BITSAGA

BITCOIN WORKSHOP

BITSAGA

Agenda

- Geld: waarom?
- Waarde
- Geld geschiedenis
- Geld: wat?
- Crypto geschiedenis
- Bitcoin
- Security & privacy
- Bitcoin technisch
- Bitcoin kopen
- Bitcoin opslaan
- Wallets & signatures
- Bitcoin gebruiken: Lightning

BITSAGA

Waarom geld?

- 150 jagers - verzamelaars (Dunbar’s number)
- Verdeling van arbeid

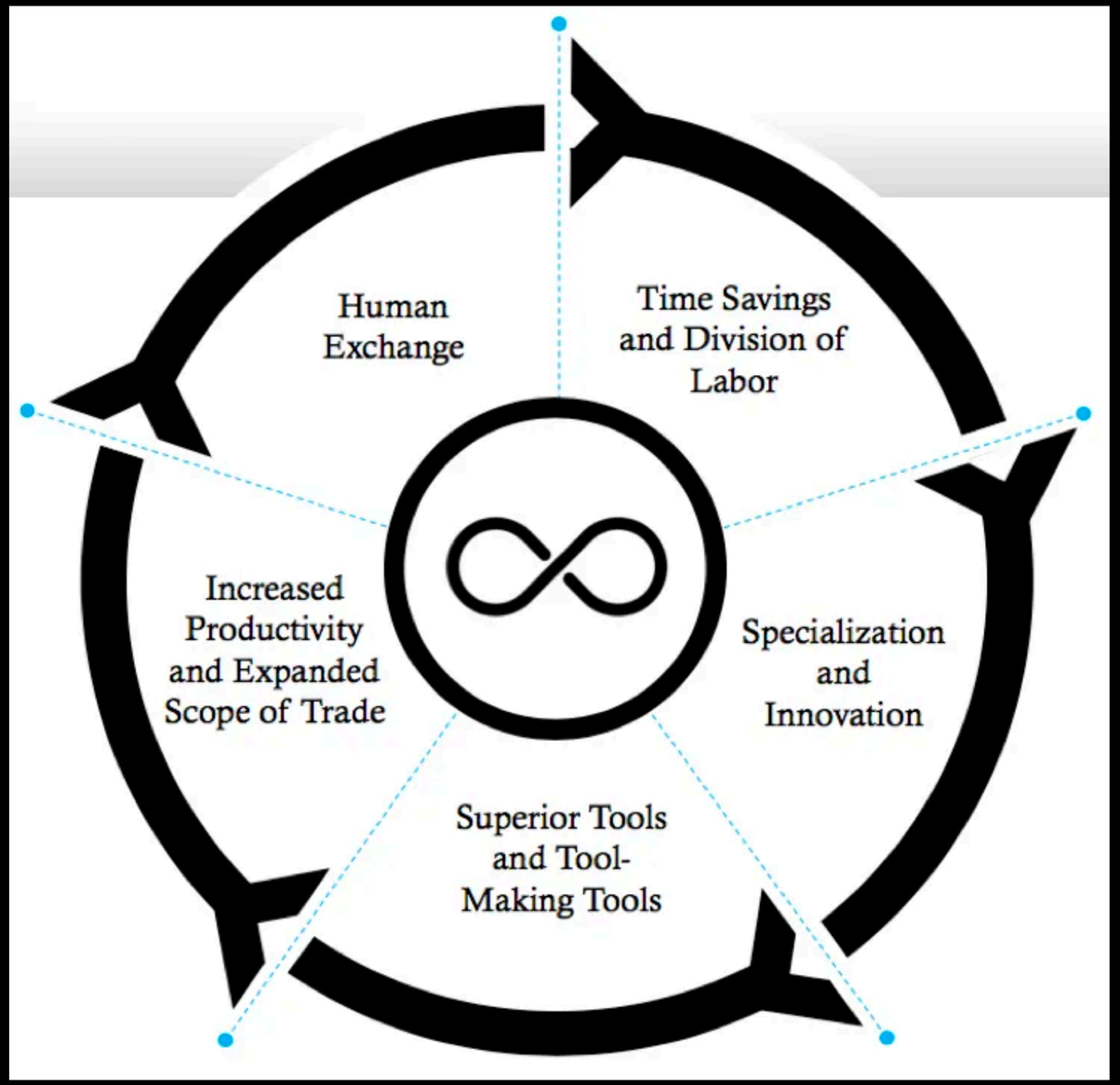
  => Specialisatie

  => Technologie

  => Productiviteit

  => Welvaart & tijd

- **Coincidence of wants**



5 WAVES OF CURRENCY EVOLUTION

CAVEMEN ONWARDS

BARTER

1200 BC

PHYSICAL TOKENS

618 AD

PAPER MONEY

1861 AD

ELECTRONIC MONEY

2009 AD

CRYPTOCURRENCIES

BITSAGA

Geschiedenis van geld

successen

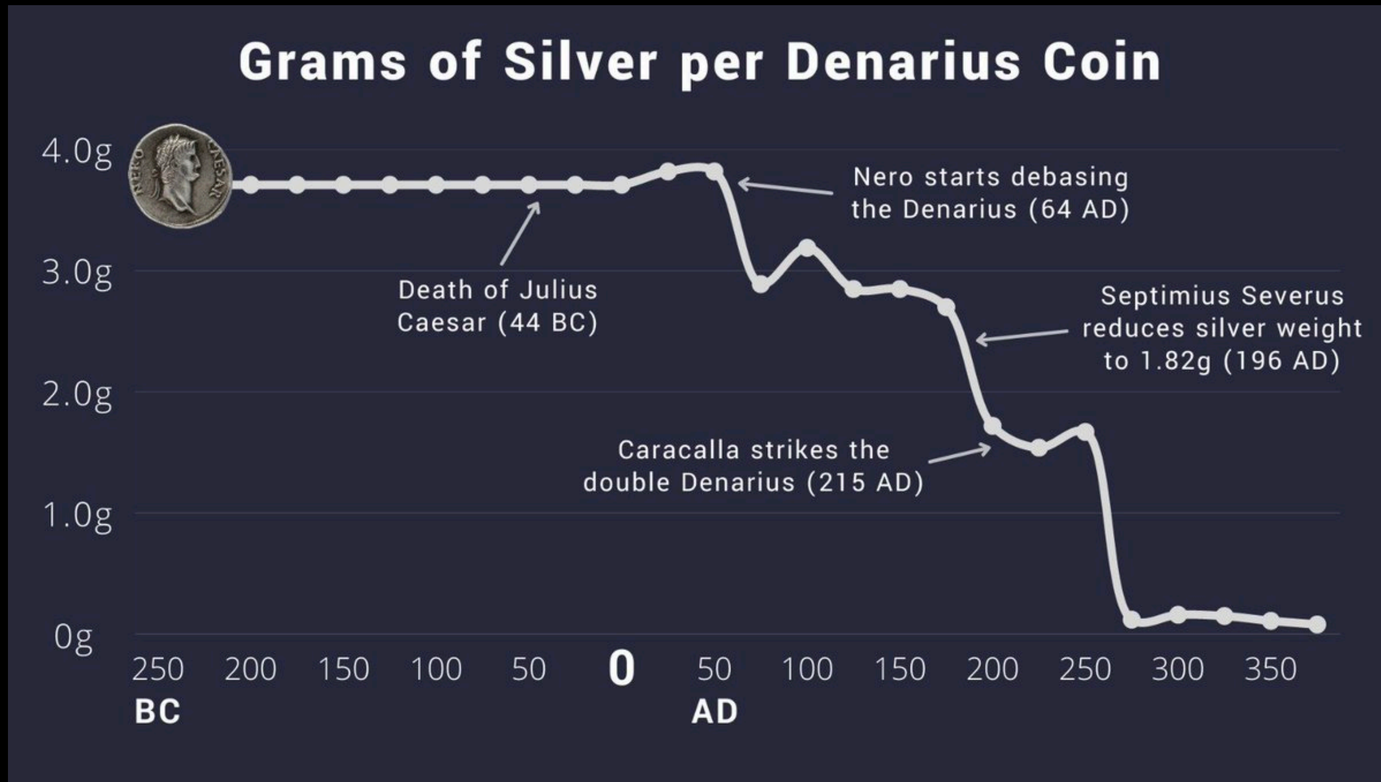
- Ruilhandel (voor 10 000 v.C.)
- Primitief geld (schelpen, dierenhuiden, kleitabletten, graan, vee - 6000 v.C.)
- Munten (brons, zilver, goud - vanaf 500 v.C.)
- Papieren Geld
  - Vanaf 800 n.C. China (ongesteund)
  - Vanaf 1600 n.C. Europa (gesteund)
- Goud standaard (UK, 1816)

BITSAGA

Geschiedenis van geld

mislukkingen

