

3ITSAGA

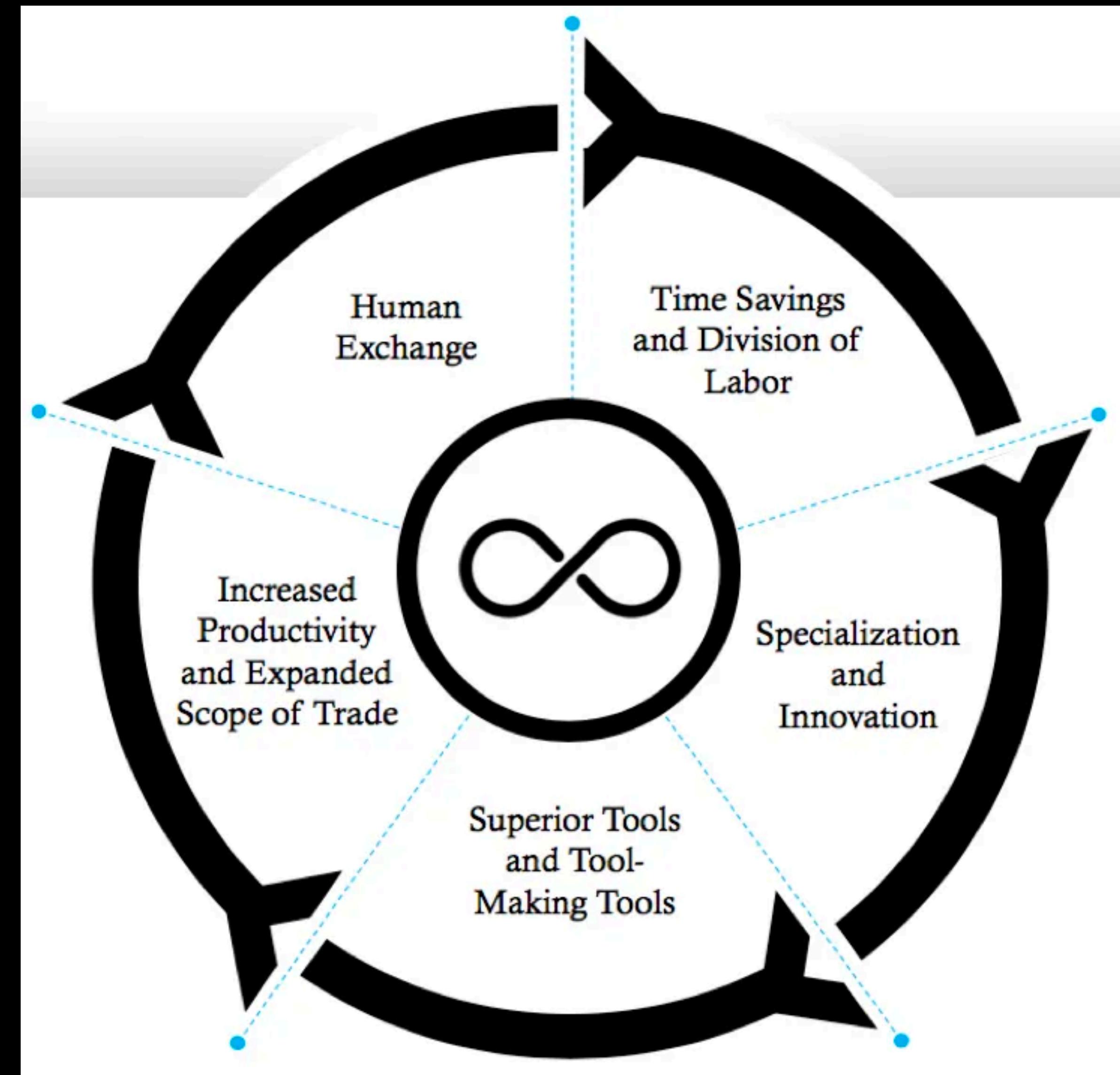
# BITCOIN WORKSHOP

# Agenda

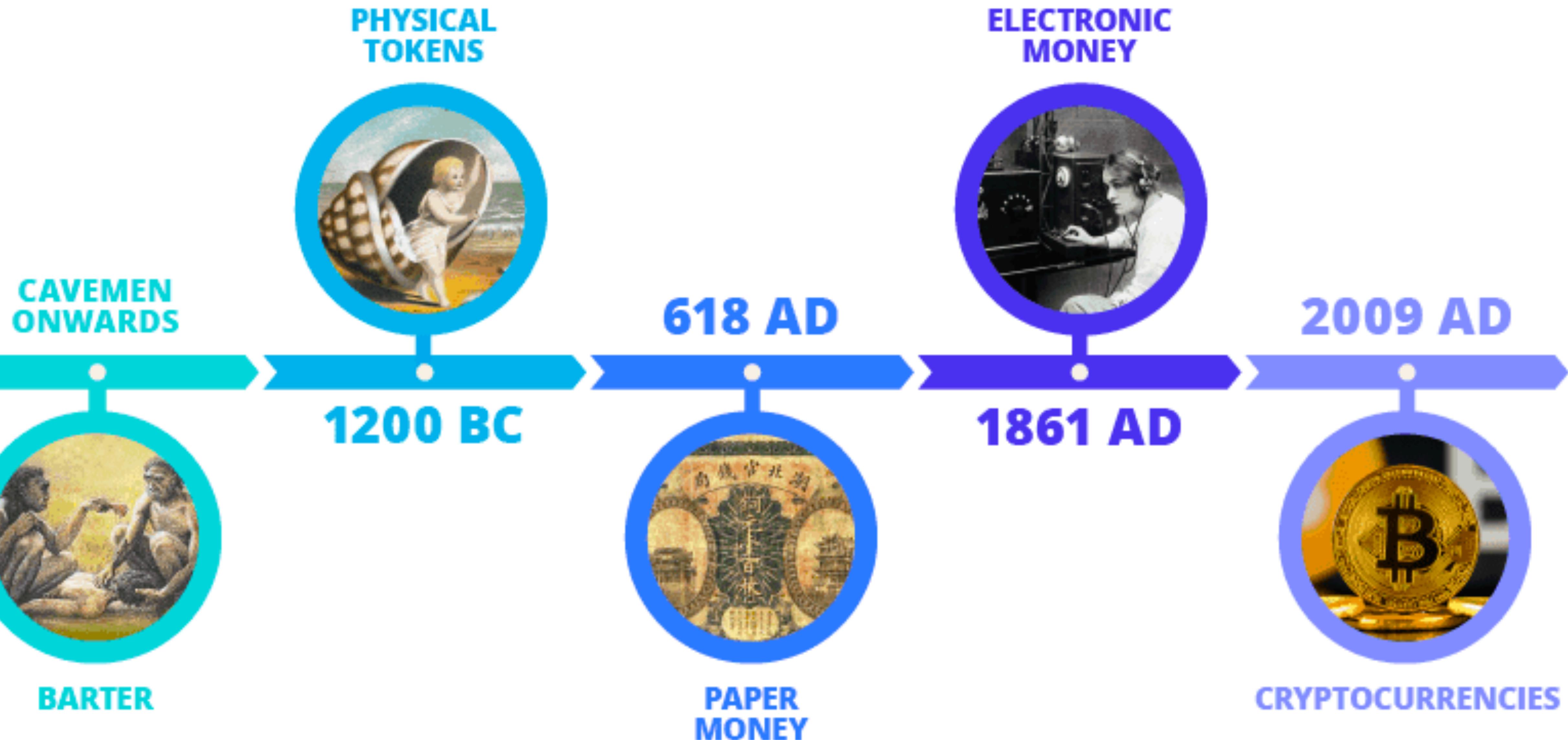
- Geld: waarom?
- Waarde
- Geld geschiedenis
- Geld: wat?
- Crypto geschiedenis
- Bitcoin
- Security & privacy
- Bitcoin technisch
- Bitcoin kopen
- Bitcoin opslaan
- Wallets & signatures
- Bitcoin gebruiken: Lightning

# Waarom geld?

- 150 jagers - verzamelaars (Dunbar's number)
- Verdeling van arbeid
  - => Specialisatie
  - => Technologie
  - => Productiviteit
  - => Welvaart & tijd
- **Coincidence of wants**



