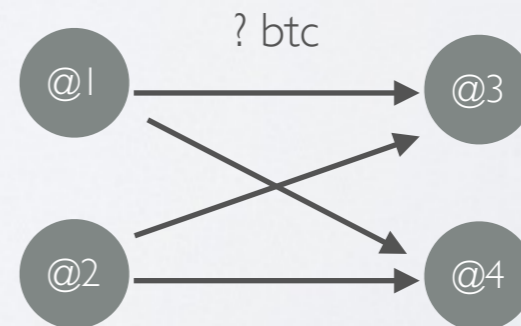
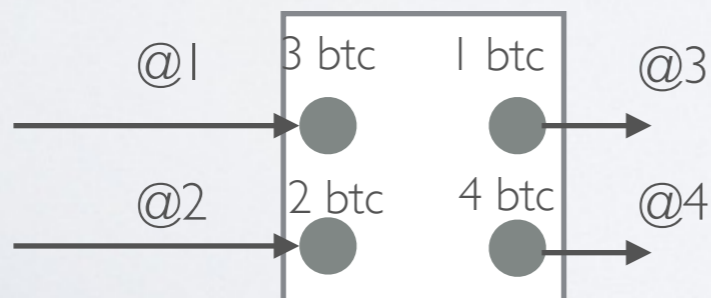


# BUILDING NETWORKS



# ADDRESS NETWORK

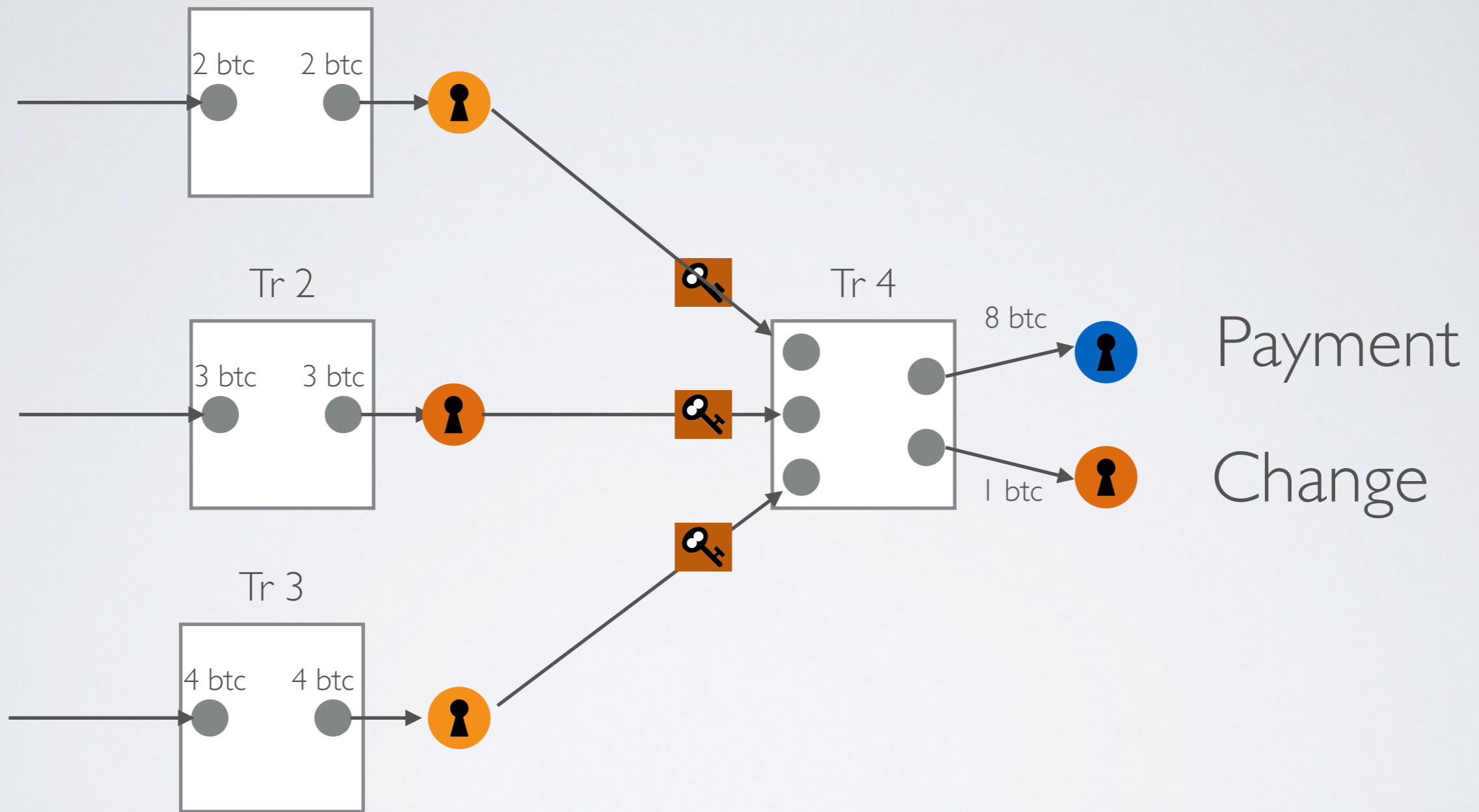
- First network, node=Address
  - Naive approach
  - One address  $\neq$  one user!
- Node: bitcoin address (public key)
- Edge: input addresses to output addresses.
- Problem: most transactions have several inputs, several outputs
  - Values ?




# ENTITIES NETWORK

- Transactions between “entities” of the bitcoin ecosystem
  - ▶ Individuals with their own private key(s) (e.g., using BRD, Atomic Wallet, etc.)
  - ▶ Companies/organisations with their own private key(s)
  - ▶ Exchanges (e.g., Binance, Coinbase, etc.)
  - ▶ Mining Pool
  - ▶ etc.
- An entity can have **many** public keys/addresses
- How to retrieve addresses belonging to the same entity?

# ENTITY NETWORK

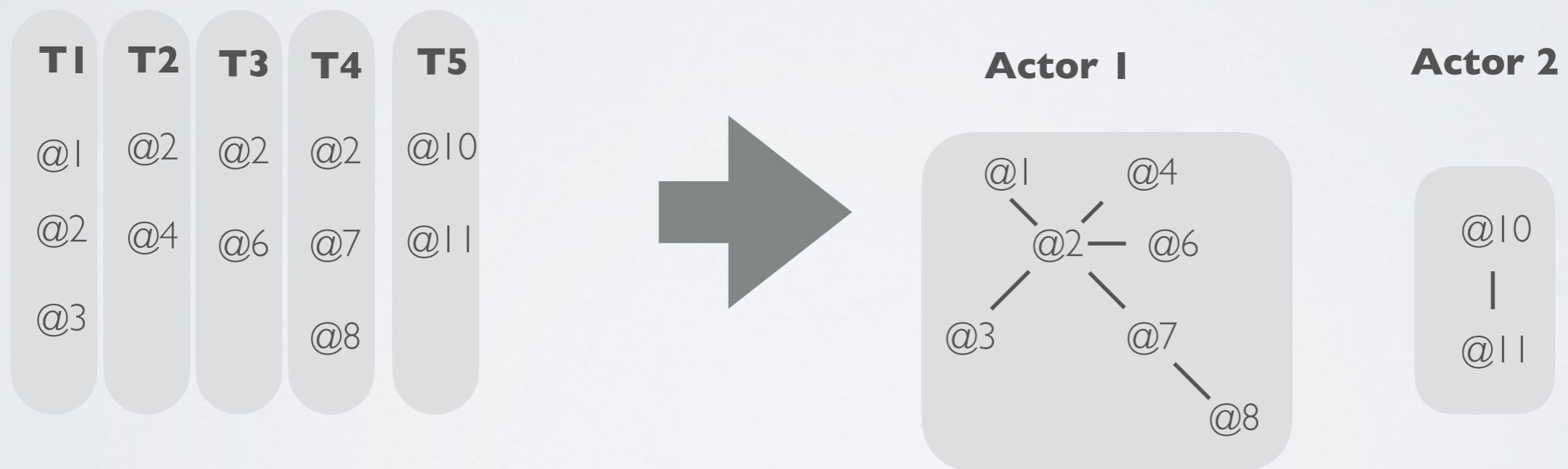


 and  are inputs of the same transaction  
=> same actor

# ENTITY NETWORK

- Entity identification: find all addresses of a same user
  - Currently a research question...
- Heuristics (input):
  - All addresses in input of a same transaction belongs to the same person

# ENTITY NETWORK

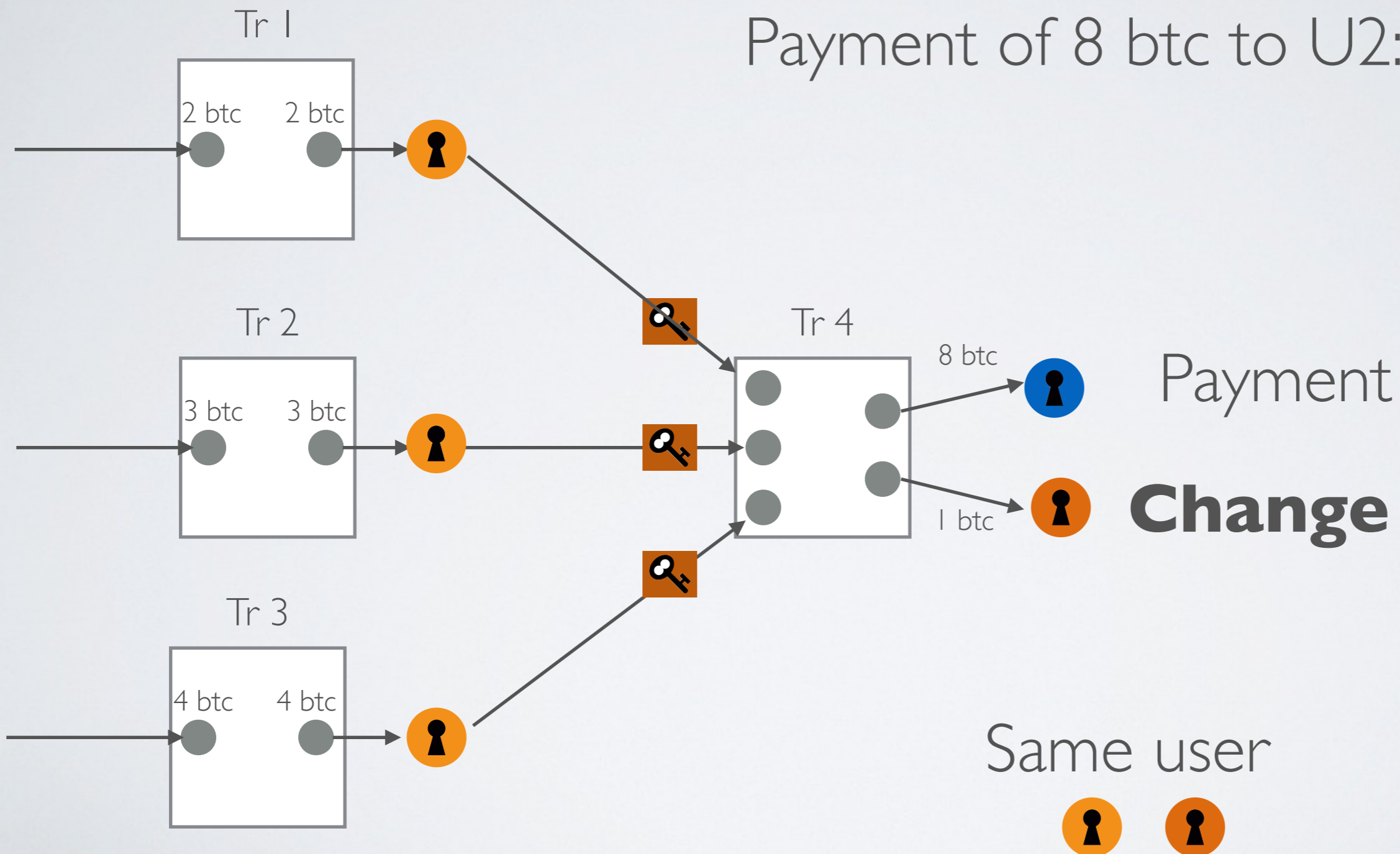


# ENTITY NETWORK

- Entity identification: find all addresses of a same user
  - Currently a research question...
- Heuristics (input):
  - All addresses in input of a same transaction belongs to the same person
- Heuristics (output):
  - One of the addresses in output is probably a **change address**, thus an address of the same user as the one in input
  - But which one ?

