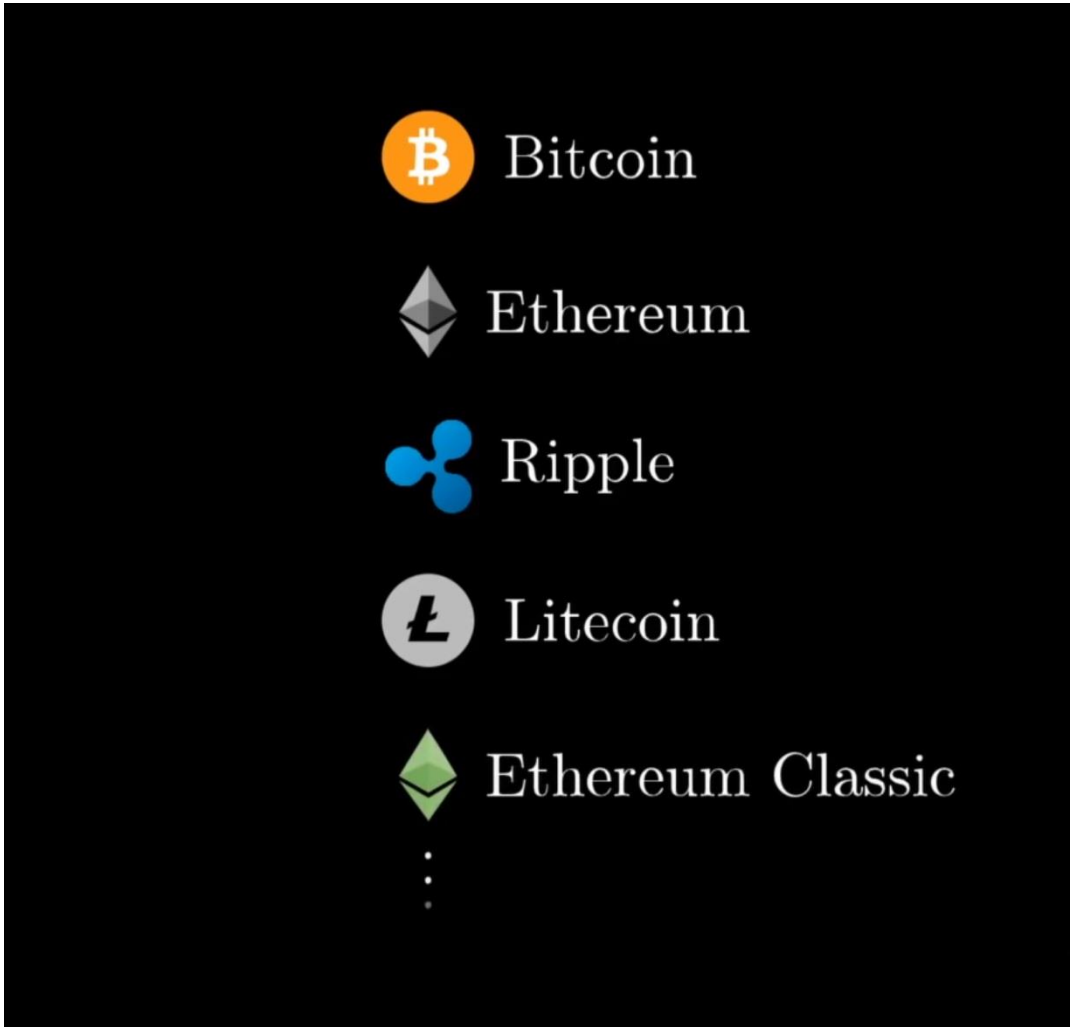
Bitcoin…of Bittere Coin


Bitcoin
Ethereum
Ripple
Litecoin
Ethereum Classic

Bitcoin-filosofie: Oostenrijkse Economische School

- Geen muntcreatie meer door centrale bankier
- Muntcreatie beperkt tot vooraf bekende totale hoeveelheid (zoals goud)
- Muntcreatie beheerst door objectieve mathematische parameters
- Appreciatie door gebruikers

Bitcoin: Wetmatigheden

- Gecertificeerde transactie – elektronische handtekening met SK en PK
- Uniciteit van transactie – gedateerd, genummerd en geboekstaafd
- Automatische correctie van duplicering – door Blockchain-methodologie
- Geldcreatie door “Proof of work” – door Mining

