FH CAMPUS WIEN
UNIVERSITY OF APPLIED SCIENCES

> TECHNIK

MASTERSTUDIUM:
> IT-SECURITY

Bitcoin: How it works.

A lightweight intro to block chains

Ulrich Haböck

Kompetenzzentrum für IT-Security, FH Campus Wien

June 26, 2017

Speaker

Ulrich Haböck
ulrich.haboeck@fh-campuswien.ac.at
PGP-key: 48F796E247BEEDE8.

- PhD Mathematics (University Vienna)
- Post-doc TU-Vienna
- since 2013 at the Competence Centre for IT-Security, FH Campus Wien
- Lecturer Bachelor *Information Technology and Telecommunications* as well as Master *IT-Security*
- Focus: mathematics and cryptography

The problem of digital cash

The problem of digital cash

- normal cash: expensive to copy/reproduce.

The problem of digital cash

- digital cash: copy and paste, even when certified (just a bunch of data!)

```
Serial-No:aabcf7...b
Value:1.24 U
Owner: Mr. Hans Pans
Issuer: Bank XYZ
Date:2017/29/02
Sig:c60cb9fc0c04bb2e
3bcb72c29dffb908e2ed
affcbd5e62d8194f3d71
9632
```

The problem of digital cash

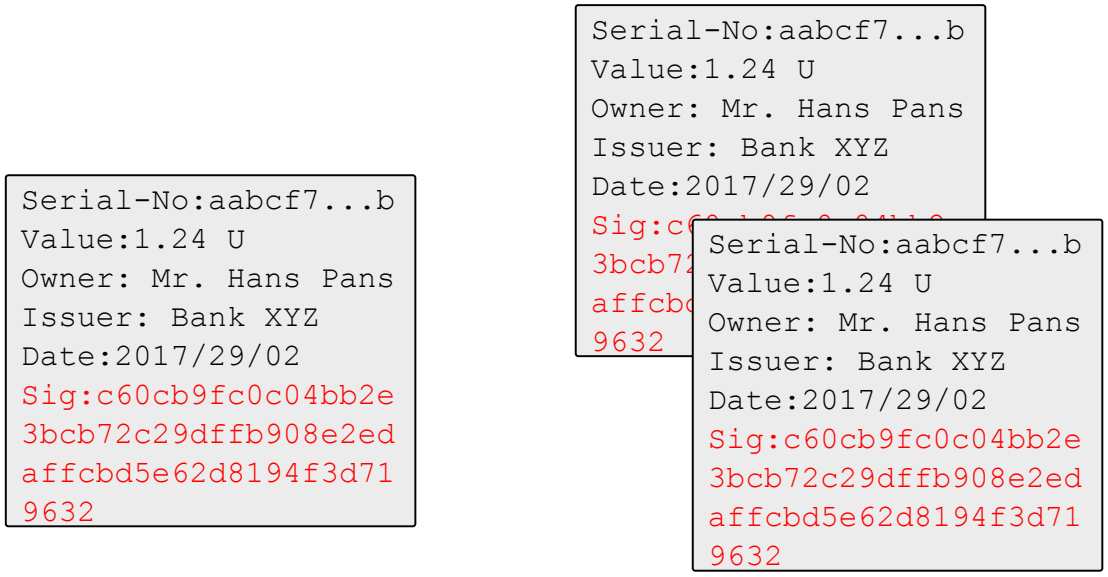
- digital cash: copy and paste, even when certified (just a bunch of data!)

```
Serial-No:aabcf7...b
Value:1.24 U
Owner: Mr. Hans Pans
Issuer: Bank XYZ
Date:2017/29/02
Sig:c60cb9fc0c04bb2e
3bcb72c29dffb908e2ed
affcbd5e62d8194f3d71
9632
```

```
Serial-No:aabcf7...b
Value:1.24 U
Owner: Mr. Hans Pans
Issuer: Bank XYZ
Date:2017/29/02
Sig:c60cb9fc0c04bb2e
3bcb72c29dffb908e2ed
affcbd5e62d8194f3d71
9632
```

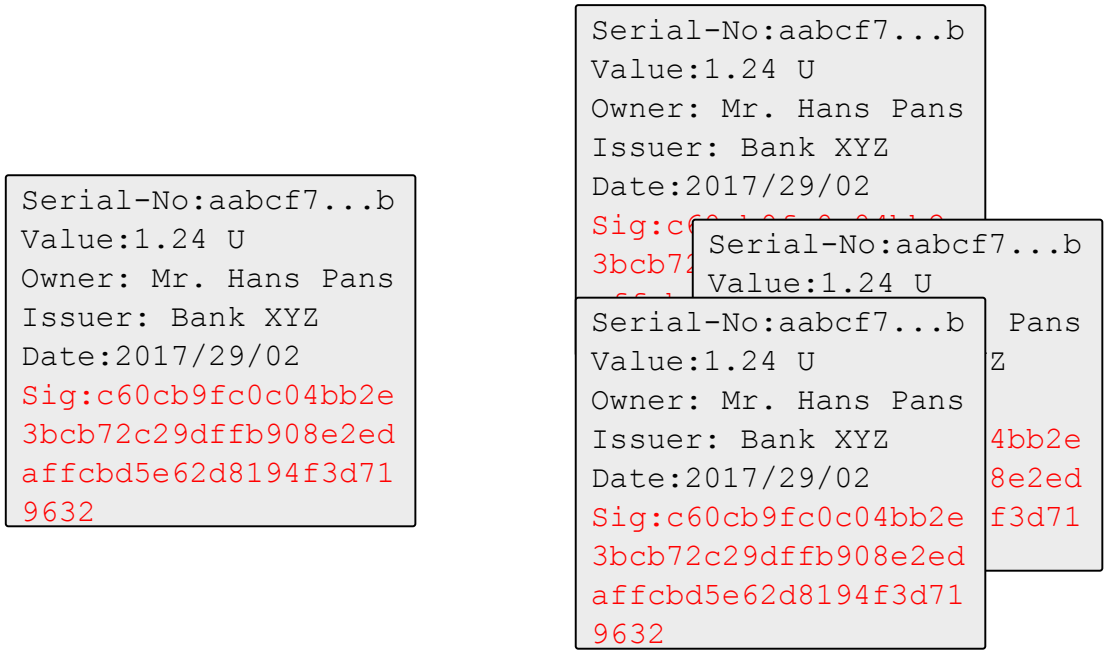
The problem of digital cash

- digital cash: copy and paste, even when certified (just a bunch of data!)



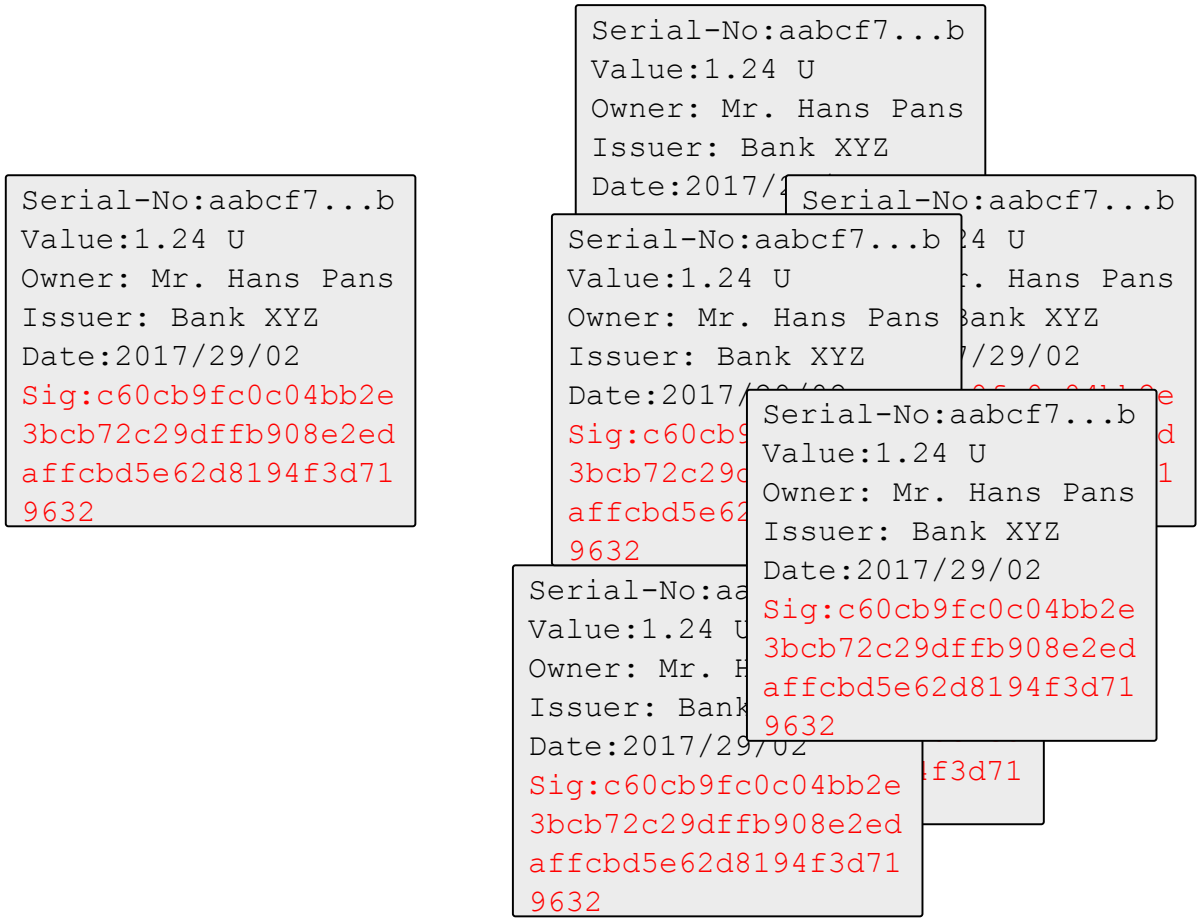
The problem of digital cash

- digital cash: copy and paste, even when certified (just a bunch of data!)



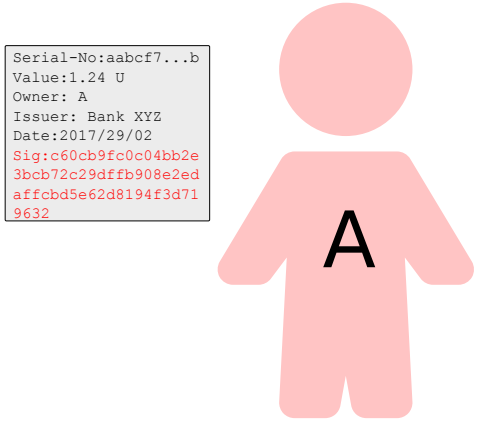
The problem of digital cash

- digital cash: copy and paste, even when certified (just a bunch of data!)