# 5 WAVES OF CURRENCY EVOLUTION



# Geschiedenis van geld

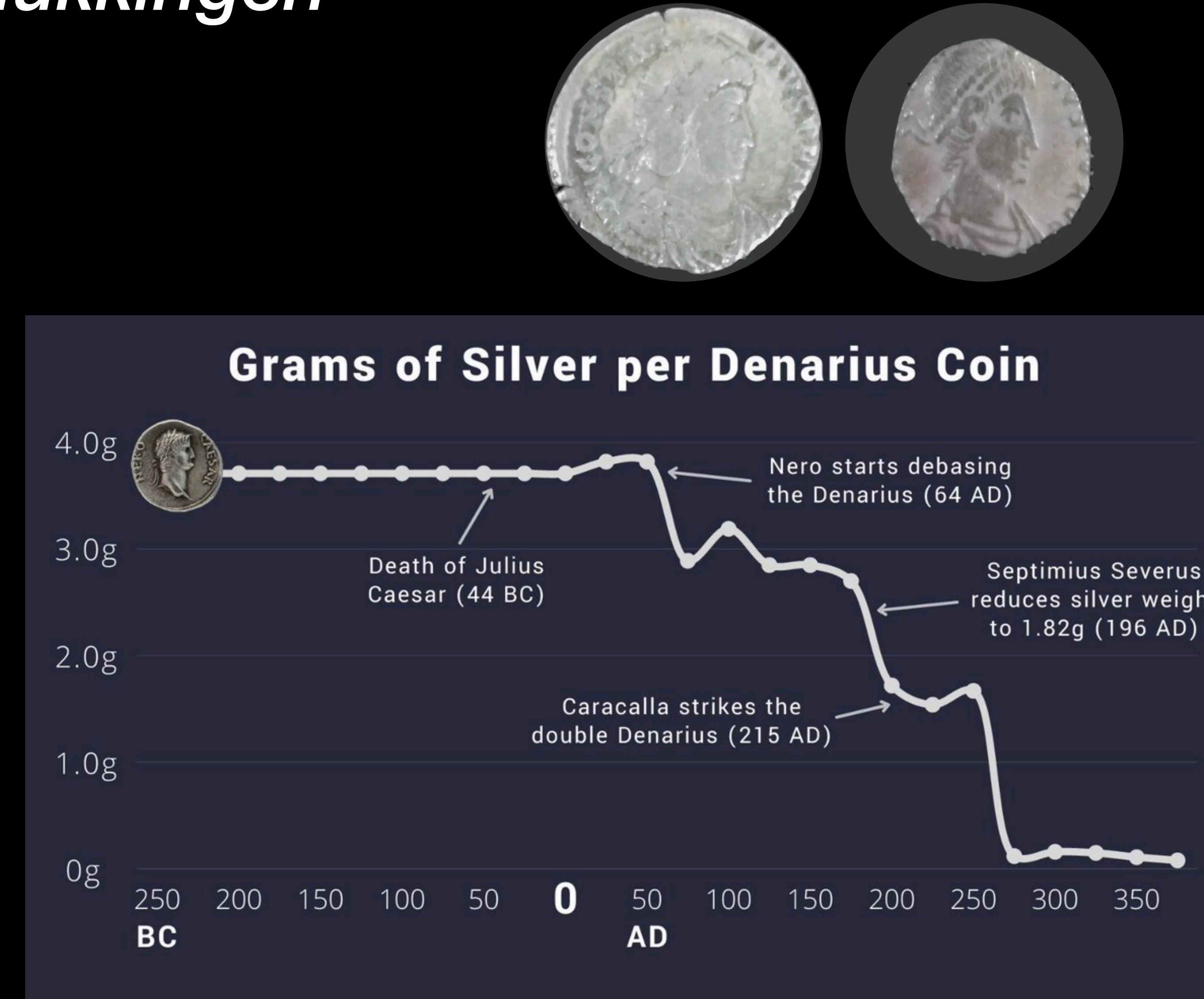
## successen

- 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)



# Geschiedenis van geld *mislukkingen*

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