# ENTITY NETWORK

Payment of 8 btc to U2:



# ENTITY NETWORK

- Heuristics (output):

- ▶ One of the addresses in output is probably a **change address**, thus an address of the same user as the one in input
- ▶ But which one ?
  - Lower value ?
  - Value with the same decimal as input?
  - Learn which one using machine learning and examples ?
  - ...



# ENTITY NETWORK

- Examples of methods:

- ▶ Cazabet, R., Baccour, R., & Latapy, M. (2017, November). Tracking bitcoin users activity using community detection on a network of weak signals. In The 6th International Conference on Complex Networks and Their Applications.
- ▶ Tubino, R. R., Robardet, C., & Cazabet, R. (2022). Towards a better identification of Bitcoin actors by supervised learning. *Data & Knowledge Engineering*, 142, 102094.
- ▶ Möser, M., & Narayanan, A. (2021). Resurrecting Address Clustering in Bitcoin

# ENTITY NETWORK

- Describe each output using features:
  - ▶ Value in satoshi
  - ▶ Value in \$
  - ▶ Value of input
  - ▶ Number of decimals in Bitcoin
  - ▶ Date
  - ▶ Fees
  - ▶ Number of inputs/outputs
  - ▶ Number of reuse
  - ▶ ...
- Train a machine learning algorithm to recognize change transactions

# ENTITY NETWORK

- Group of addresses => Anonymous Entity
  - ▶ Can we know who is this Entity?
  - ▶ It is sufficient to identify *one* address
  - ▶ One transaction with a person/company => we know one of its addresses
  - ▶ On the internet, many company/individuals provide their addresses.
  - ▶ For some entities, we might infer their category
    - => Miners
    - => Large transactions profiles VS low transaction profiles
    - Has made transactions to identified money laundering services => suspicious
    - Machine learning => Automatically recognize profiles, identify similar entities, ...
    - etc.

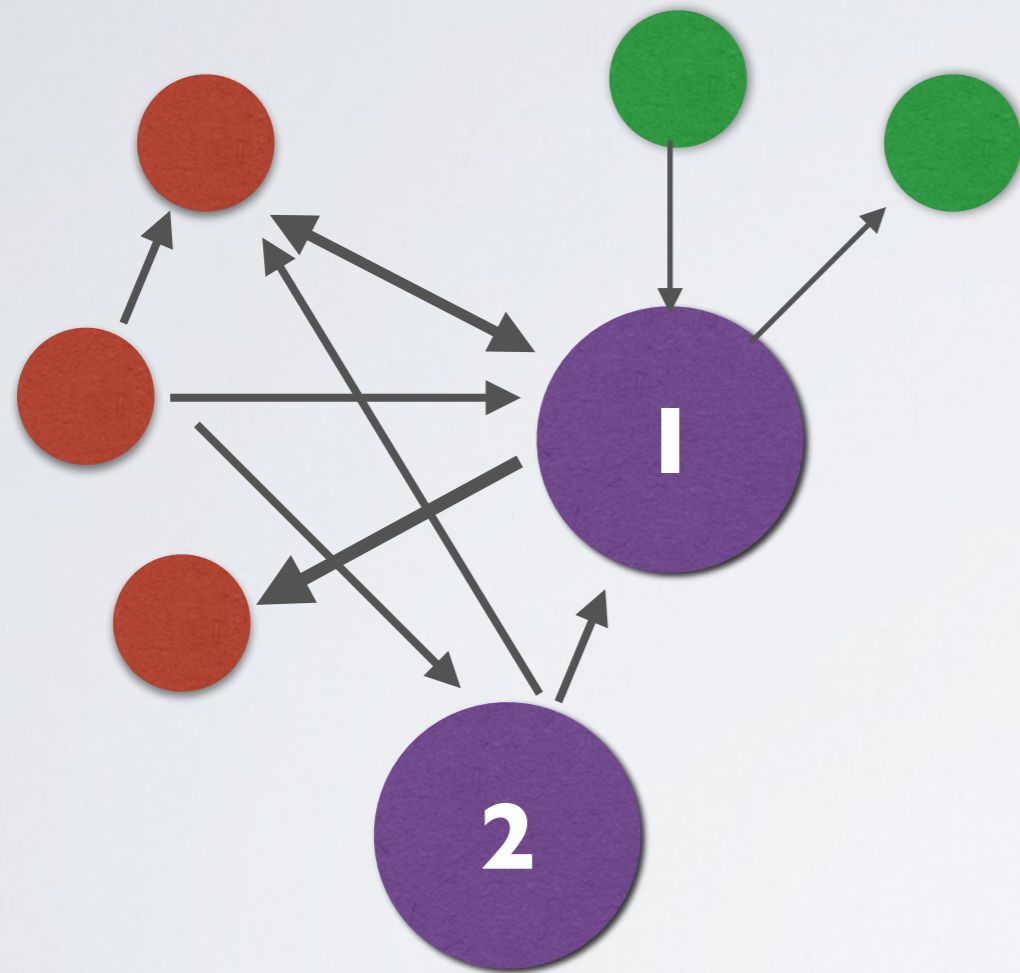
# ENTITY NETWORK

List of actors addresses, for instance: <https://www.walletexplorer.com>

## Top wallets

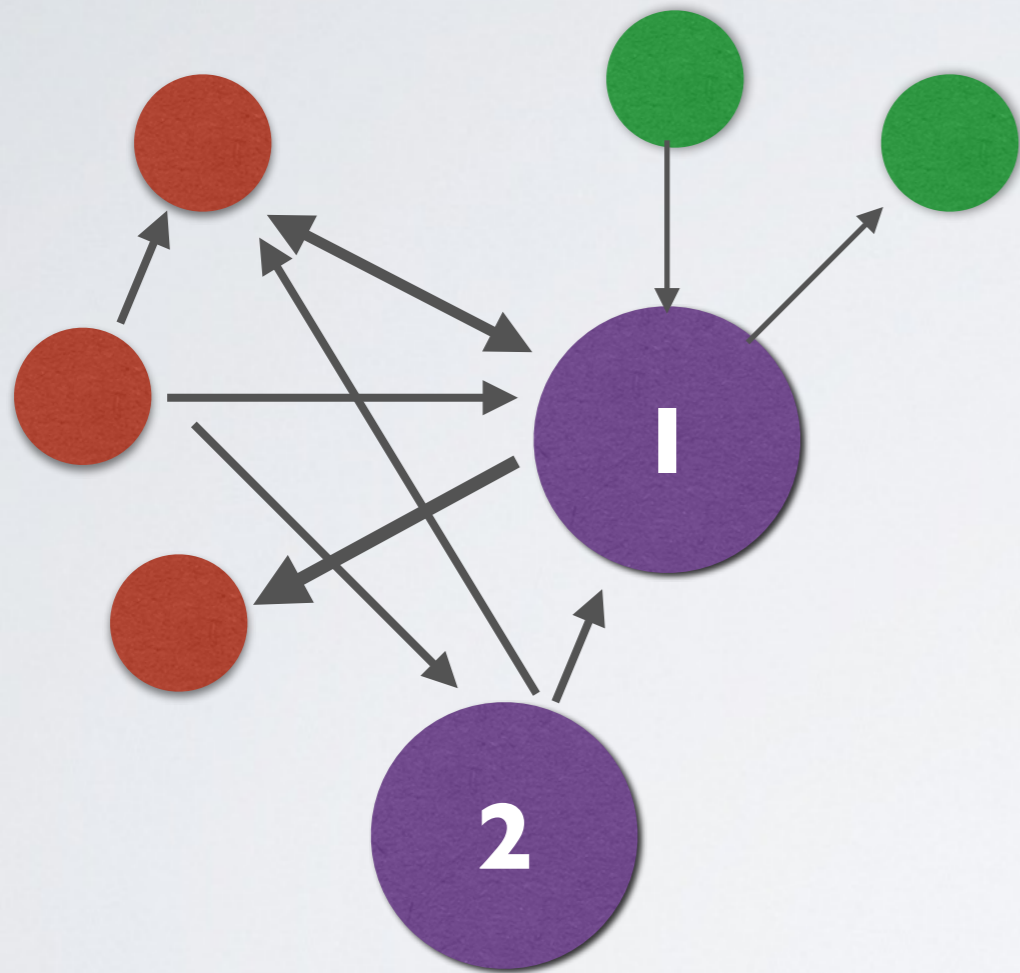
| Exchanges:   | Pools:  | Services/others:  | Gambling:   | Old/historic:   |
|--|---|---|---|---|
| <a href="#">Huobi.com</a> (2)<br><a href="#">Bittrex.com</a><br><a href="#">Poloniex.com</a><br><a href="#">Luno.com</a><br><a href="#">BTC-e.com</a> (output) (old)<br><a href="#">Kraken.com</a> (old)<br><a href="#">LocalBitcoins.com</a> (old)<br><a href="#">Bitstamp.net</a> (old)<br><a href="#">MercadoBitcoin.com.br</a><br><a href="#">BitZlato.com</a><br><a href="#">Cryptsy.com</a> (old)<br><a href="#">Bitcoin.de</a> (old)<br><a href="#">Cex.io</a><br><a href="#">Binance.com</a> (old)<br><a href="#">BtcTrade.com</a><br><a href="#">YoBit.net</a><br><a href="#">OKCoin.com</a> (2)<br><a href="#">BTCC.com</a> (old) (old2)<br><a href="#">BX.in.th</a><br><a href="#">HitBtc.com</a> (old)<br><a href="#">MaiCoin.com</a><br><a href="#">Bter.com</a> (old) (old2) (old3) (cold)<br><a href="#">CoinSpot.com.au</a><br><a href="#">Hashnest.com</a><br><a href="#">AnxPro.com</a><br><a href="#">BitBay.net</a><br><a href="#">Bleutrade.com</a><br><a href="#">Bitfinex.com</a> (old) (old2)<br><a href="#">Matbea.com</a><br><a href="#">Bit-x.com</a><br><a href="#">VirWoX.com</a><br><a href="#">Paxful.com</a><br><a href="#">BitBargain.co.uk</a> | <a href="#">BTCPOOL</a><br><a href="#">SlushPool.com</a> (old) (old2)<br><a href="#">GHash.io</a><br><a href="#">AntPool.com</a> (old) (old2)<br><a href="#">BitMinter.com</a><br><a href="#">EclipseMC.com</a> (old) (old2) (old3)<br><a href="#">KnCMiner.com</a><br><a href="#">Bitfury.org</a><br><a href="#">BW.com</a><br><a href="#">Eligius.st</a><br><a href="#">Kano.is</a> (old)<br><a href="#">Telco214</a> | <a href="#">CoinPayments.net</a><br><a href="#">Xapo.com</a><br><a href="#">Cubits.com</a><br><a href="#">Cryptonator.com</a> (old)<br><a href="#">BitPay.com</a> (old) (old2) (old3)<br><a href="#">BitoEX.com</a><br><a href="#">HaoBTC.com</a><br><a href="#">Cryptopay.me</a> (old)<br><a href="#">AlphaBayMarket</a> (old)<br><a href="#">NucleusMarket</a><br><a href="#">BitcoinFog</a><br><a href="#">CoinJar.com</a><br><a href="#">BitcoinWallet.com</a><br><a href="#">HolyTransaction.com</a><br><a href="#">HelixMixer</a> (old) (old2) (old3) (old4) (old5) (old6) (old7) (old8) (old9) (old10) (old11) (old12) (old13) (old14) (old15) (old16) (old17) (old18) (old19) (old20) (old21) (old22) (old23) (old24) (old25) (old26) (old27) (old28) (old29) (old30) (old31) (old32) (old33) (old34)<br><a href="#">BTCJam.com</a><br><a href="#">VIP72.com</a><br><a href="#">MoonBit.co.in</a><br><a href="#">CoinKite.com</a><br><a href="#">FaucetBOX.com</a><br><a href="#">OkLink.com</a><br><a href="#">Purse.io</a><br><a href="#">ePay.info</a><br><a href="#">Loanbase.com</a><br><a href="#">GermanPlazaMarket</a><br><a href="#">Paymium.com</a><br><a href="#">Bitbond.com</a><br><a href="#">CrimeNetwork.co</a> (old) | <a href="#">SatoshiDice.com</a> (original)<br><a href="#">LuckyB.it</a> (chatbot)<br><a href="#">BitZillions.com</a><br><a href="#">999Dice.com</a><br><a href="#">CoinGaming.io</a><br><a href="#">PrimeDice.com</a> (old) (old2) (old3) (old4)<br><a href="#">CloudBet.com</a><br><a href="#">SatoshiMines.com</a><br><a href="#">NitrogenSports.eu</a><br><a href="#">SecondsTrade.com</a><br><a href="#">PocketDice.io</a><br><a href="#">FortuneJack.com</a><br><a href="#">Rollin.io</a><br><a href="#">BitZino.com</a><br><a href="#">BitcoinVideoCasino.com</a> (old) (old2)<br><a href="#">Betcoin.ag</a> (old)<br><a href="#">YABTCL.com</a><br><a href="#">SatoshiBet.com</a><br><a href="#">SafeDice.com</a><br><a href="#">Coinroll.com</a><br><a href="#">Crypto-Games.net</a><br><a href="#">Betcoin.tm</a><br><a href="#">SwCPoker.eu</a><br><a href="#">SatoshiRoulette.com</a><br><a href="#">BTCOracle.com</a><br><a href="#">Peerbet.org</a><br><a href="#">AnoniBet.com</a><br><a href="#">Satoshi-Karoshi.com</a> (old)<br><a href="#">777Coin.com</a><br><a href="#">BitStarz.com</a><br><a href="#">SatoshiCircle.com</a><br><a href="#">Coinichiwa.com</a> | <a href="#">AgoraMarket</a><br><a href="#">BetcoinDice.tm</a><br><a href="#">SilkRoadMarketplace</a><br><a href="#">DeepBit.net</a><br><a href="#">SilkRoad2Market</a><br><a href="#">EvolutionMarket</a><br><a href="#">Instawallet.org</a><br><a href="#">UpDown.BT</a><br><a href="#">AbraxasMarket</a><br><a href="#">MintPal.com</a><br><a href="#">SealsWithClubs.eu</a><br><a href="#">PandoraOpenMarket</a><br><a href="#">MiddleEarthMarketplace</a><br><a href="#">BtcDice.com</a><br><a href="#">McxNOW.com</a><br><a href="#">SheepMarketplace</a><br><a href="#">DiceOnCrack.com</a><br><a href="#">BlackBankMarket</a><br><a href="#">BTCGuild.com</a><br><a href="#">Coin-Swap.net</a><br><a href="#">BlueSkyMarketplace</a><br><a href="#">Justcoin.com</a><br><a href="#">PinballCoin.com</a><br><a href="#">Inputs.io</a><br><a href="#">BitAces.me</a> (old)<br><a href="#">AllCoin.com</a><br><a href="#">Bitcoin-24.com</a> (old) (old-hotwallet)<br><a href="#">Betcoins.net</a><br><a href="#">CrimeNetwork.biz</a><br><a href="#">Bitcoin-Roulette.com</a><br><a href="#">Bitmit.net</a><br><a href="#">Cryptorush.in</a> |

