Blockchain: Beyond the headlines...

Gaurav Chadha

About me...

- SAP Labs India
- Genpact
- SAP Research India
- D. E. Shaw India Pvt. Ltd.
- 04 CA 12


https://github.com/sayhigaurav

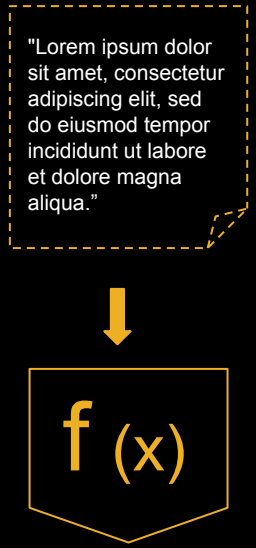

sayhigaurav@gmail.com

Agenda

- Basics
  - Hashing
  - Asymmetric Cryptography
  - Merkle Tree
- Blockchain
  - Block, Transactions and Chaining
  - Proof of Work
- Bitcoin
  - Mining
- Consensus Algorithms
- War of frameworks
- DAPPS
- Applications

Hashing

“Hashing is a cryptographic technique which maps data of arbitrary size to data of a fixed size.”



92d5c7cb0cd26507f7bba985bbb96600c7d3ee59e7f99d4e171f9c52afd556d1

Hashing

A perfect hash function is one which returns a unique hash value of fixed length for unique inputs, consistently and asymmetrically.

- If we change even a bit of an input and feed it to a hash function, the resulting hash value would differ.
- It is mathematically impossible to get the value of the input from its hash value.

Examples of Hashing Algorithms

- Message Digest Algorithm (MD5)
- Secure Hash Algorithms 2
  - SHA-224, SHA-256, SHA-384, SHA-512
- Secure Hash Algorithms 3
  - SHA3-224, SHA3-256, SHA3-384, SHA3-512
  - Based on KECCAK function
  - US National Institute of Standards and Technology (NIST) hash function competition: KECCAK function (winner), BLAKE, JH, Grostl, Skein

Asymmetric Cryptography

Asymmetric Cryptography, is an cryptographic system that uses a pair of keys: public and private key to accomplish:

1. Encryption: private key holder can decrypt the message encrypted with the public key
2. Authentication: public key verifies that the owner of paired private key signed the message