Randvoorwaarden:
Internet, Open Source en Cryptografie met SHA

$$Ch(x, y, z) = (x \wedge y) \oplus (\neg x \wedge z)$$

$$Maj(x, y, z) = (x \wedge y) \oplus (x \wedge z) \oplus (y \wedge z)$$

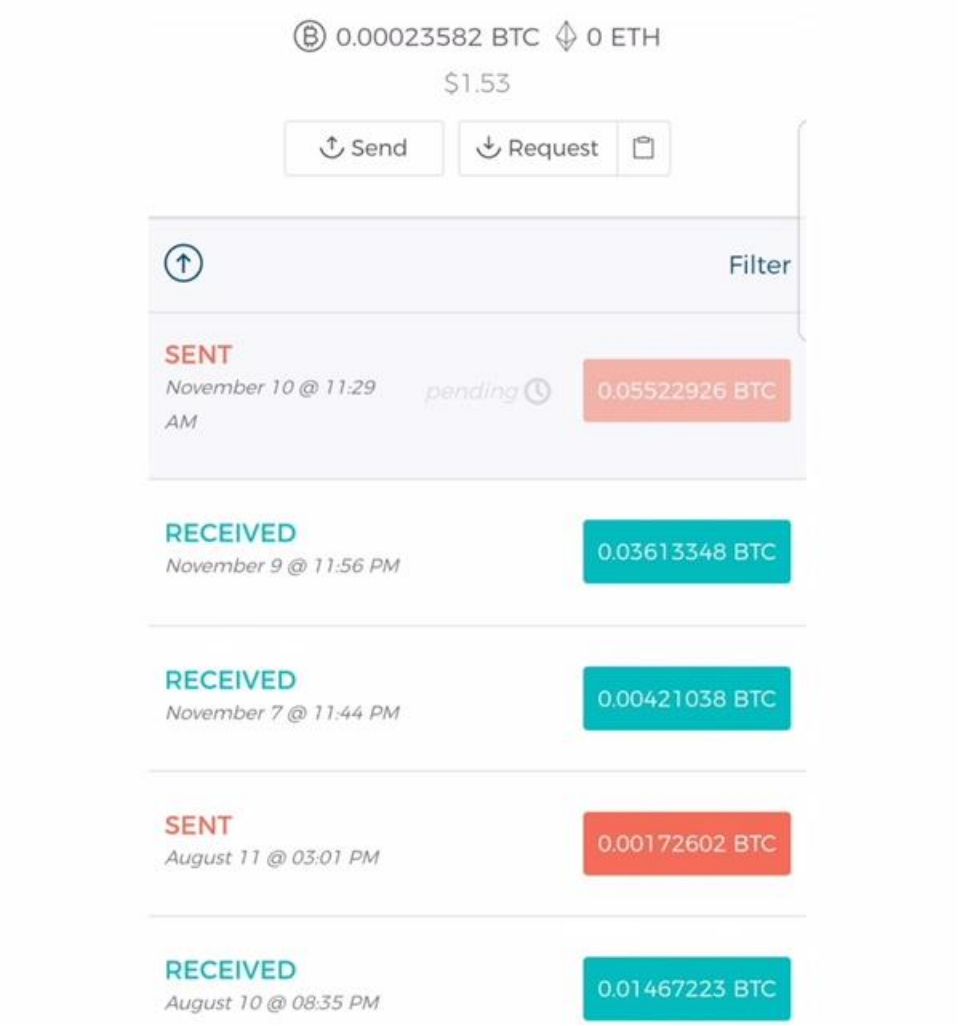
$$\Sigma_0^{\{256\}}(x) = ROTR^2(x) \oplus ROTR^{13}(x) \oplus ROTR^{22}(x)$$