Intrinsieke waarde  
bestaat niet

# *Wat is geld?*

## Functies

- Waardeopslag
- Ruilmiddel
- Rekeneenheid

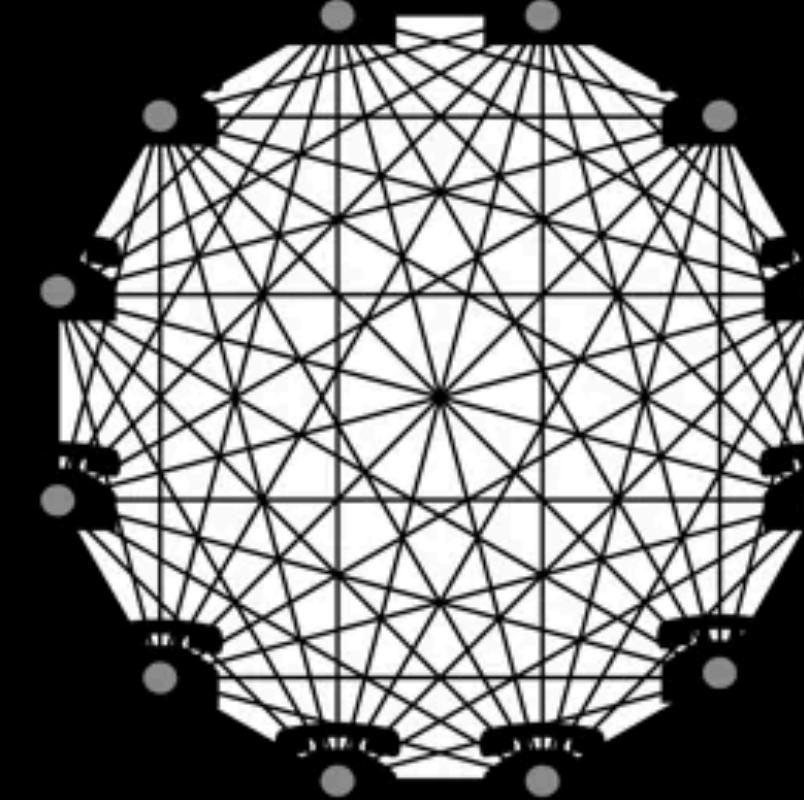
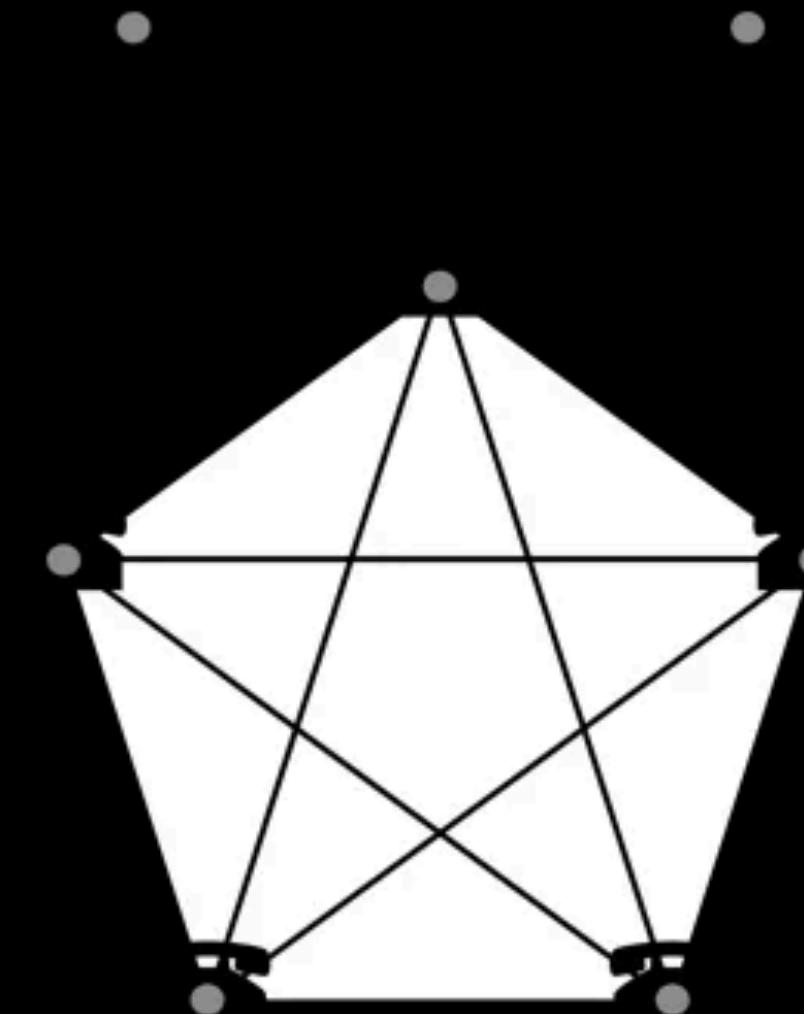
## Eigenschappen