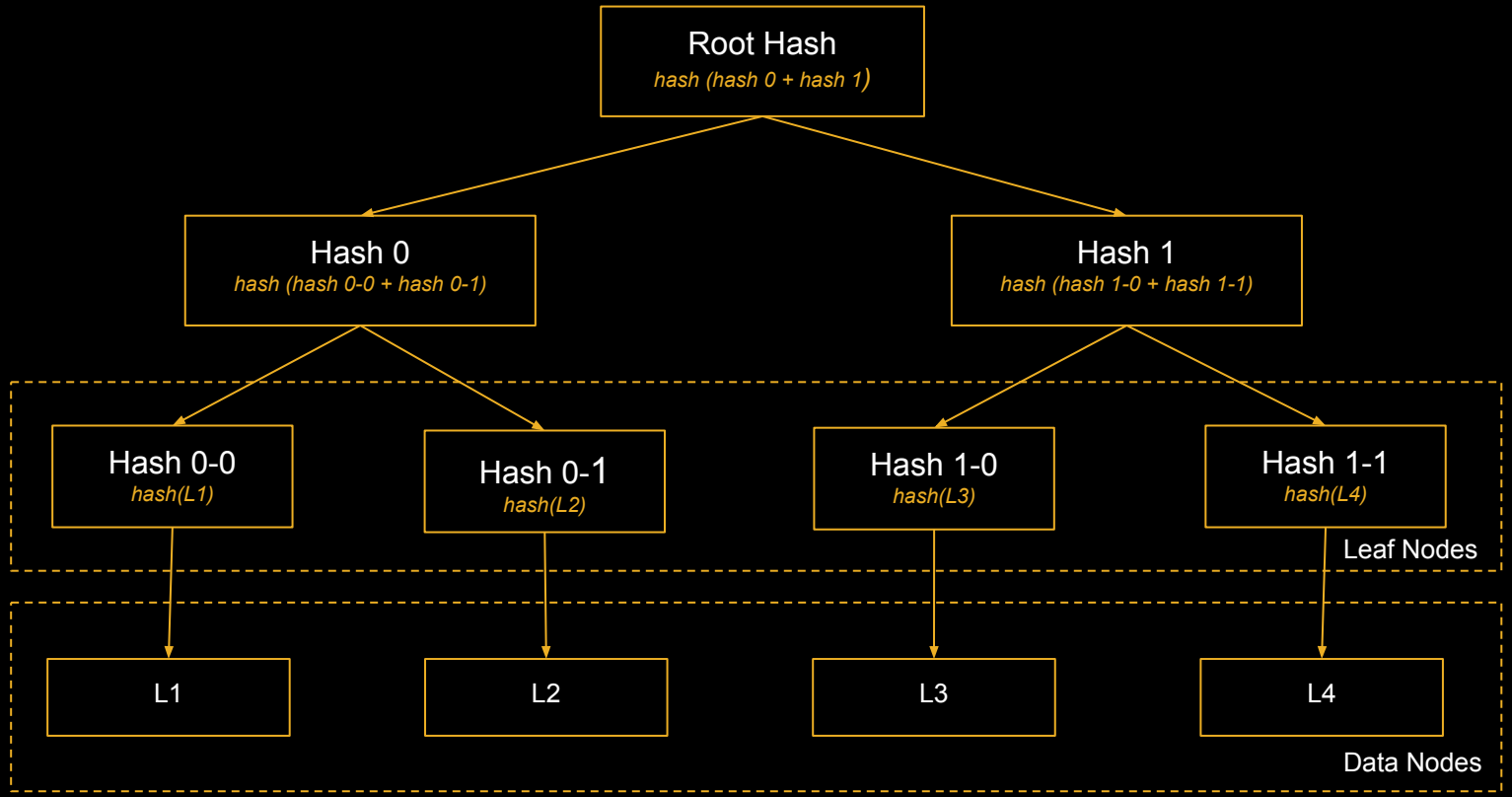
Merkle Tree

Merkle tree is a tree data structure in which:

- every leaf node is labelled with the hash of a data block and
- every non-leaf node is labelled with the cryptographic hash of the labels of its child nodes.

Merkle trees allow efficient and secure verification of the contents of large data structures.

Merkle Tree


Root Hash
hash (hash 0 + hash 1)
Hash 0
hash (hash 0-0 + hash 0-1)
Hash 1
hash (hash 1-0 + hash 1-1)
Hash 0-0
hash(L1)
Hash 0-1
hash(L2)
Hash 1-0
hash(L3)
Hash 1-1
hash(L4)
Leaf Nodes
L1
L2
L3
L4
Data Nodes

Blockchain

"An open, distributed ledger that can record transactions between two parties efficiently and in a verifiable and permanent way"

Blockchain

"An open, distributed ledger that can record transactions between two parties efficiently and in a verifiable and permanent way"

- open distributed ledger
  - open for anyone to read and append
  - managed by a peer to peer network
  - adhering to a set of rules for communication and adding new blocks

Blockchain

"An open, distributed ledger that can record transactions between two parties efficiently and in a verifiable and permanent way"

- open distributed ledger
  - open for anyone to read and append
  - managed by a peer to peer network
  - adhering to a set of rules for communication and adding new blocks
- verifiable
  - blocks are signed using cryptographic techniques