The problem of digital cash

- Double-spending: same certified unit spent twice

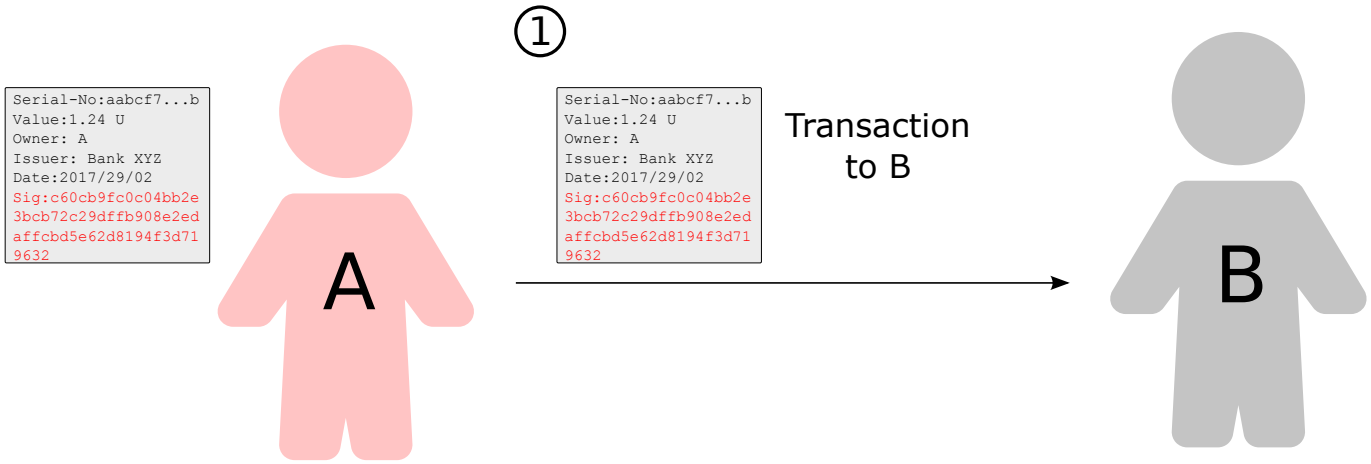


The problem of digital cash

- Double-spending: same certified unit spent twice

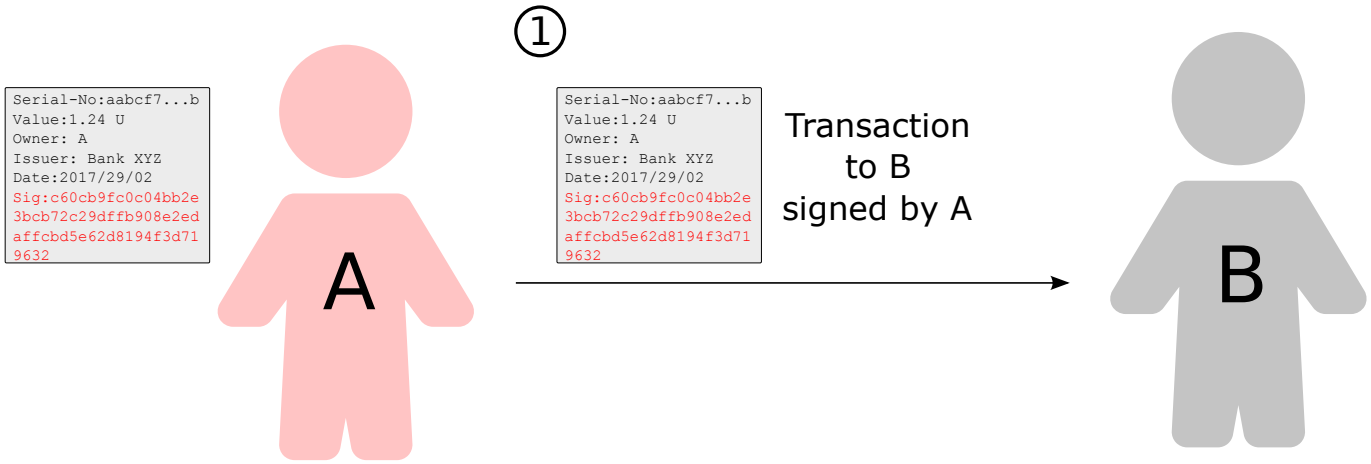
The problem of digital cash

- Double-spending: same certified unit spent twice



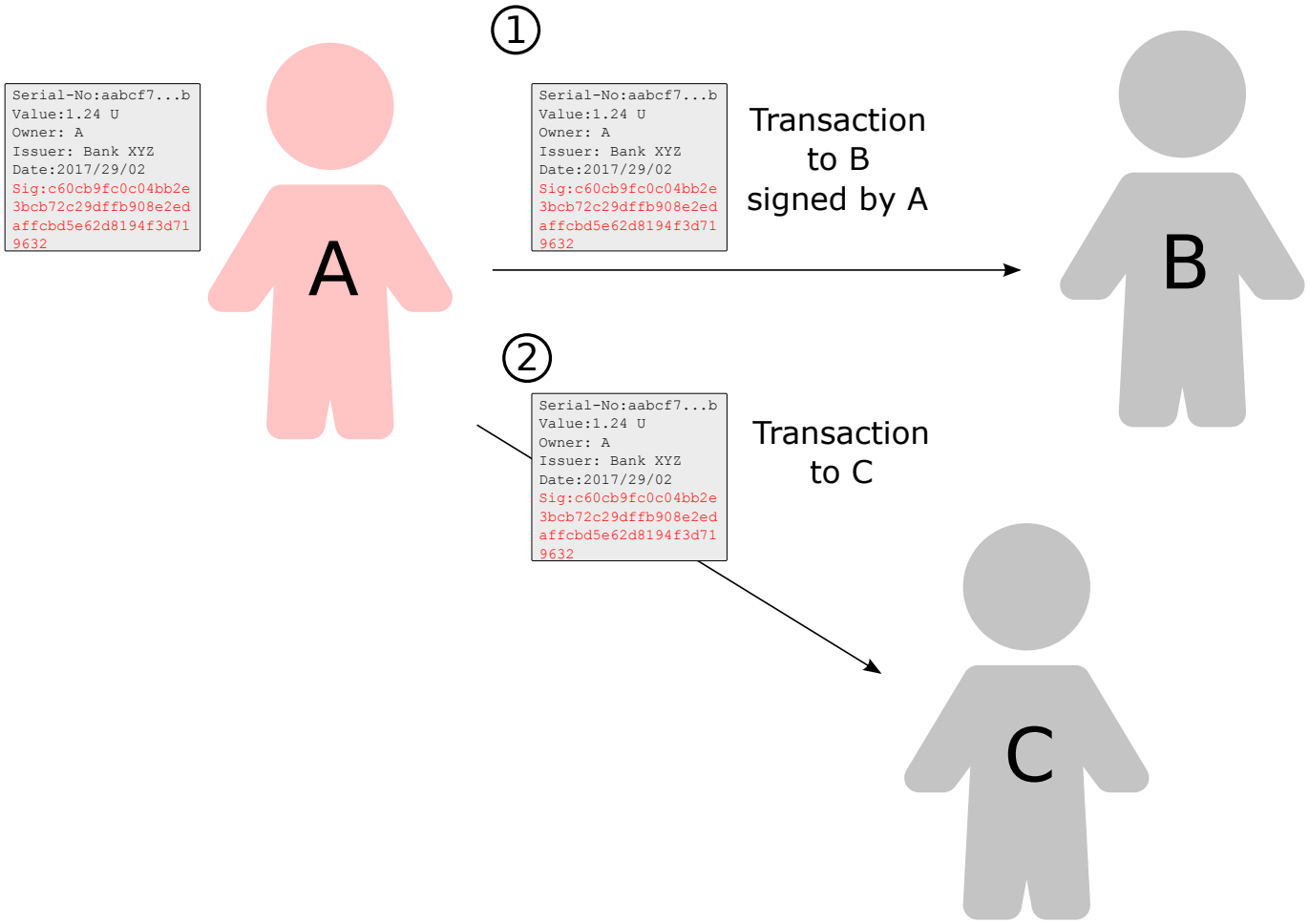
The problem of digital cash

- Double-spending: same certified unit spent twice



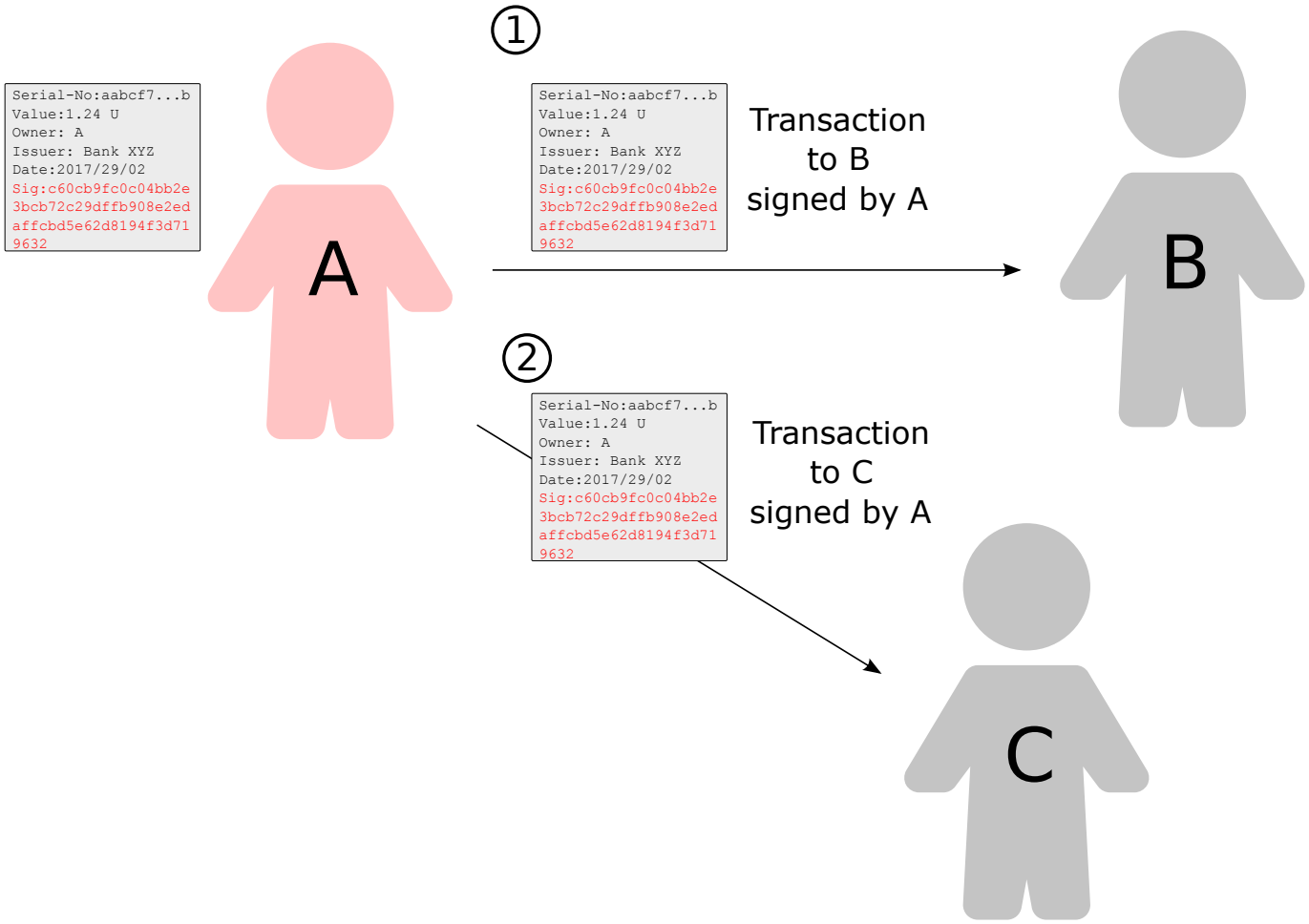
The problem of digital cash

- Double-spending: same certified unit spent twice



The problem of digital cash

- Double-spending: same certified unit spent twice

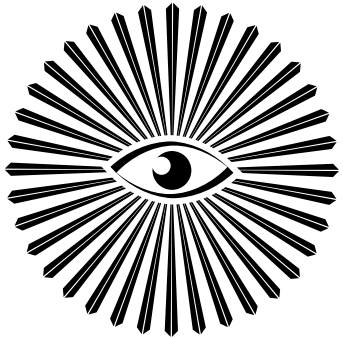


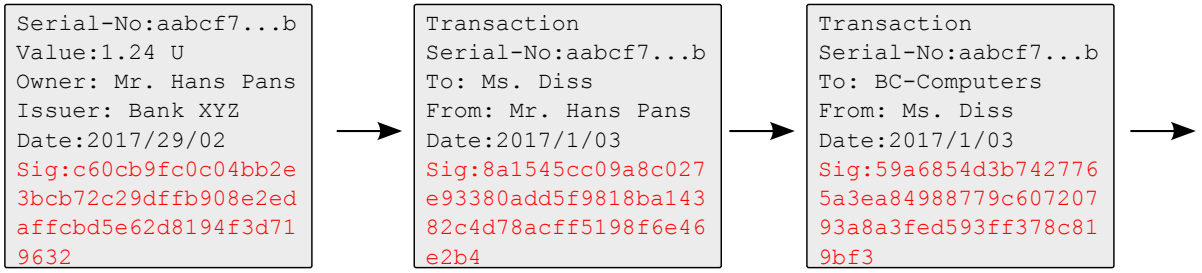
The problem of digital cash

One way to prevent *double-spending*

The problem of digital cash

One way to prevent *double-spending* : online log of *entire* transaction history





The problem of digital cash

Inherent issues:

The problem of digital cash

Inherent issues:

- centralised reglementation (e.g. Bank): set under pressure easily by powerful players,

The problem of digital cash

Inherent issues:

- centralised reglementation (e.g. Bank): set under pressure easily by powerful players,
- decentralised reglementation: robust, secure consensus necessary

Bitcoin

Bitcoin

BITCOIN

Mutmaßlicher Erfinder will Technologie patentieren lassen

Datum: 02.03.2017 16:12 Uhr

Die digitale Währung erlebt derzeit einen Höhenflug: Ein einziger Bitcoin war zuletzt über 1200 US-Dollar wert. Craig Wright sieht sich selbst als Erfinder der Währung und will diese nun mit einem Patent versehen.

Bitcoin

Bitcoins und die Blockchain-Technologie könnten vor einer Patentierung stehen.

Bitcoin

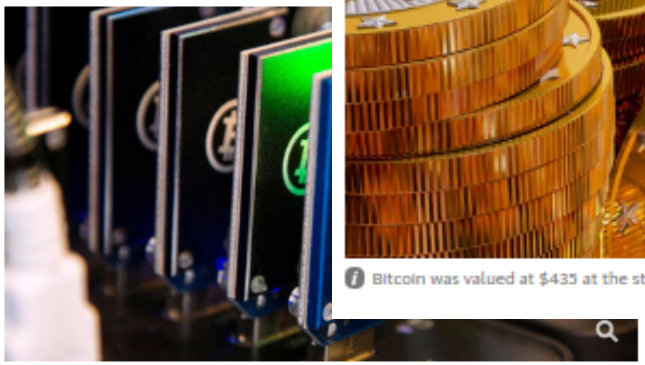
BITCOIN

Mutmaßlicher Erfir Technologie patent

Datum: 02.03.2017 16:12 Uhr

Die digitale Währung erlebt derzeit e einziger Bitcoin war zuletzt über 120 Wright sieht sich selbst als Erfinder nun mit einem Patent versehen.

Facebook Twitter Google



Bitcoin

Bitcoins und die Blockchain-Technologie könnten vor einer Patentierung stehen.

Value of bitcoins in circulation hits record high of $14bn

Price per coin at $875 as cryptocurrency's value doubles in a year, with experts linking it to depreciation of Chinese yuan

Bitcoin was valued at $435 at the start of the year. Photograph: Alamy

FH CAMPUS WIEN

Bitcoin

Dienstag, 14.03.2017 - 19:40 Uhr

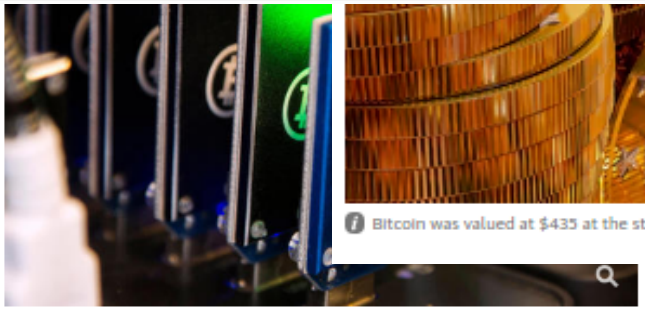
BITCOIN - Nein zum BTC-ETF! Was nun?

Die US-Börsenaufsicht hat letzten Freitag die Zulassung eines Bitcoin-ETFs abgelehnt, worauf der BTC-Kurs um 25% einbrach. Mittlerweile wurden die Verluste fast vollständig aufgeholt. Zeit für eine Aufarbeitung der Geschehnisse der letzten Tage...

ation hits

ibles in a year, with experts

Bitcoin was valued at $435 at the start of the year. Photograph: Alamy



Bitcoin

Bitcoins und die Blockchain-Technologie könnten vor einer Patentierung stehen.

FH CAMPUS WIEN

Bitcoin

Dienstag, 14.03.2017 - 19:40 Uhr

BITCOIN - Nein zum BTC-ETF! Was nun?

Die US-Börsenaufsicht hat letzten Freitag die Zulassung eines Bitcoin-ETFs abgelehnt, worauf der BTC-Kurs um 25% einbrach. Mittlerweile wurden die Verluste fast vollständig aufgeholt. Zeit für eine Aufarbeitung der Geschehnisse der letzten Tage...

ation hits

ibles in a year, with experts

Bitcoin unter Druck: Steht die Kryptowährung vor einer Aufspaltung?

Montag, 27.03.2017 12:42 von Annalee McWilliams

Teilen 2 Twittern G+1 0 0

Die Online-Währung Bitcoin ist in der vergangenen Woche unter die wichtige Marke von 1.000 US-Dollar gefallen. Der Kurs sank binnen weniger Tage um rund 22 Prozent ab. Dabei sorgt nicht nur die nicht erteilte Zulassung für den ersten Bitcoin-ETF durch US-amerikanische Behörden für Gesprächsstoff. Es geht um eine mögliche Aufspaltung der Währung.

Die digitale Währung Bitcoin macht ihrem Ruf als

Spekulation über eine Bitcoin-Aufspaltung sorgen für hohe Volatilität bei der Kryptowährung. - © istock.com/Tsokur

Bitcoin was valued at $435 at the start of the year. Photograph: Alamy

Bitcoin

Bitcoins und die Blockchain-Technologie könnten vor einer Patentierung stehen.

Bitcoin

Dienstag, 14.03.2017 - 19:40 Uhr

BITCOIN - Nein zum BTC-ETF! Was nun?

Die U … ation hits
abgel
Verlu
der le

Teenage bitcoin millionaire can see the cryptocurrency's value shooting as high as $1 million

Published: June 22, 2017 2:30 a.m. ET

106

… iner

Aa

Teilen 2 Twittern G+1 0 0

Die Online-Währung Bitcoin ist in der vergangenen Woche unter die wichtige Marke von 1.000 US-Dollar gefallen. Der Kurs sank binnen weniger Tage um rund 22 Prozent ab. Dabei sorgt nicht nur die nicht erteilte Zulassung für den ersten Bitcoin-ETF durch US-amerikanische Behörden für Gesprächsstoff. Es geht um eine mögliche Aufspaltung der Währung.

Die digitale Währung Bitcoin macht ihrem Ruf als …

Spekulation über eine Bitcoin-Aufspaltung sorgen für hohe Volatilität bei der Kryptowährung. - © istock.com/Tsokur

Bitcoin was valued at $435 at the start of the year. Photograph: Alamy

Bitcoin

Bitcoins und die Blockchain-Technologie könnten vor einer Patentierung stehen.

Bitcoin

Dienstag, 14.03.2017 - 19:40 Uhr

BITCOIN - Nein zum BTC-ETF! Was nun?

Die U
abgel
Verlu
der le

Teena
crypto
$1 mil
Published: Jur

ation hits
e
gh as
iner

By Joseph Young

JUN 20, 2017

Suddenly, Bitcoin to Be Officially Legal in India

75358 Total views 2141 Total shares

Aa

r eine Bitcoin-Aufspaltung
Volatilität bei der
. - © istock.com/Tsokur

Bitcoin

Bitcoins und die Blockchain-Technologie könnten vor einer Patentierung stehen.

Bitcoin

Dienstag, 14.03.2017 - 19:40 Uhr

BITCOIN - Nein zum BTC-ETF! Was nun?

Die U Teena
abgel
Verlu crypto
der le $1 mil
Published: Jur

ation hits
JUN 20, 2017
e
gh as
iner

By Joseph Young

Suddenly, Bitcoin to Be Officially Legal in India

75358 Total views 2141 Total shares

Aa

Move Over, Bitcoin. Ether Is the Digital Currency of the Moment.

By NATHANIEL POPPER JUNE 19, 2017

Bitcoin

Bitcoins und die Blockchain-Technologie könnten vor einer Patentierung stehen.

r eine Bitcoin-Aufspaltung
Volatilität bei der
. - © istock.com/Tsokur

Bitcoin

Dienstag, 14.03.2017 - 19:40 Uhr

BITCOIN - Nein zum BTC-ETF! Was nun?

Die U Teena abgel Verlu crypto der le $1 mil

Published: Jur

ation hits

JUN 20, 2017

By Joseph Young

Suddenly, Bitcoin to Be Officially Legal in India

gh as

iner

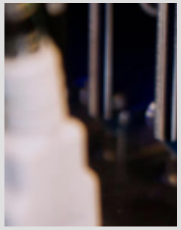
75358 Total views 2141 Total shares

Aa

What is Bitcoin?

Move Over, Bitcoin. Ether Is the Digital Currency of the Moment.