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

# Geld is een sociaal netwerk

Metcalf's law

Network effect



# DECENTRALIZATION OF INFORMATION

Encyclopedia Britanica



Centralized  
Content

Wikipedia



Decentralized  
Content

# Decentralisatie

Informatie

Monnikenwerk

Boekdrukkunst

Encyclopedie

Wikipedia

# Decentralisatie

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

# Decentralisatie

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

# Decentralisatie

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

# Decentralisatie

Informatie	Software development	Computing	Bestuur
Monnikenwerk	Individuele developers	Gesoleerd (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**

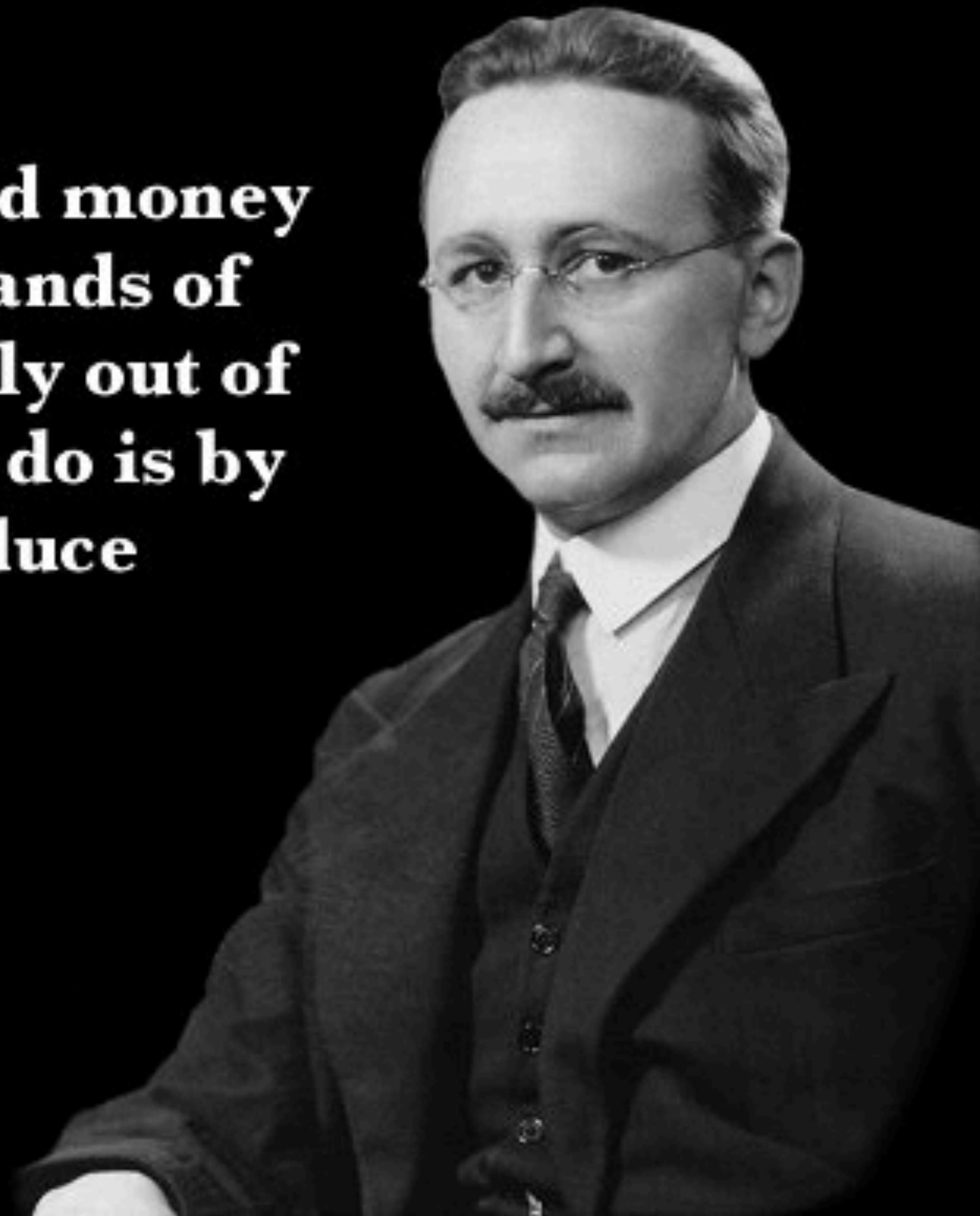
=> Ontwaarding leid tot stagflatie

- **Eigenschappen van geld**

=> deelbaarheid, duurzaamheid, draagbaarheid, herkenbaarheid, schaarste

**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**



A composite image featuring two characters from The Matrix. The top half shows Keanu Reeves as Neo, looking slightly off-camera with a serious expression. The bottom half shows Laurence Fishburne as Trinity, wearing his signature sunglasses and a dark hooded cloak.