- Romeinse keizers: Bezant & Denari
- Spaanse kolonies: El Dorado?
- Chinese dynastieen: Song & Yuan (jiaozi)



BITSAGA

Intrinsieke waarde bestaat niet

BITSAGA

Wat is geld?

Functies

- Waardeopslag
- Ruilmiddel
- Rekeneenheid

Eigenschappen

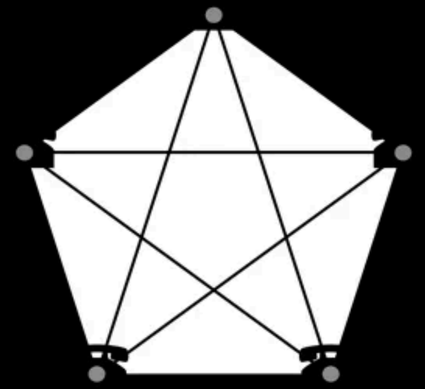
- Deelbaarheid
- Duurzaamheid
- Draagbaarheid
- Herkenbaarheid
- **Schaarste**

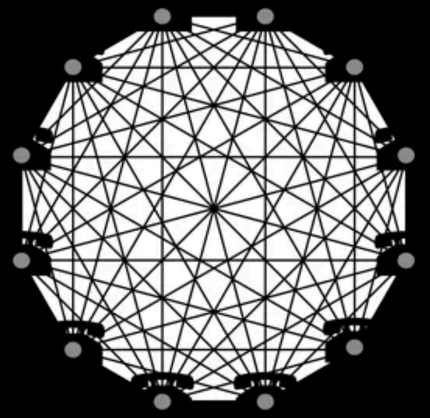
BITSAGA

Geld is een sociaal netwerk

Metcalfe’s law

Network effect





DECENTRALIZATION OF INFORMATION

Encyclopedia Britanica

Centralized
Content

Wikipedia

Decentralized
Content

BITSAGA

Decentralisatie

Informatie
Monnikenwerk
Boekdrukkunst
Encyclopedie
Wikipedia

BITSAGA

Decentralisatie

Informatie	Software development
Monnikenwerk	Individuele developers
Boekdrukkunst	Hierarchy
Encyclopedie	Open source
Wikipedia	Clones en forks (github)

BITSAGA

Decentralisatie

Informatie	Software development	Computing
Monnikenwerk	Individuele developers	Geisoleerd (geen netwerk)
Boekdrukkunst	Hierarchy	mainframe
Encyclopedie	Open source	server-client
Wikipedia	Clones en forks (github)	peer-to-peer