By NATHANIEL POPPER JUNE 19, 2017



Bitcoin

Bitcoins und die Blockchain-Technologie könnten vor einer Patentierung stehen.

r eine Bitcoin-Aufspaltung
Volatilität bei der
. - © istock.com/Tsokur

Bitcoin

Bitcoin

- is a digital currency

Bitcoin

- is a digital currency
- (partially) anonymous (*pseudonymous*)

Bitcoin

- is a digital currency
- (partially) anonymous (*pseudonymous*)
- decentralised, based on *blockchain* technology

Bitcoin

- 1992: E.Hughes, T.May: cipherpunks

Bitcoin

- 1992: E.Hughes, T.May: cipherpunks
- 1997,98: Proof of work to mitigate spam emails (*hash cash*), W.Dai's *b-money*, N.Szabo's *Bit Gold*

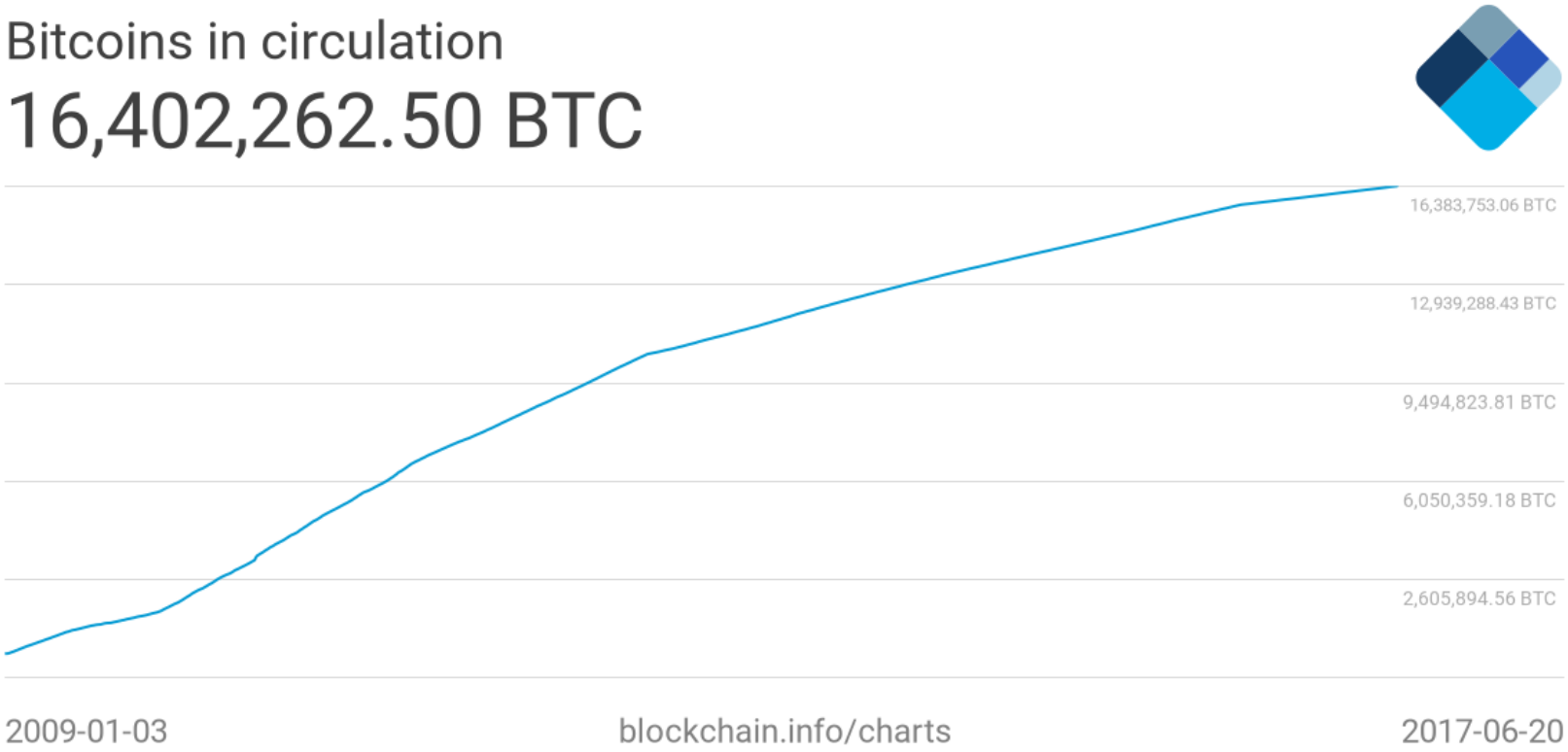
Bitcoin

- 1992: E.Hughes, T.May: cipherpunks
- 1997,98: Proof of work to mitigate spam emails (*hash cash*), W.Dai's *b-money*, N.Szabo's *Bit Gold*
- 2008: S. Nakamoto's white paper on Bitcoin

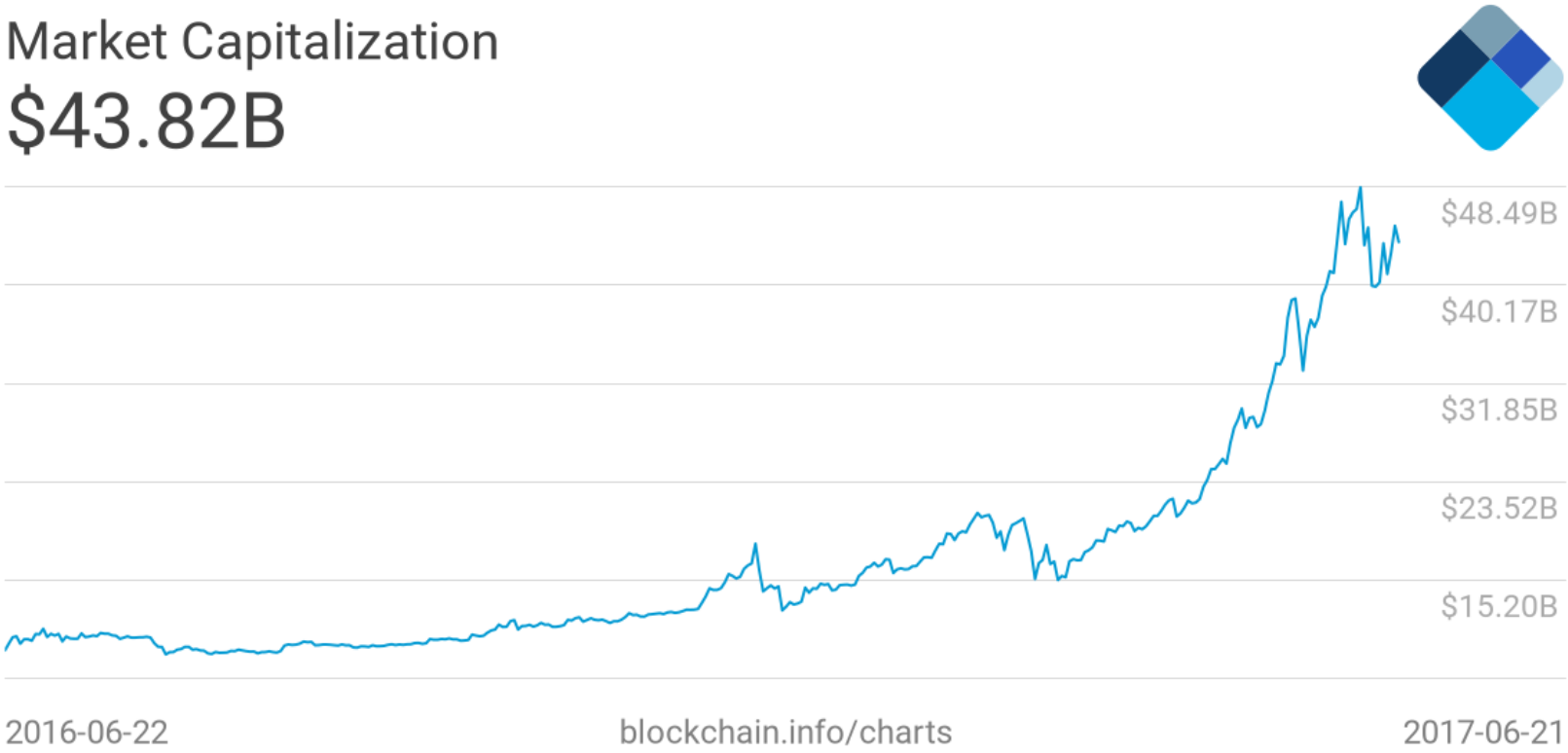
Bitcoin

- 1992: E.Hughes, T.May: cipherpunks
- 1997,98: Proof of work to mitigate spam emails (*hash cash*), W.Dai's *b-money*, N.Szabo's *Bit Gold*
- 2008: S. Nakamoto's white paper on Bitcoin
- Jan 2009: initial release of bitcoin core (Windows), first bitcoin network in practice

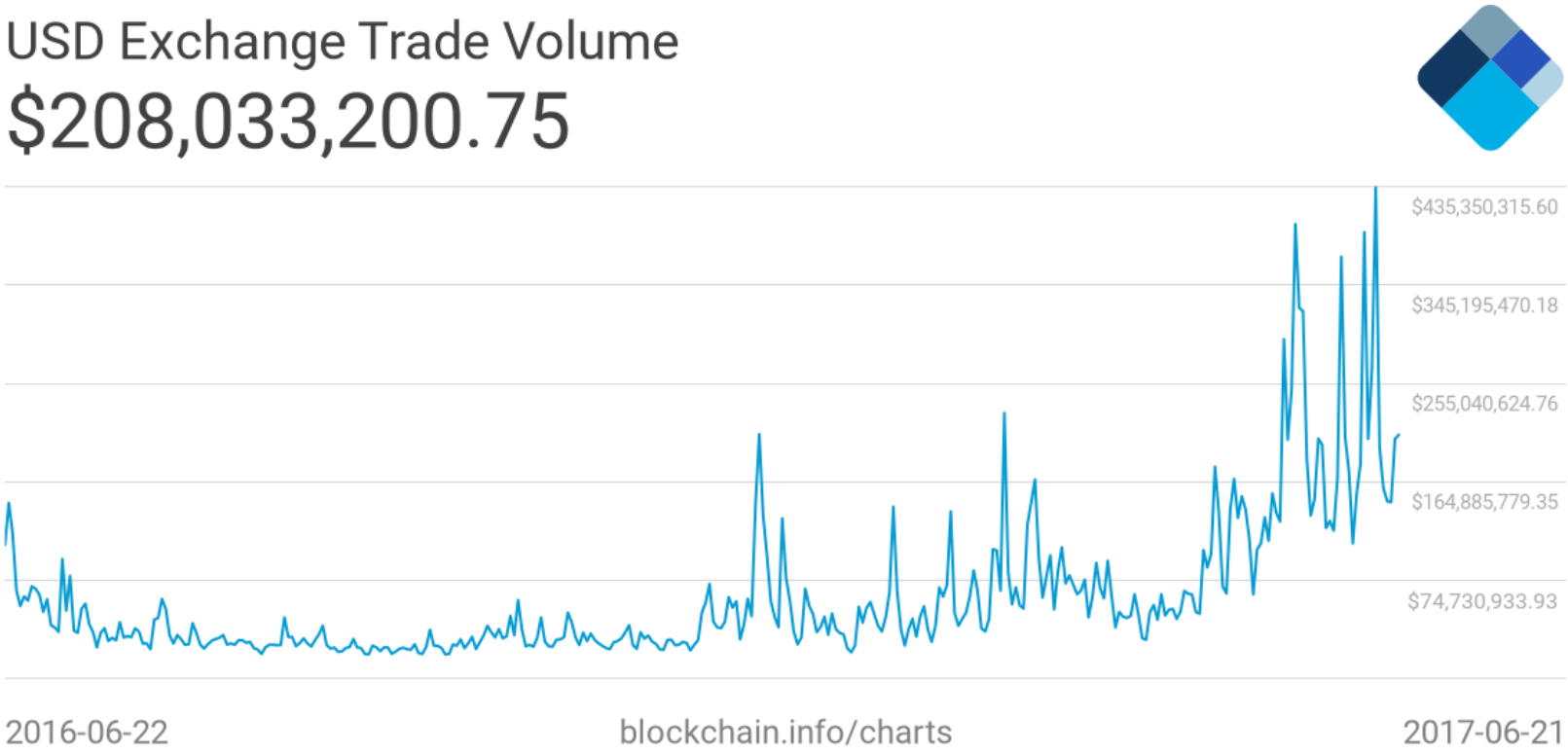
Bitcoin


Bitcoins in circulation
16,402,262.50 BTC
16,383,753.06 BTC
12,939,288.43 BTC
9,494,823.81 BTC
6,050,359.18 BTC
2,605,894.56 BTC
2009-01-03
blockchain.info/charts
2017-06-20

Bitcoin

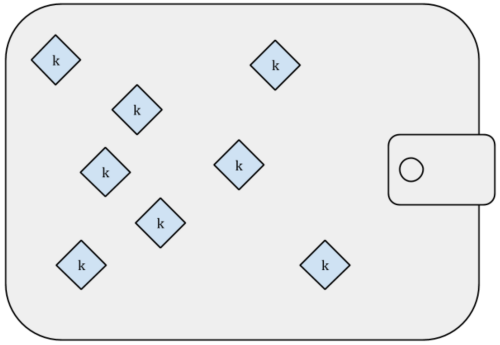

Market Capitalization
$43.82B
$48.49B
$40.17B
$31.85B
$23.52B
$15.20B
2016-06-22
blockchain.info/charts
2017-06-21

Bitcoin


USD Exchange Trade Volume
$208,033,200.75
$435,350,315.60
$345,195,470.18
$255,040,624.76
$164,885,779.35
$74,730,933.93
2016-06-22
blockchain.info/charts
2017-06-21

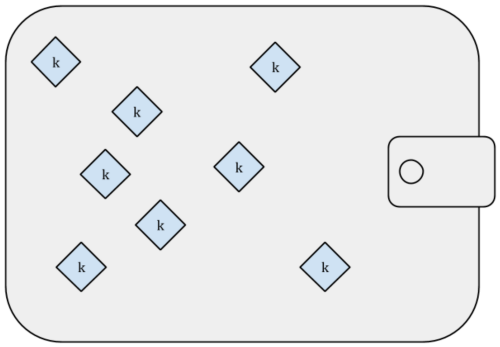
Bitcoin wallets

Every participant (user) can create a wallet full of *random keys* (Bitcoin addresses)



Bitcoin wallets

Every participant (user) can create a wallet full of *random keys* (Bitcoin addresses)

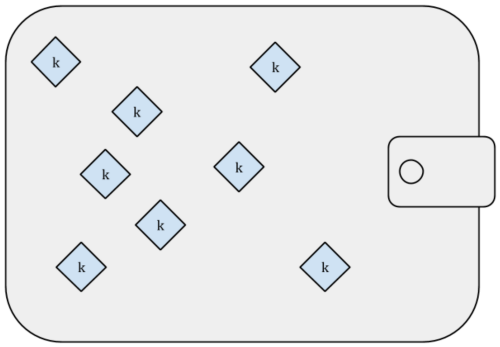


e.g.

`1D3hJ52SXjZamJDSWHN4w6qPwYYDS6zFxq`, or
`3J6atJNyitmTCmoE4e26w5tTceVBtYQ7TY`, or
`1AYDLj29QcTgYNc86umbwdyDV3CgCBvu1f`.

Bitcoin wallets

Every participant (user) can create a wallet full of *random keys* (Bitcoin addresses)



e.g.

`1D3hJ52SXjZamJDSWHN4w6qPwYYDS6zFxq`, or
`3J6atJNyitmTCmoE4e26w5tTceVBtYQ7TY`, or
`1AYDLj29QcTgYNc86umbwdyDV3CgCBvu1f`.

addresses are not a-priori bound to any value!