# OBTAINED NETWORK

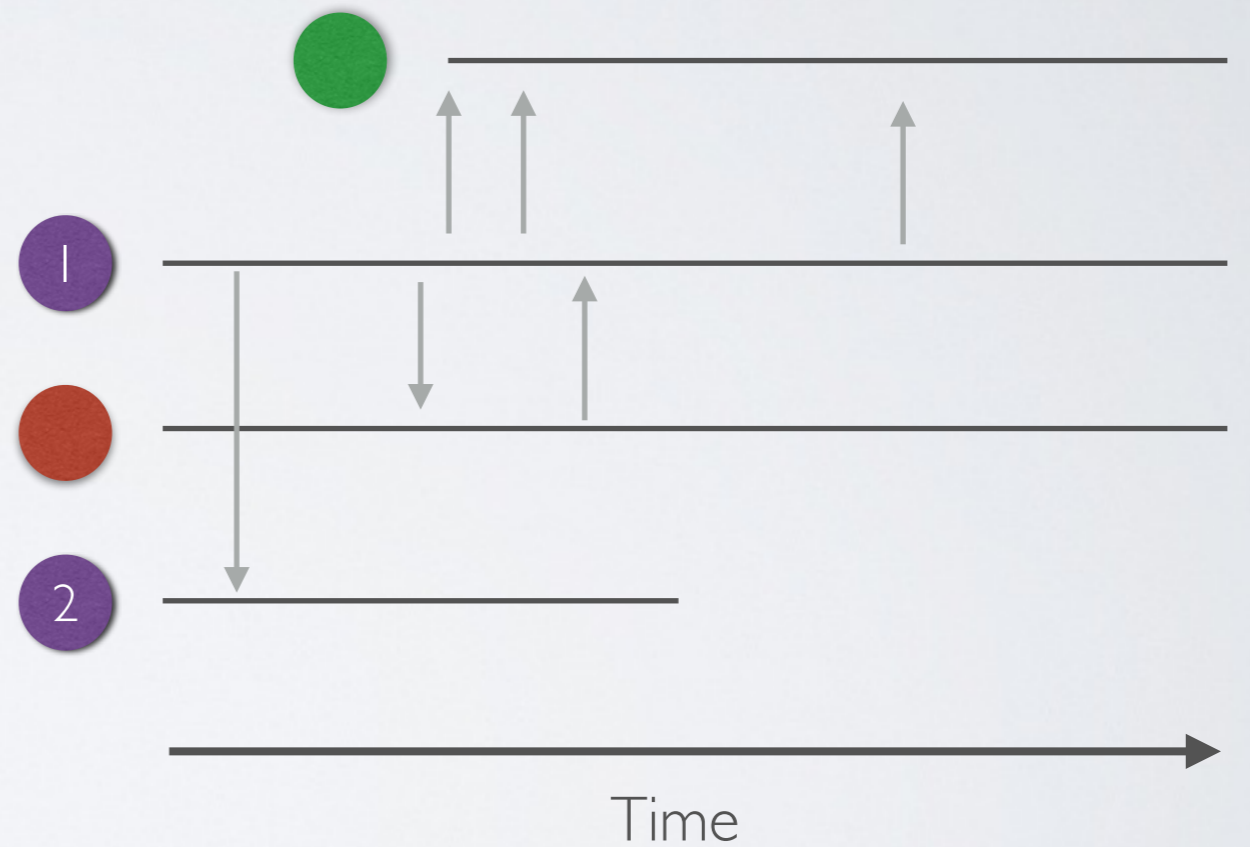


- Identified nodes
- Category 1
- Category 2

# OBTAINED NETWORK



- Identified nodes
- Category 1
- Category 2



# ENTITY NETWORK

- Example: 2 days (August 2&3 2016)
- Address network
  - ▶ # Transactions: 490 441
  - ▶ # Transaction outputs: 1 210 004 (avg. 2,46)
  - ▶ # Transaction inputs 1 211 790 (avg. 2.47)
  - ▶ # Addresses: 933 645
  - ▶ # @->@ Edges: 3 014 350
- Entity network
  - ▶ # Clusters: 456 012
  - ▶ Largest clusters sizes: 20 023, 19 381, 17 244
  - ▶ # Edges (Entity -> Entity) : 956 347

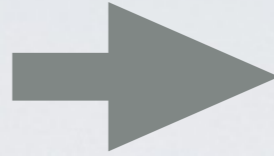
# BITCOIN BLOCKCHAIN ACTIVITY TRACKING EXAMPLE



1

Traditional Bank

Transfer (€)



→ deposited 75.00 € processed 2/10/2017

Operations

| Account   | Name      | Amount   | Date                |
|-----------|-----------|----------|---------------------|
| available | operation | +75.00 € | 2/10/2017 - 3:28 PM |

2

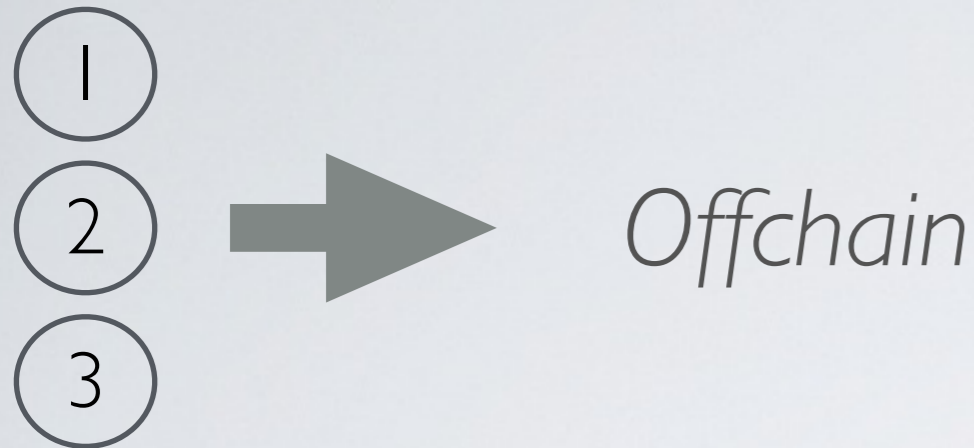
Initial Bitcoin purchase (trading)

↑ bought 0.05423052 btc for 921.99 € average filled 2/10/2017

3

“Trading”

|          |                |                |         |        |           |
|----------|----------------|----------------|---------|--------|-----------|
| ↓ sold   | 0.07130000 btc | for 1,059.00 € | average | filled | 2/22/2017 |
| ↑ bought | 0.07136414 btc | for 1,008.91 € | average | filled | 2/18/2017 |
| ↓ sold   | 0.07400000 btc | for 980.17 €   | average | filled | 2/18/2017 |
| ↑ bought | 0.05076142 btc | for 985.00 €   | average | filled | 2/17/2017 |
| ↓ sold   | 0.02600000 btc | for 975.01 €   | average | filled | 2/16/2017 |



- How it works (probably)