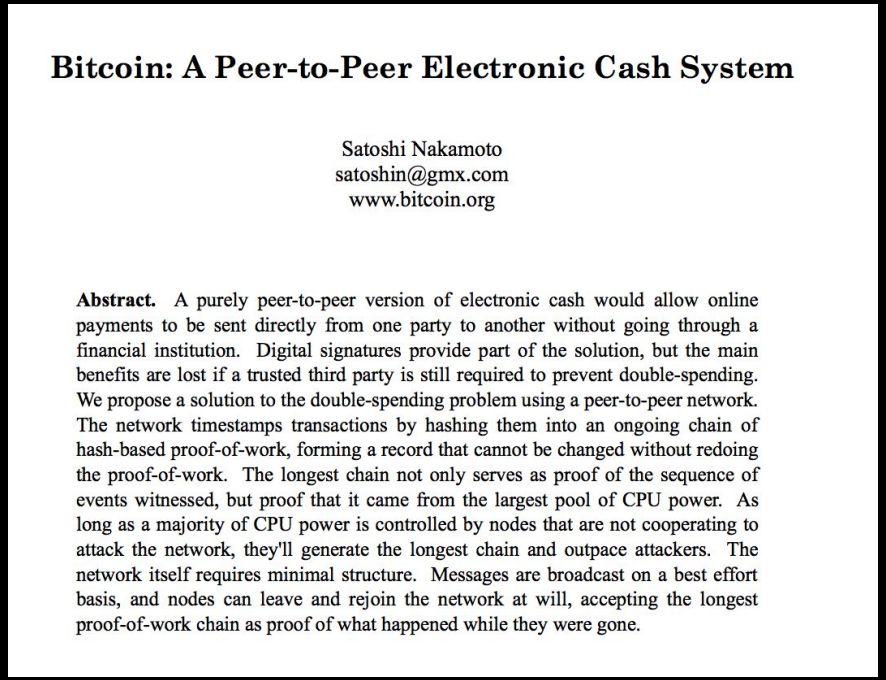
Blockchain

"An open, distributed ledger that can record transactions between two parties efficiently and in a verifiable and permanent way"

- open distributed ledger
  - open for anyone to read and append
  - managed by a peer to peer network
  - adhering to a set of rules for communication and adding new blocks
- verifiable
  - blocks are signed using cryptographic techniques
- permanent
  - immutable
  - once added to the ledger, blocks cannot be modified

Blockchain

Blockchain was implemented to serve as the public transaction ledger of the cryptocurrency bitcoin.