Transactions

tx

Transaction

bbe597aa8216e66b29f54f223d783e6de9b7373e6e66f0e6d19d289c98841f20

17Pzib2jtmEwLePkczNPP2gDbo5BnfR6uZ (0.0768146 BTC - Output)

12tAEpaJtQcwdfWSEZc2wjcGDg5eqjknPt - (Unspent)

1PvArGhDLiPRvUyA4PtWqBwGHVD8xwbHUF 0.03146665 BTC

- (Unspent) 0.04374795 BTC

1 Confirmations | 0.0752146 BTC

Transactions

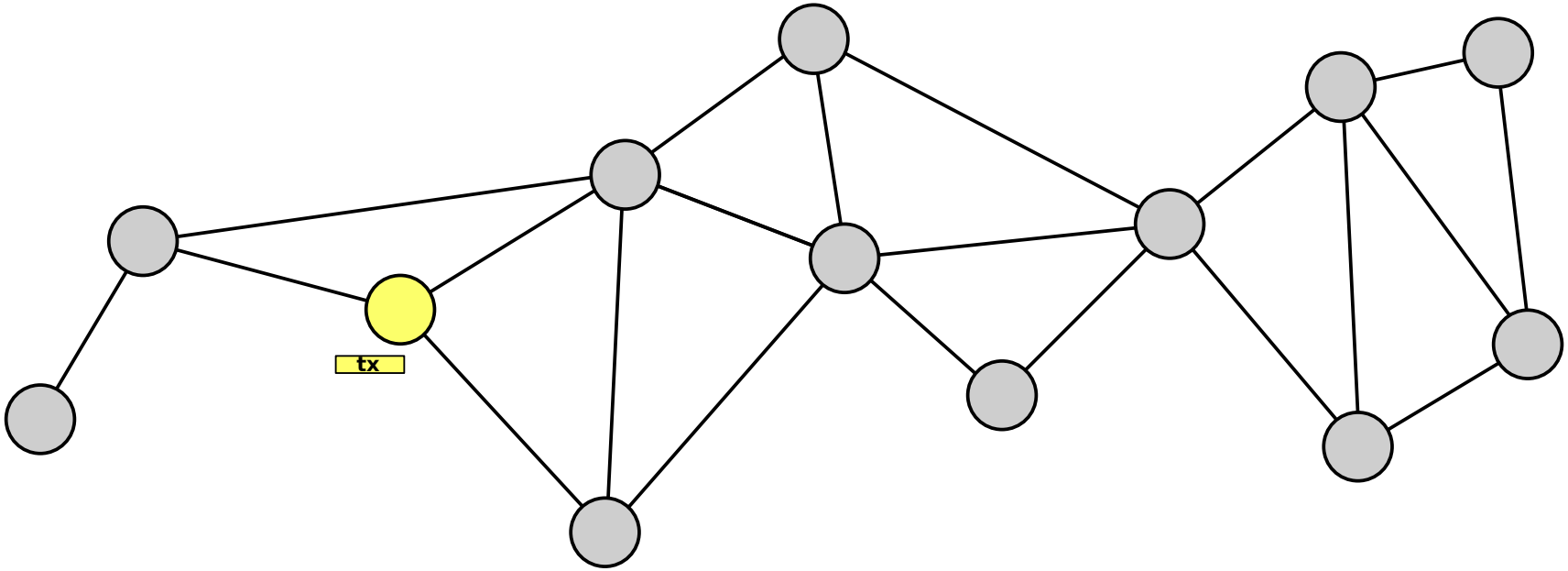
tx

Transaction

$\longrightarrow$ signed with the key of incoming address

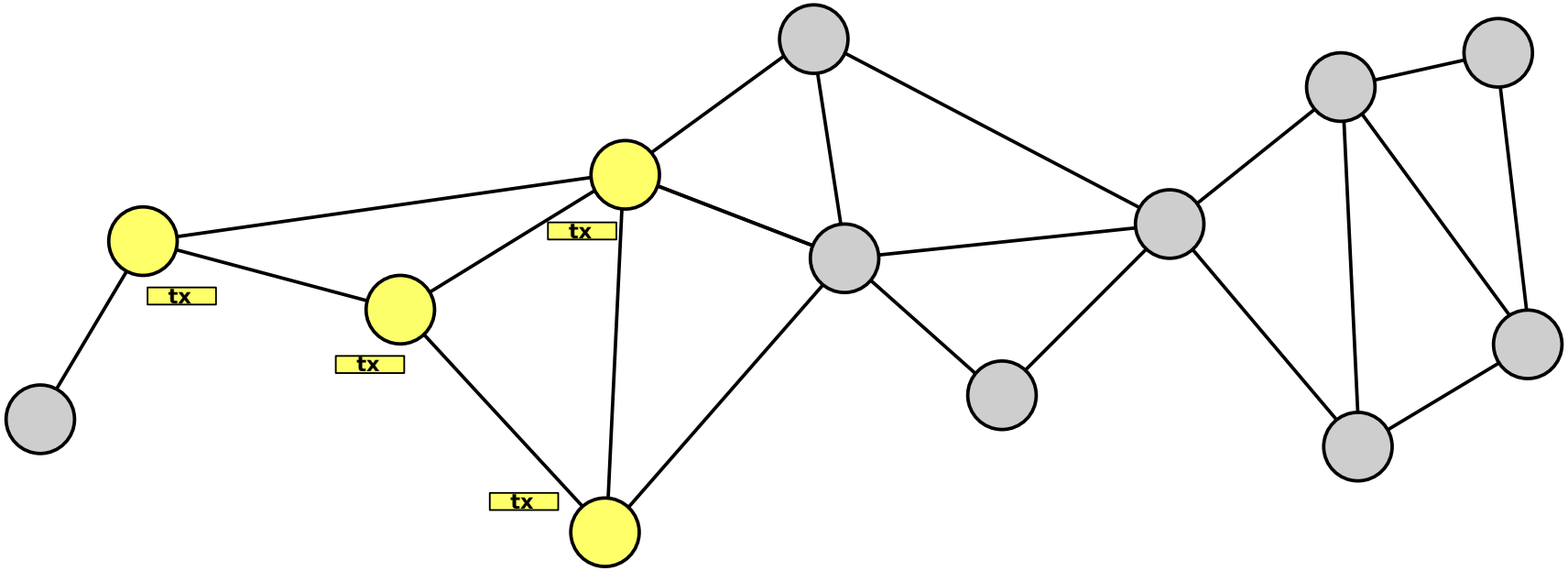
Transactions

. . . are distributed over Bitcoins P2P-network



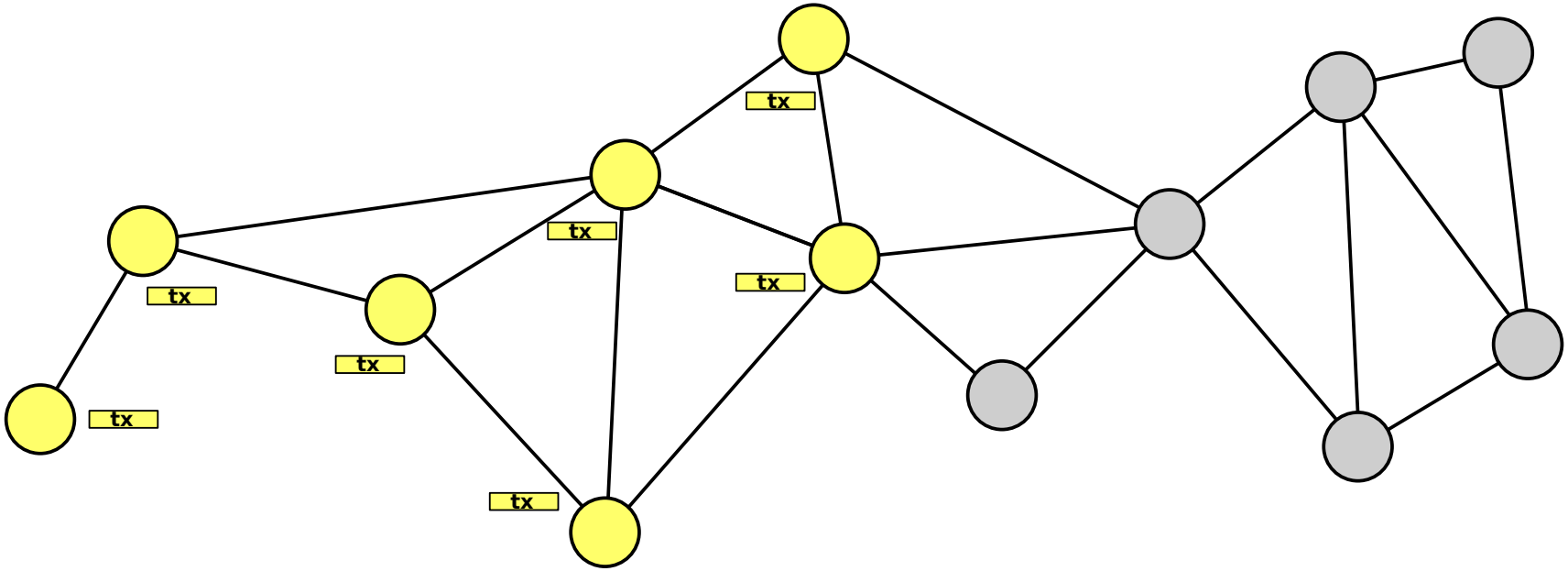
Transactions

. . . are distributed over Bitcoins P2P-network



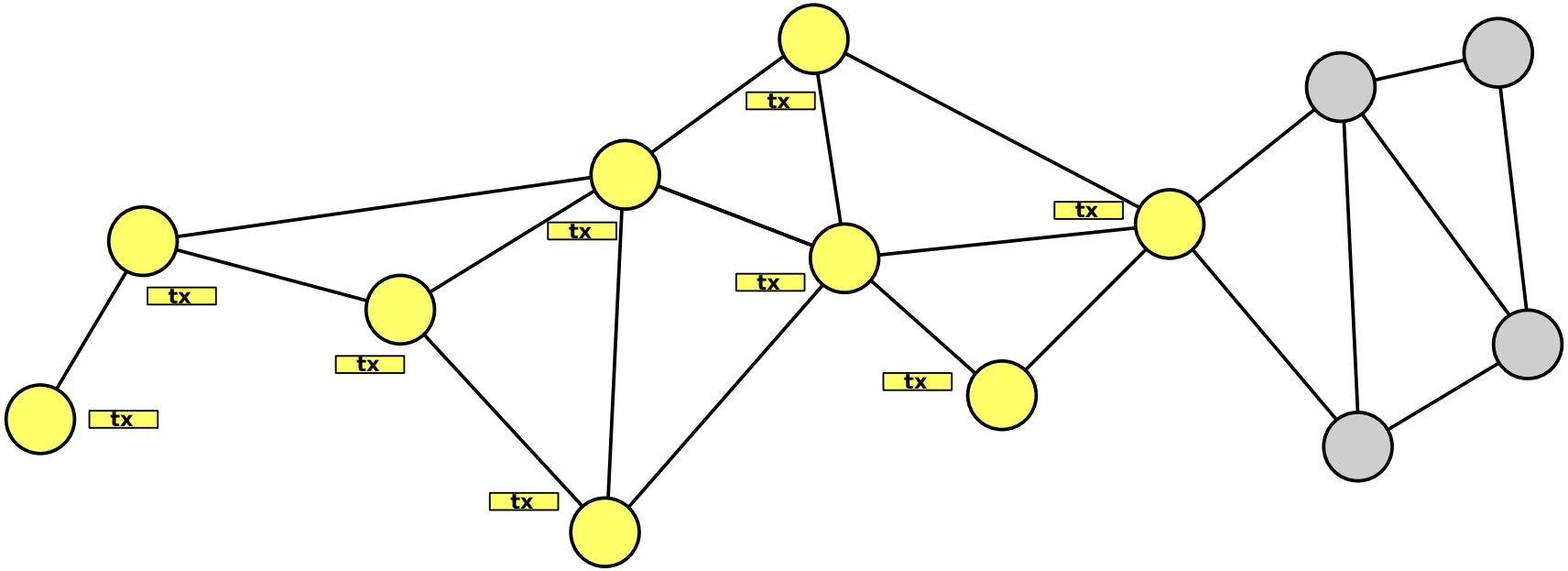
Transactions

. . . are distributed over Bitcoins P2P-network



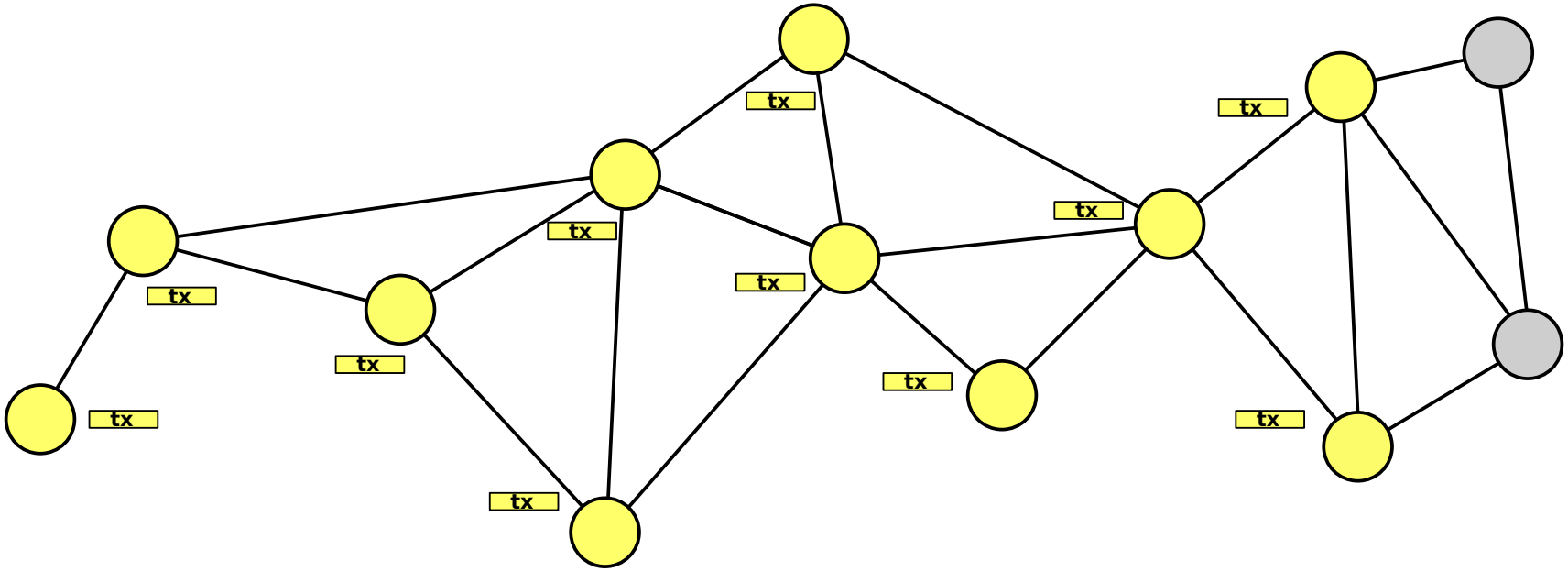
Transactions

. . . are distributed over Bitcoins P2P-network



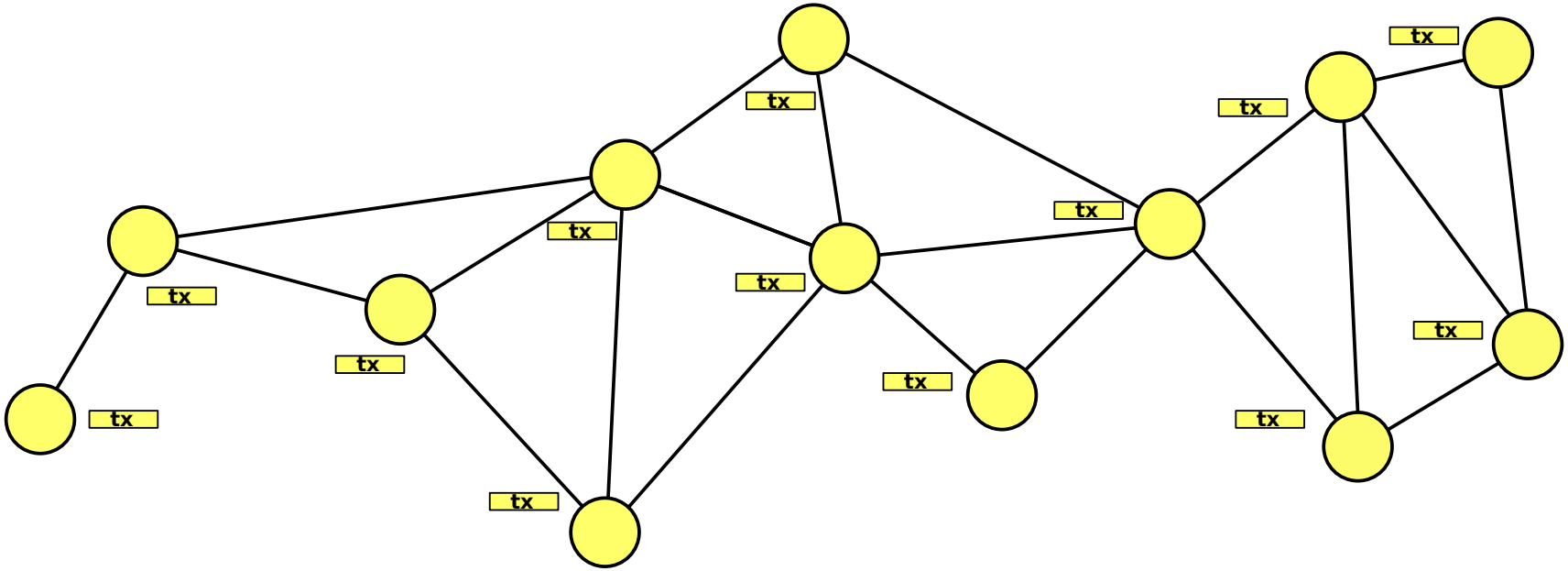
Transactions

. . . are distributed over Bitcoins P2P-network



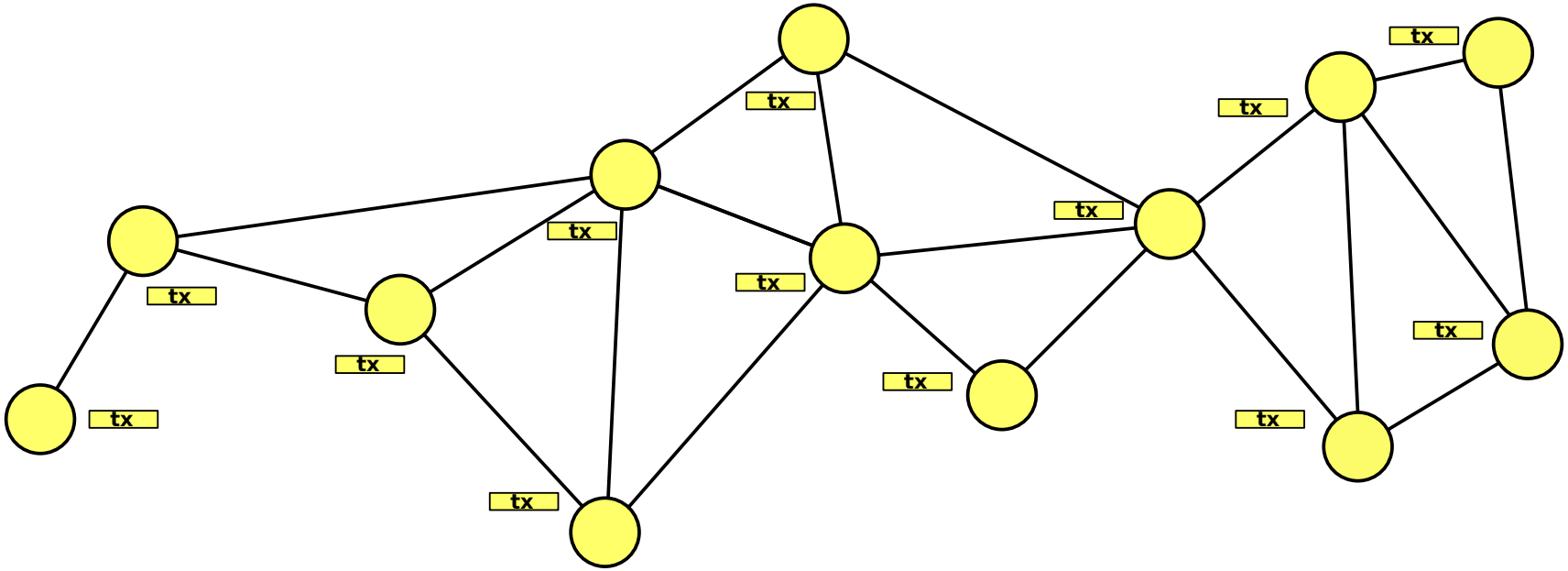
Transactions

. . . are distributed over Bitcoins P2P-network



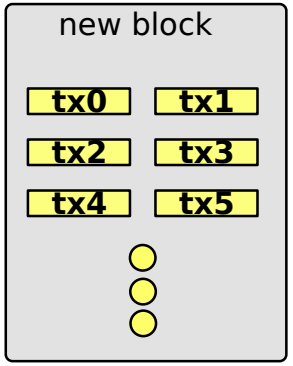
Transactions

. . . are distributed over Bitcoins P2P-network



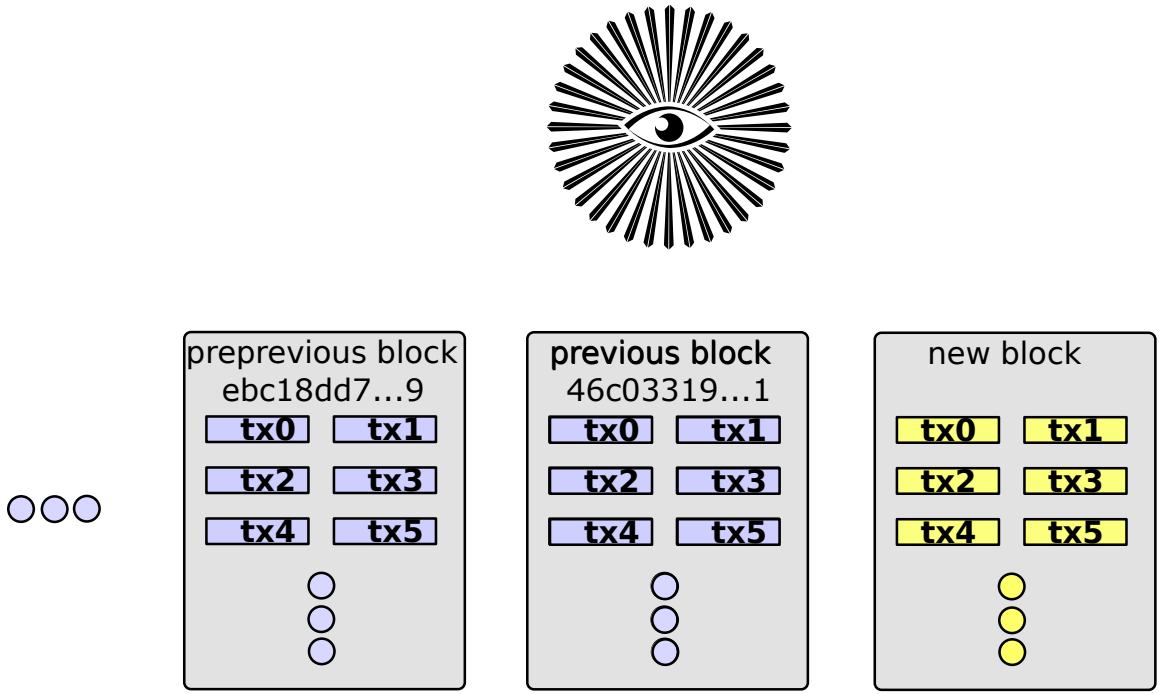
verified & collected by *full nodes* in Mempool

Blockchain & mining



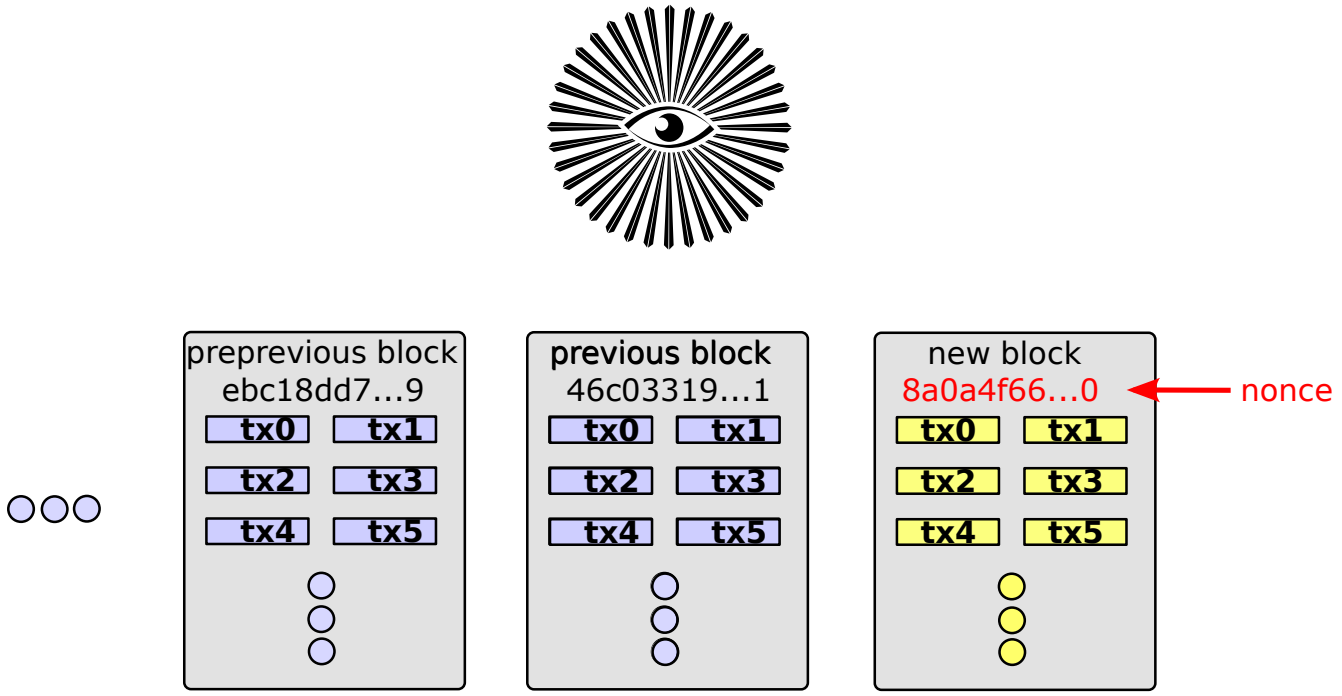
so-called *miners* take tx's from Mempool in block