- ▶ The exchange company owns a stock of Bitcoin
- ▶ It maintains a list of customer accounts, and how much each customer owns at time  $t$
- ▶ When customer  $c_1$  buys BTC to a customer  $c_2$ , change in the internal database of the company (scripture)
  - Goal: no transaction fees, easier to manage
- ▶ The company itself certainly buys and sell on the market to ensure liquidity
  - Success=more customers who want to buy=>need to provide fresh coins
  - Need of buying/selling on the blockchain
- ▶ The company needs enough reserve since customers can order bitcoin transactions from their (*virtual*) account to a *real bitcoin wallet*

bought

0.05417748 btc for 1,974.99 € average

filled 5/28/2017

9:23GMT+1

| timestamp | sender     | receiver                 | value     | date                | value_btc |
|-----------|------------|--------------------------|-----------|---------------------|-----------|
| 619503540 | 1495929670 | -192947146 Paymium.com   | 4276511   | 2017-05-28 00:01:10 | 0.042765  |
| 619622203 | 1495940615 | 35172026 Paymium.com     | 21408870  | 2017-05-28 03:03:35 | 0.214089  |
| 619627952 | 1495940615 | 36676998 Paymium.com     | 1278580   | 2017-05-28 03:03:35 | 0.012786  |
| 619641058 | 1495941084 | 320110 Paymium.com       | 2889754   | 2017-05-28 03:11:24 | 0.028898  |
| 619678470 | 1495946218 | 234 Paymium.com          | 50000000  | 2017-05-28 04:36:58 | 0.500000  |
| 619720731 | 1495953357 | 21 Paymium.com           | 500000000 | 2017-05-28 06:35:57 | 5.000000  |
| 619724954 | 1495954071 | Poloniex.com Paymium.com | 90000000  | 2017-05-28 06:47:51 | 0.900000  |
| 619734802 | 1495953492 | 15195288 Paymium.com     | 563100    | 2017-05-28 06:38:12 | 0.005631  |
| 619742071 | 1495956403 | 32328334 Paymium.com     | 300000000 | 2017-05-28 07:26:43 | 3.000000  |
| 619749598 | 1495956760 | Bitstamp.net Paymium.com | 500000000 | 2017-05-28 07:32:40 | 5.000000  |
| 619773769 | 1495962103 | Poloniex.com Paymium.com | 5990000   | 2017-05-28 09:01:43 | 0.059900  |
| 619813537 | 1495968880 | Poloniex.com Paymium.com | 299990000 | 2017-05-28 10:54:40 | 2.999900  |
| 619814805 | 1495969178 | -193097249 Paymium.com   | 5000000   | 2017-05-28 10:59:38 | 0.050000  |
| 619816324 | 1495969665 | -193098289 Paymium.com   | 501097    | 2017-05-28 11:07:45 | 0.005011  |
| 619859643 | 1495972870 | Bitstamp.net Paymium.com | 99900000  | 2017-05-28 12:01:10 | 0.999000  |
| 619870536 | 1495971407 | -193116479 Paymium.com   | 4113900   | 2017-05-28 11:36:47 | 0.041139  |
| 619874781 | 1495972455 | 5224442 Paymium.com      | 1373550   | 2017-05-28 11:54:15 | 0.013735  |
| 619877124 | 1495973819 | -193121122 Paymium.com   | 365283    | 2017-05-28 12:16:50 | 0.003653  |
| 619880471 | 1495972455 | -193122823 Paymium.com   | 59539     | 2017-05-28 11:54:15 | 0.000595  |
| 619880482 | 1495972455 | -193122827 Paymium.com   | 58606     | 2017-05-28 11:54:15 | 0.000586  |
| 619882043 | 1495973387 | Paymium.com 16096        | 620000    | 2017-05-28 12:09:47 | 0.006200  |
| 619882044 | 1495973387 | Paymium.com 222          | 6800000   | 2017-05-28 12:09:47 | 0.068000  |

Paymium on-chain activity on 2017-05-28

Hard to say what it corresponds too...  
But my exact transaction is not there

... (153 total)

# 4 Sending 0.005 btc from Paymium exchange to my personal wallet



← transferred 0.00500000 btc 👁 processed 2/10/2017

| Hash  | 2017-02-10 19:48                      |
|---|---------------------------------------|
| 1431198bef5645bcce667c11f988257292c...            |                                       |
| 1FNhjTqbogGenAtiVn... 0.03000000 BTC              | 1FBov1eSTzbEWFhNP... 0.04811430 BTC   |
| 1FNhjTqbogGenAtiVn... 0.29980000 BTC              | 1FnJ7ifPVs6pVzPAHj... 0.15385554 BTC  |
| 1ChT8jHwnu28S8Gse... 0.00552015 BTC               | 1PLS2uFx9RCXj6y7o... 0.03240000 BTC   |
| 134JTcD1rwYzf3mJh... 0.01066365 BTC               | 1JPDfDbpYu7ZMN54... 0.11000000 BTC    |
| 1F2DnSngMqhx3Bc5t... 0.00102304 BTC               | 1Acekhv2vRYE8JUY... 0.10000000 BTC    |
| 1PmJouprMuWvnuz1... 0.00060627 BTC                | 125UVAGTHgRpUWu... 5.00000000 BTC     |
| 1CNKsJdKEGAfk7A6... 0.02800000 BTC                | 1LCy45fGKy5DDyLX7... 0.19080000 BTC   |
| 1Jv324ZskcMwVaHo... 0.04971298 BTC                | 1JQAJC1as3zqGvh3R... 0.10780000 BTC   |
| 1Jv324ZskcMwVaHo... 0.02700664 BTC                | 1uQWT55a31oXbG7y... 0.06000000 BTC    |
| 1FyJw1oF7ojJVfb... 200.00000000 BTC               | 1AtG2dZL2QT9Anob... 0.26000000 BTC    |
| <a href="#">Load more inputs... (1 remaining)</a> | 19P2i6fCFLyhsZWVd... 0.05476170 BTC   |
|   | 1NAr6doa9jzdAtjfcED... 0.00100000 BTC |
|   | 1GZjj8XvbdVvMgiSm... 0.21500000 BTC   |
|   | 32SRuobXXWbxRYeLt... 0.11180000 BTC   |
|   | 1DtnwrYpuj2AviHBKL... 0.31386546 BTC  |
|   | 1mxx5bDua8844zAik... 0.03416878 BTC   |
|   | 1X9rcMVx8SvZ5uPz... 0.00500000 BTC    |
|   | 1Hxm69VGPXfGu7kB... 0.01000000 BTC    |
|   | 1CEoEkc1xzb5mBhpa... 0.00547958 BTC   |
|   | 3ErsNJgohjZ9DeJcz... 0.56630000 BTC   |
|   | 13sSQcEjasD7S5PZn... 0.01185000 BTC   |
|   | 17McVX1jhiEMg5Mnt... 0.85516806 BTC   |
|   | 1LHY6mAeqHVYbpZ... 0.37096600 BTC     |
|   | 15Gw27cNPkqgUxqe... 0.26954988 BTC    |
|   | 15wgdri64ZuV8QY... 0.26955280 BTC     |
|   | 1KbB2KsEV2wUkAAx... 0.10780000 BTC    |
|   | 1Bjkr17q2TF37nvTdC... 1.00000000 BTC  |
|   | 16zFtGxAF7RWnpZay... 0.10712284 BTC   |
|   | 14qiXwDXJLUM5P7h... 0.04280000 BTC    |
|   | 1FyJw1oF7ojJVfbM... 193.37661929 BTC  |

Fee 0.00150000 BTC (55.310 sat/B - 13.827 sat/WU - 2712 bytes) +0.00500000 BTC

4

The screenshot shows a Bitcoin transaction interface. At the top, the hash '1431198bef5645bcce667c11f988257292c...' and the date '2017-02-10 19:48' are visible. The transaction is divided into two columns of inputs and outputs. A red circle highlights the first input: '1FNhjTqbogGenAtiVn... 0.03000000 BTC'. Another red circle highlights the first output: '1FBov1eSTzbEWFhNP... 0.04811430 BTC'. A third red circle highlights the final output: '1FyJw1oF7ojJVfbM... 193.37661929 BTC'. At the bottom left, the fee is '0.00150000 BTC (55.310 sat/B - 13.827 sat/WU - 2712 bytes)'. At the bottom right, a green box shows '+0.00500000 BTC'. A green arrow points from the first input to the first output.

| Hash  | Amount       | Unit            |
|---|--------------|-----------------|
| 1431198bef5645bcce667c11f988257292c...      |              |                 |
| 1FNhjTqbogGenAtiVn...                       | 0.03000000   | BTC             |
| 1FNhjTqbogGenAtiVn...                       | 0.29980000   | BTC             |
| 1ChT8jHwnu28S8Gse...                        | 0.00552015   | BTC             |
| 134JTcD1rwYzf3mJh...                        | 0.01066365   | BTC             |
| 1F2DnSngMqhx3Bc5t...                        | 0.00102304   | BTC             |
| 1PmJouprMuWvnuz1...                         | 0.00060627   | BTC             |
| 1CNKsJdKEGafk7A6...                         | 0.02800000   | BTC             |
| 1Jv324ZskcMwVaHo...                         | 0.04971298   | BTC             |
| 1Jv324ZskcMwVaHo...                         | 0.02700664   | BTC             |
| 1FyJw1oF7ojJVfb...                          | 200.00000000 | BTC             |
| Load more inputs... (1 remaining)           |              |                 |
| 1FBov1eSTzbEWFhNP...                        | 0.04811430   | BTC             |
| 1FnJ7ifPVs6pVzPAHj...                       | 0.15385554   | BTC             |
| 1PLS2uFx9RCXj6y7o...                        | 0.03240000   | BTC             |
| 1JPDFdbpYu7ZMN54...                         | 0.11000000   | BTC             |
| 1Acehkhv2vRYE8JUJ...                        | 0.10000000   | BTC             |
| 125UVAGTHgRpUWu...                          | 5.00000000   | BTC             |
| 1LCy45fGKy5DDyLX7...                        | 0.19080000   | BTC             |
| 1JQAJC1as3zqGvh3R...                        | 0.10780000   | BTC             |
| 1uQWT55a31oXbG7y...                         | 0.06000000   | BTC             |
| 1AtG2dZL2QT9Anob...                         | 0.26000000   | BTC             |
| 19P2i6fCFLyhsZWVd...                        | 0.05476170   | BTC             |
| 1NAr6doa9jzdAtjfcED...                      | 0.00100000   | BTC             |
| 1GZjj8XvbdVvMgiSm...                        | 0.21500000   | BTC             |
| 32SRuobXXWbxRYeLt...                        | 0.11180000   | BTC             |
| 1DtnwrYpuj2AviHBKL...                       | 0.31386546   | BTC             |
| 1MXx5bDua8844zAiK...                        | 0.03416878   | BTC             |
| 1X9rcMVx8SvZ5uPz...                         | 0.00500000   | BTC             |
| 1Hxm69vGPXrGu7kB...                         | 0.01000000   | BTC             |
| 1CEoEkc1xzb5mBhpa...                        | 0.00547958   | BTC             |
| 3ErsNJgohjZ9DeJcz...                        | 0.56630000   | BTC             |
| 13sSQcEjasD7S5PZn...                        | 0.01185000   | BTC             |
| 17McVX1jhiEMg5Mnt...                        | 0.85516806   | BTC             |
| 1LHY6mAeqHVVYbpZ...                         | 0.37096600   | BTC             |
| 15Gw27cNPkqgUxqe...                         | 0.26954988   | BTC             |
| 15wgdri64ZuV8QY...                          | 0.26955280   | BTC             |
| 1KbB2KsEV2wUkAAx...                         | 0.10780000   | BTC             |
| 1Bjkr17q2TF37nvTdC...                       | 1.00000000   | BTC             |
| 16zFtGxAF7RWNpZAY...                        | 0.10712284   | BTC             |
| 14giYwDXJLUM3P7i...                         | 0.04280000   | BTC             |
| 1FyJw1oF7ojJVfbM...                         | 193.37661929 | BTC             |
| Fee   | 0.00150000   | BTC             |
| (55.310 sat/B - 13.827 sat/WU - 2712 bytes) |              |                 |
|   |              | +0.00500000 BTC |

The exchange do not write on-chain transaction for each custom activity, but instead factorize them.

It reduces individual transaction fees.

Same for inputs.