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

Cerf and Kahn, "A Protocol for Packet Network Intercommunication" (1974) – TCP/IP

Whitfield Diffie and Martin Hellman, "New Directions in Cryptography" (1976)

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

RSA Public-key Cryptosystems (1978)

David Chaum, "Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms" (1981)

David Chaum, "Blind Signatures for Untraceable Payments" (1983)

Timothy C. May, "The Crypto-Anarchist's Manifesto" (1988)

Phil Zimmerman, Pretty Good Privacy – PGP (1991)

S. Haber, W.S. Stornetta, "How to time-stamp a digital document," (1991)

Cypherpunks founded in SF (1992)  
by Eric Hughes, Timothy C. May and John Gilmore

Tim Berners-Lee, World Wide Web (1992)

Eric Hughes, "A Cypherpunk's Manifesto" (1993)

Timothy C. May, "The Cyphernomicon" (1994)

Bitcoin launched,  
"Chancellor on brink of second bailout for banks"  
(Jan 3, 2009)

Satoshi Nakamoto,  
"Bitcoin: A Peer-to-peer Electronic Cash System"  
(Oct 31, 2008)

Lehman Bankruptcy  
(Sep 15, 2008)

1973

1976

1978

1980

1981

1982

1983

1985

1988

1989

1991

1992

1993

1994

1996

1997

1998

1999

2001

2004

2006

2008

2009

Ralph Merkle,  
"Protocols for public key cryptosystems"  
(1980)

Murray Rothbard, "The Ethics of Liberty" (1982)

David Chaum,  
Founded DigiCash (1989)

CyberCash (1994)  
E-gold (1996)  
NSA, "How To Make a Mint" (1996)

Adam Back, HashCash, DOS counter-measure w/ proof-of-work (1997)

Nick Szabo, "Formalizing and Securing Relationships on Public Networks" (1997) –  
Smart Contracts, Third party vulnerabilities

Nick Szabo, "Securing Property Titles with Owner Authority" (1998) – Timestamped database  
Bit Gold (1998)

Wei Dai, "B-money" (1998) – decentralized database to record txs and using a type of proof-of-work

Liberty Reserve  
(2006)

Hal Finney, "Reusable Proof-of-work" (2004)

Bram Cohen, BitTorrent (2001)

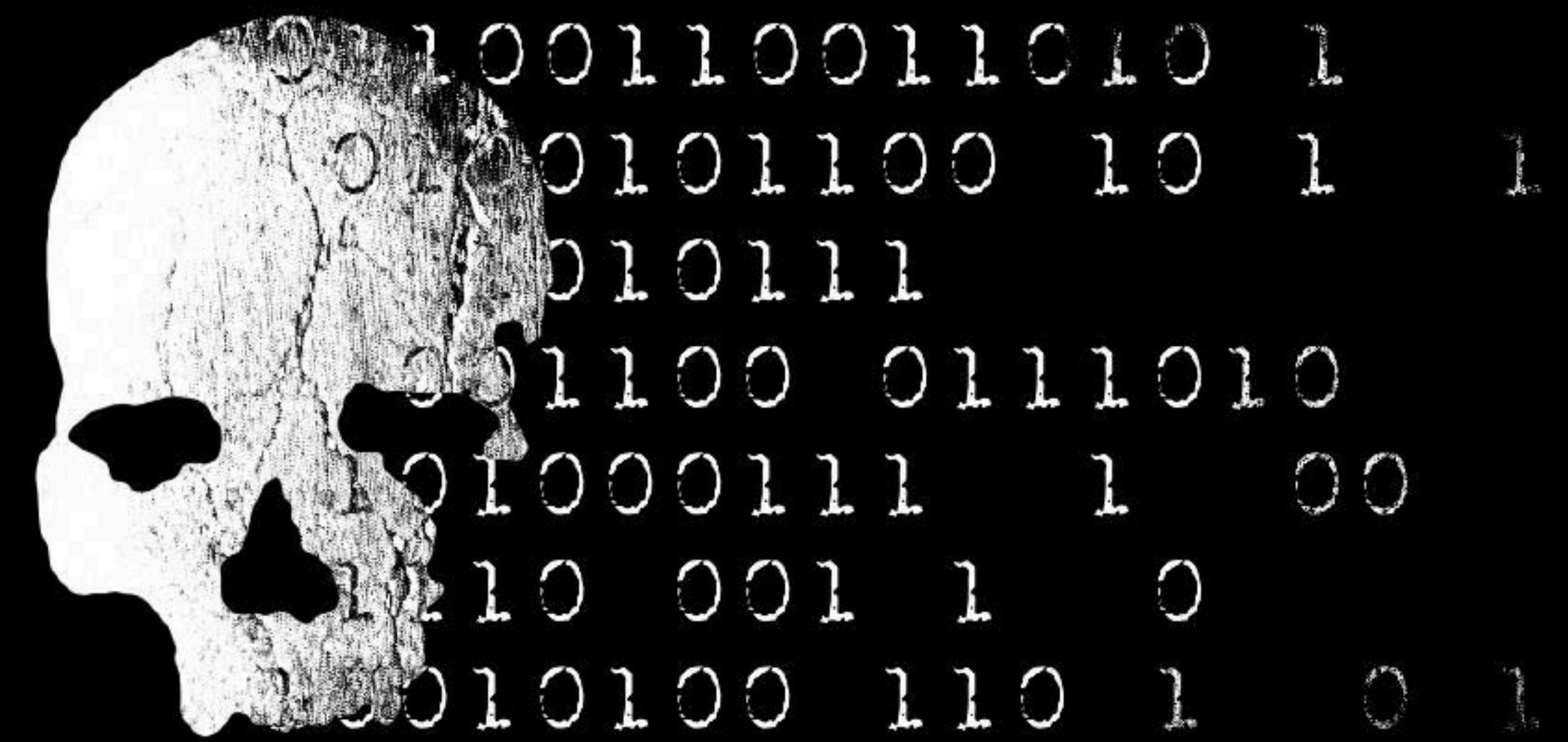
Distributed Hash Tables (2001)