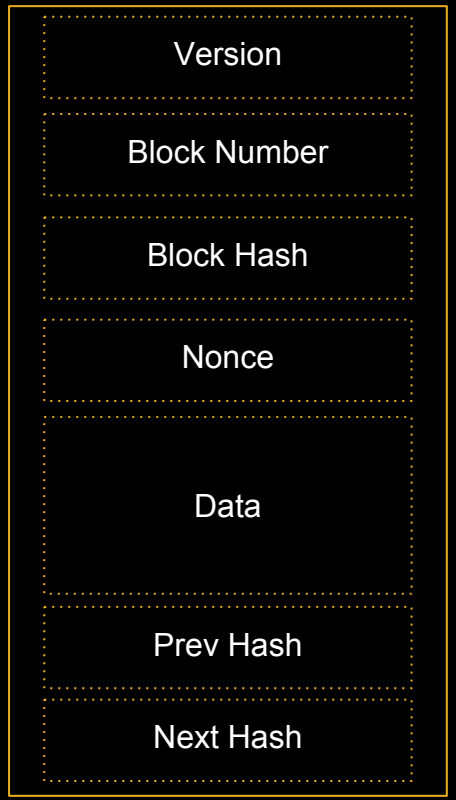


Bitcoin: A Peer-to-Peer Electronic Cash System

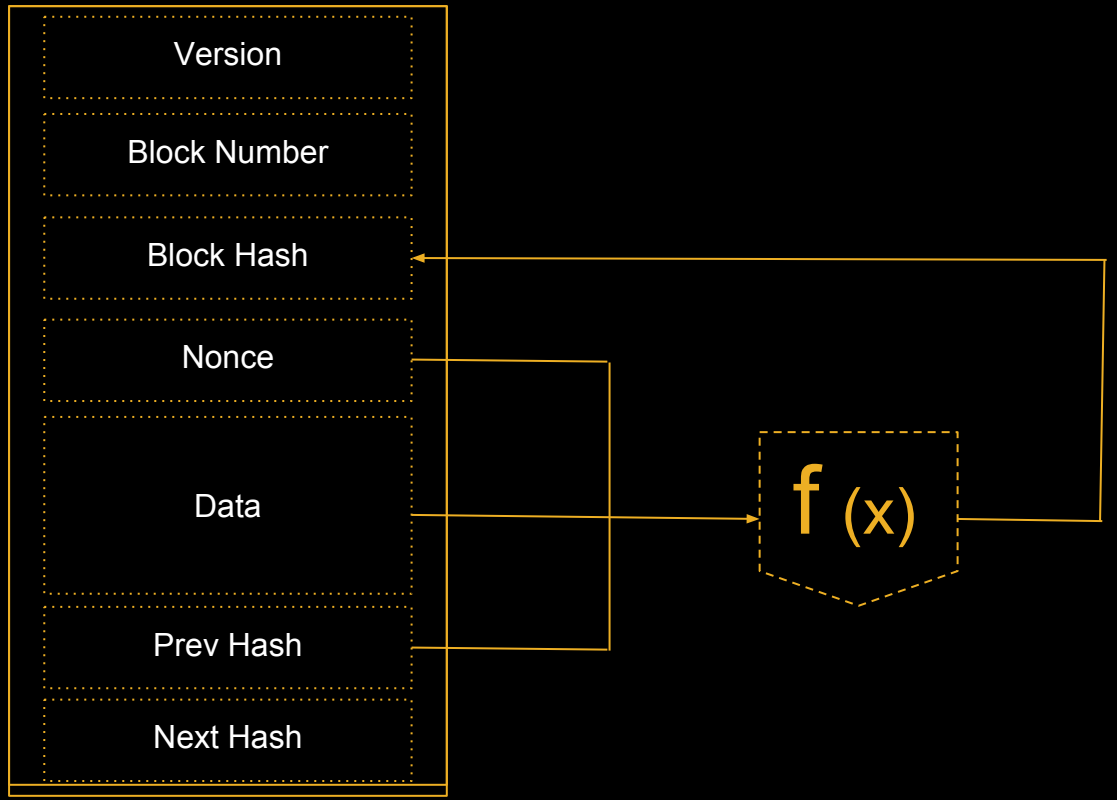
Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

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 proof-of-work chain as proof of what happened while they were gone.

