A General Introduction to

Bitcoin

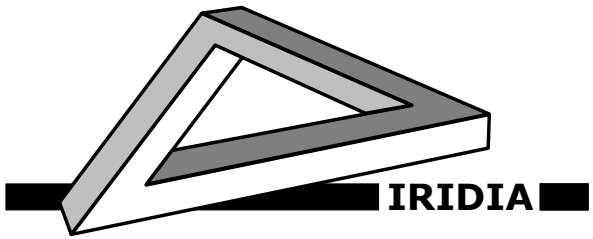
Jérémie Dubois-Lacoste – Arne Brutschy

jeremie|arne@bitcoinassociation.be

Université Catholique de Louvain (UCL) 12/05/2015

About us

- Post-doc researchers in Computer Science (AI lab of ULB)
- Founders & Organizers of “Bitcoin Brussels” meetup group (260 members)
- Founders & Directors of ASBL/VZW “Belgian Bitcoin Association”
- Involved in several Bitcoin projects since 2012



Institut de Recherches Interdisciplinaires
et de Développements en Intelligence Artificielle

About the BBA

Our mission:

- Support, education and promotion
- Representing Bitcoin in Belgium and beyond
- Providing clarity and understanding
- Local point of contact (Bitcoin has none!) for the representatives of the media, government, and industry

Disclaimer

- We own some bitcoins
- Bitcoin should (still) be seen as an experiment
- We're geeks and computer scientists, neither economists nor cryptographers

Outline

Outline

Electronic cash

Basic problem

How to exchange money over an untrusted network with people you don't trust?

- Money based on cryptography: an old cypherpunk ideal

Centralized electronic cash

- is easy – even Blizzard did it in World of Warcraft ;)
- . . . but you have to trust the central authority
- not different that “normal” money

. . . and **Decentralized** electronic cash?

Very difficult problems to solve:

- How to prevent to create money by forgery?
- How to prevent spending money twice (*double-spending*)?
- How to prevent spending money by others?
- How to handle money creation and emittance?

Outline

The cypherpunk movement

- Human right to use cryptography for personal empowerment and fight its usage prohibition (example: cryptography considered weapon by USA)
- Personal privacy, security and liberty by use of cryptographic tools
- Widespread usage of cryptography as a mean for social and political change

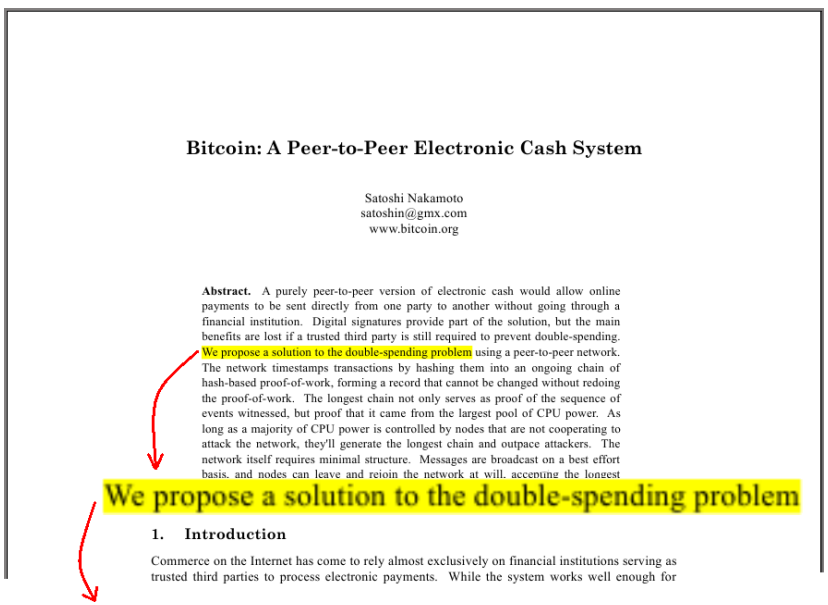
Apparition of Bitcoin

- **betabucks etc** (early ’90, Chaum/Brands)
- **hashcash** (1997, Adam Back)
- **b-money** (1999, Wei Dai)
- **bitgold** (2005, Nick Szabo)

Main issue with these attempts: requires a trusted, central third-party to avoid “double-spending”

The Tour de Force of "Satoshi Nakamoto"

Scientific Article (November 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

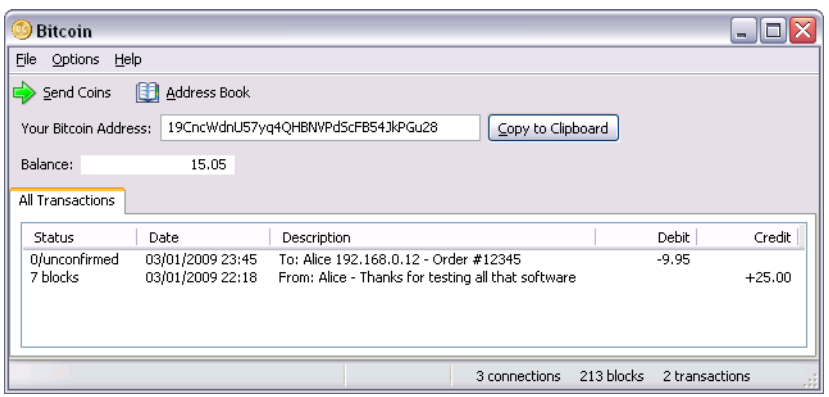
We propose a solution to the double-spending problem

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

Introduce the idea of the *blockchain*

Implementation (January 2009)



Outline

What is Bitcoin? (1/3)

Formal Answer

- **Bitcoin**: Information exchange protocol (like http, smtp...), that allows the transfer of units of account; these units behave like the money we are used to.
  - Durability
  - Portability
  - Fungibility
  - Divisibility
  - Relative scarcity

- **bitcoin(s)**: name of the unit of account circulating on the Bitcoin network

What is Bitcoin? (2/3)

Informal Answer - Micro Scale

A system for people to send and receive payments

- Without depending on any third-party
- Reasonably privately
- Instantly
- Reliably
- Typical transaction fee today: zero or 0.03€