BITSAGA

Decentralisatie

Informatie	Software development	Computing	Bestuur
Monnikenwerk	Individuele developers	Geisoleerd (geen netwerk)	anarchy
Boekdrukkunst	Hierarchy	mainframe	monarchy
Encyclopedie	Open source	server-client	feudalism
Wikipedia	Clones en forks (github)	peer-to-peer	democracy

BITSAGA

Decentralisatie

Informatie	Software development	Computing	Bestuur
Monnikenwerk	Individuele developers	Geisoleerd (geen netwerk)	anarchy
Boekdrukkunst	Hierarchy	mainframe	monarchy
Encyclopedie	Open source	server-client	feudalism
Wikipedia	Clones en forks (github)	peer-to-peer	democracy

Weerstand

Stabiliteit

Kwaliteit

- **Waarom geld**

  => Coincidence of wants & transporteren van waarde

- **Geschiedenis van geld**

  => Ontwaarding leid tot stagflatie

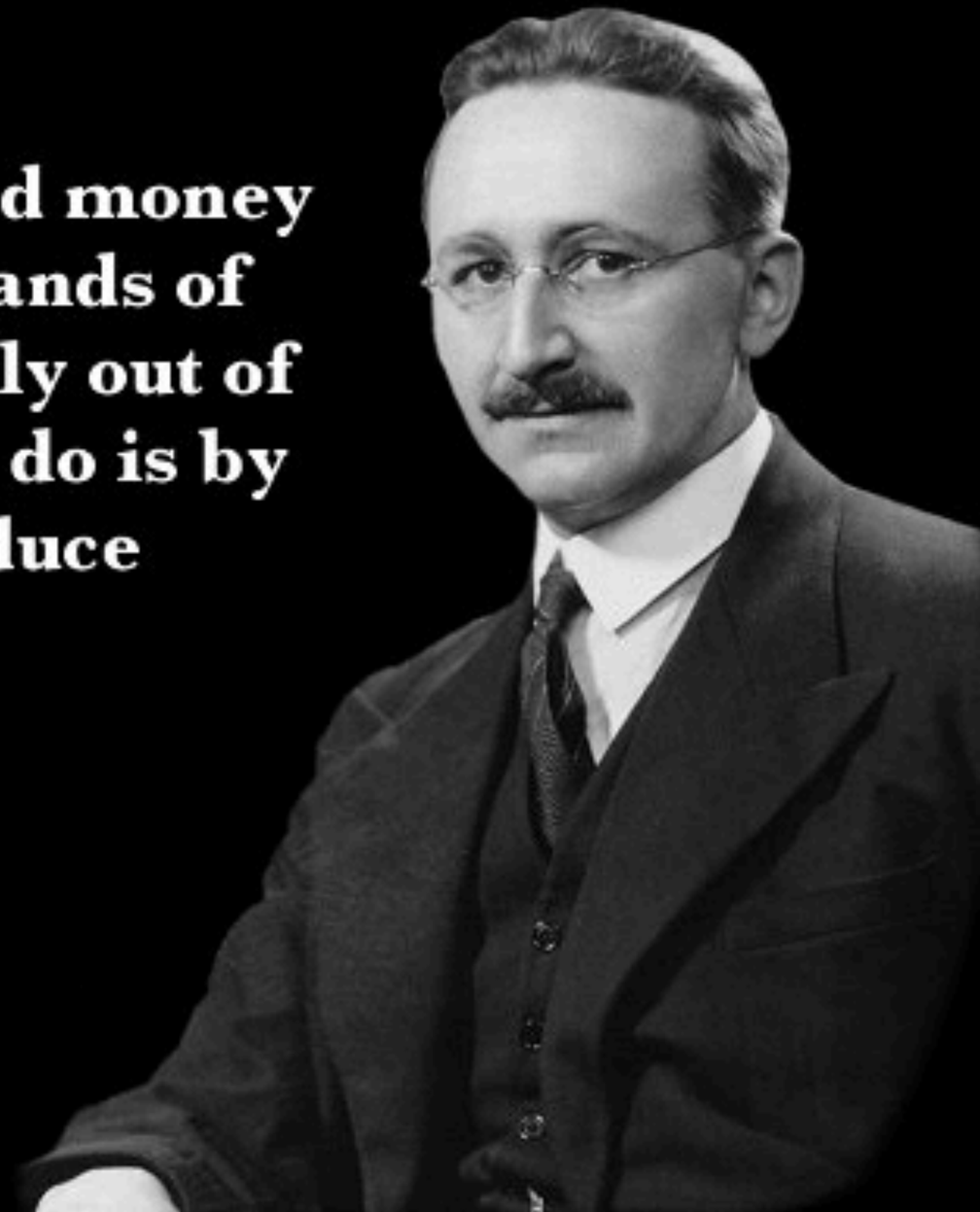
- **Eigenschappen van geld**

  => deelbaarheid, duurzaamheid, draagbaarheid, herkenbaarheid, schaarste

BITSAGA

I don't believe we shall ever have good money again before we take it out of the hands of government. We can't take it violently out of the hands of government. All we can do is by some sly, roundabout way introduce something they can't stop.