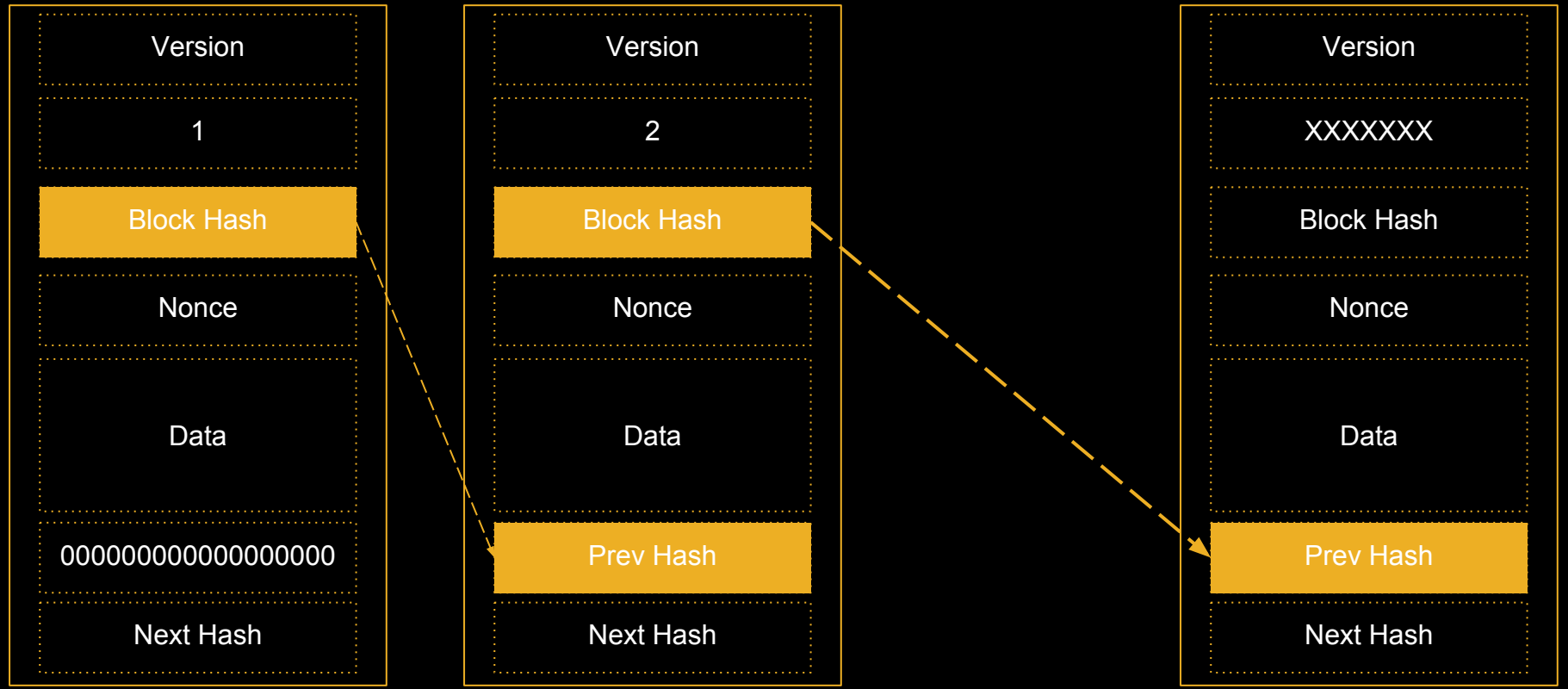
Blockchain


Version
Block Number
Block Hash
Nonce
Data
Prev Hash
Next Hash

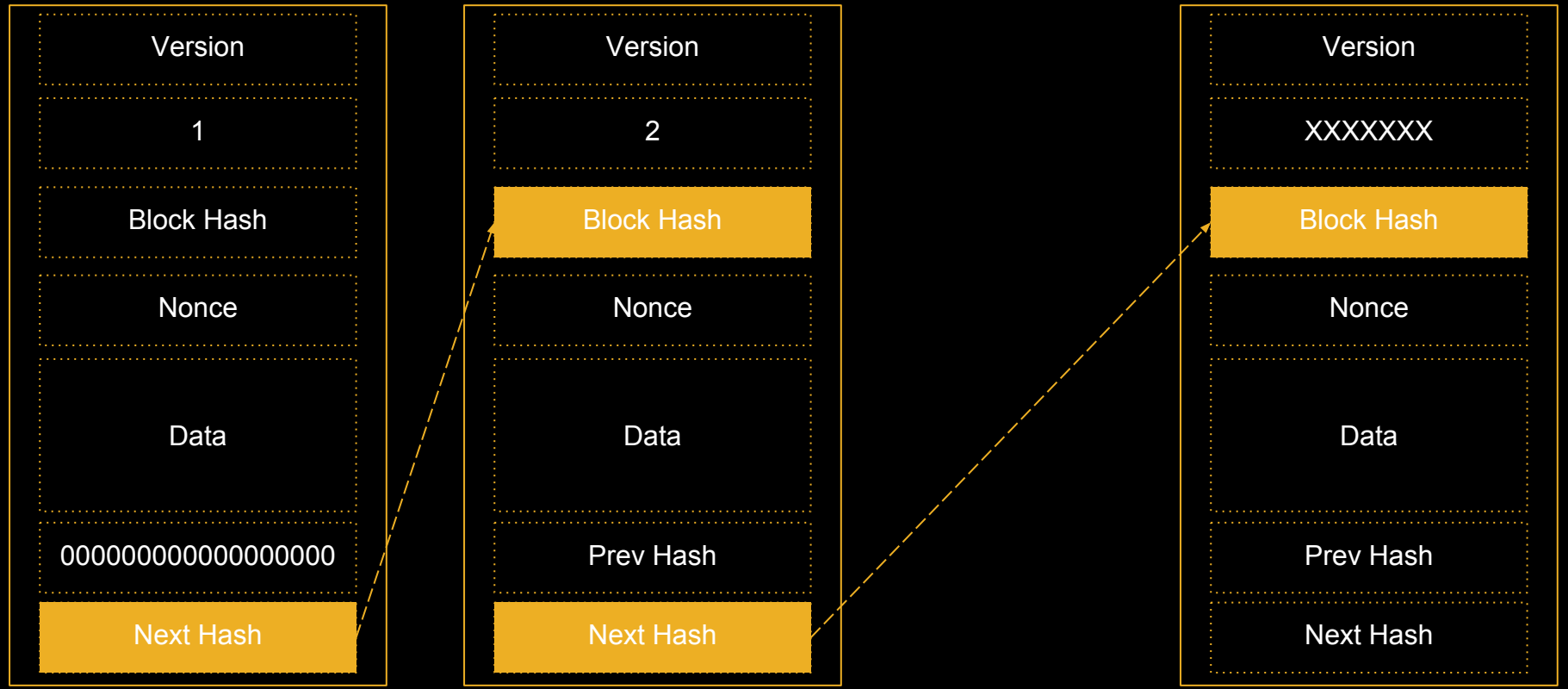
Blockchain


Version
Block Number
Block Hash
Nonce
Data
Prev Hash
Next Hash
f (x)