Note the change address with a large amount

5

# Sending back **0.001** from Wallet to Paymium Exchange

Address I received payment to


Address provided by Paymium





|      |  |   |
|------|--|---|
| Hash | 40a08e1ff76d8133c151705f816bec87c75a8d7dd0957b4bd1ecd...         | 2017-02-11 07:56  |
|      | <a href="#">1X9rcMVx8SvZ5uPzpjaaPn6psXkw5LZhB</a> 0.00500000 BTC | <a href="#">1NdhZ1TBi1dE8uk1qzUqYR2x7dRi52j5wr</a> 0.00100000 BTC |
|      | <a href="#">1ArvJf54cVwJ2Y6gH6nic63ofQeiN32jbf</a>               | 0.00380700 BTC  |
| Fee  | 0.00019300 BTC<br>(85.778 sat/B - 21.444 sat/WU - 225 bytes)     | 0.00480700 BTC  |

High fees:  
20% of the amount sent

Change  
(My address in my wallet)

















# What happens with coins sent at this address?

Hash `40a08e1ff56d8133c151705f816bec87c75a8d7dd0957b4bd1ecd...`  2017-02-11 07:56

`1X9rcMVx8SvZ5uPzpjaaPn6psXkw5LZhB` 0.00500000 BTC   `1NdhZ1TBi1dE8uk1qzUqYR2x7dRi52j5wr` 0.00100000 BTC   
`1ArvJf54cVwJ2Y6gH6nic63ofQeiN32jbf` 0.00380700 BTC 

Fee 0.00019300 BTC  
(85.778 sat/B - 21.444 sat/WU - 225 bytes) 0.00480700 BTC

Hash `59c821350e1291c55ae8e0286b05e3627...` 2017-02-11 14:09

`1HsSSUvaMuL3VUw...` 0.72080588 BTC   `1544JSQRTLCKfhJ1E...` 0.05040000 BTC   
`1NdhZ1TBi1dE8uk1qz...` 0.00100000 BTC  `1HzGDkZN7fe4rAmW...` 0.04910000 BTC   
`1KM3b551HzSQ4MQ...` 0.00951400 BTC  `128DsHfMjaeCDunze...` 0.44900000 BTC   
`1HUxJ5kTqLNhuMZy...` 0.45732080 BTC  `1NCe8eAhHzyZPneYh...` 0.11000000 BTC   
`1BoBVfPfk3BxaN1M1...` 0.03900991 BTC  `1CjcXagRZviJwWSH...` 0.06900000 BTC   
`1MgQhKRk4QqMTgeY...` 0.01447889 BTC  `1A4wdSpiToSc3rw1G...` 2.30000000 BTC   
`1FyJw1oF7ojJVfbM...` 193.18850960 BTC  `19DBZUM62sYv66up...` 0.05344623 BTC   
`1PKmMMR7S26Usjrkj...` 0.34257068 BTC   
`17puCgUUALRV222V...` 2.09300000 BTC   
`1HoEKSQfmCebgcKo...` 0.04000000 BTC 

[Load more outputs... \(19 remaining\)](#)

Fee 0.00150000 BTC  
(72.886 sat/B - 18.222 sat/WU - 2058 bytes) -0.00100000 BTC

“My” coins have been spent the same day, and not by me!  
=> 1Ndh... Is not “my” address, it’s paymium’s address.  
It’s just that when coins are sent to this address, Paymium *credit* my customer account of the same amount.

6

# Using my wallet coins to buy some real things (Amazon gift card)

Hash: 40a08e1ff56d8133c151705f816bec87c75a8d7dd0957b4bd1ecd... 2017-02-11 07:56

1X9rcMVx8SvZ5uPzpjaaPn6psXkw5LZhB 0.00500000 BTC → 1NdhZ1Tbi1dE8uk1qzUqYR2x7dRi52j5wr 0.00100000 BTC  
1ArvJf54cVwJ2Y6gH6nic63ofQeiN32jbf 0.00380700 BTC

Fee: 0.00019300 BTC (85.778 sat/B - 21.444 sat/WU - 225 bytes) 0.00480700 BTC

Hash: 1650dd5cd9233705193aa83e42d8460d... 2021-01-27 23:16

1ArvJf54cVwJ2Y6gH... 0.00380700 BTC → bc1qcp8uuxkx48ylrg... 0.00060200 BTC  
3JnJU19y21FgySKoX... 0.00300300 BTC

Fee: 0.00020200 BTC (91.403 sat/B - 22.851 sat/WU - 221 bytes) -0.00380700 BTC

Company selling gift card

Hash: 7578596ecc510bb93d662d97d8bf6c8b7... 2021-01-28 05:08

3PXW8ghgJuC4J5y1... 0.00438600 BTC → bc1qj4zp28m9r3elw5... 7.00529441 BTC  
3Q2xe5JyvuL5mvxn... 0.01404900 BTC  
38LwzsRkxqXe3jfSD... 0.00806700 BTC  
3C8i2YX1EWurpK9qt... 0.00318400 BTC  
34Z85bRMu4jE5mRm... 0.00212500 BTC  
35zcYgpERQo9SUUo... 0.01549100 BTC  
3GZ2PMcvphAiYdA2... 0.00325000 BTC  
349AFe7DdK4bfJZ7R... 0.00212600 BTC  
3N3W124kvbjPQ89u... 0.02365300 BTC  
32dkoFUb5bh9ECPG... 0.00314300 BTC

Load more inputs... (776 remaining)

Fee: 0.00163316 BTC (1.211 sat/B - 0.571 sat/WU - 134825 bytes) -0.00300300 BTC



SOME ADDITIONAL TOPICS...

# LAYER 2

- Cryptocurrencies allow to transmit a “script”, coding the transaction itself, but not only (stored forever...)
  - ▶ The script can be as simple as a text message
    - Several love letters stored in the blockchain...
  - ▶ A dataset
    - Some Wikileaks data stored on the blockchain
  - ▶ A source code
    - The code to read the Wikileaks data for instance...
  - ▶ A picture
    - And what if it is some illegal e.g., child pornography ?
  - ▶ Executable code

# LAYER 2: TOKENS

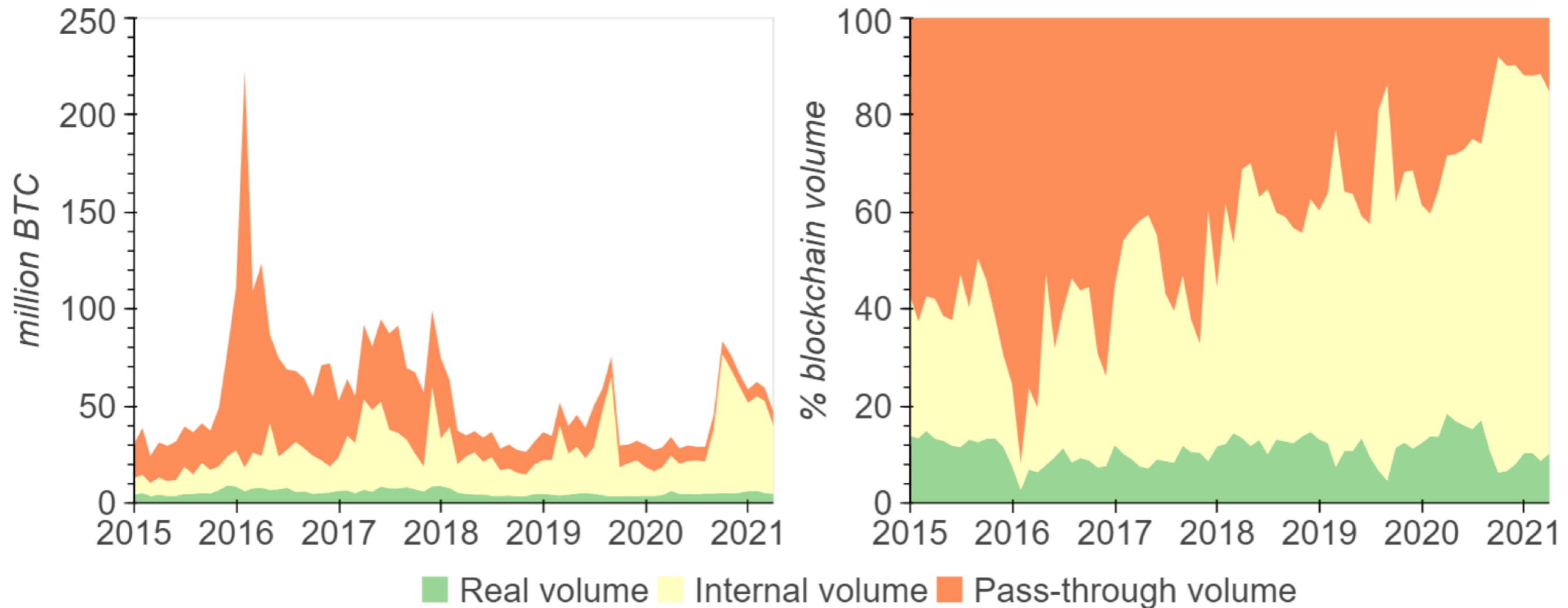
- Tether (stablecoin) is a *token*, a currency existing in the layer 2 of a blockchain
  - ▶ As ERC-20 in Ether
  - ▶ On bitcoin too
- Blockchain Bitcoin: Omni-layer allows to create L2 tokens
  - ▶ But a “hack” of the original system. Bitcoin not thought for that.
  - ▶ (Unlike Ether)
- Another L2 possibility on Bitcoin: Lightning network

# WRAPPED BITCOIN

- There is an ERC-20... corresponding to Bitcoin.
- A stable coin with parity fixed to Bitcoin.
- Same mechanism as Tether
  - But possible to check in the Bitcoin Blockchain that the backing reserve exists.
- Allows to exchange Bitcoin against other ERC20 inside Ether (DeFi...)
  - Bitcoin supposed to play the role of gold in the digital economy, being the most stable, reliable as a currency...