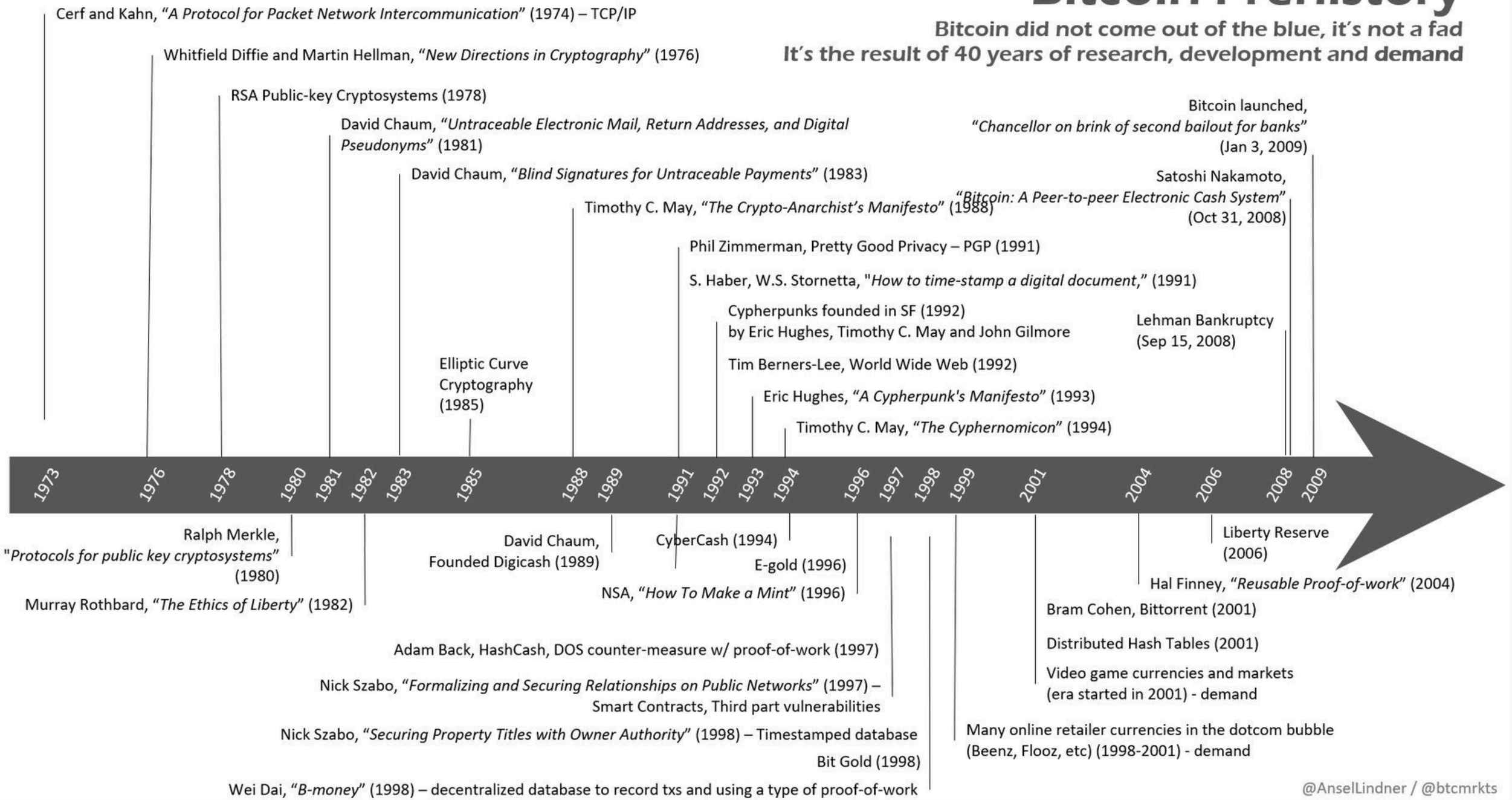
- F.A. Hayek




What are you trying to tell me, that I can trade my bitcoin for millions someday?
No Neo, I'm trying to tell you that when you're ready...
you won't have to.

Bitcoin Prehistory

Bitcoin did not come out of the blue, it's not a fad
It's the result of 40 years of research, development and demand



@AnselLindner / @btcmrkts

BITSAGA

“What is needed is an electronic payment system based on cryptographic proof instead of trust”

- Open-source & decentralised
- Peer-to-peer & global
- Reliable & secure
- Scalable & flexible
- Anonymous

“We propose a peer-to-peer distributed server to generate computational proof of the chronological order of transactions”