$$\Sigma_1^{\{256\}}(x) = ROTR^6(x) \oplus ROTR^{11}(x) \oplus ROTR^{25}(x)$$

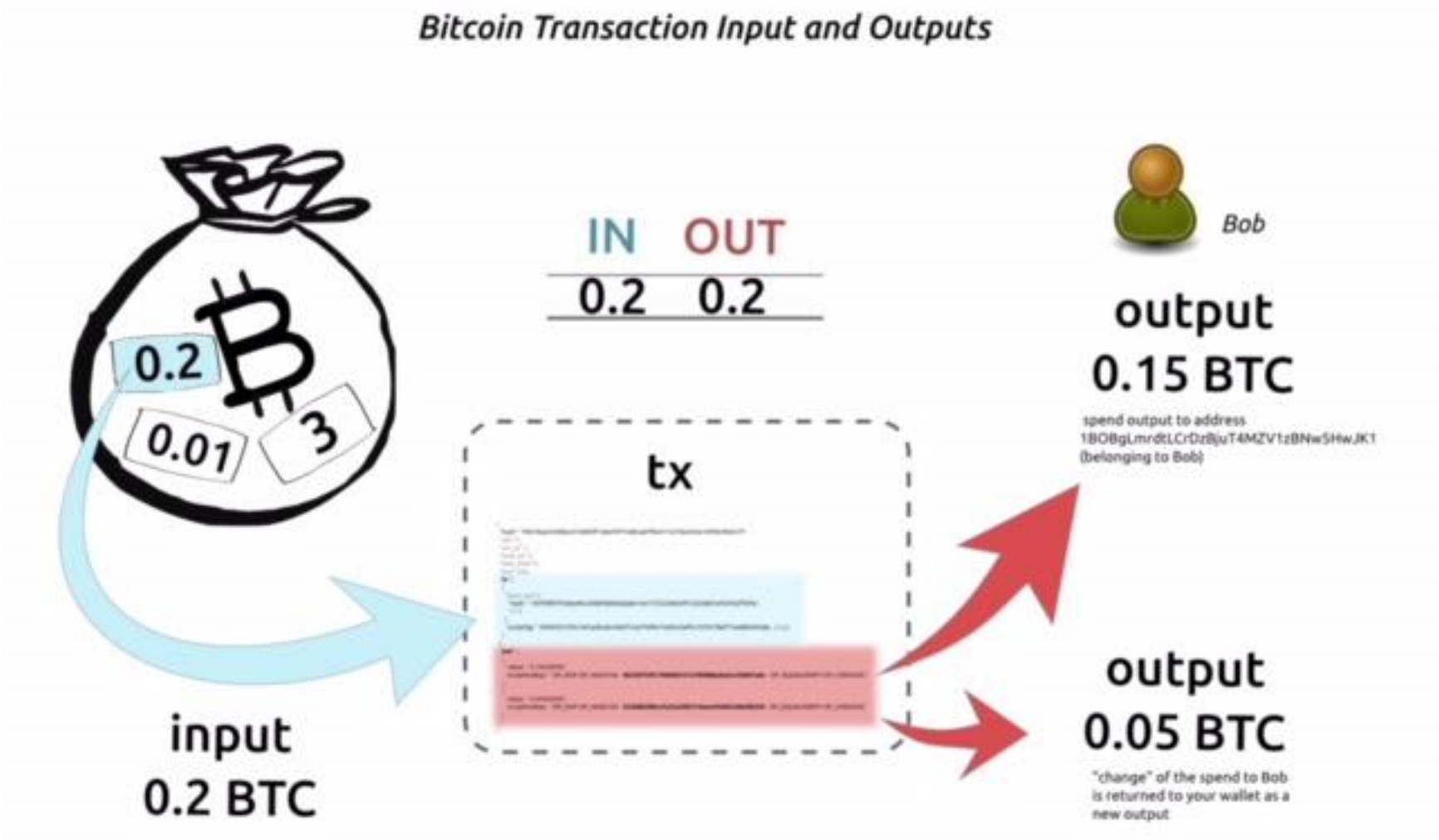
$$\sigma_0^{\{256\}}(x) = ROTR^7(x) \oplus ROTR^{18}(x) \oplus SHR^3(x)$$

$$\sigma_1^{\{256\}}(x) = ROTR^{17}(x) \oplus ROTR^{19}(x) \oplus SHR^{10}(x)$$

Wallet


0.00023582 BTC
0 ETH
$1.53
Send
Request
Filter
SENT
November 10 @ 11:29 AM
pending
0.05522926 BTC
RECEIVED
November 9 @ 11:56 PM
0.03613348 BTC
RECEIVED
November 7 @ 11:44 PM
0.00421038 BTC
SENT
August 11 @ 03:01 PM
0.00172602 BTC
RECEIVED
August 10 @ 08:35 PM
0.01467223 BTC