Video game currencies and markets  
(era started in 2001) - demand

Many online retailer currencies in the dotcom bubble  
(Beenz, Flooz, etc) (1998-2001) - demand

**“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



cypherpunk

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





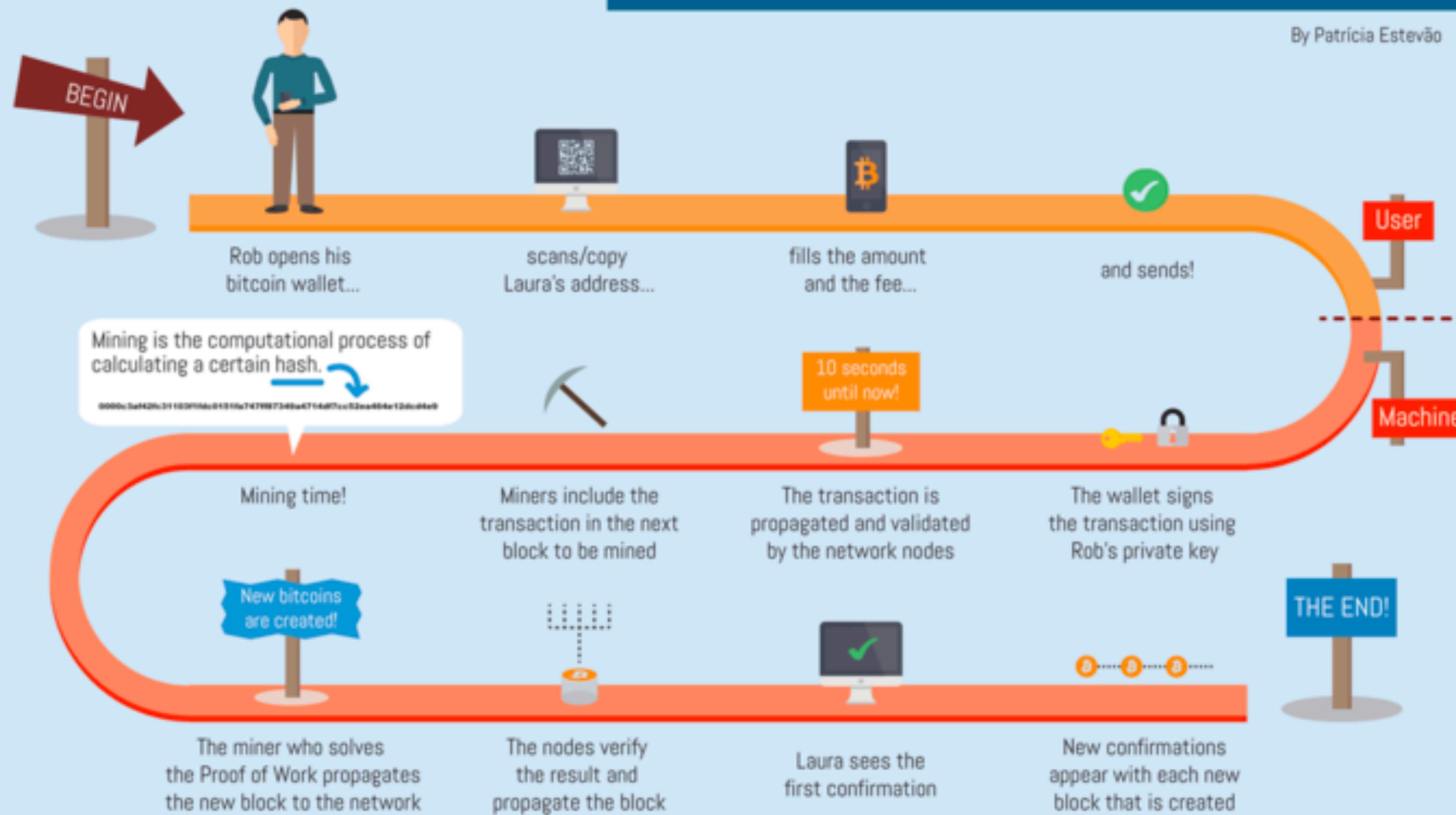
Bitcoin  
&  
bitcoin