BITSAGA

Bitcoin
&
bitcoin

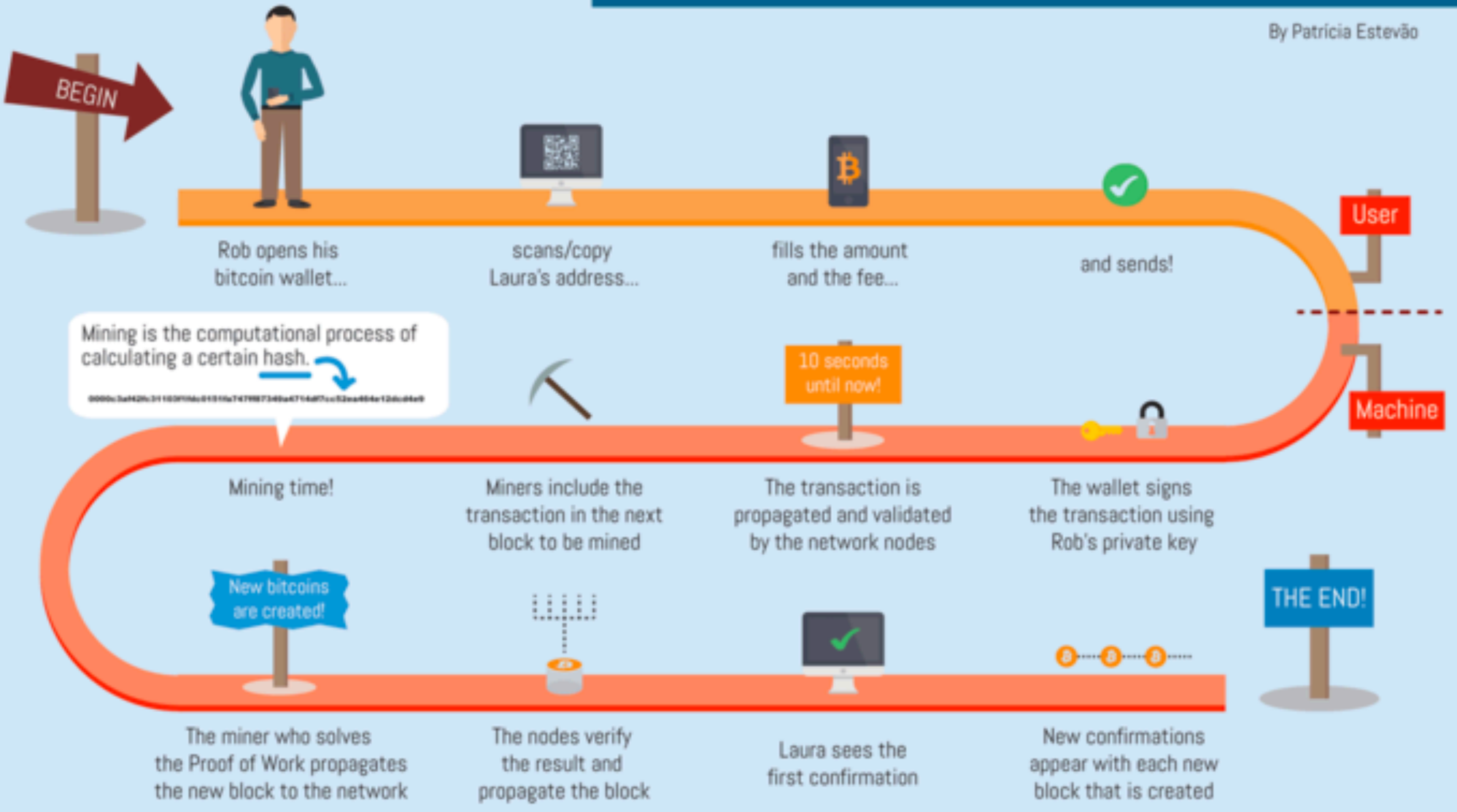
BITSAGA


Someone can build more real estate
Someone can issue more stock
Someone can print more fiat
Someone can mine more gold
No one can create more bitcoin