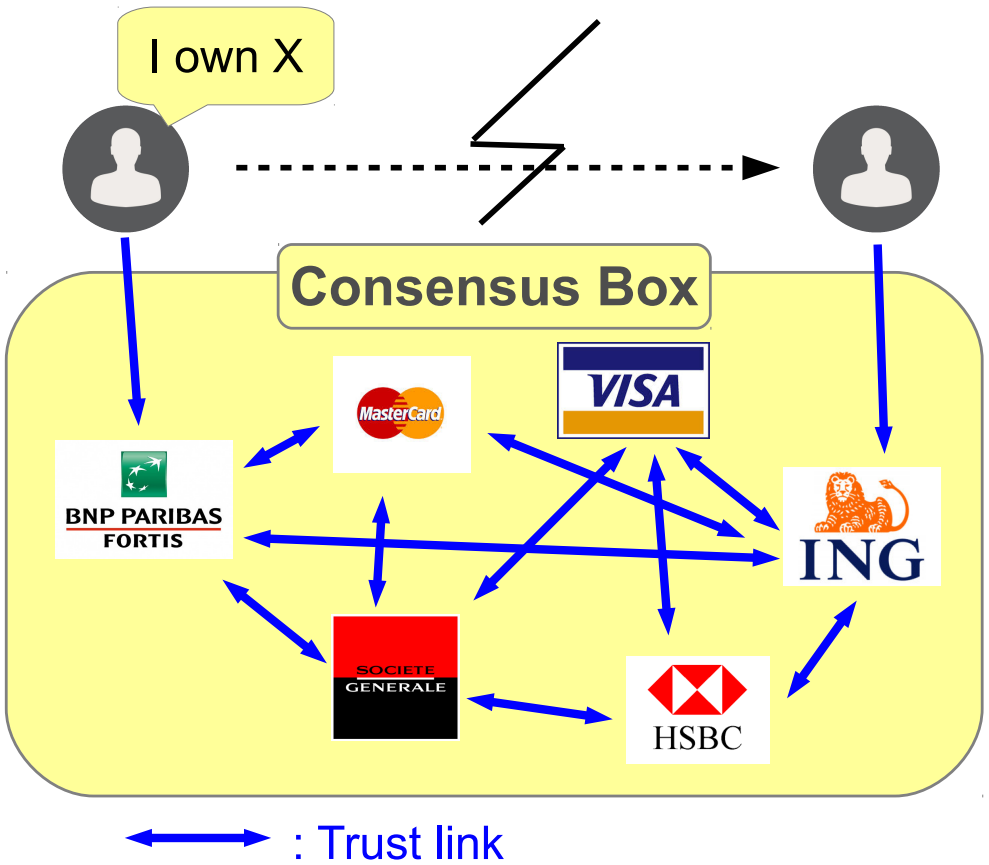
What is Bitcoin? (3/3)

Informal Answer - Macro Scale

- Money supply policy governed by maths; known in advance
- Without borders
- Distributed
- Open source software; community developed

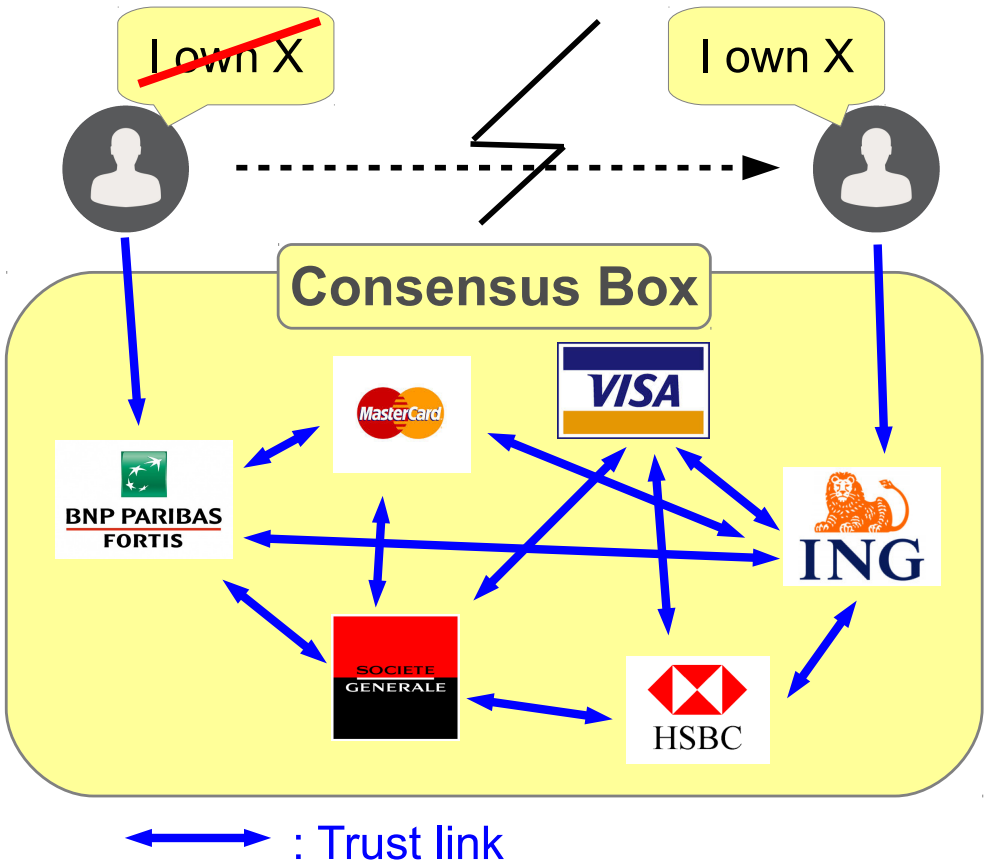
Core innovation of Bitcoin?

In the “usual” world



Core innovation of Bitcoin?

In the “usual” world



Core innovation of Bitcoin?

In the “usual” world

- *Trusted* third parties are “keeping the books”
- *Centralized* consensus

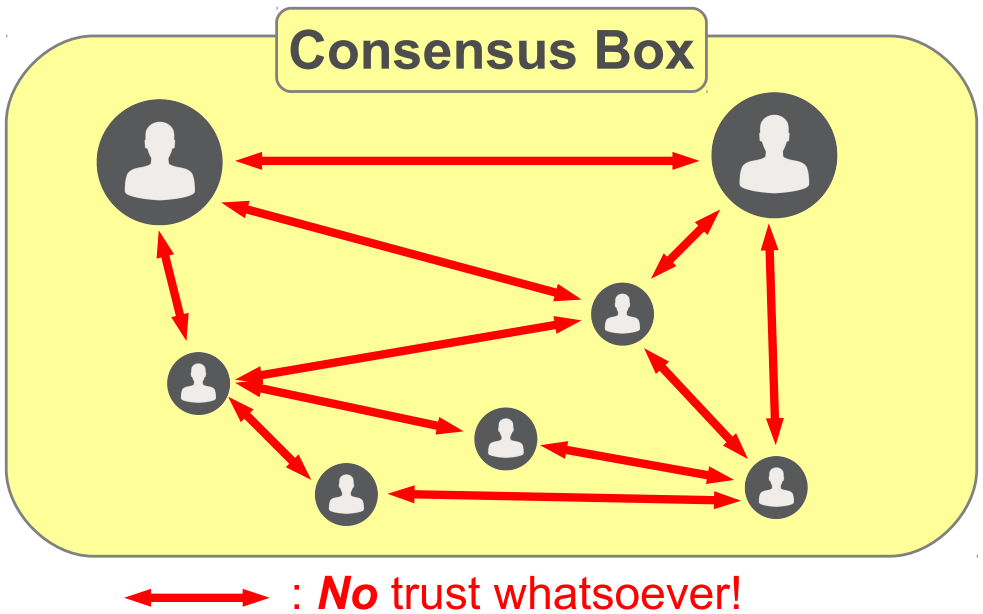
Core innovation of Bitcoin?