# THE BITCOIN TRANSACTION LIFE CYCLE

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

By Patricia Estevāo



## 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.

# Asymmetric cryptography & hash functions



Original Message



ENCRYPTION



Encrypted Message



DECRYPTION



Original Message

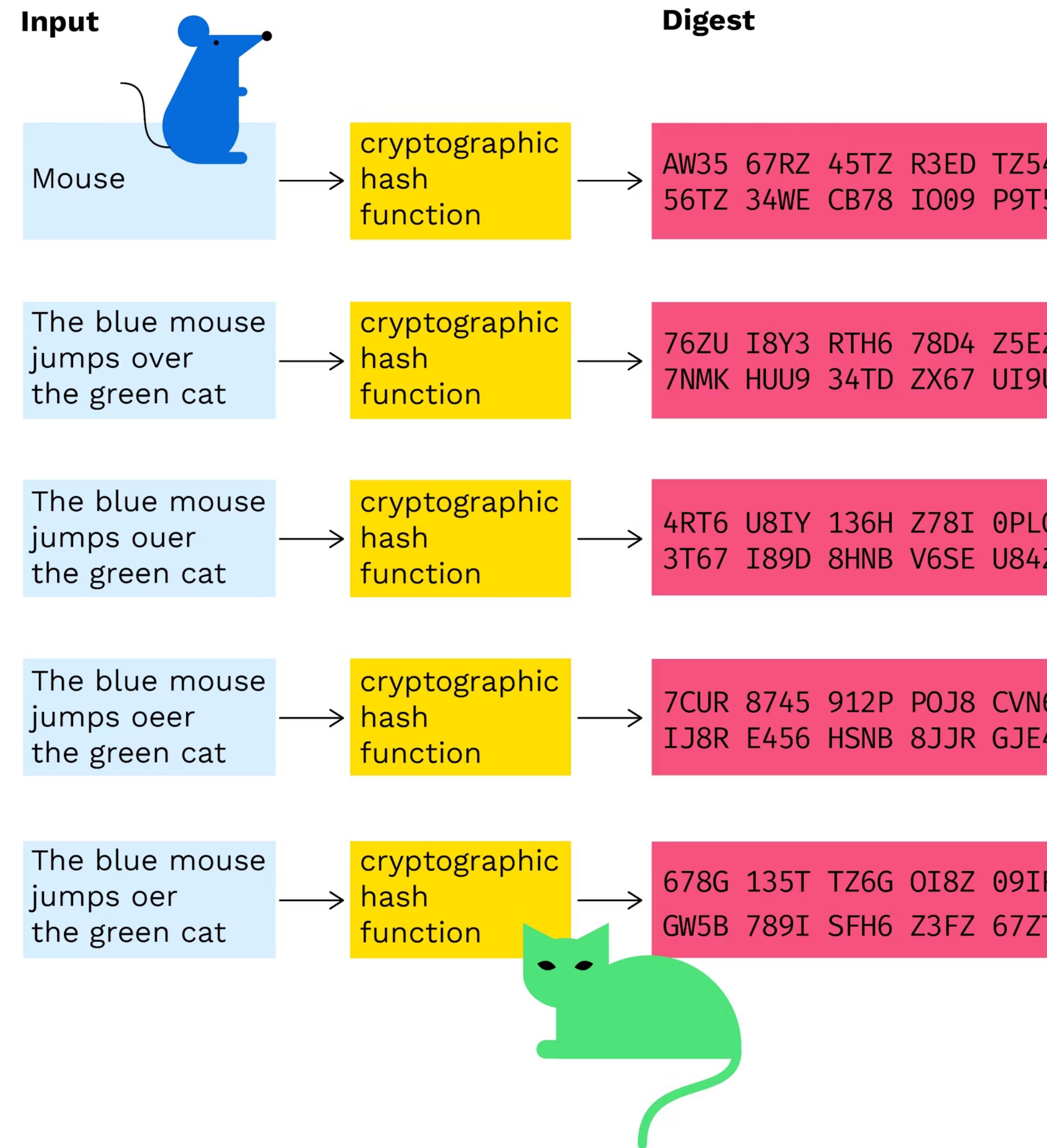


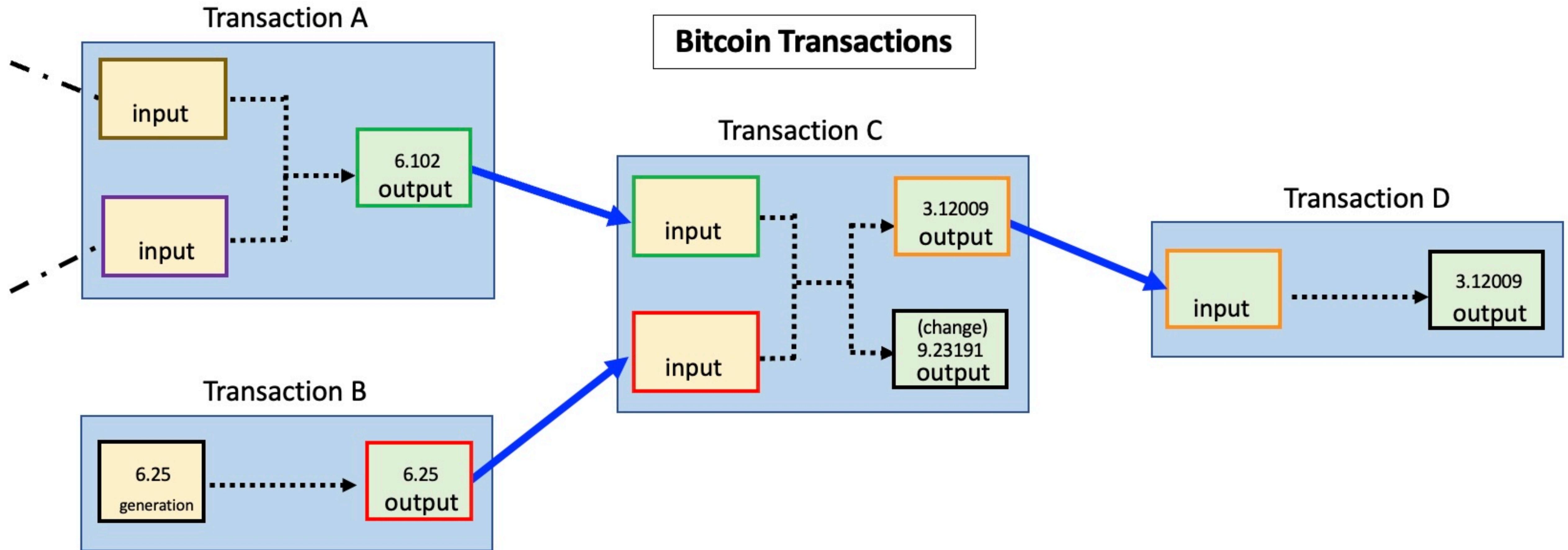