THE BITCOIN TRANSACTION LIFE CYCLE

Rob's quest to send 0.3 BTC to his friend Laura

By Patrícia Estevão

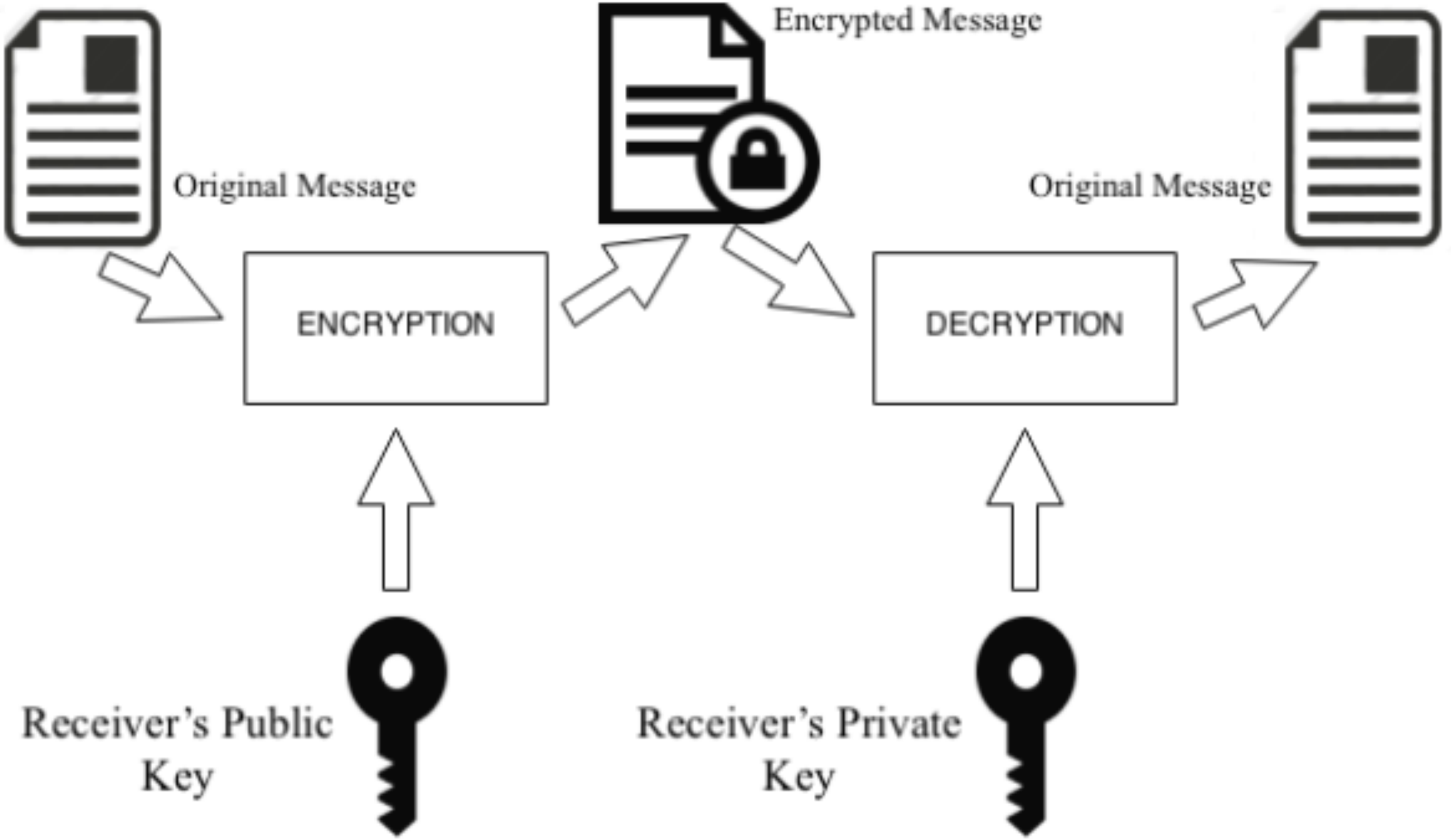


A chain of digital signatures

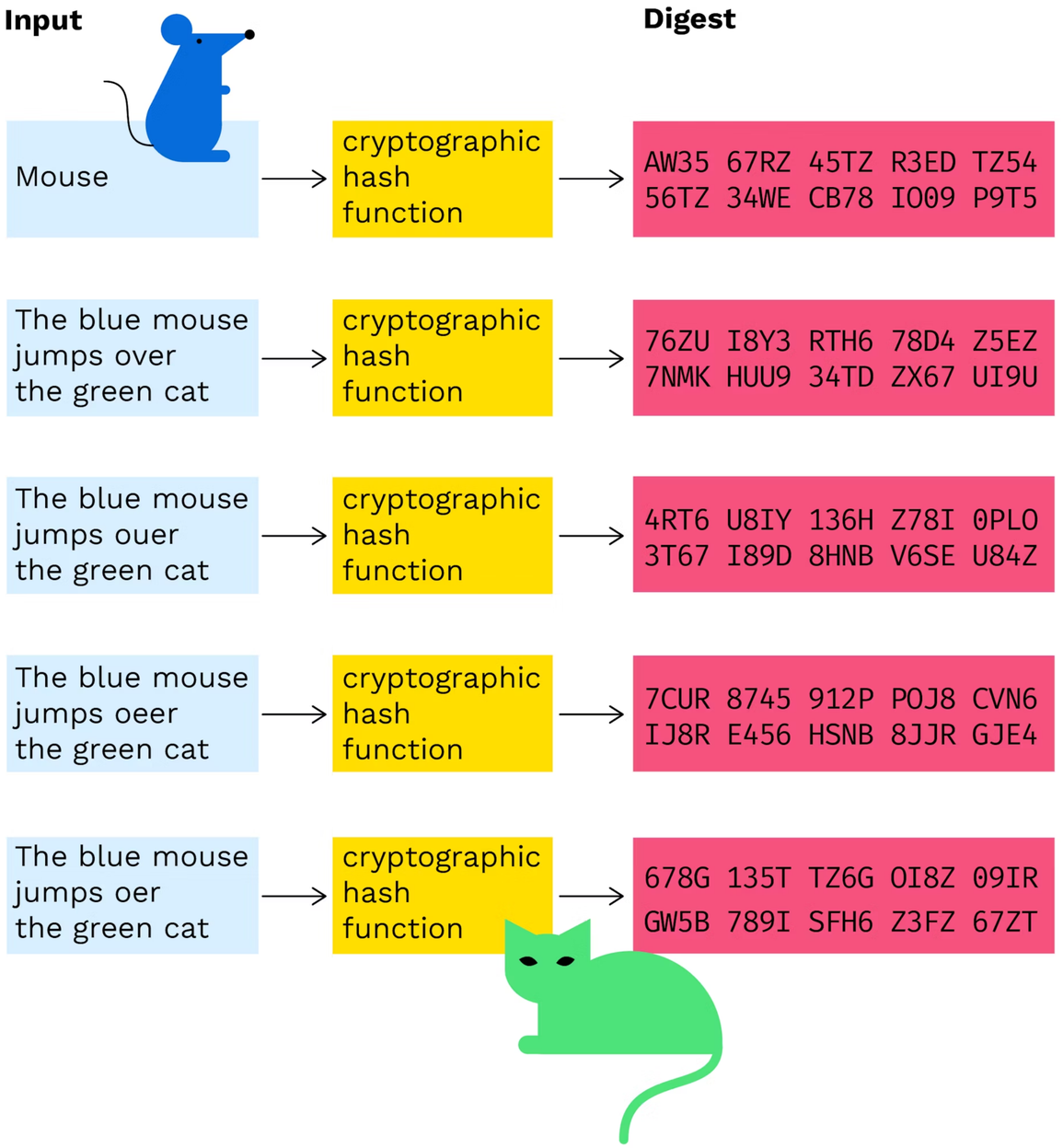
Owner transfers coins by digitally signing a hash of the previous transaction and the public key of the next owner and adding these to the end. A payee can verify the signatures to verify the chain of ownership.