Transactie


Bitcoin Transaction Input and Outputs
IN OUT
0.2 0.2
0.2
0.01
3
input
0.2 BTC
tx
Bob
output
0.15 BTC
spend output to address
1BOBgLmrdtLCrDzBjuT4MZV1zBNwSHwJK1
(belonging to Bob)
output
0.05 BTC
"change" of the spend to Bob
is returned to your wallet as a
new output

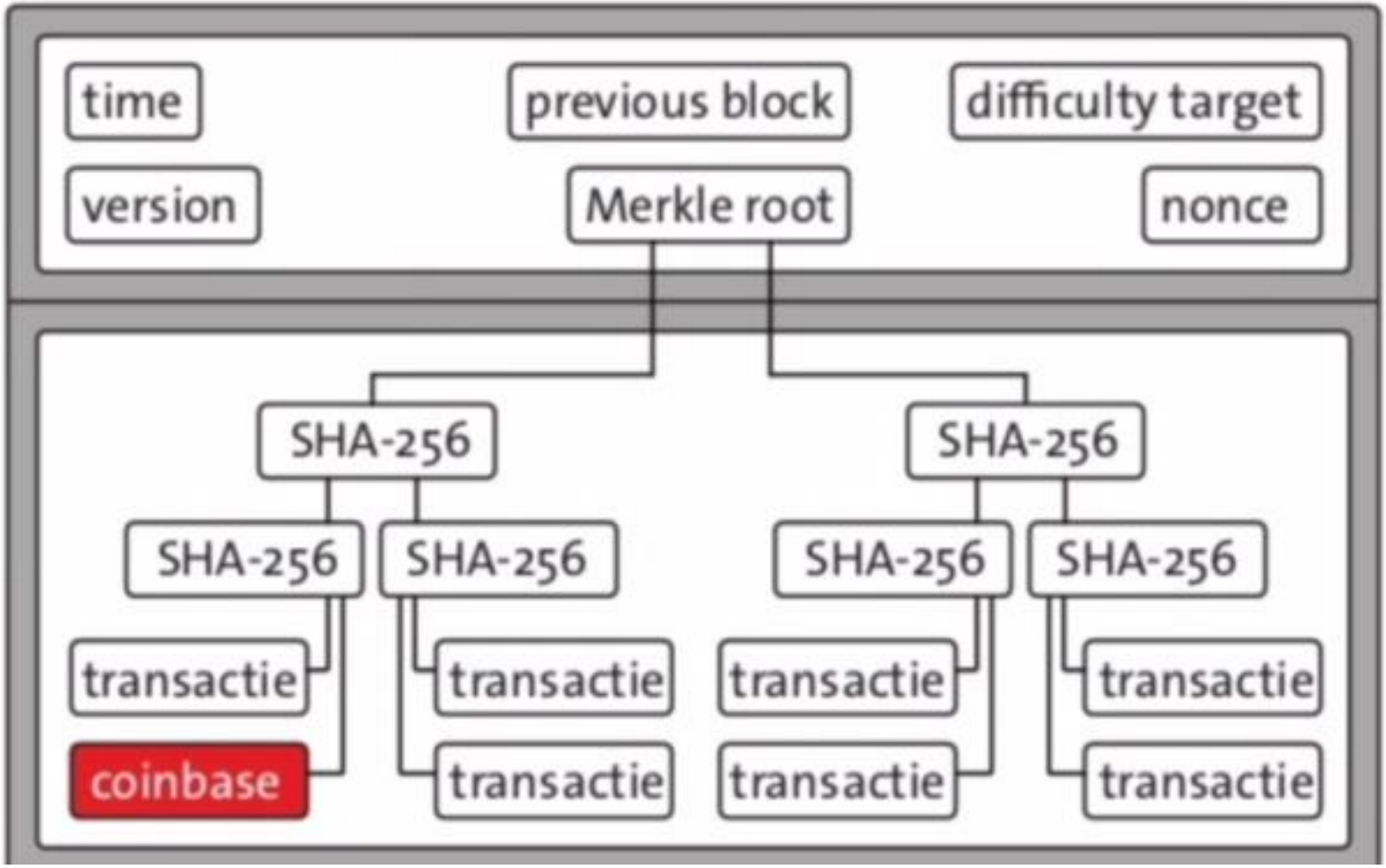
(Block # 286819)