# EXAMPLES OF ANALYSIS

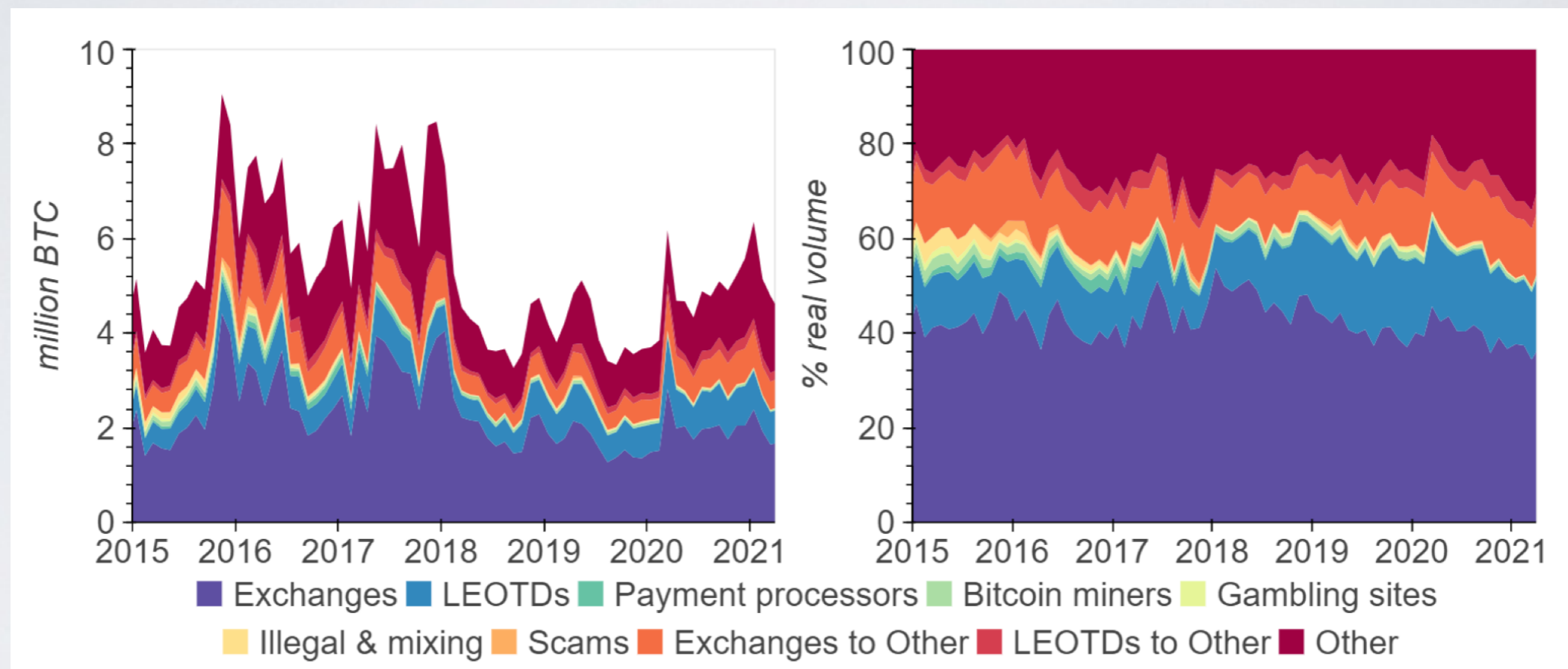
# ANALYSIS OF USAGES



pass-through=peeling chain=false transactions

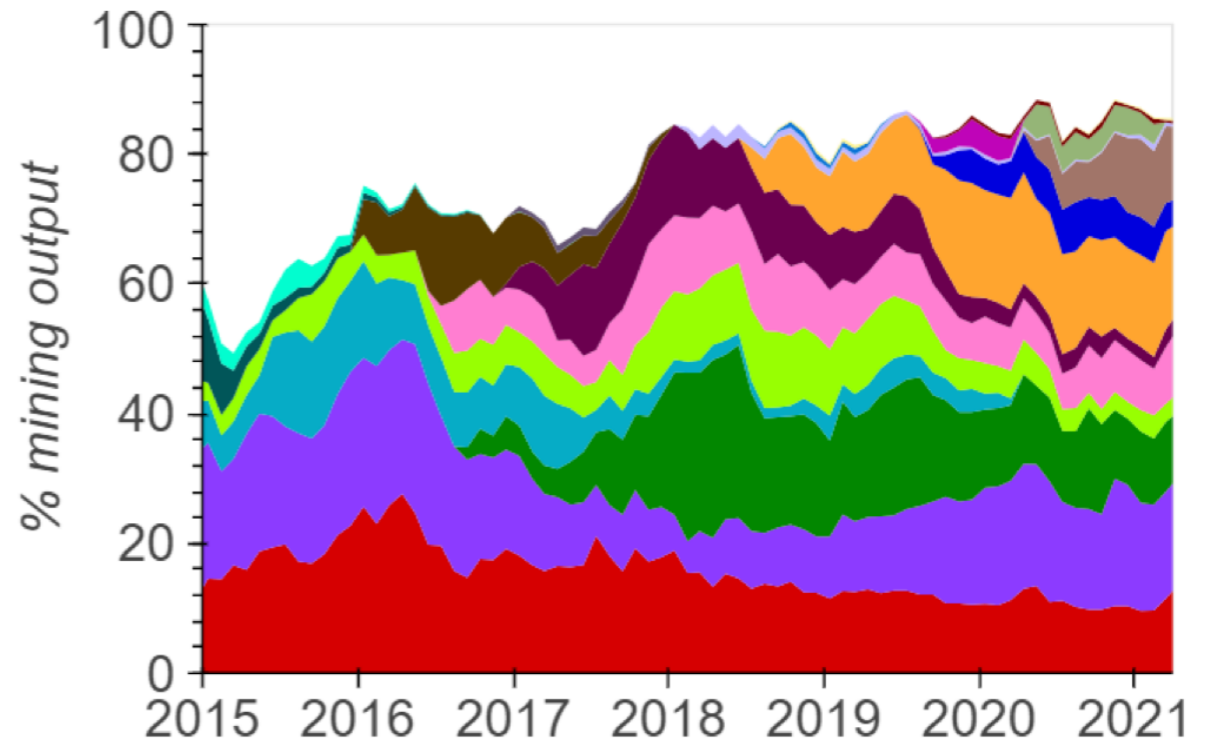
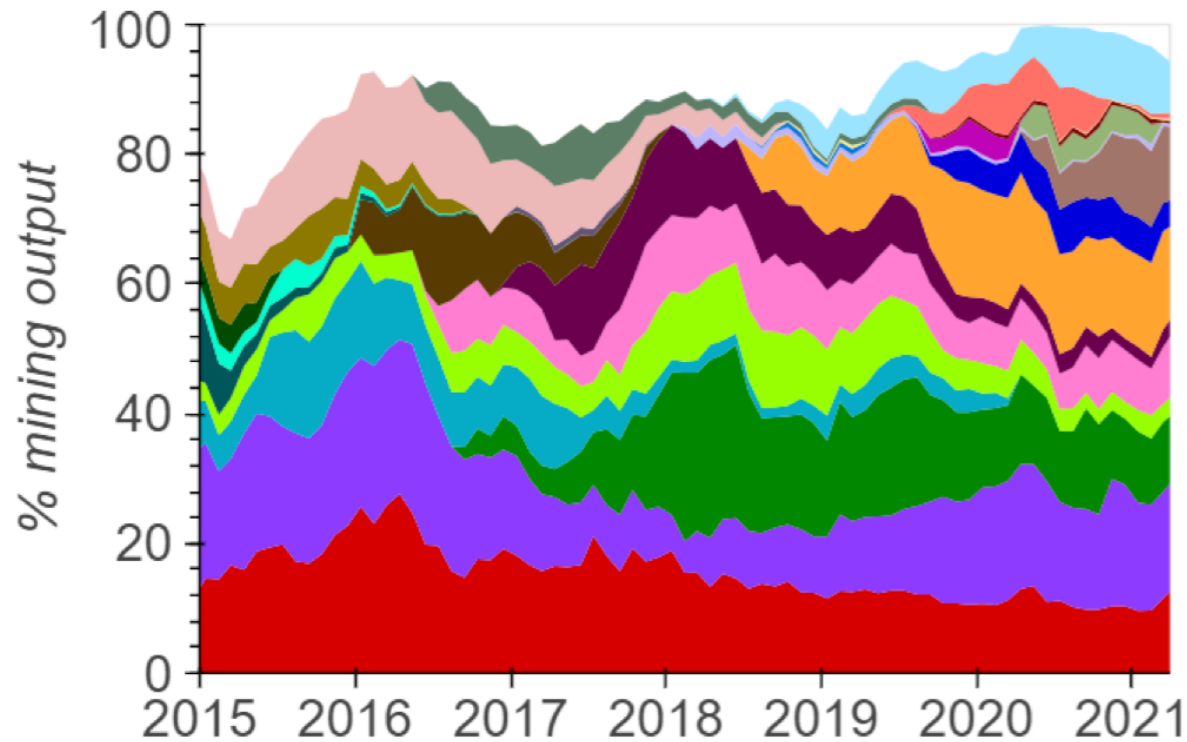
[https://www.nber.org/system/files/working\\_papers/w29396/w29396.pdf](https://www.nber.org/system/files/working_papers/w29396/w29396.pdf)

# ANALYSIS OF USAGES



[https://www.nber.org/system/files/working\\_papers/w29396/w29396.pdf](https://www.nber.org/system/files/working_papers/w29396/w29396.pdf)

# ANALYSIS OF USAGES

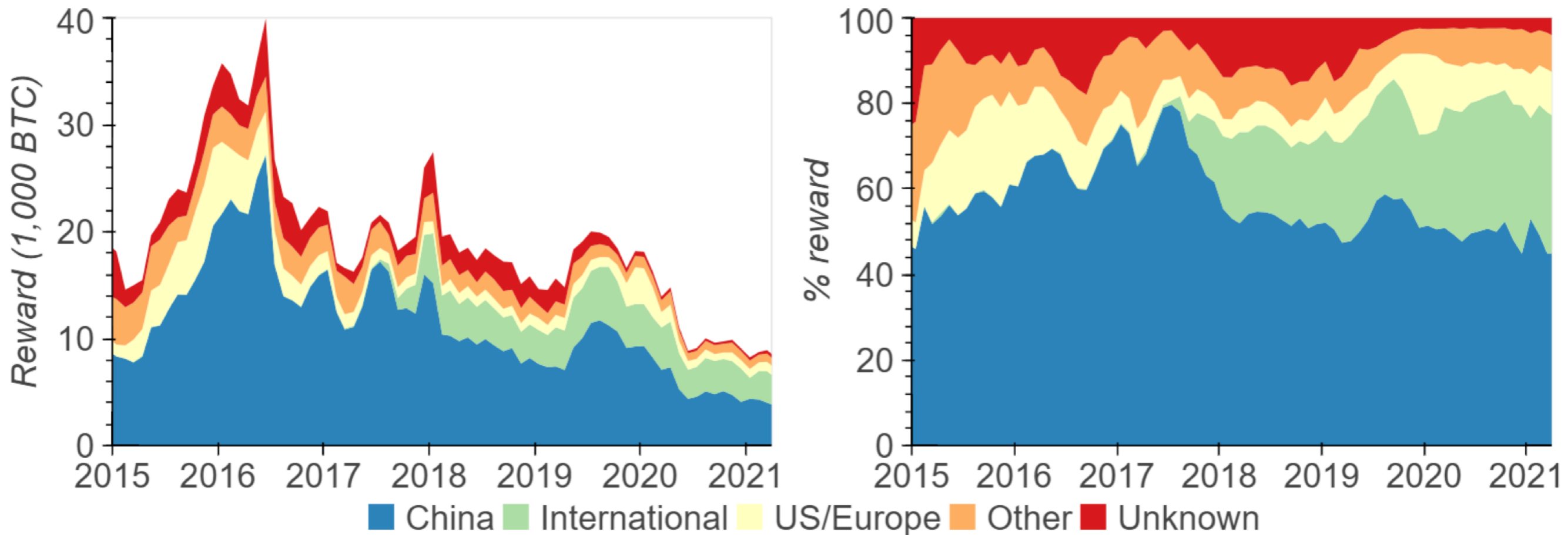


AntPool F2Pool BTC.com BitFury SlushPool ViaBTC BTC.TOP Poolin BWPool GHash.IO  
1THash Eligius Binance Pool WAYI.CN Lubian.com BytePool BATPOOL SpiderPool  
tigerpool.net Sigmoidpool.com BTC Guild KnCMiner OKExPool BTCC Bixin Huobi Pool