Receiver's Public  
Key

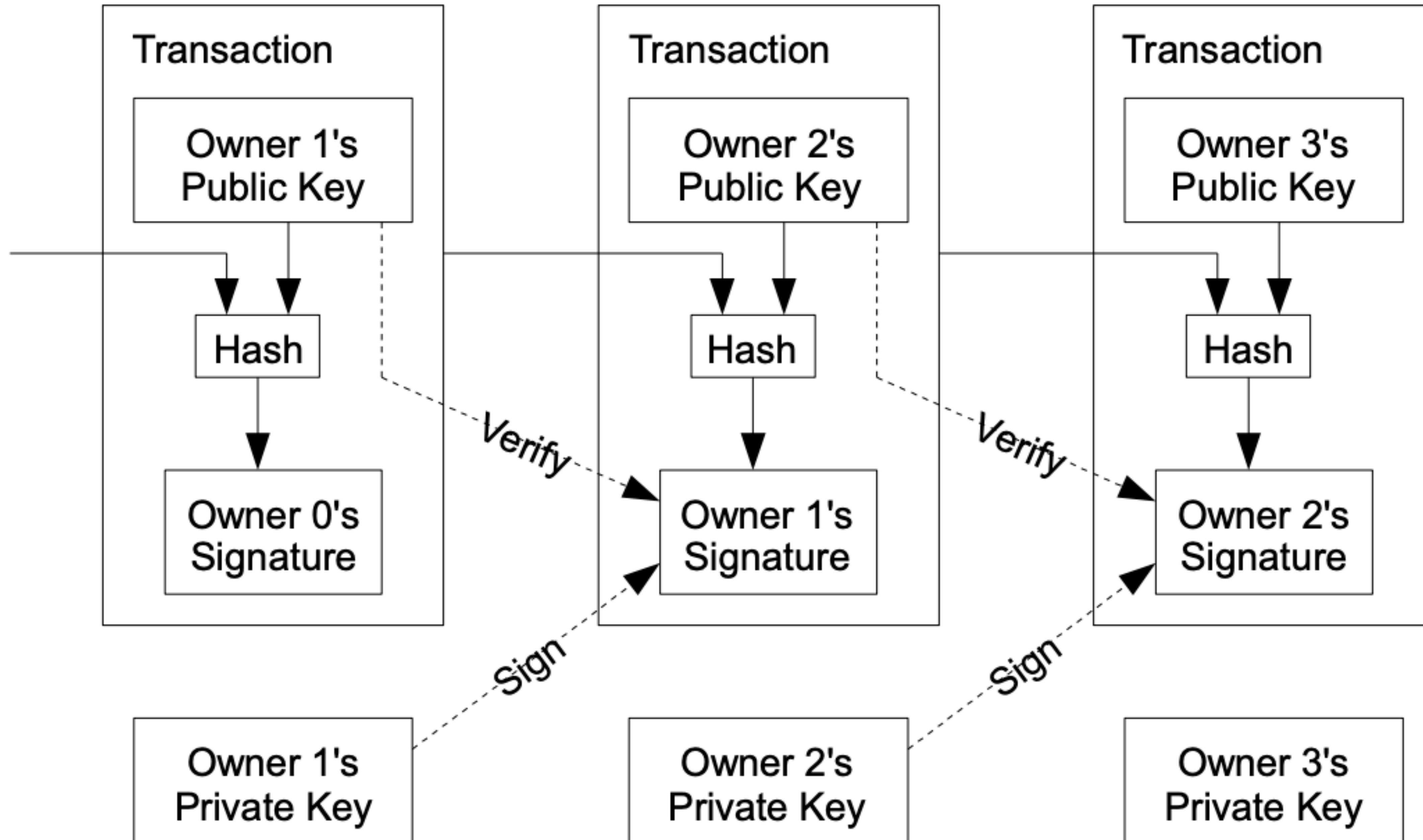


Receiver's Private  
Key

# What is a hash function?







**“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





Buy Bitcoin



Made in Switzerland



Buy Bitcoin

[Free Guide](#) 



### Set up a bank transfer



## Positive bitscan

Vragen?



[rob@bitsaga.be](mailto:rob@bitsaga.be)