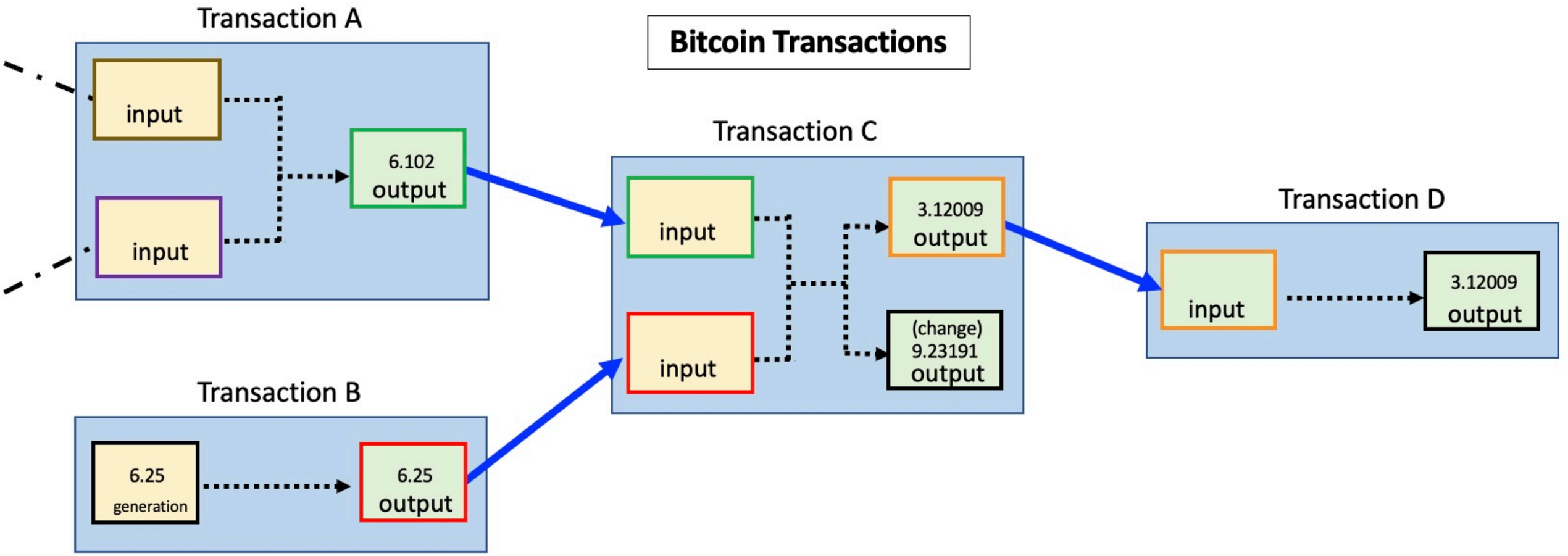
BITSAGA

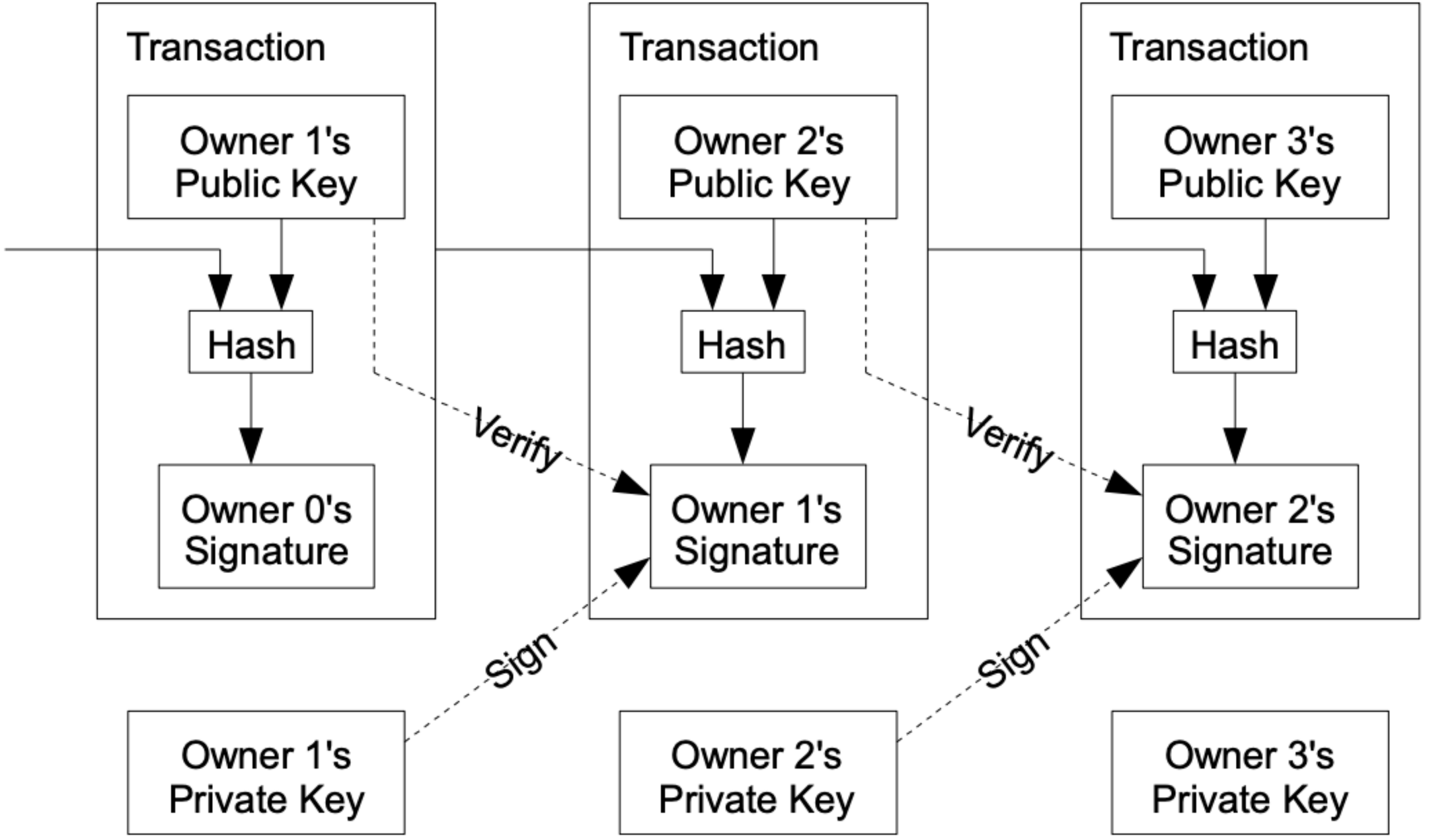
Asymmetric cryptography & hash functions


Original Message
ENCRYPTION
Encrypted Message
DECRYPTION
Original Message
Receiver's Public Key
Receiver's Private Key

What is a hash function?