In Bitcoin world

 : ***No*** trust whatsoever!

Core innovation of Bitcoin?

In Bitcoin world



Core innovation of Bitcoin?

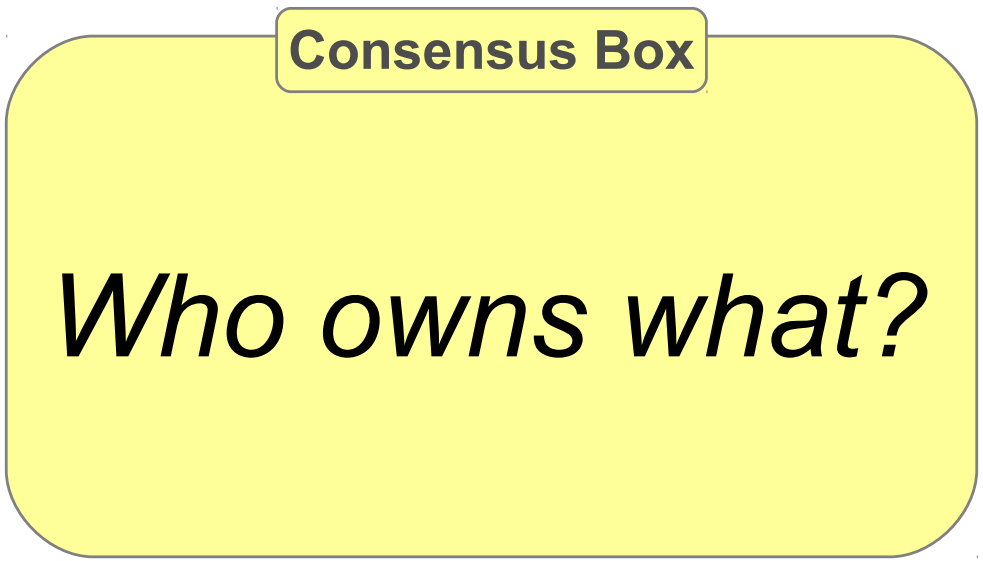
In Bitcoin world

- No trusted parties, “keeping the books” is done collectively *without* trust
- *Decentralized* consensus
- The mechanism to allow that is called the *blockchain*

Core innovation of Bitcoin?

In Bitcoin world

Remark: Bitcoin uses decentralized consensus to determine ownership.



Much more can be done (outside the scope of this lecture...)

Outline

Addresses and keys

- Assymetric ECDSA cryptography (public/private key pair)
- Bitcoins exchanged between *addresses*:

`19KFPnuEMbbTdh4MaVDLUJhTUjyHbPMxeF` =

  - Everybody can see the amount associated to an address

- Only owners of corresponding *private key* can spend them

Addresses in details

- Address is (basically) hash of private key with check sum
  - X = VERSION_BYTE + RIPEMD160(SHA256(pubkey))
  - Y = last-4-bytes(SHA256(SHA256(X)))
  - Z = X + Y
  - Address = Base58(Z)

Private keys can be stored...

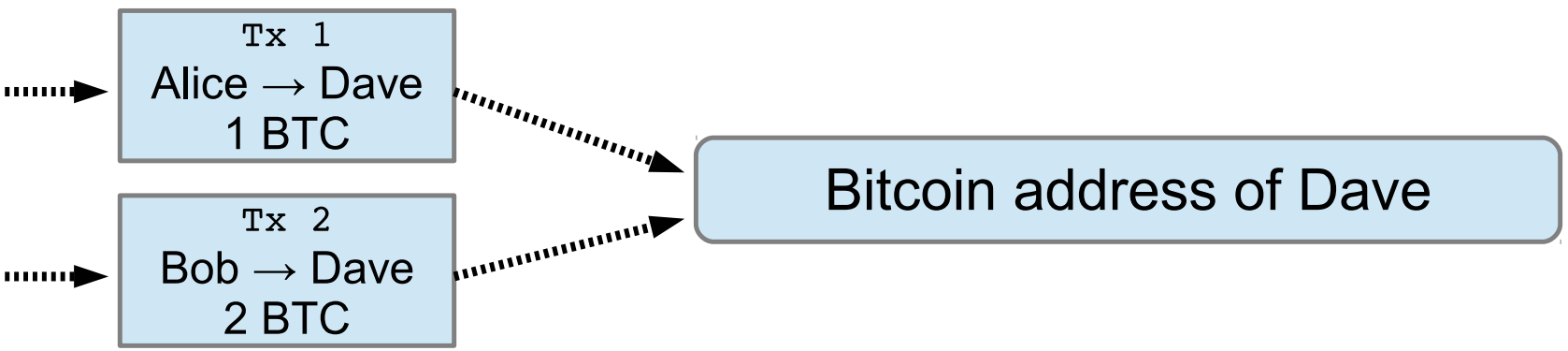
- On a computer
- On a USB stick, a DVD-Rom
- Printed or written on paper
- Only in your memory: “brain-wallet”
- On a specific device
- In poetry
- etc.

Outline

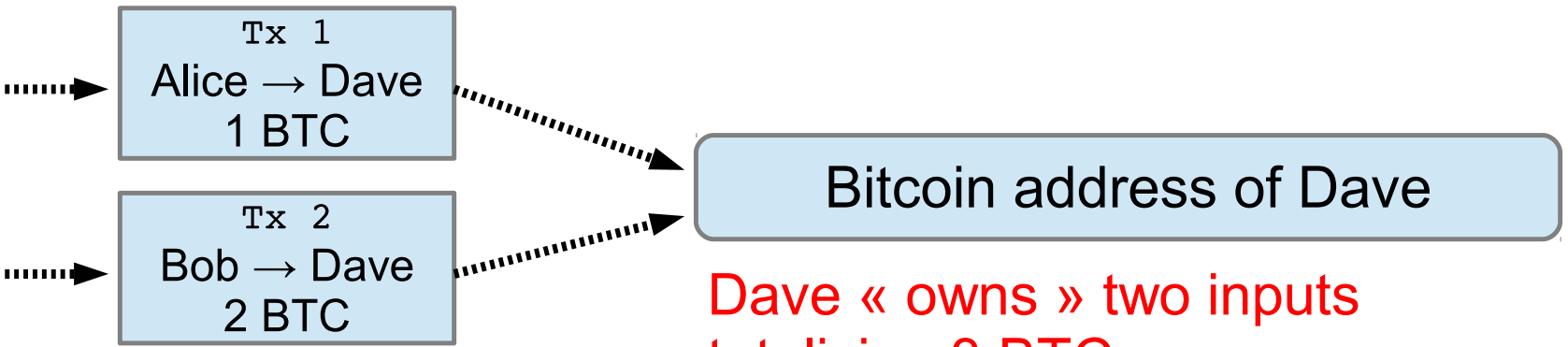
Transactions principle

- They spend old *inputs* previously received
- They create new *outputs*
- New outputs will become inputs of future transactions
- An input can only be spent **entirely**