Blockchain & mining



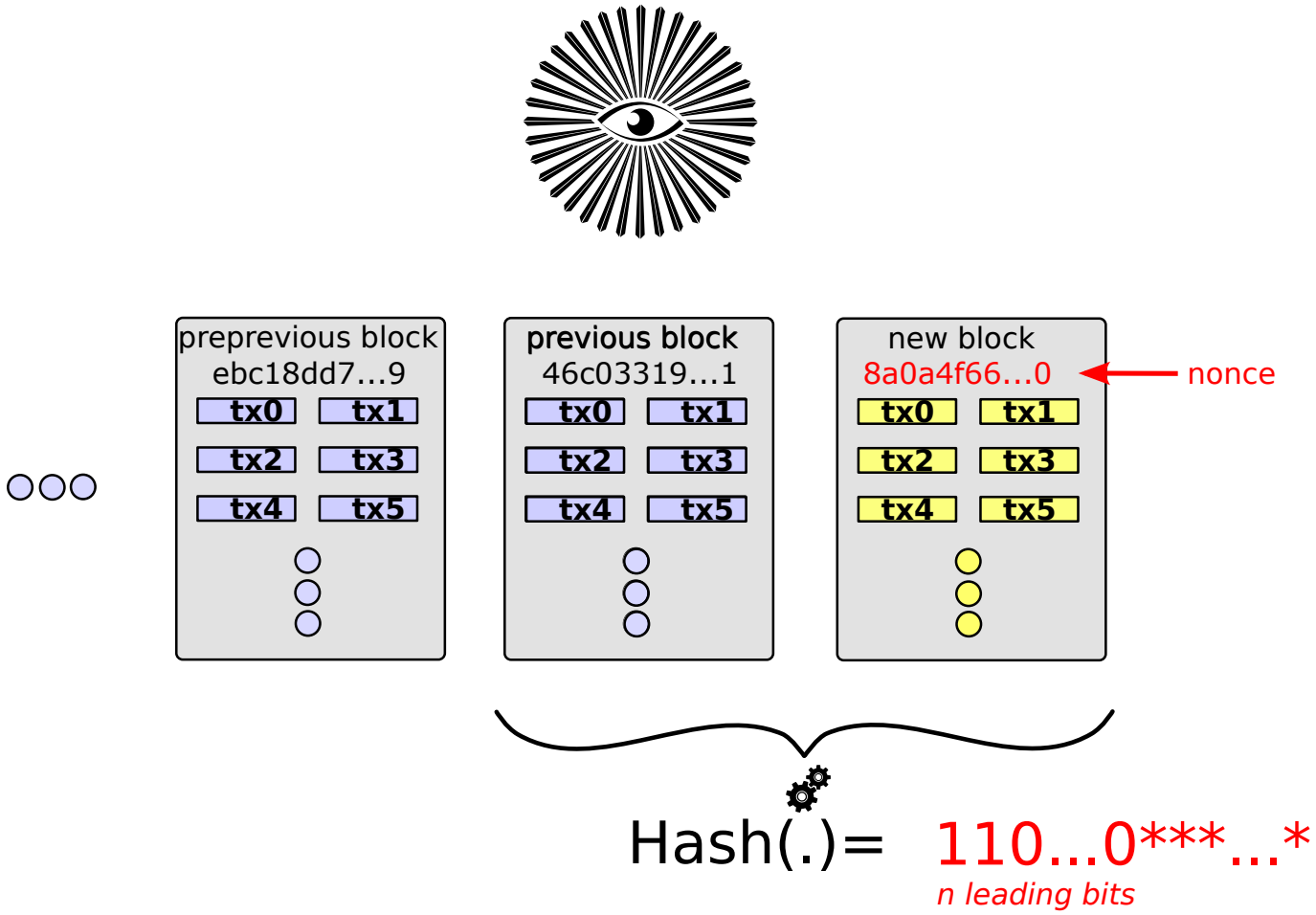
and solve a block depending puzzle

Blockchain & mining



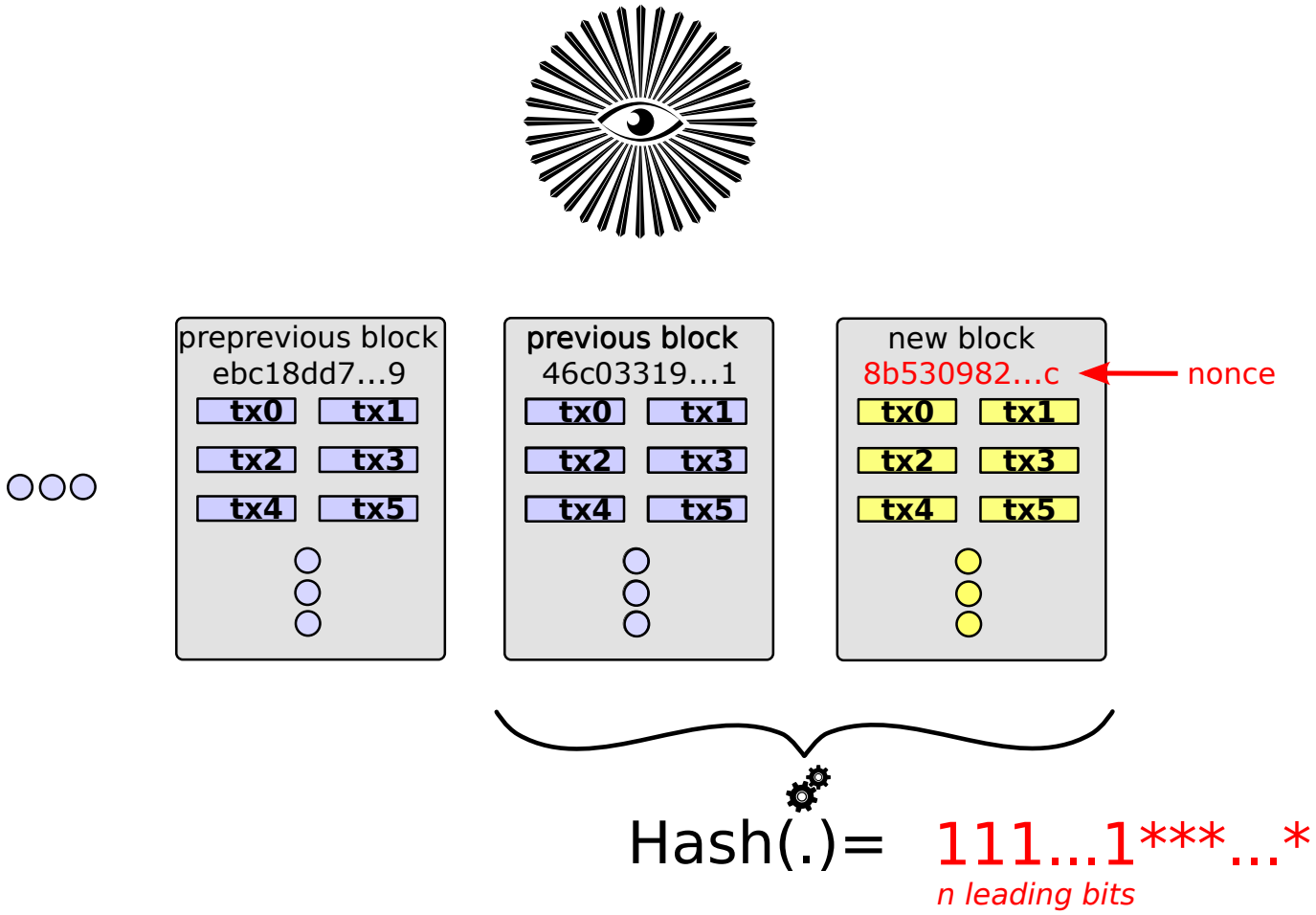
and solve a block depending puzzle

Blockchain & mining



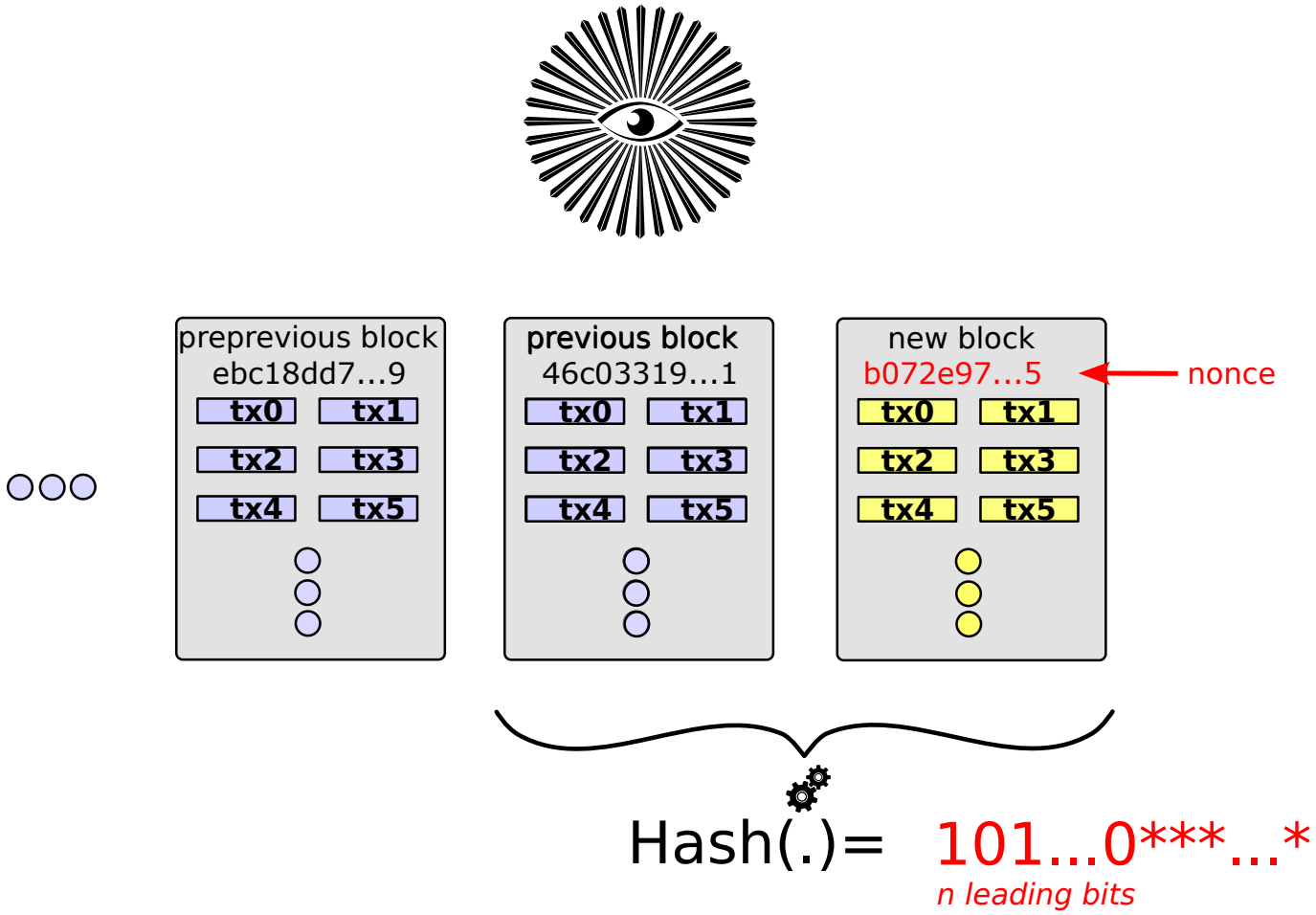
and solve a block depending puzzle

Blockchain & mining



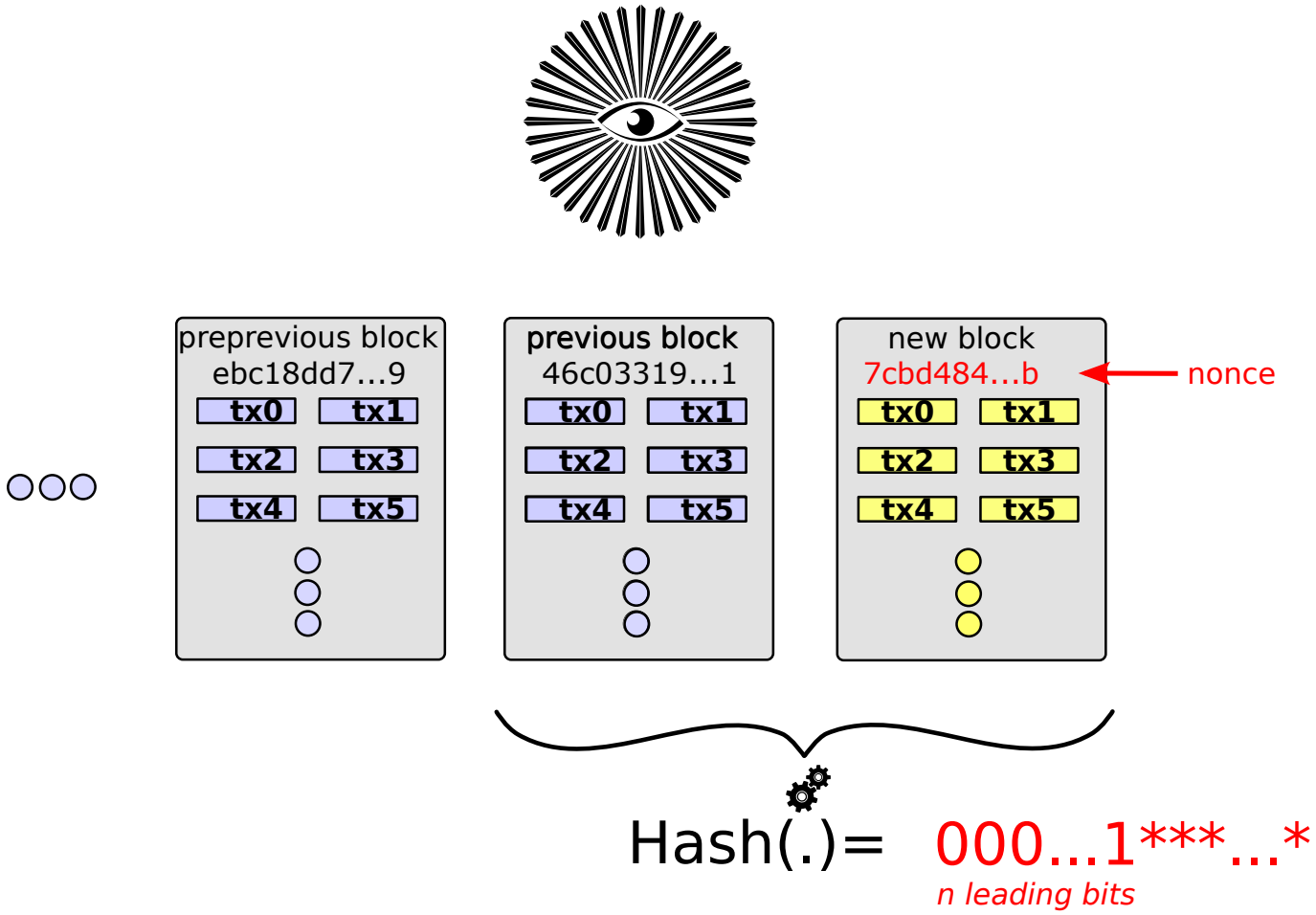
and solve a block depending puzzle

Blockchain & mining



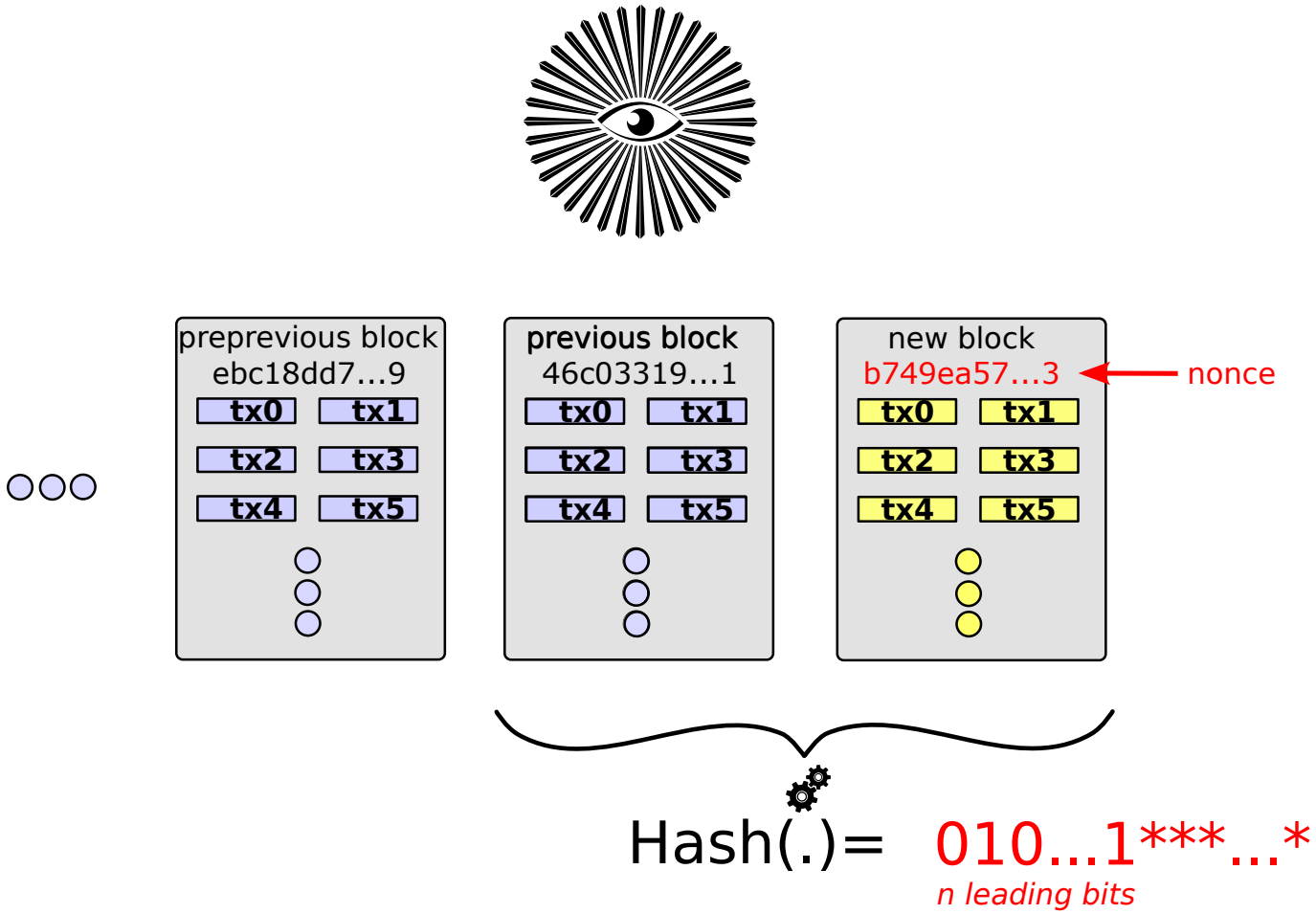
and solve a block depending puzzle

Blockchain & mining



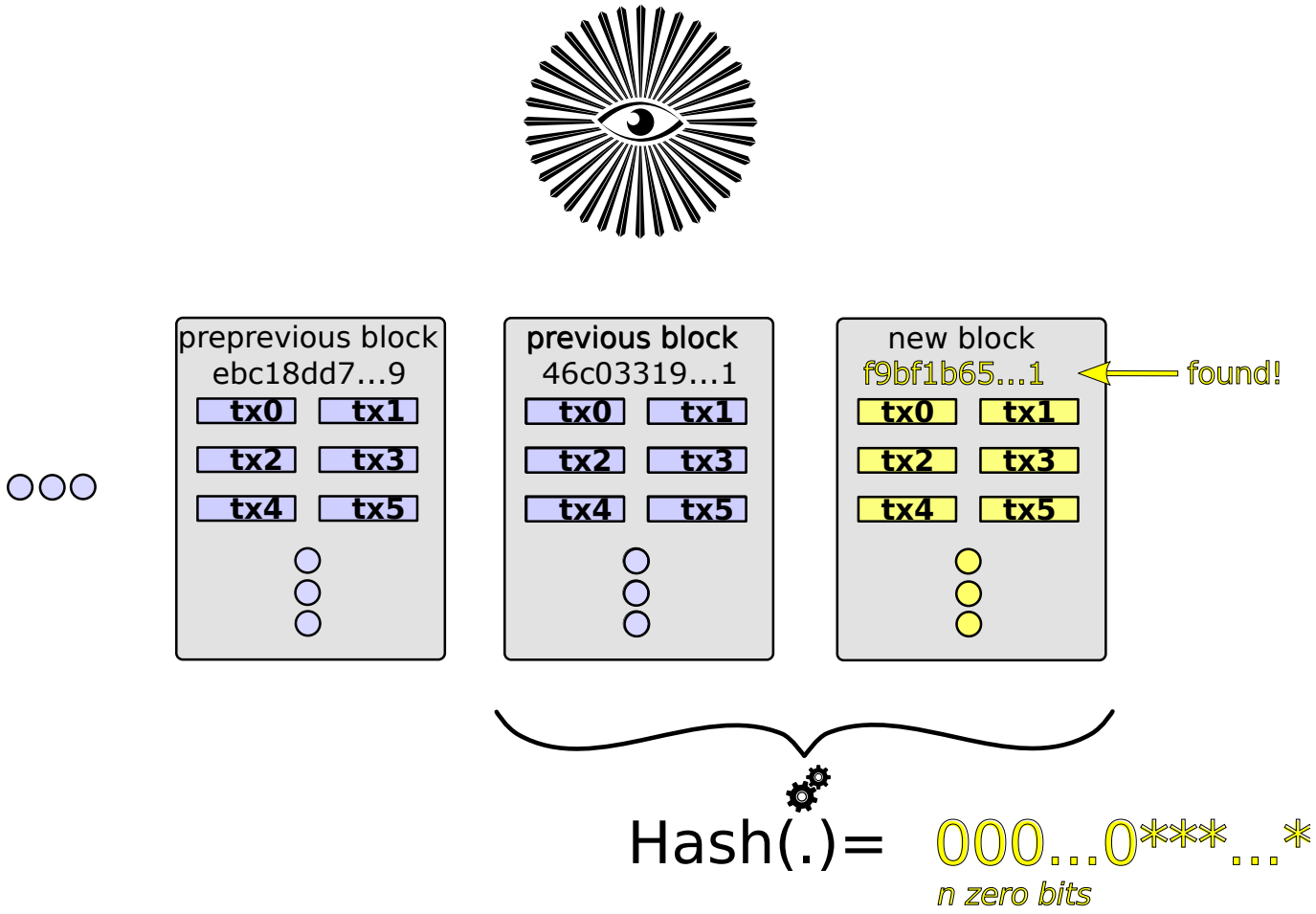
and solve a block depending puzzle

Blockchain & mining



and solve a block depending puzzle

Blockchain & mining



and solve a block depending puzzle

Blockchain & mining

- When nonce found $\longrightarrow$ miner distributes *Block + nonce* over the network.

Blockchain & mining

- When nonce found $\longrightarrow$ miner distributes *Block + nonce* over the network.