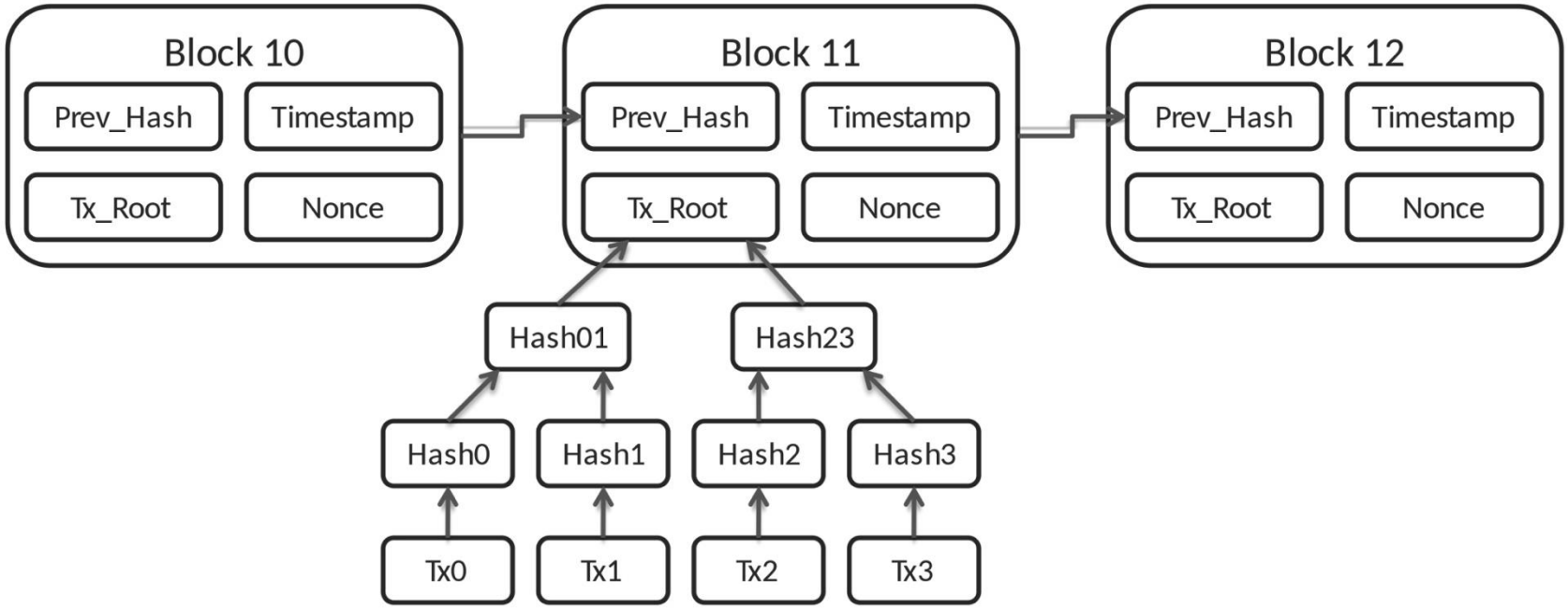
version	02000000
previous block hash (reversed)	17975b97c18ed1f7e255adf297599b55 330edab87803c81701000000000000000
Merkle root (reversed)	8a97295a2747b4f1a0b3948df3990344 c0e19fa6b2b92b3a19c8e6badc141787
timestamp	358b0553
bits	535f0119
nonce	48750833
transaction count	63
coinbase transaction	
transaction	
...	

Block hash

0000000000000000 e067a478024addfe cdc93628978aa52d 91fabd4292982a50

nonce	hash
0	5c56c2883435b38aeba0e69fb2e0e3db3b22448d3e17b903d774dd5650796f76
1	28902a23a194dee94141d1b70102accd85fc2c1ead0901ba0e41ade90d38a08e
2	729577af82250aaf9e44f70a72814cf56c16d430a878bf52fdaceeb7b4bd37f4
3	8491452381016cf80562ff489e492e00331de3553178c73c5169574000f1ed1c
39	03fd5ff1048668cd3cde4f3fb5bde1ff306d26a4630f420c78df1e504e24f3c7
990	0001e3a4583f4c6d81251e8d9901dbe0df74d7144300d7c03cab15eca04bd4bb
52117	0000642411733cd63264d3bedc046a5364ff3c77d2b37ca298ad8f1b5a9f05ba
1813152	00000c94a85b5c06c9b06ace1ba7c7f759e795715f399c9c1b1b7f5d387a319f
19745650	000000cdccf49f13f5c3f14a2c12a56ae60e900c5e65bfe1cc24f038f0668a6c
243989801	0000000ce99e2a00633ca958a16e17f30085a54f04667a5492db49bcae15d190
856192328	0000000000000000e067a478024addfecdc93628978aa52d91fabd4292982a50


time
previous block
difficulty target
version
Merkle root
nonce
SHA-256
SHA-256
SHA-256
SHA-256
transactie
transactie
transactie
transactie
coinbase
transactie
transactie
transactie