Example

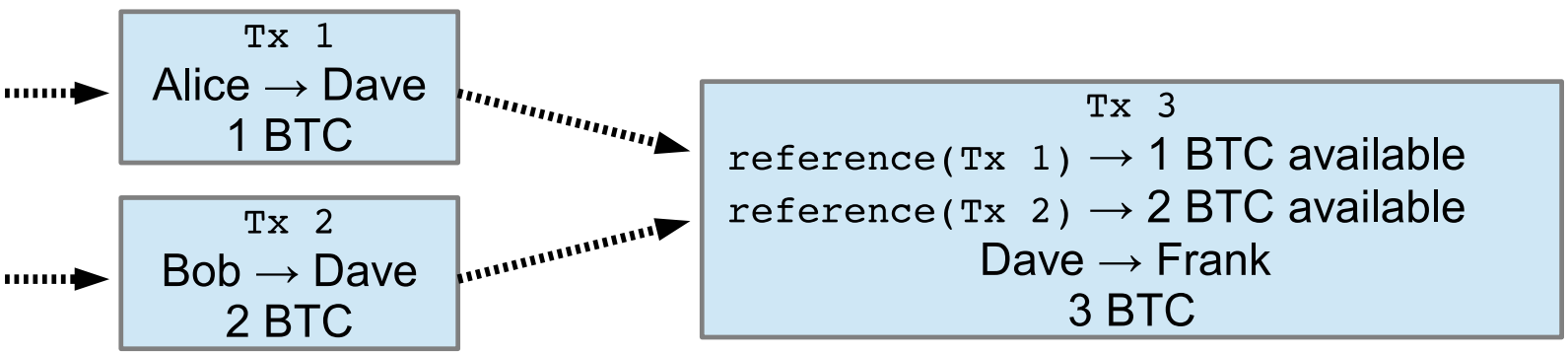

Tx 1
Alice → Dave
1 BTC
Tx 2
Bob → Dave
2 BTC
Bitcoin address of Dave

Dave received 3 BTC via 2 transactions

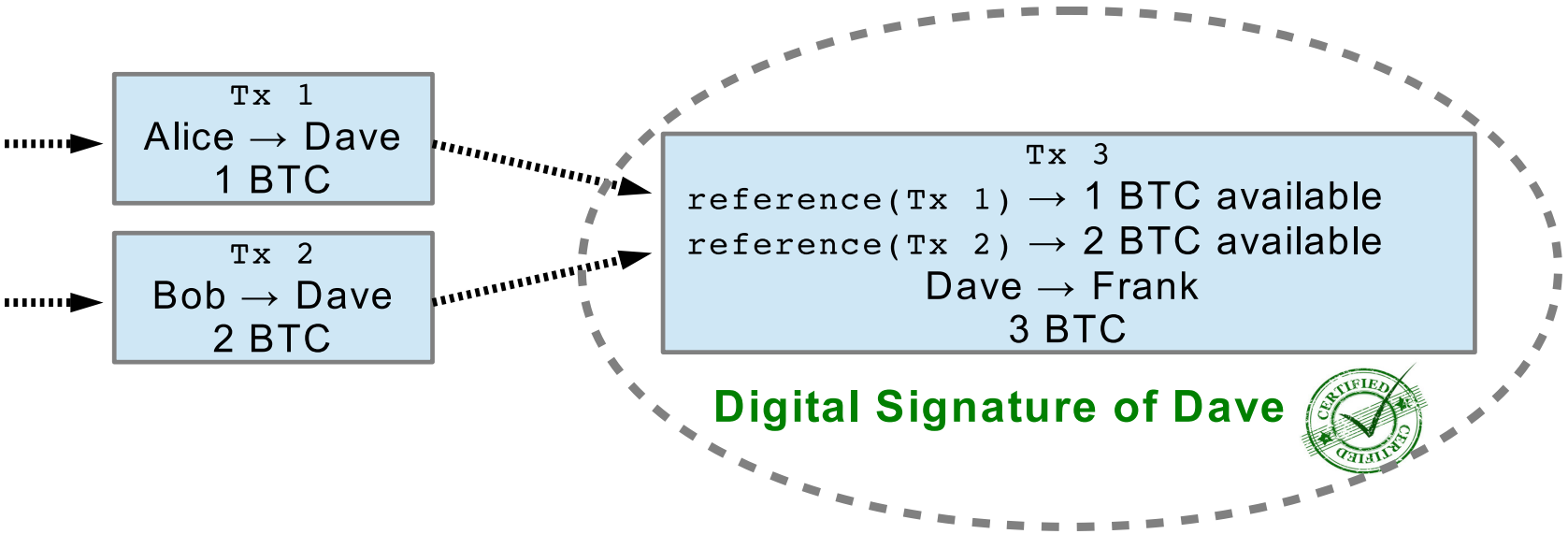


Dave « owns » two inputs totalizing 3 BTC

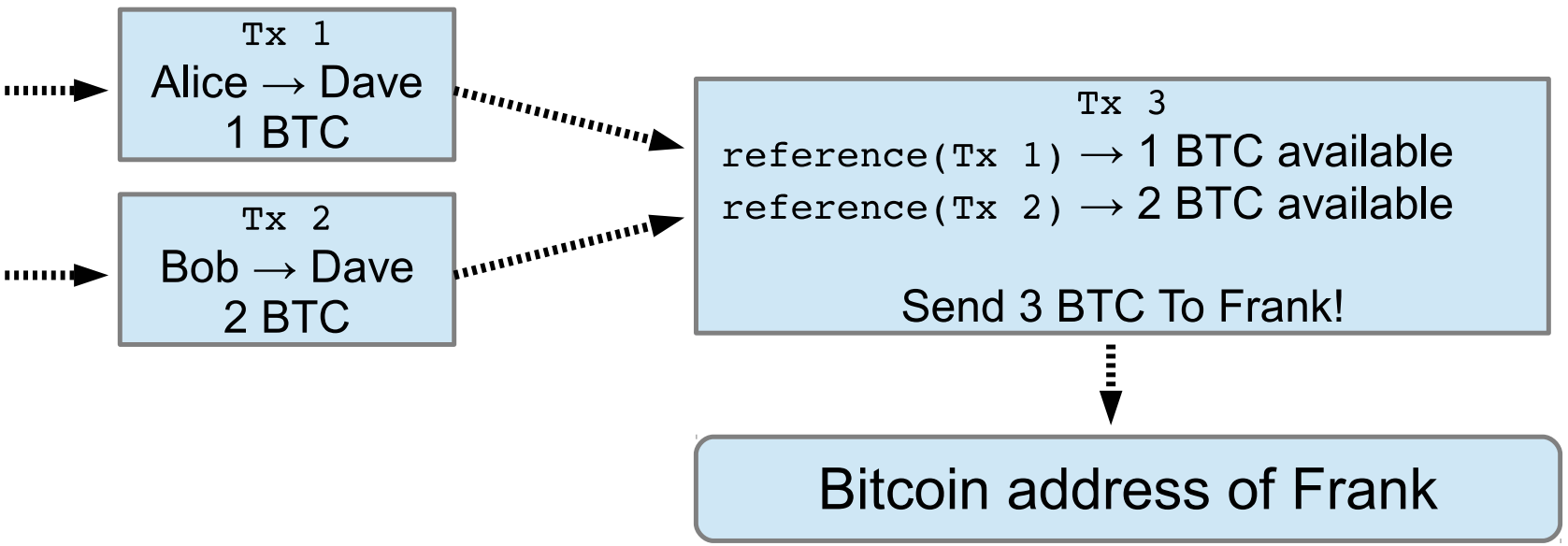
Dave wants to send 3 BTC to Frank



Dave wants to send 3 BTC to Frank



Once the transaction is confirmed



Frank « owns » one input totalizing 3 BTC (and Dave, 0)

How to do this without trusted third-party?

- How does Frank know that Dave really had 3 BTC available?

- How to avoid that Dave spends them again after sending to Frank?

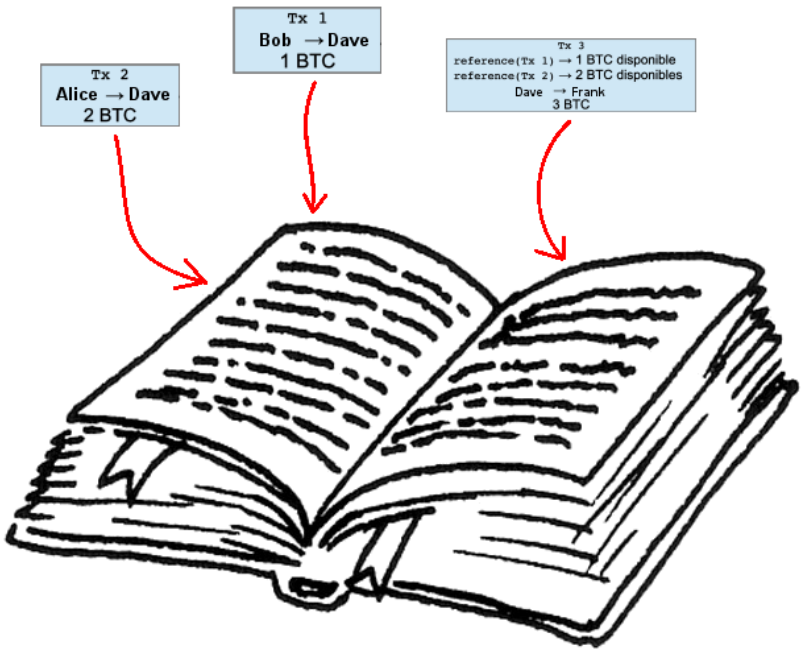
How to do this without trusted third-party?

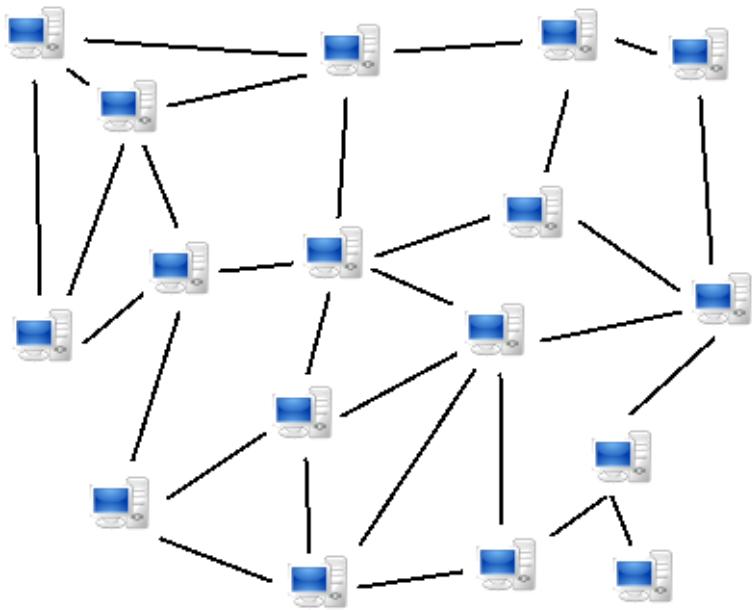
- How does Frank know that Dave really had 3 BTC available?
- How to avoid that Dave spends them again after sending to Frank?
- $\longrightarrow$ Blockchain

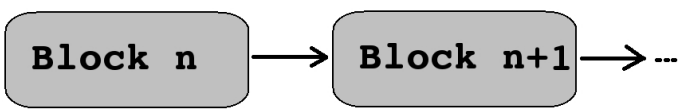
Outline

Blockchain

Contains all transactions and copied on every p2p nodes







Ensure all copies are the same: Secured by “Mining”

- The miners “clear” transactions and secure the blockchain by recording them in *blocks*, using a large *computing power*
- In exchange, they are rewarded with new bitcoins created ex-nihilo (at a fix rate)