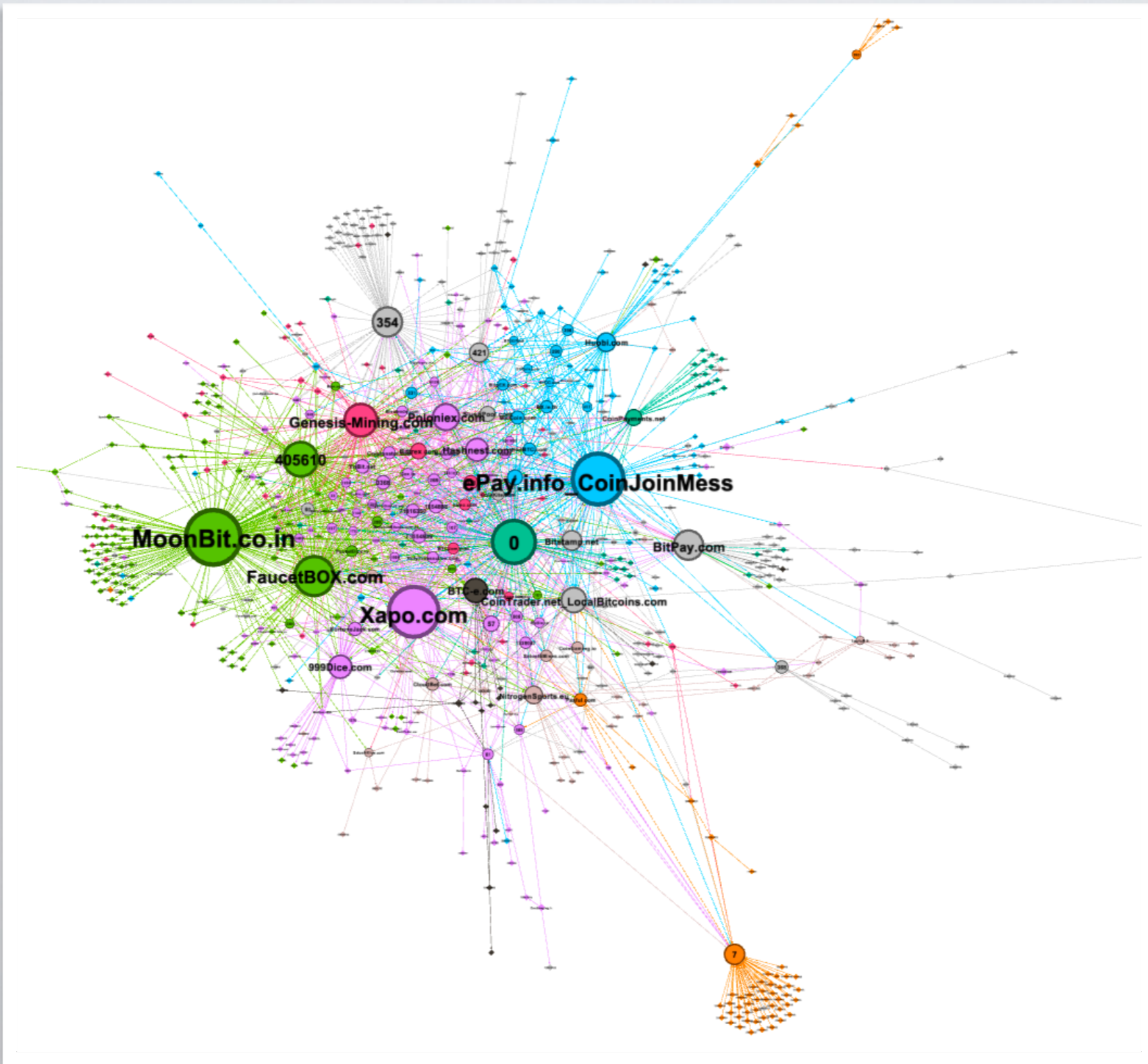
[https://www.nber.org/system/files/working\\_papers/w29396/w29396.pdf](https://www.nber.org/system/files/working_papers/w29396/w29396.pdf)

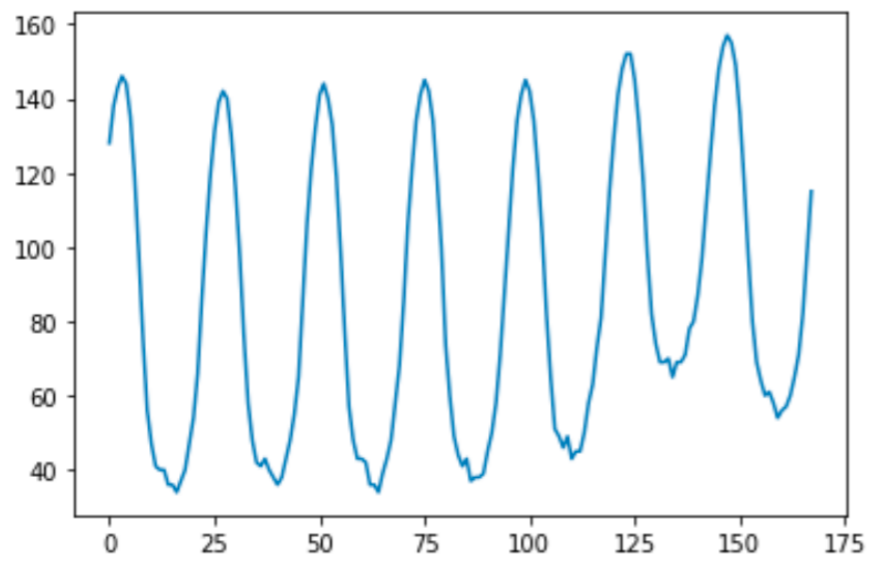


# POOL LOCATION

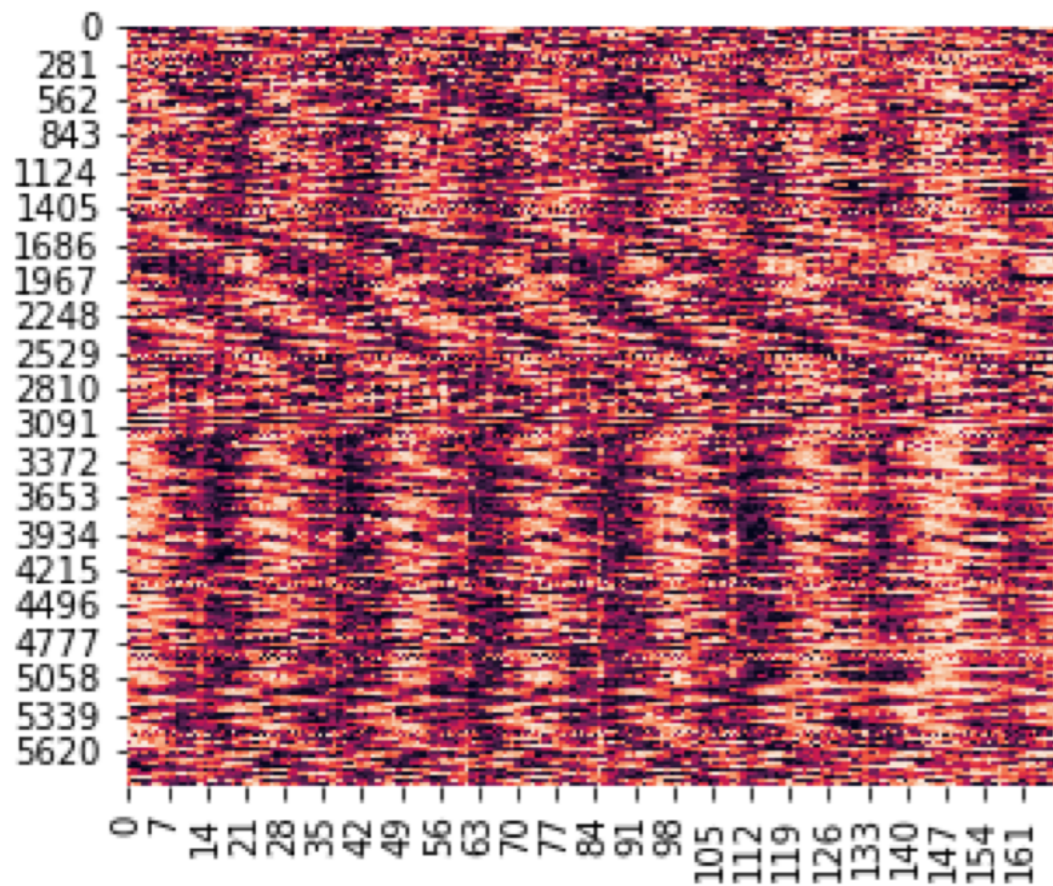


[https://www.nber.org/system/files/working\\_papers/w29396/w29396.pdf](https://www.nber.org/system/files/working_papers/w29396/w29396.pdf)