Block 10
Prev_Hash
Timestamp
Tx_Root
Nonce
Block 11
Prev_Hash
Timestamp
Tx_Root
Nonce
Block 12
Prev_Hash
Timestamp
Tx_Root
Nonce
Hash01
Hash23
Hash0
Hash1
Hash2
Hash3
Tx0
Tx1
Tx2
Tx3

Bedenkingen

- Vooralsnog geen stabiliteitsrisico
- Extreem volatiel

Evolutie waarde BT

- 2009: 10000 BT = 2 pizza's

- April 2011 1BT = 1 $
- Juni 2011 = 10 $
- April 2013 = 100 $
- November 2013 = 1.000$
- December 2017 = 10.000$

Volatiel


BTC/EUR (Dagelijks)
-5.93 (-1.02%)
07/12/2016 08:36:37
BTC / EUR:573.96
700.00
680.00
660.00
640.00
620.00
600.00
573.96
560.00
540.00
520.00
500.00
480.00
460.00
440.00
420.00
400.00
380.00
360.00
650.58
622.65
531.17
404.72
Investing.com
04/14/2016
04/30/2016
05/13/2016
05/26/2016
06/08/2016
06/21/2016
07/12/2016

Pro

- Disruptief
- Veilig
- Anoniem

Contra

- Schaars
- Traag
- Energieverslindend
- Witwaspraktijken
- Regulatoire onzekerheid

Energieverbruik

- Per transactie: 250Kwh
- Jaarproduktie van nieuwe BT: 32Twh

= maandverbruik gezin

= 1 jaar elektriciteitsverbruik Denemarken

Toekomst

- A. Experiment Bitcoin
  - Onderworpen aan de wet van de onvoorziene gebeurtenissen
  - Met steeds meer geïdentificeerde risico’s

- B. Experiment Blockchain
  - Schept vertrouwen uit wantrouwen
  - Toekomst: Smart Contracts
  - Te combineren met Rekeneenheid ipv Cryptomunt

Blockchain: 2017

- Financiële dienstverlening
  - ECB, Santander, Royal Bank of Canada, JPMorgan, Citibank, BNWMelon, American Express, Visa, MasterCard, GoldmanSachs, MoneyGram, WesternUnion
- Automobiel
  - Volkswagen, Toyota, Daimler
- Luchtvaart
  - Airbus, KLM, Lufthansa, AirFrance
- Scheepvaart, Telecom, Internet of Things
  - Maersk, AT&T, British Telecom, Orange, VerizonVentures, Sisco, Bosch
- Retail
  - Walmarts, Alibaba, DeBeers

Blockchain: 2018

- Paradigmawissel
  - Internet 1.0 naar Internet 3.0
- Groeipad
  - R&D – Proof of Concept – Pilot Tests – Octrooien
- Disruptieve risico’s
  - Zekerheid door transparantie
  - Samenwerking vs Mededinging
  - Experiment vs Regulering
  - De Check van de Genesis-Block

Info voor Bitcoin-nerds

Ken Shirriff's blog:

- Bitcoin mining the hard way: the algorithms, protocols, and bytes http://www.righto.com/2014/02/bitcoin-mining-hard-way-algorithms.html

- Bitcoins the hard way: Using the raw Bitcoin protocol http://www.righto.com/2014/02/bitcoins-hard-way-using-raw-bitcoin.html

Info voor Bitcoin-nerds

En mbt Blockchain:

- **19 Industries The Blockchain Will Disrupt**
https://youtu.be/G3psxs3gyf8

- Steven Johnson, Beyond the Bitcoin Bubble, The New York Times, Jan. 16, 2018https://www.nytimes.com/2018/01/16/magazine/beyond-the-bitcoin-bubble.html