- Miner receives

Blockchain & mining

- When nonce found $\longrightarrow$ miner distributes *Block + nonce* over the network.
- Miner receives

  reward (newly generated, mined coins)

Blockchain & mining

- When nonce found $\longrightarrow$ miner distributes *Block + nonce* over the network.
- Miner receives

  reward (newly generated, mined coins)
  + transaction fees

Why the puzzle??

Why the puzzle??

Proof of work is essential for stable and robust consensus

Why the puzzle??

Proof of work is essential for stable and robust consensus

+

yields the basis of worth for the currency (like gold was for traditional currencies)

Difficulty

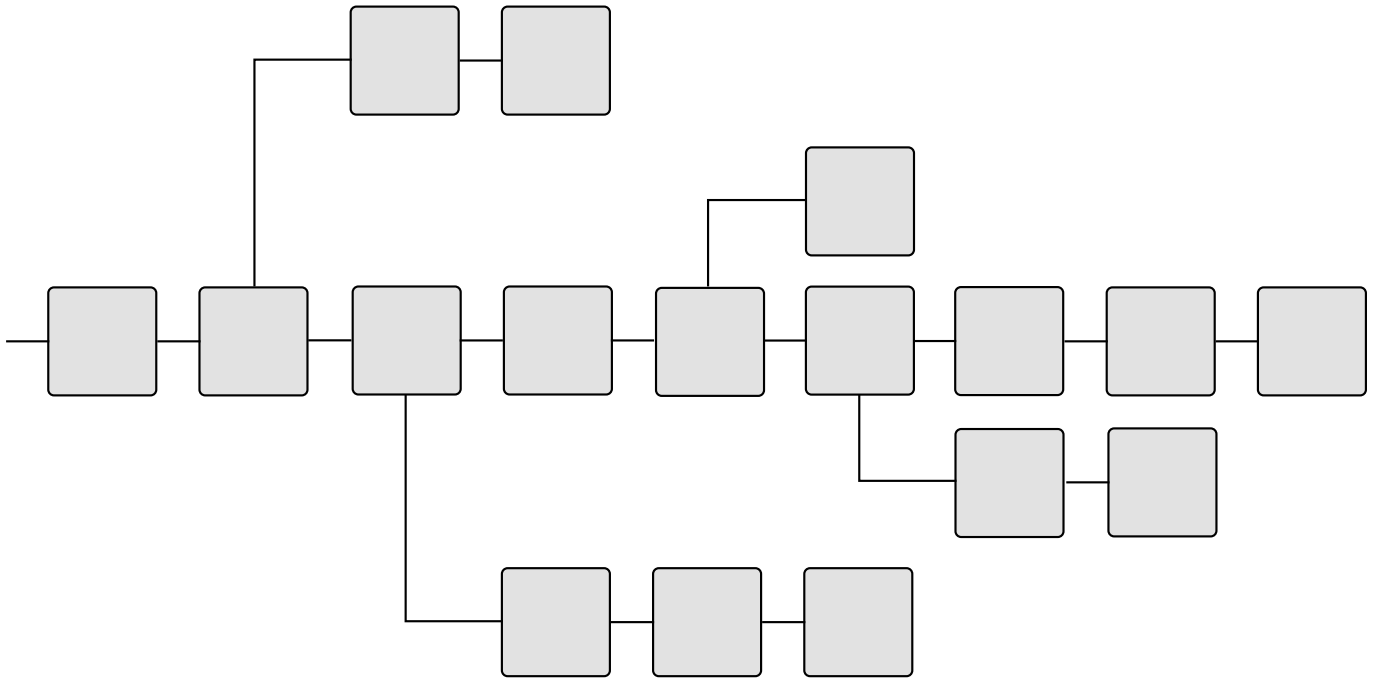
As of June 2017, hash puzzles have a difficulty of ≈ 75 leading zero Bits, e.g.

```
h=000000000000000002f47c8785c85cd6
      e7dc5e8249ebb7c9ba065408ec03209
```