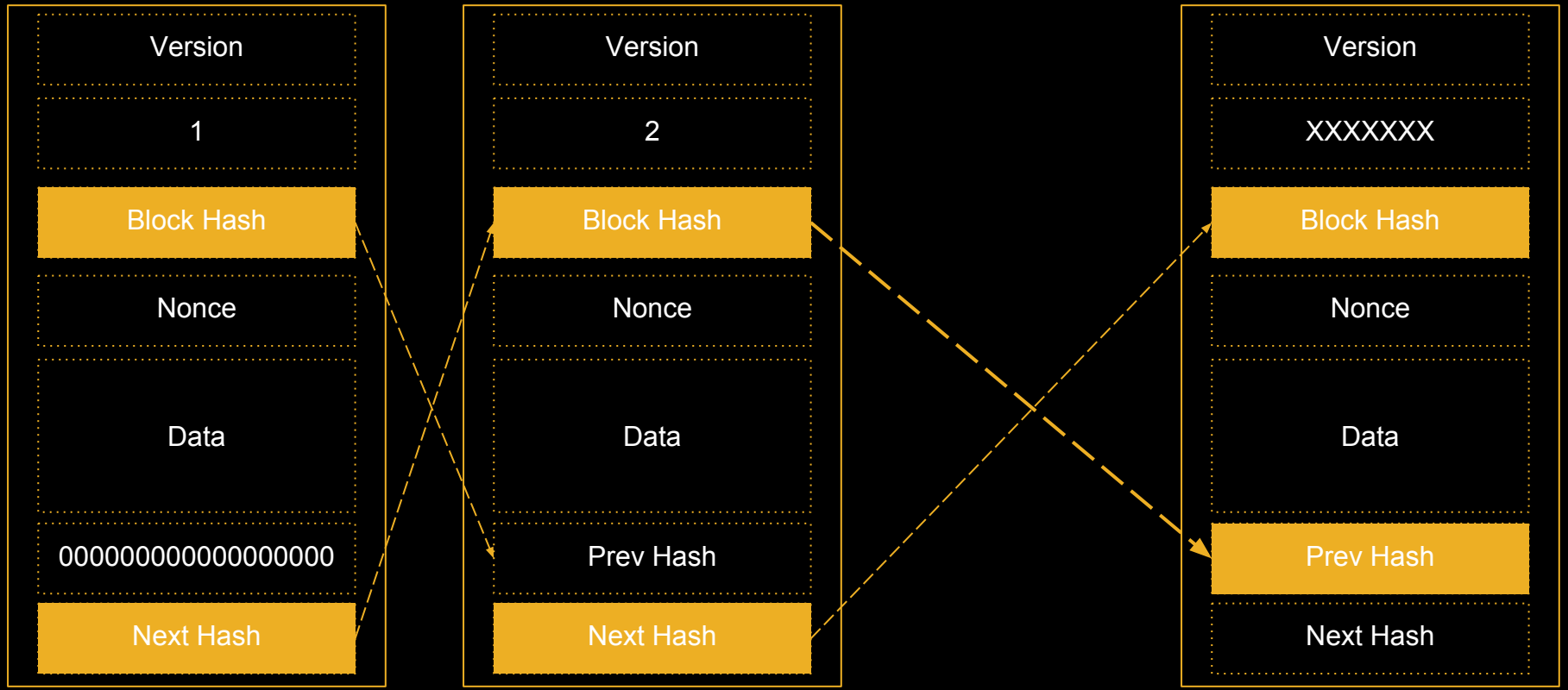
Blockchain


Version
1
Block Hash
Nonce
Data
0000000000000000000
Next Hash
Version
2
Block Hash
Nonce
Data
Prev Hash
Next Hash
Version
XXXXXXX
Block Hash
Nonce
Data
Prev Hash
Next Hash