Bitcoin Transactions
Transaction A
input
input
6.102
output
Transaction B
6.25
generation
6.25
output
Transaction C
input
input
3.12009
output
(change)
9.23191
output
Transaction D
input
3.12009
output


Transaction
Owner 1's Public Key
Hash
Owner 0's Signature
Transaction
Owner 2's Public Key
Hash
Owner 1's Signature
Transaction
Owner 3's Public Key
Hash
Owner 2's Signature
Verify
Verify
Sign
Sign
Owner 1's Private Key
Owner 2's Private Key
Owner 3's Private Key

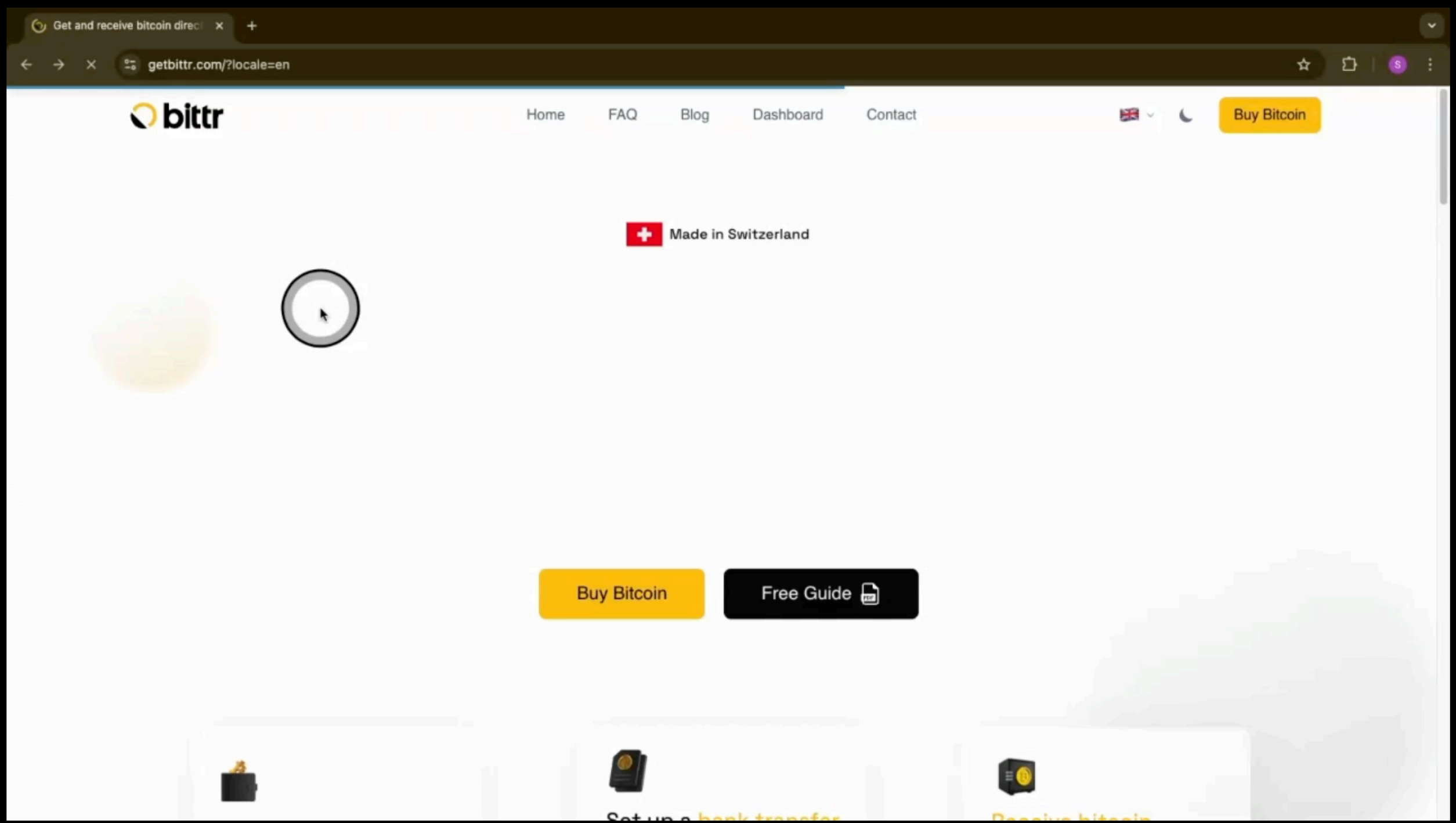
“The absolute scarcity of Bitcoin makes it perfect for storing and transacting the only other absolutely scarce resource — time.”

–Robert Breedlove

ZeroTrust

- Level 1: coins on exchange
- Level 2: hot wallet
- Level 3: cold wallet
- Level 4: airgap
- Level 5: node
- Level 6: multi sig
- Level 7: P2P & mixing
- Level 8: inheritance


bittr


Get and receive bitcoin direct
getbittr.com/?locale=en
bittr
Home
FAQ
Blog
Dashboard
Contact
Buy Bitcoin
Made in Switzerland
Buy Bitcoin
Free Guide

Vragen?

BITSAGA.be

rob@bitsaga.be