The consensus mechanism

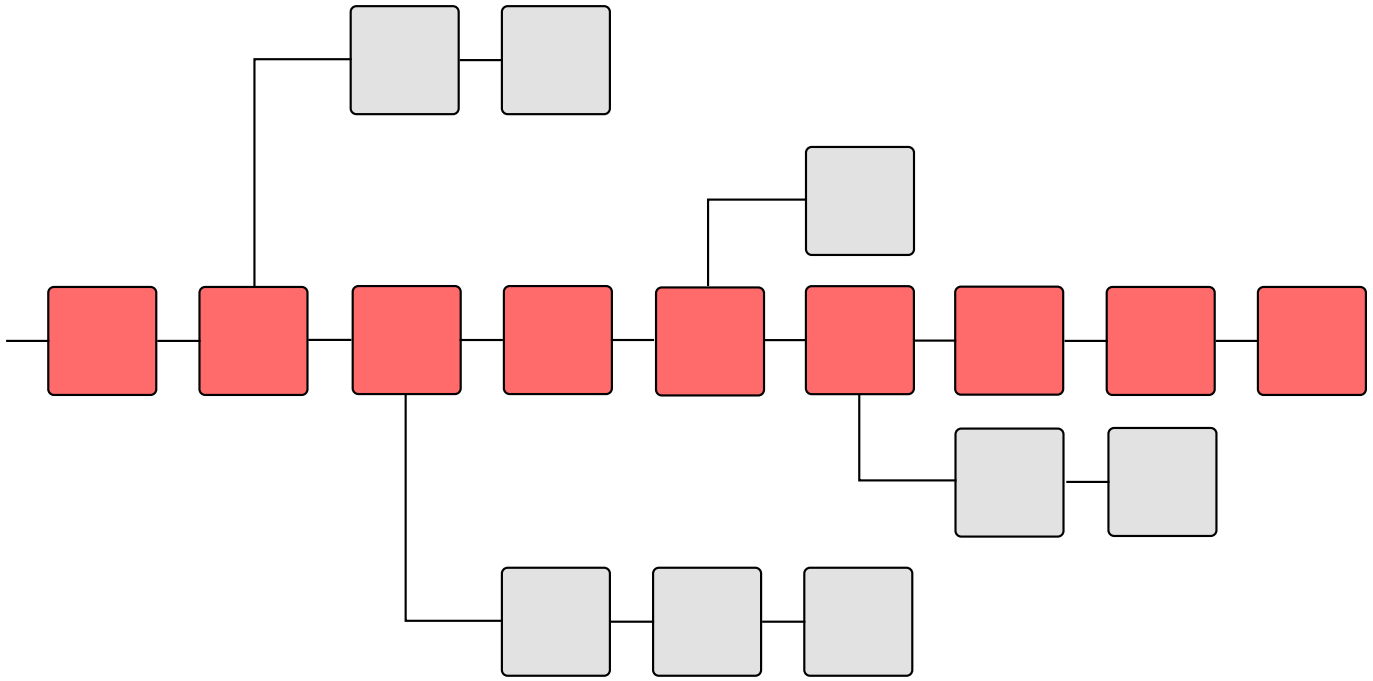
The consensus mechanism

Rule:



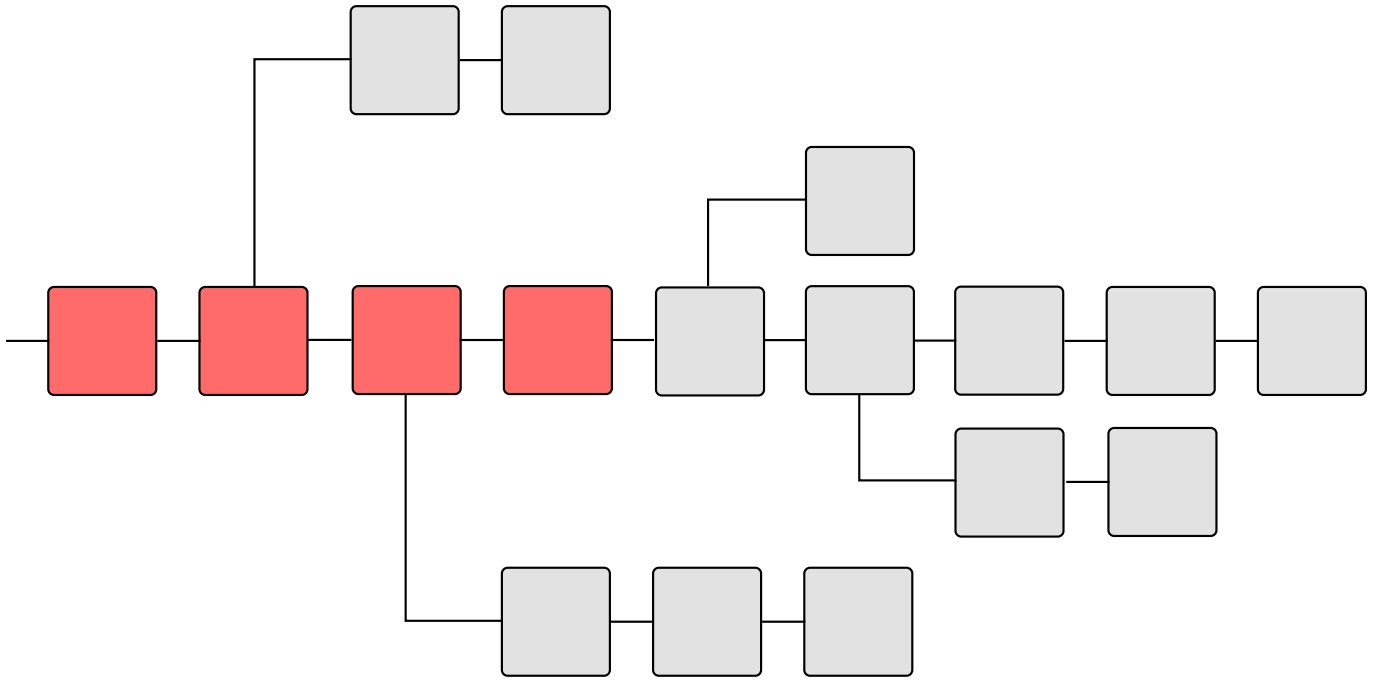
The consensus mechanism

Rule: Truth is defined by the longest chain



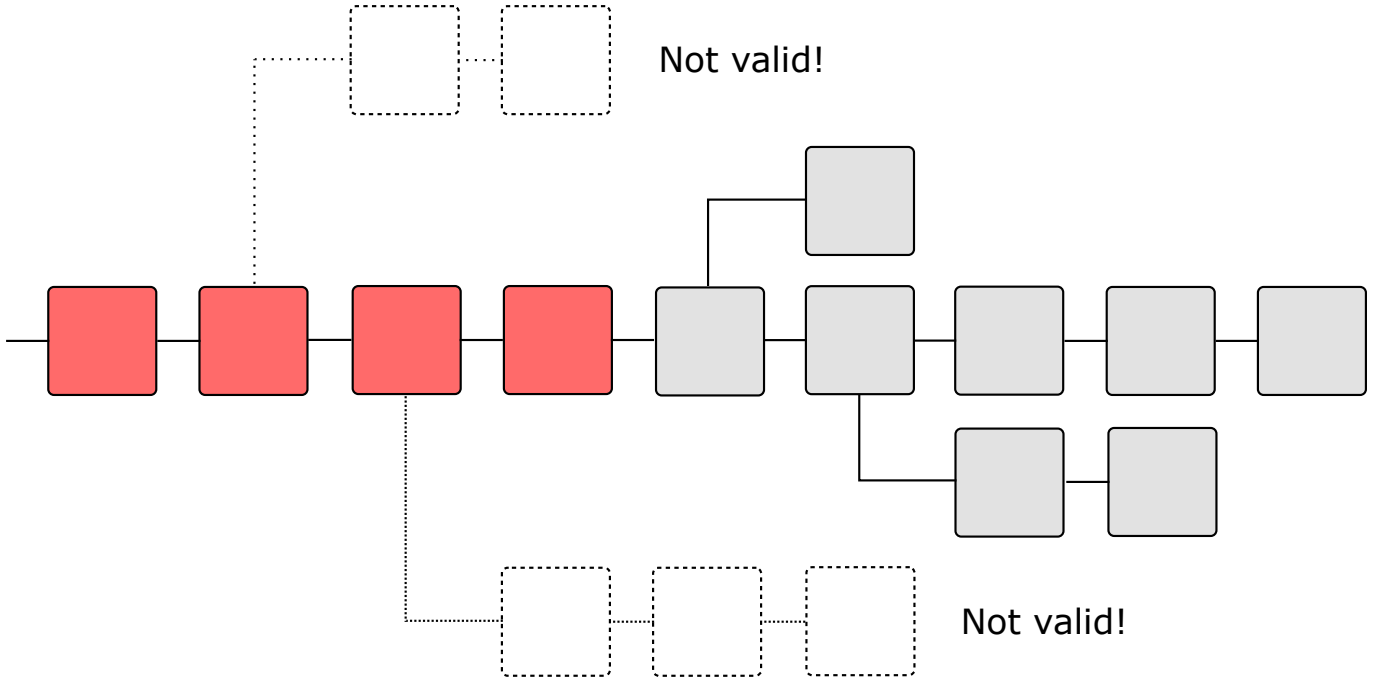
The consensus mechanism

Rule: Truth is defined by the longest chain (minus last five blocks)



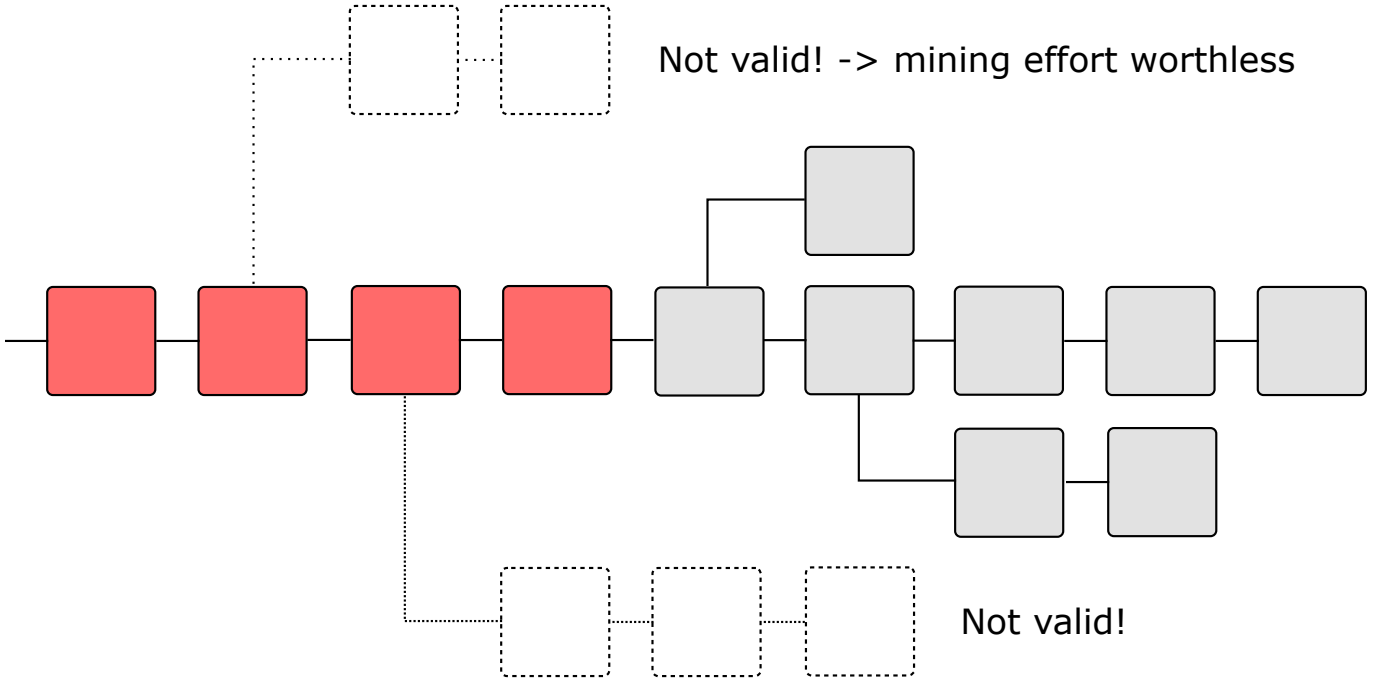
The consensus mechanism

Rule: Truth is defined by the longest chain (minus last five blocks)



The consensus mechanism

Rule: Truth is defined by the longest chain (minus last five blocks)



The consensus mechanism

Hence miners always work on *longest* chain

The consensus mechanism

Hence miners always work on *longest* chain

- it is the most profit promising

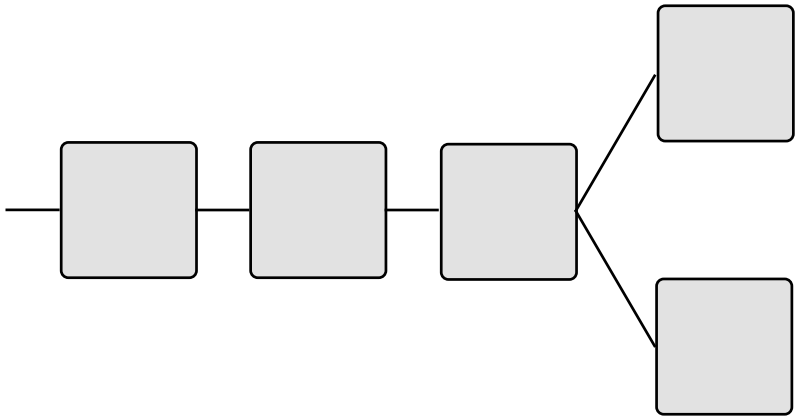
The consensus mechanism

Hence miners always work on *longest* chain

- it is the most profit promising
- otherwise mining effort eventually rewardless

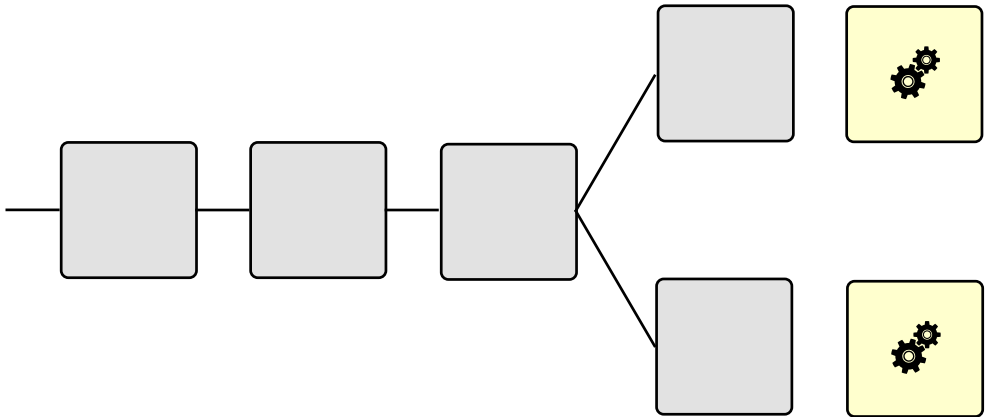
The consensus mechanism

Stability: forks are not stable!



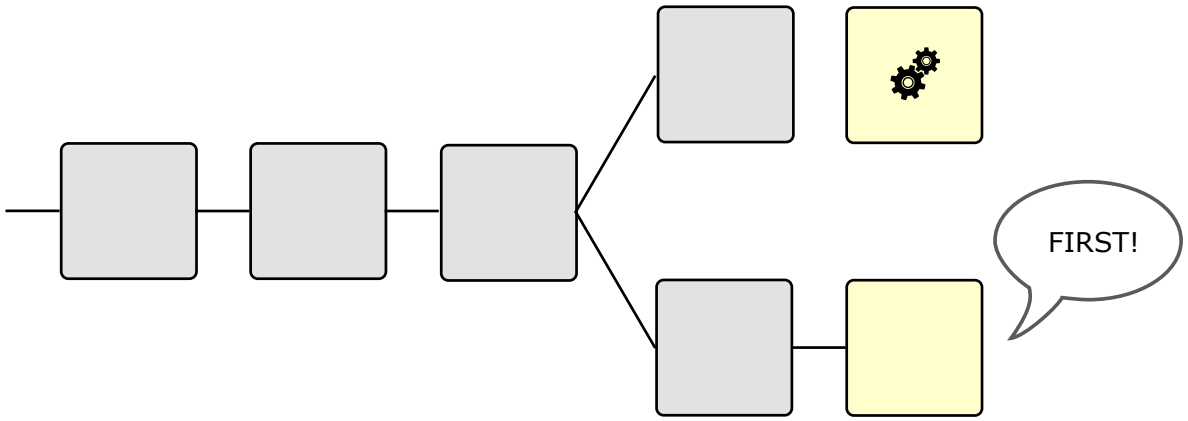
The consensus mechanism

Stability: forks are not stable!