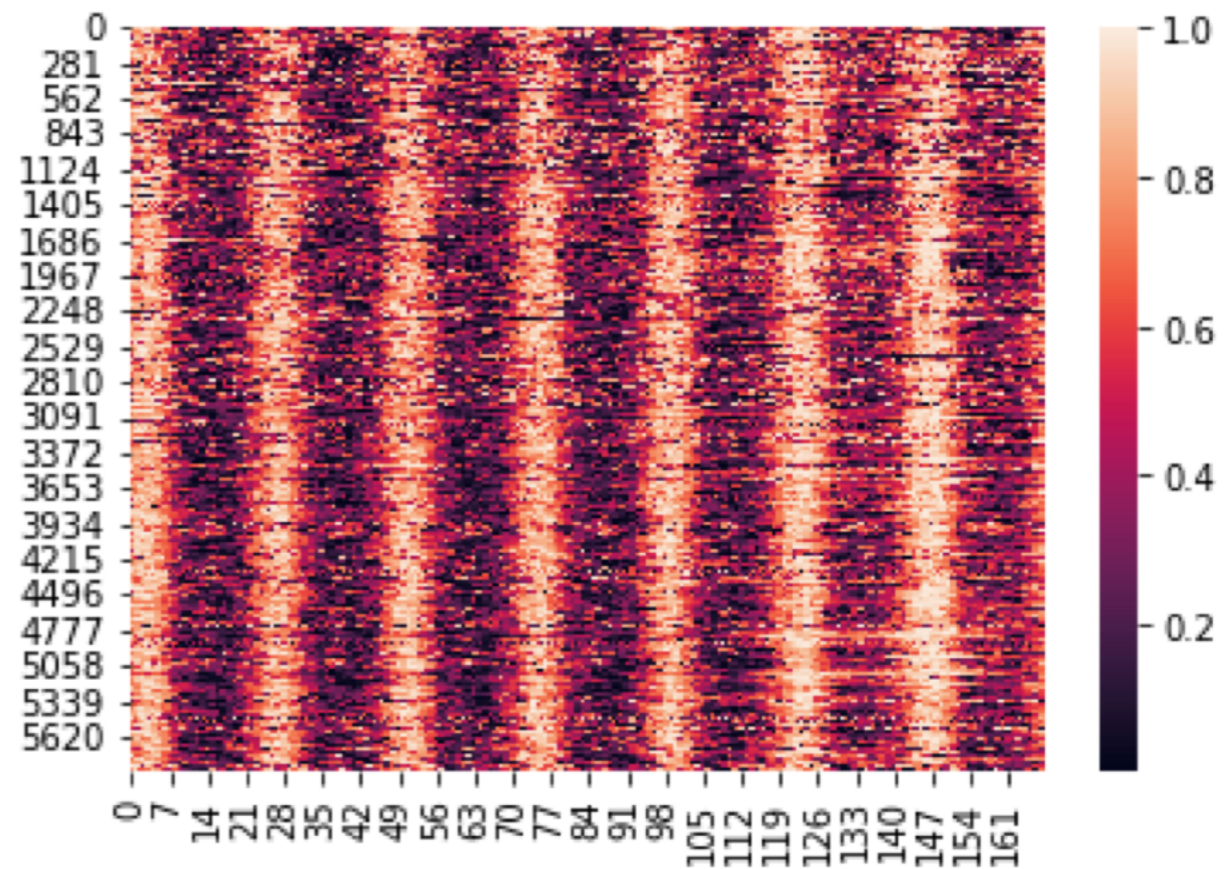




Weekly pattern of one entity

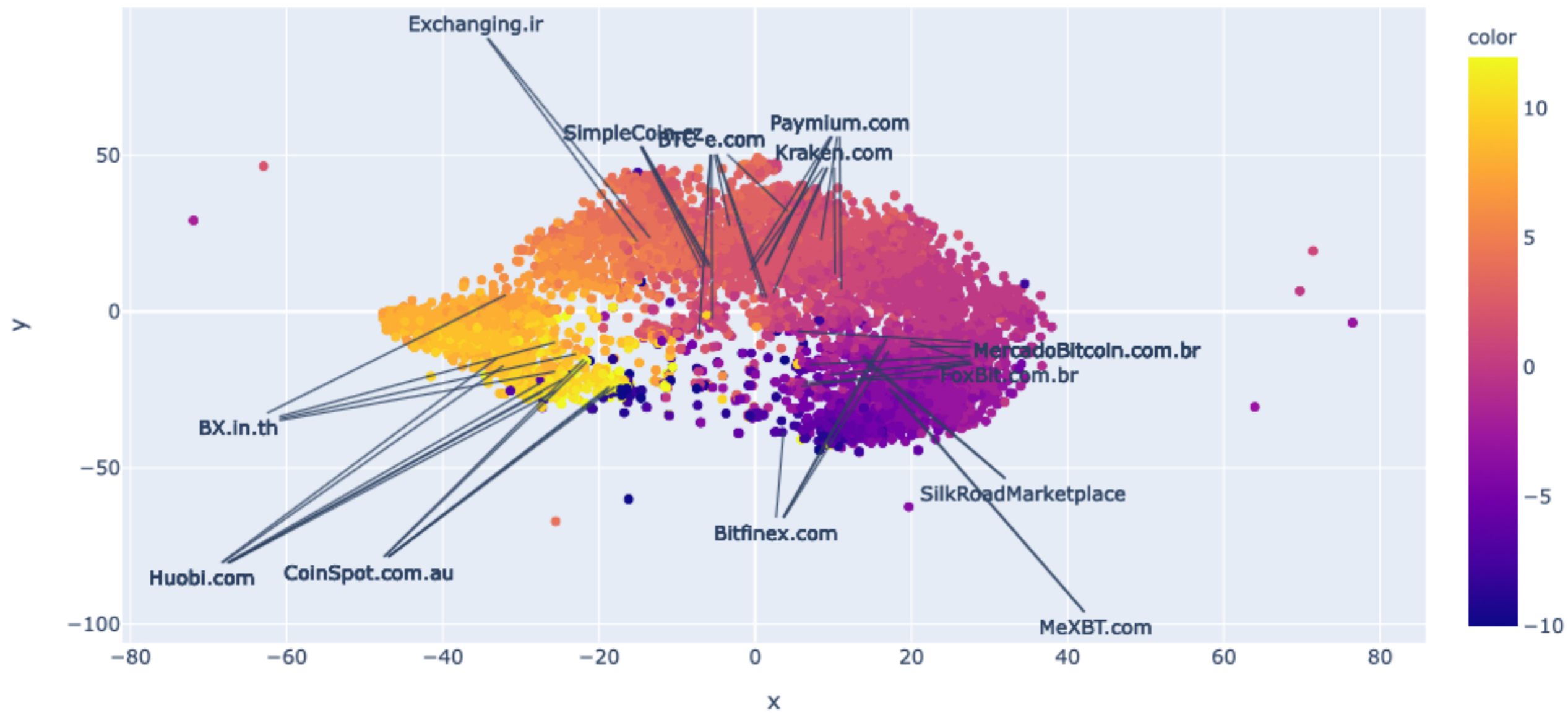


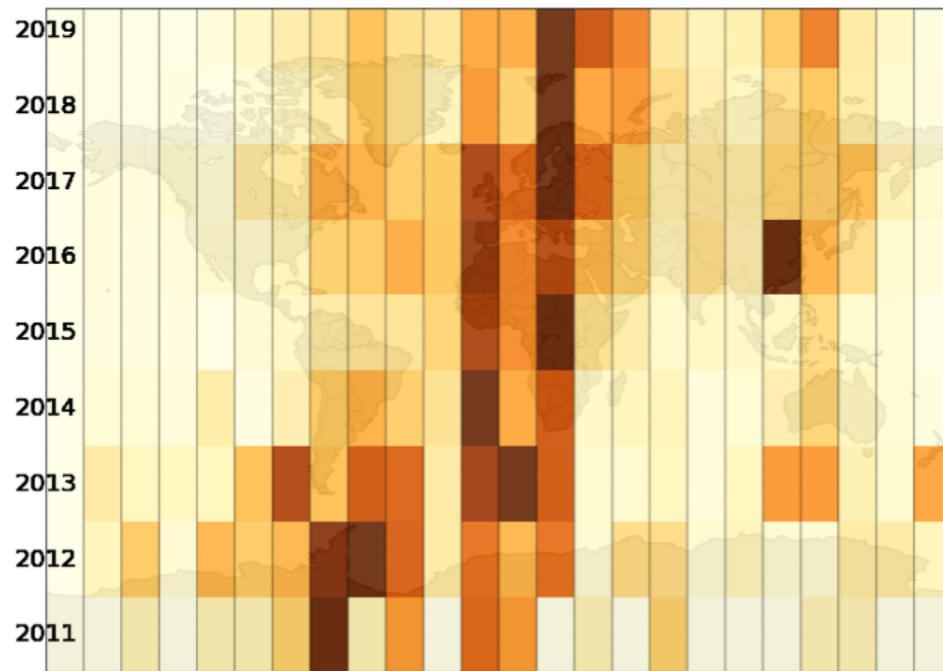
(a) Normalized patterns,  
before alignment



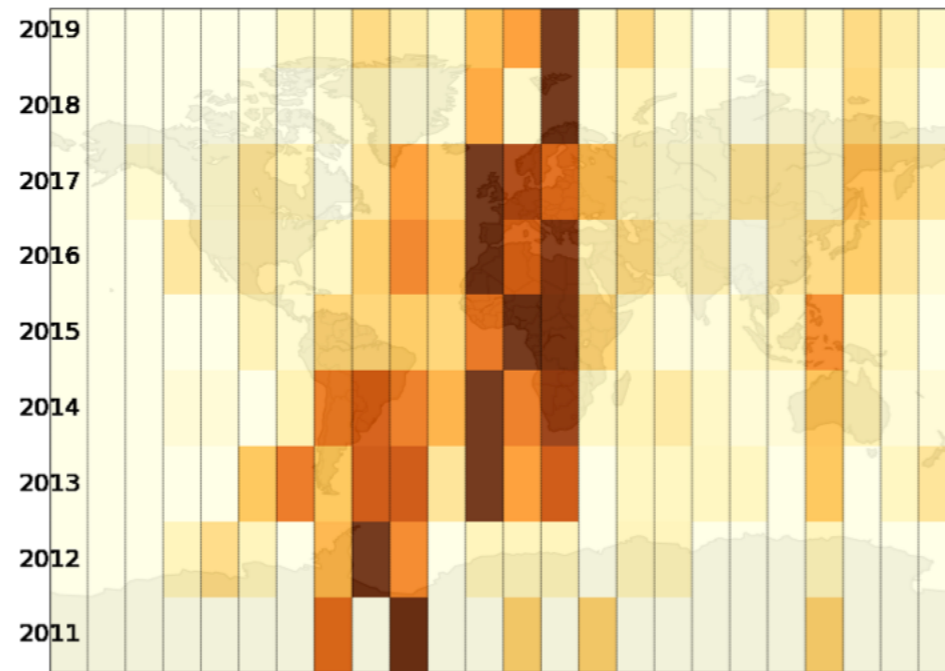
(b) Normalized patterns,  
after alignment

| Entity                | Expected Country | Approx. Time Zone | Avg. Estimated Shift |
|-----------------------|------------------|-------------------|----------------------|
| MeXBT.com             | Mexico           | GMT-6             | -4.00                |
| MercadoBitcoin.com.br | Brazil           | GMT-3             | -2.12                |
| FoxBit.com.br         | Brazil           | GMT-3             | -1.50                |
| Paymium.com           | France           | GMT+2             | +1.80                |
| SimpleCoin.com.cz     | Czech Republic   | GMT+2             | +2.00                |
| BTC-e.com             | Russia           | GMT+3             | +3.00                |
| Exchanging.ir         | Iran             | GMT+3:30          | +4.50                |
| BX.in.th              | Thailand         | UTC+07            | +8.75                |
| Huobi.com             | China            | GMT+08            | +9.67                |
| CoinSpot.com.au       | Australia        | GMT+8/GMT+10      | +11.40               |
| Bitfinex.com          | Unknown          | Unknown           | -3.50                |
| SilkRoadMarketPlace   | Unknown          | Unknown           | -3.00                |

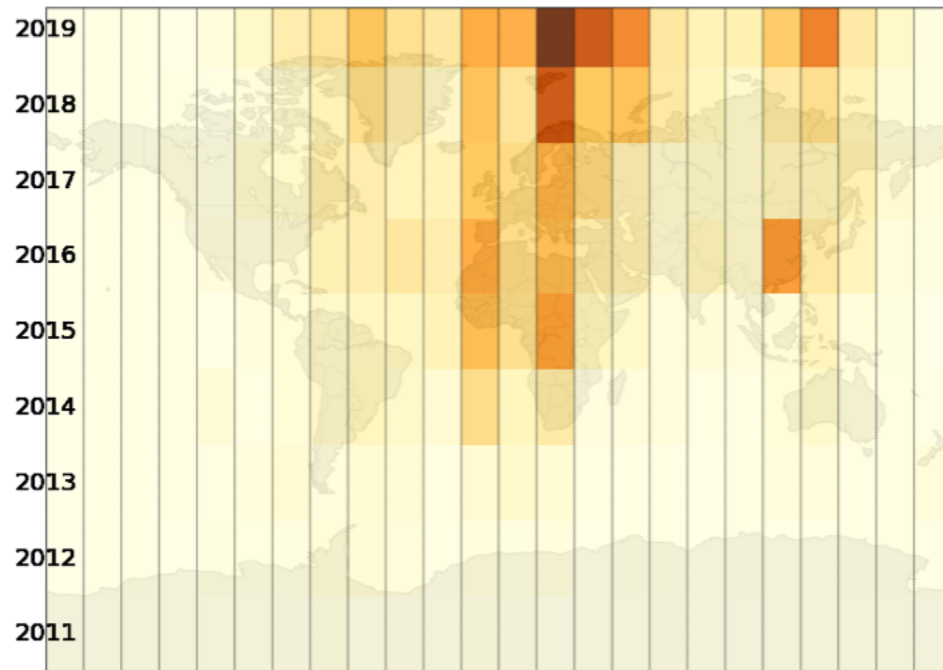




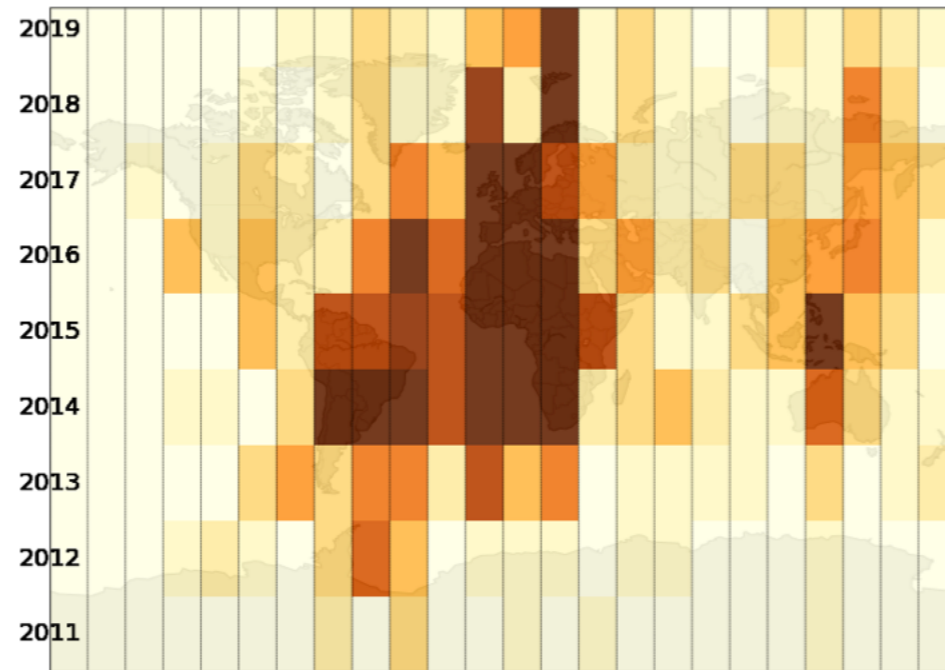
(a) All FR, yearly normalization



(b) WalletExplorer only, yearly normalization



(c) All FR, global normalization



(d) WalletExplorer only, global normalization