- If miners don’t have majority of total computing power, they earn more bitcoins by being honest than dishonest
- Emerging behavior: the system as a whole acts honestly as long as a large enough majority acts honestly

Outline

Hashing Algorithms

Hashing Algorithms take inputs of any size, and produce outputs (hash) of standard sizes:

```
"haha"        -> bcb4fe6563d225fbc7b0e90571fc670f1ee197f18ba18e52a39c2ca80672812f

"hello world" -> a948904f2f0f479b8f8197694b30184b0d2ed1c1cd2a1ec0fb85d299a192a447
```

Hashing Algorithms: SHA256

SHA256 State-of-the-art hashing algorithm, used for many applications in the world, and also for bitcoin mining.

- Public, many open source implementations, can be downloaded or implemented yourself.
- Typically installed on every computer.

Hashing Algorithms: SHA256

SHA256 State-of-the-art hashing algorithm, used for many applications in the world, and also for bitcoin mining.

- Public, many open source implementations, can be downloaded or implemented yourself.
- Typically installed on every computer.
- Let's play with it!

Quite chaotic

Example!

Not Reversible: Brute force!

Find the English word that produces the hash:

`3dc3ae00e6d09d5e491895aca9237b14a87deabad03bfb9f5679eb49ff8b9744`

Example!