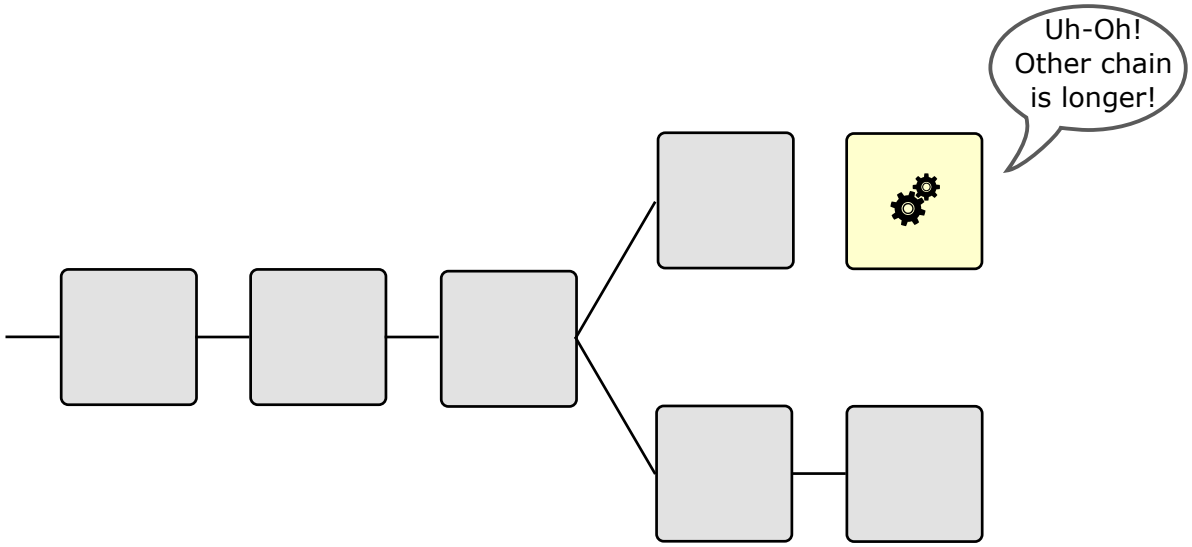
The consensus mechanism

Stability: forks are not stable!



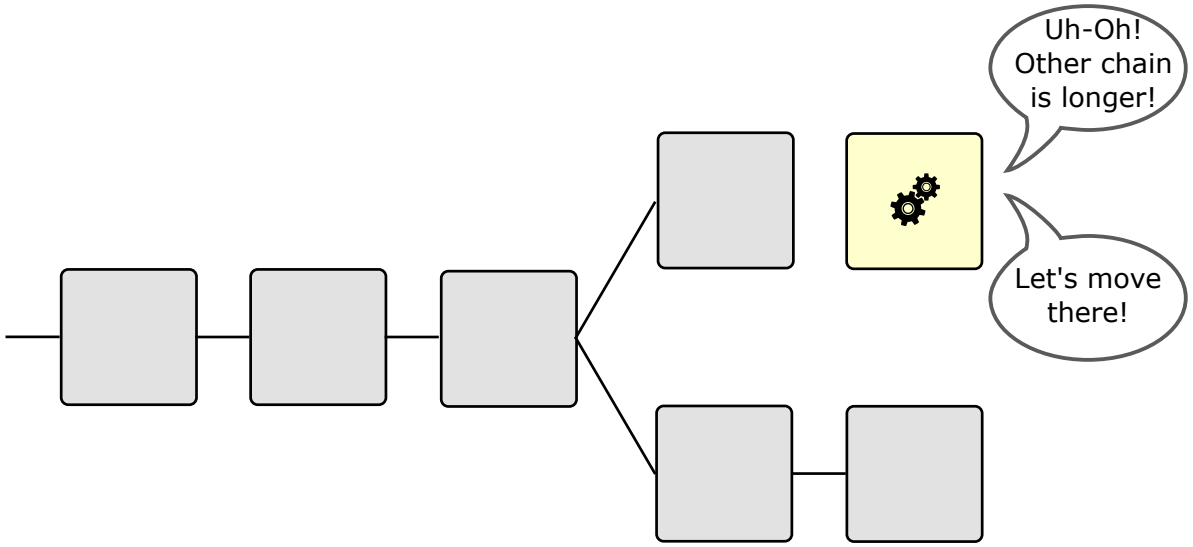
The consensus mechanism

Stability: forks are not stable!



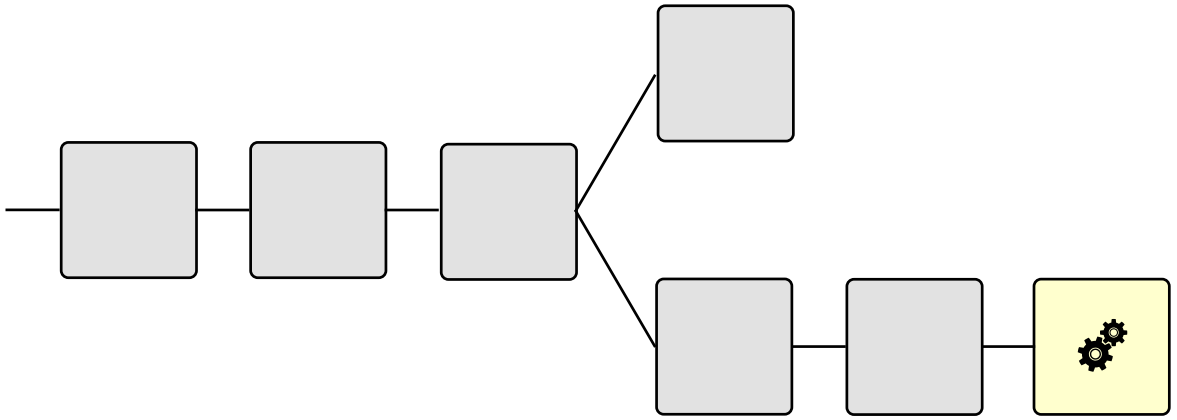
The consensus mechanism

Stability: forks are not stable!



The consensus mechanism

Stability: forks are not stable!

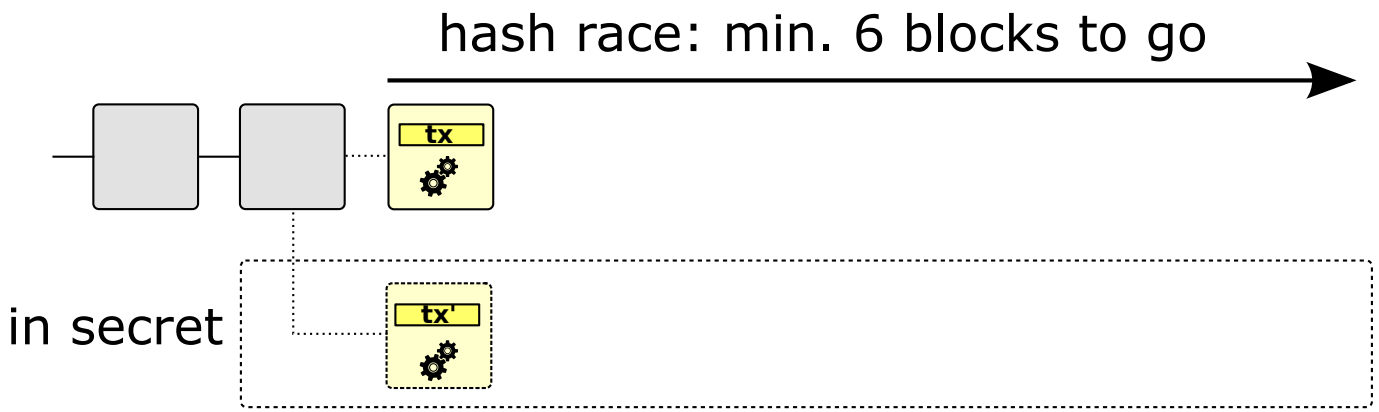


The consensus mechanism

Robustness: double spending attack not feasible

The consensus mechanism

Robustness: double spending attack not feasible



The consensus mechanism

Not feasible $\neq$ impossible

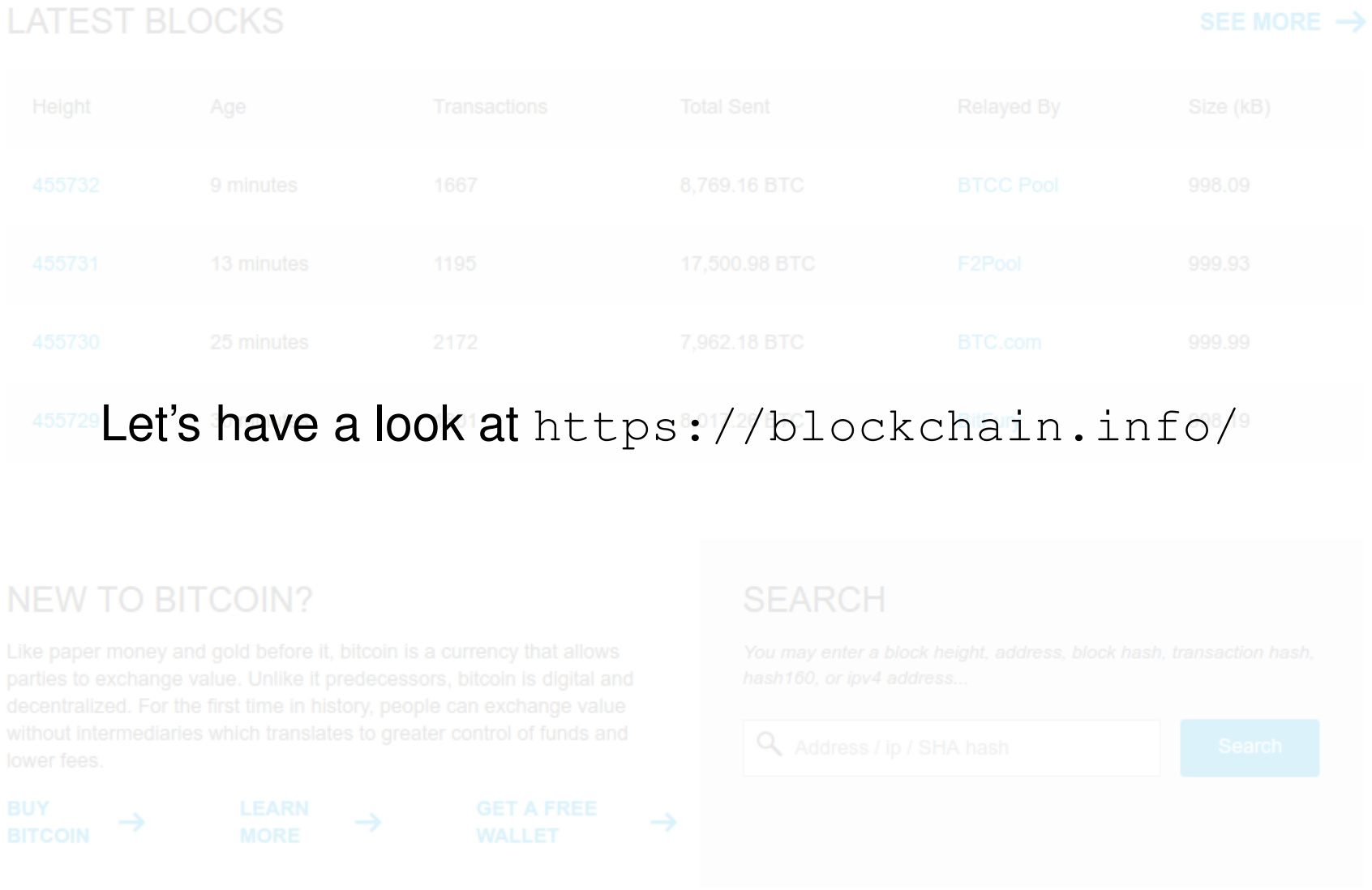
The consensus mechanism

Not feasible $\neq$ impossible

computing power (% of entire network)	success probability
50%	1.
40%	0.550625
30%	0.177352
20%	0.0274155
10%	0.00678378
5%	0.0000287455

Blockchain stats

Blockchain stats



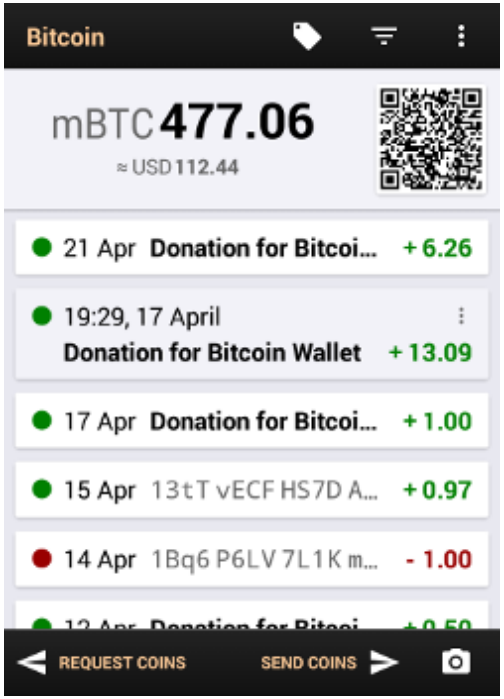
Let's have a look at `https://blockchain.info/`

How to start

Choose wallet software

How to start

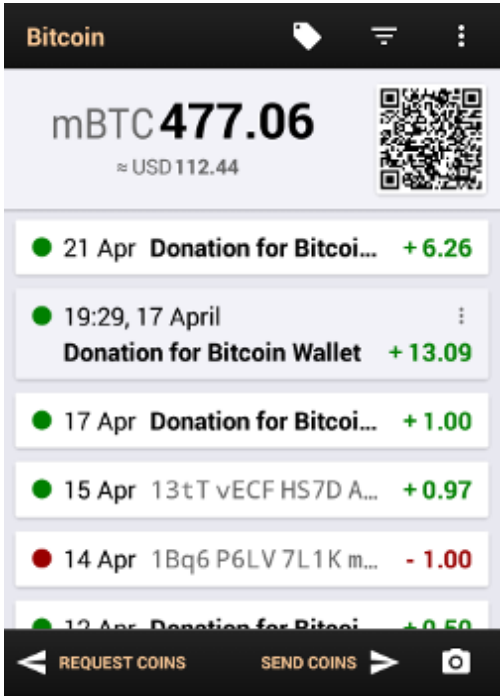
Choose wallet software



breadwallet
Bither
GreenBits
Coinomi
Coin.Space
Simple Bitcoin
Bitcoin Wallet
ArcBit
Copay
Airbitz
Mycelium
Green Address

How to start

Choose wallet software



breadwallet Bither GreenBits Coinomi Coin.Space Simple Bitcoin

Bitcoin Wallet ArcBit Copay Airbitz Mycelium Green Address

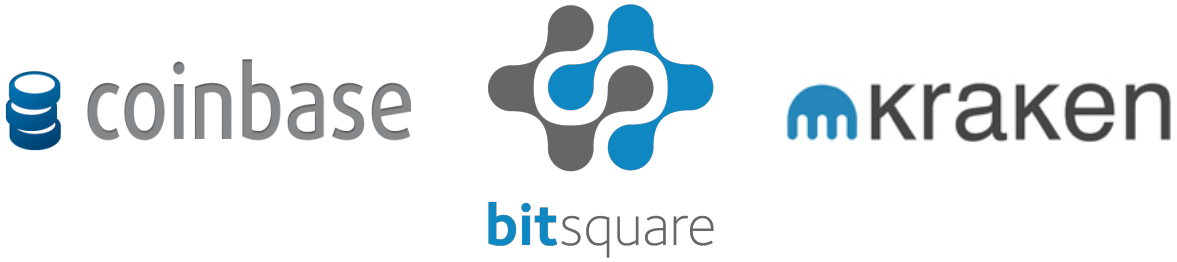
Be careful, not all wallets offer same features / security $\longrightarrow$

see `https://bitcoin.org`

Where can I buy bitcoins?

Where can I buy bitcoins?

- online marketplaces, e.g.



Where can I buy bitcoins?

- online marketplaces, e.g.

coinbase bitsquare kraken

- local exchange, e.g. paper wallets

Thank you!

some links

- https://bitcoin.org/en/
- https://blockchain.info/
- A.M. Antonopoulos, Mastering Bitcoin, O'Reilly 2014.
- http://zerocash-project.org/
- https://www.ethereum.org/