Not Reversible: Brute force!

Find the English word that produces the hash:

`3dc3ae00e6d09d5e491895aca9237b14a87deabad03bfb9f5679eb49ff8b9744`

Example!

- Must try all words in English dictionary until you try with “zebra”

Link with bitcoin mining

- Bitcoin mining is nothing else than “brute force” as we just did, but there is no dictionary
- Goal in bitcoin mining is not to find input with specific hash (too hard)
- Goal is to find input with a hash that starts with enough ’0’ at the beginning:

```
0000000006d09d5e491895aca9237b14a87482b6d03bfb9f5679eb49ff8b9744 -> OK

adc3ae4af8ec45b812ac2e5f6b4c5d79114d4741av1895aca9237b14a87dea78 -> not OK
```

Let's be a Miner!

- Our goal is to find a hash starting with one '0'.
- Input is the recent transactions that happened on the bitcoin network, that are not yet confirmed in a block. We simplify all these data to the string of characters "block-data":

Example!

Let's be a Miner!

- Our goal is to find a hash starting with one '0'.
- Input is the recent transactions that happened on the bitcoin network, that are not yet confirmed in a block. We simplify all these data to the string of characters "block-data":

Example!

  - Hash NOT OK
  - We can include an arbitrary number ("nonce") to obtain more hashes for our data. So we "mine" (brute force) this: "`block-data free-number=<we_can_choose>`"

Let's be a Miner: Success!

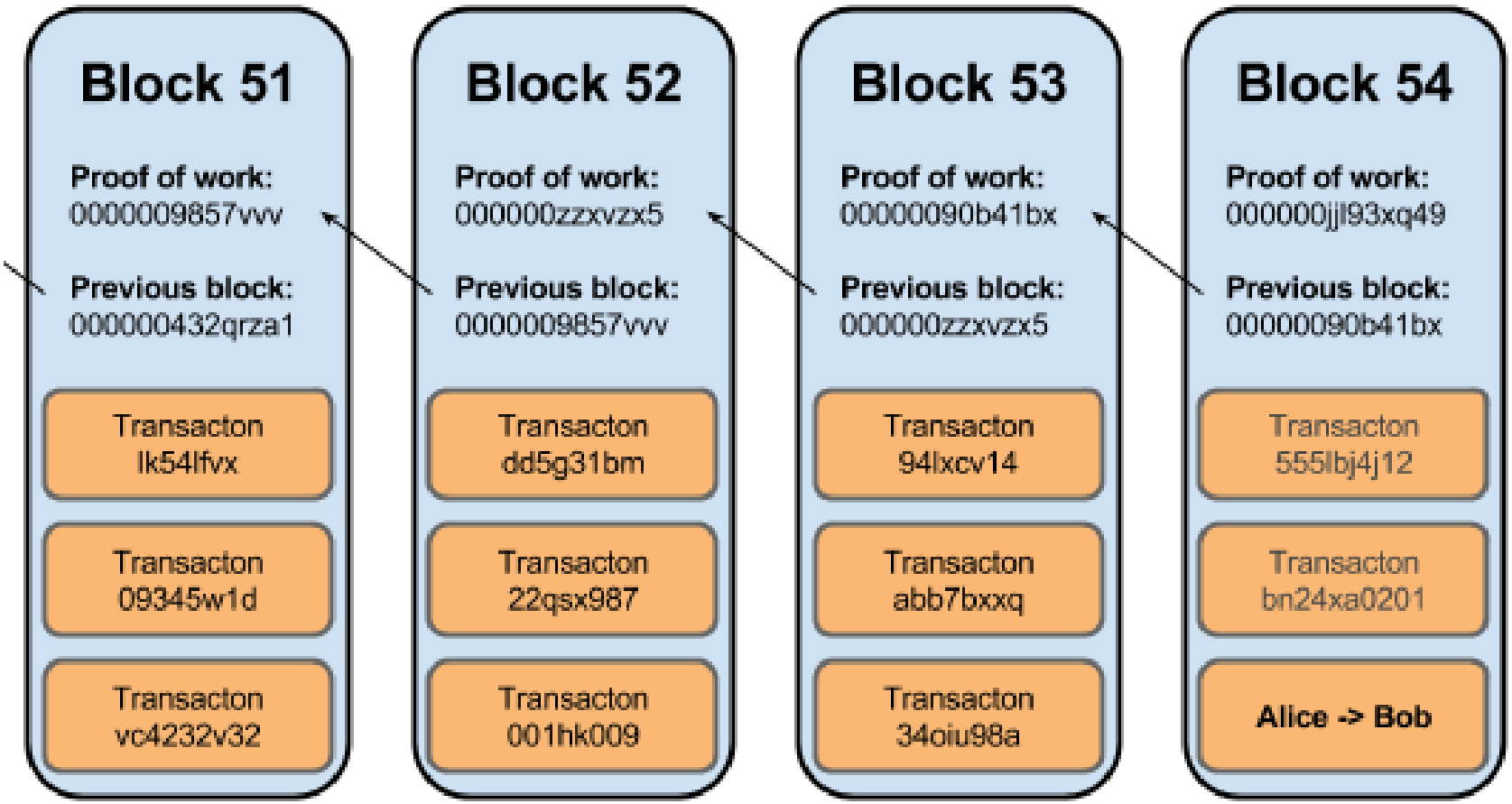
- We found a hash OK, we can *confirm the block* and tell everyone. They check themselves that indeed the hash is OK
- We earned 25 BTC
- Bitcoin mining is nothing more complex than that

Real Bitcoin Mining: same thing but (much) harder

- In reality, the (current) goal is to find hashes starting with 17 ’0’ in a row
- We did 4 trials in few seconds to mine a block starting with one ’0’
- Miners together are doing 350 thousands of billions of trials per second (350 Peta hashes / s) to find hashes starting with 17 ’0’
- The *difficulty* adapts automatically to the total hash rate, to keep one block confirmation every 10mn

Bitcoin total mining power

Blockchain = sequence of blocks “linked”



Result: distributed consensus

- The blockchain is a database that everybody can **freely** read...
- But it is **hard** to expand...
- And **excessively hard** to “rewrite”

Outline

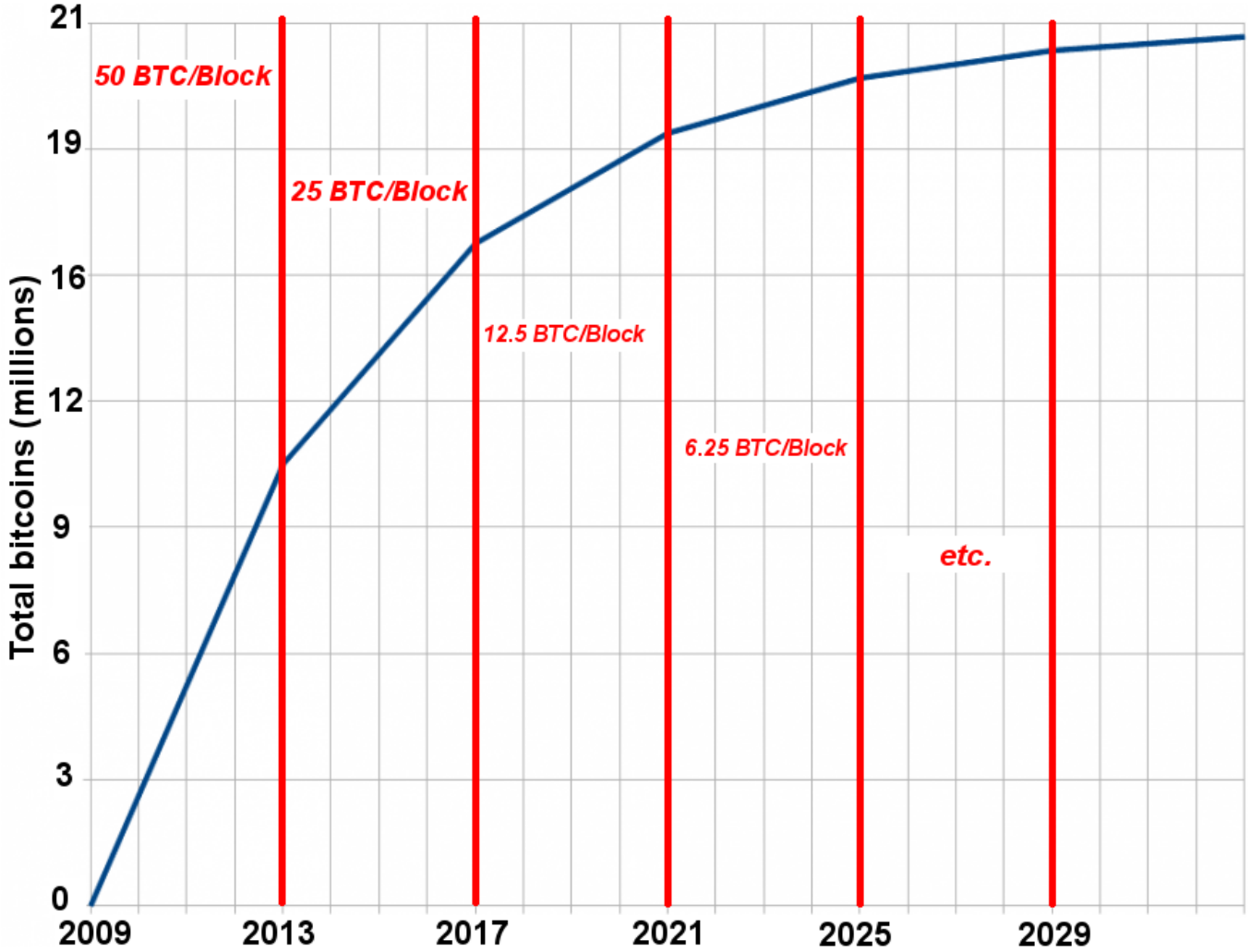
Money supply of Bitcoin

- Central bank, state-backed currency:
  Monetary policy decided/updated regularly

- Bitcoin:
  Fixed since the very beginning, known in the future forever

Money supply of Bitcoin

Inspired from gold mining



Outline

Number of units

- 21 Millions of BTC will exist maximum, ever
- Divisible up to 8 decimals (for now...)
- In fact, this number has very little economic relevance!

Outline

Price

- The bitcoin system itself does not include any price setting mechanism

- Like any scarce resource, supply and demand determine price wrt. things *outside of the system*.
  Price discovery happens only *at the boundaries* of the system where it meets another one (think forex)

Outline

Financial Privacy

- Financial privacy is important for a payment system
  - (Nobody want to have their private financial details publicly available)
- Anti-money laundering laws, taxation, etc. are possible even when the payment system ensures privacy

Privacy in Bitcoin

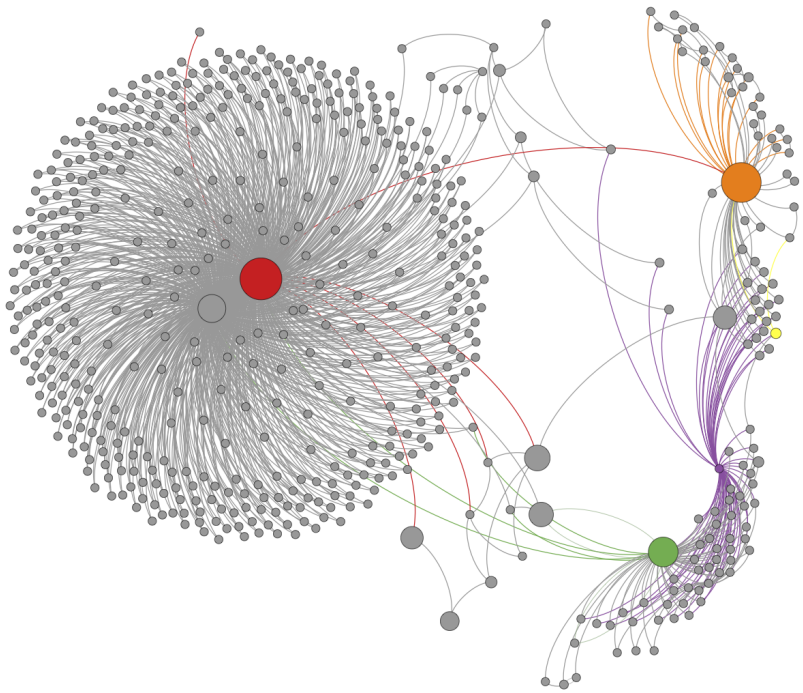
Bitcoin is not anonymous, it is *pseudonymous*. Pseudonymity is very fragile in daily life:

- Linking of transactions reduces privacy;
- Usage leaves traces everywhere on the Internet;
- Privacy-enhancing measures (tumblers/CoinJoin etc.) are costly.

As a result, the analysis of the Bitcoin blockchain can reveal identities.

Practical ways to analyse the blockchain

- Change addresses
- Correlation of transactions
- Addresses of public services (pools, exchanges, merchants, etc.)
- Leaked business records
- Scraping of web resources
- ...



Bitcoin blockchain analysis: a booming field

- Network-focused blockchain analysis is a thriving research field since a few years already.
- Today, an increasing number of high-level analysis tools are available:
  - https://bitiodine.net/
  - http://coinalytics.co/
  - http://www.quantabytes.com/
  - ...
- Permanent nature of blockchain ensures that privacy only ever **decreases**!

Outline

What is fungibility?

Formal definition

Fungibility is the property of a good or a commodity whose individual units are capable of mutual substitution.
That is, it is the property of essences or goods which are "capable of being substituted in place of one another."

TL;DR: Fungibility means that units are **interchangable**.

Why do we care?

Fungibility is a **fundamental property** of currencies.

- In centralized currencies, fungibility is guaranteed by the government.
- . . . and in decentralized currencies?

Fungibility in decentralized currencies

The formal description of Bitcoin:

Information exchange protocol, that allows the transfer of units of account; These units behave like the money we are used to, having these properties:

- Durability
- Portability
- Divisibility
- Relatively rare
- **Fungibility**

Is Bitcoin really fungible?

- Social pressure not to accept *tainted* coins (theft/fraud...)
- If privacy can be broken, fungibility is **voluntary**.

The lack of privacy in Bitcoin threatens its fungibility.

Services that track taint render bitcoins non-fungible, eg.:

- http://www.coinvalidation.com/
- http://coinalytics.co/
- https://chainalysis.com/

What can we learn from Bitcoin?

- Voluntary fungibility does not work.
- Fungibility in cryptocurrencies requires privacy.
- People becoming more aware of the fungibility issue in Bitcoin.
- Many approaches to fix this exist nowadays.

Outline

Bitcoin's main security difficulties

- bank payments (wire transfers, credit card payments etc) can be reversed (*"charge back"*)
- bitcoin payments **cannot** be reversed
- this creates new challenges for users and businesses

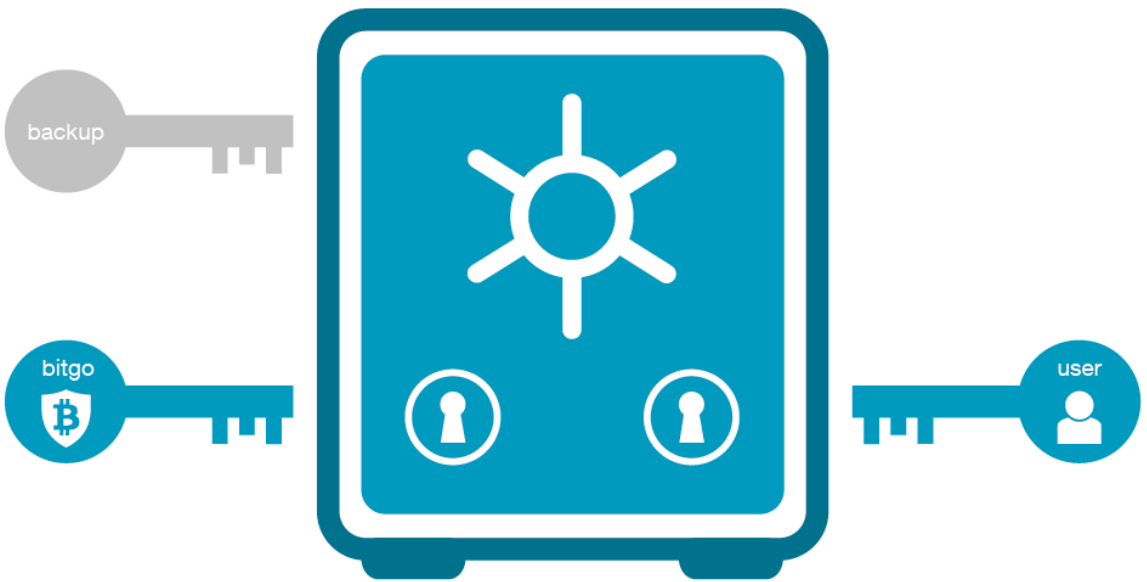
Bitcoin's main security difficulties

- End-users and businesses cannot deal with the newly gained responsibility (yet)

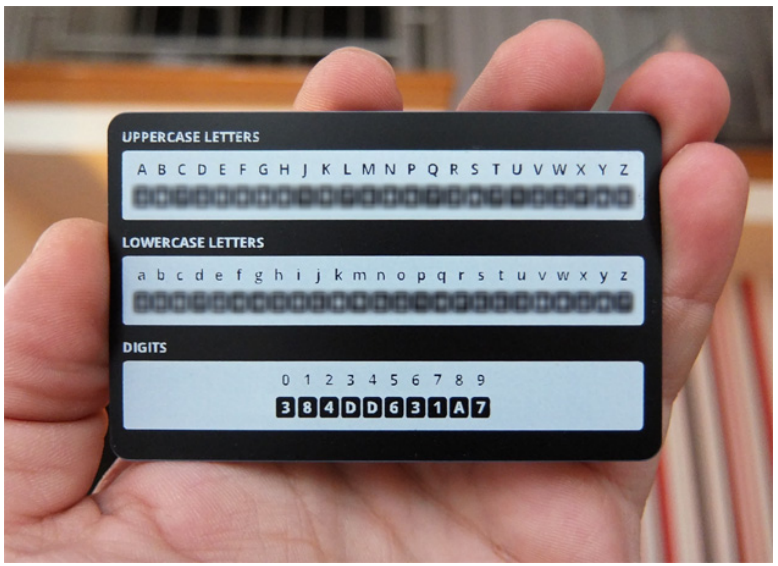
Security challenges for the user

- most people struggle to secure their PC for normal use
- people are used to offload responsibility to banks
- once money is involved, they become highly profitable targets
- early tools in bitcoin were very hard to use

Multi-signature wallets



Hardware wallets



Security challenges for businesses

- bitcoin-enabled applications are much more complex than a “normal” applications
- due to bitcoin’s nature, bitcoin businesses have the highest threat-level on the internet
- business must be prepared against all kinds of attacks

Security challenges for businesses

- furthermore, bitcoin mixes IT with finance in areas where people are not used to finance
- fractional reserves, financial strategies etc. pose problems to young companies
- it's early in bitcoin's history, so many past problems were created by hobbyists not knowing what they're doing

Outline

Technological Innovation with major impact

- State-issued currency is a pillar of today's governments
- Central bank policy is a political tool
- Modern economies strongly depend on banks
- AML & KYC were a given due to centralization, now voluntary
- Sudden leap towards globalisation of labor market

Enabling direct trades between people...

- used on a daily basis in real life (cash)
- wanted by users for electronic cash as well
- . . . but makes it very hard to enforce regulations: *Dark markets*

Outline

Summary

- First time we have decentralized consensus in digital age
- First time we have unicity of information in digital age
- First time we have censorship-free way to transfer value on the internet
- First time we have a timestamped database that makes authority
- First time . . .
- Positive? Negative? Bitcoin cannot be “de-invented”
- Frustrated?
  - *“The first five times you think you understand bitcoin, you don’t”*
    – Dan Kaminski

Selected sources

- https://en.bitcoin.it/wiki
- https://blockchain.info/
- http://www.meetup.com/Bitcoin-Brussels/
- “Mastering Bitcoin: Unlocking Digital Cryptocurrencies” Andreas Antonopoulos, O’Reilly

jeremie|arne@bitcoinassociation.be