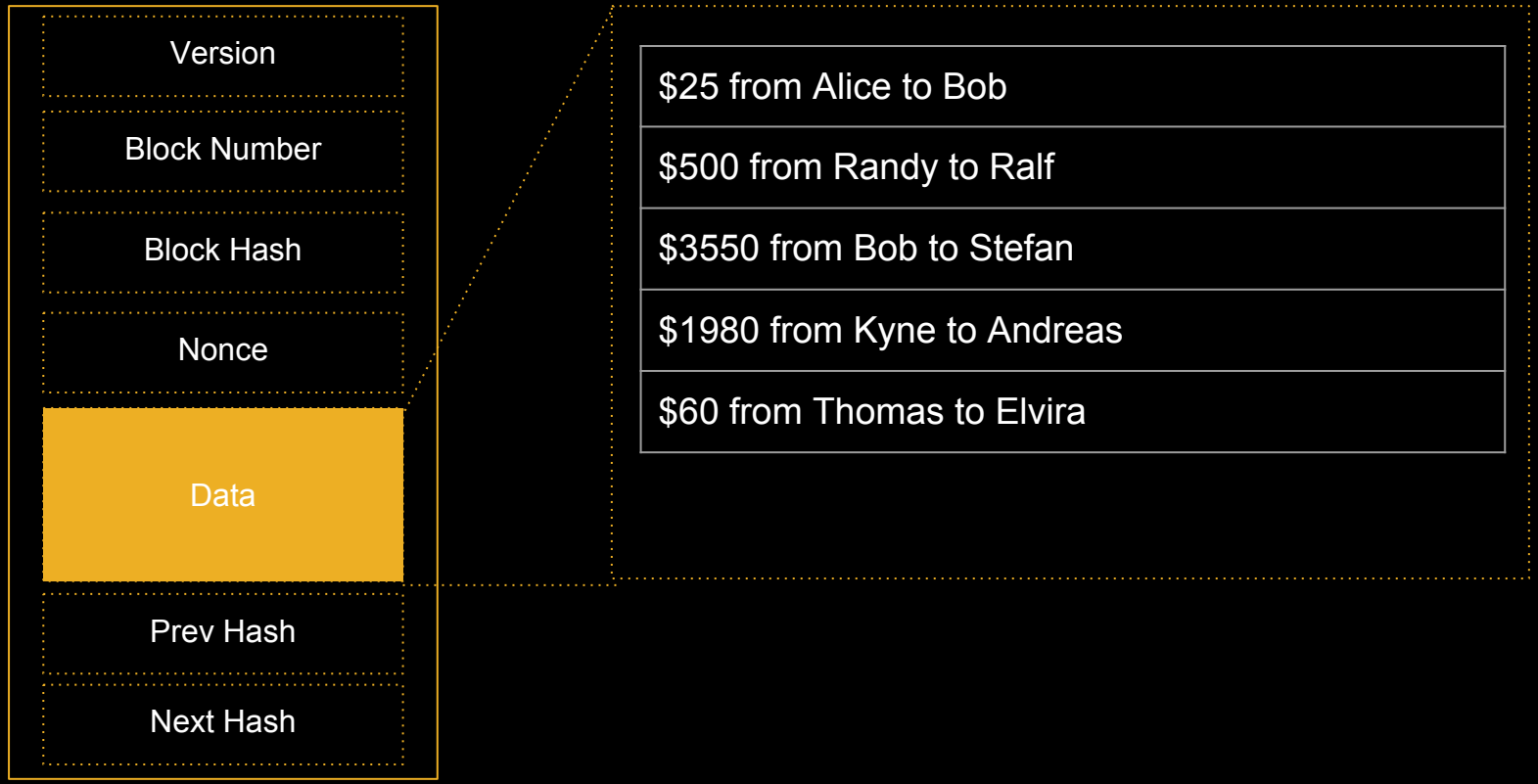
Blockchain


Version
1
Block Hash
Nonce
Data
0000000000000000000
Next Hash
Version
2
Block Hash
Nonce
Data
Prev Hash
Next Hash
Version
XXXXXXX
Block Hash
Nonce
Data
Prev Hash
Next Hash

Blockchain


Version
1
Block Hash
Nonce
Data
0000000000000000000
Next Hash
Version
2
Block Hash
Nonce
Data
Prev Hash
Next Hash
Version
XXXXXXX
Block Hash
Nonce
Data
Prev Hash
Next Hash

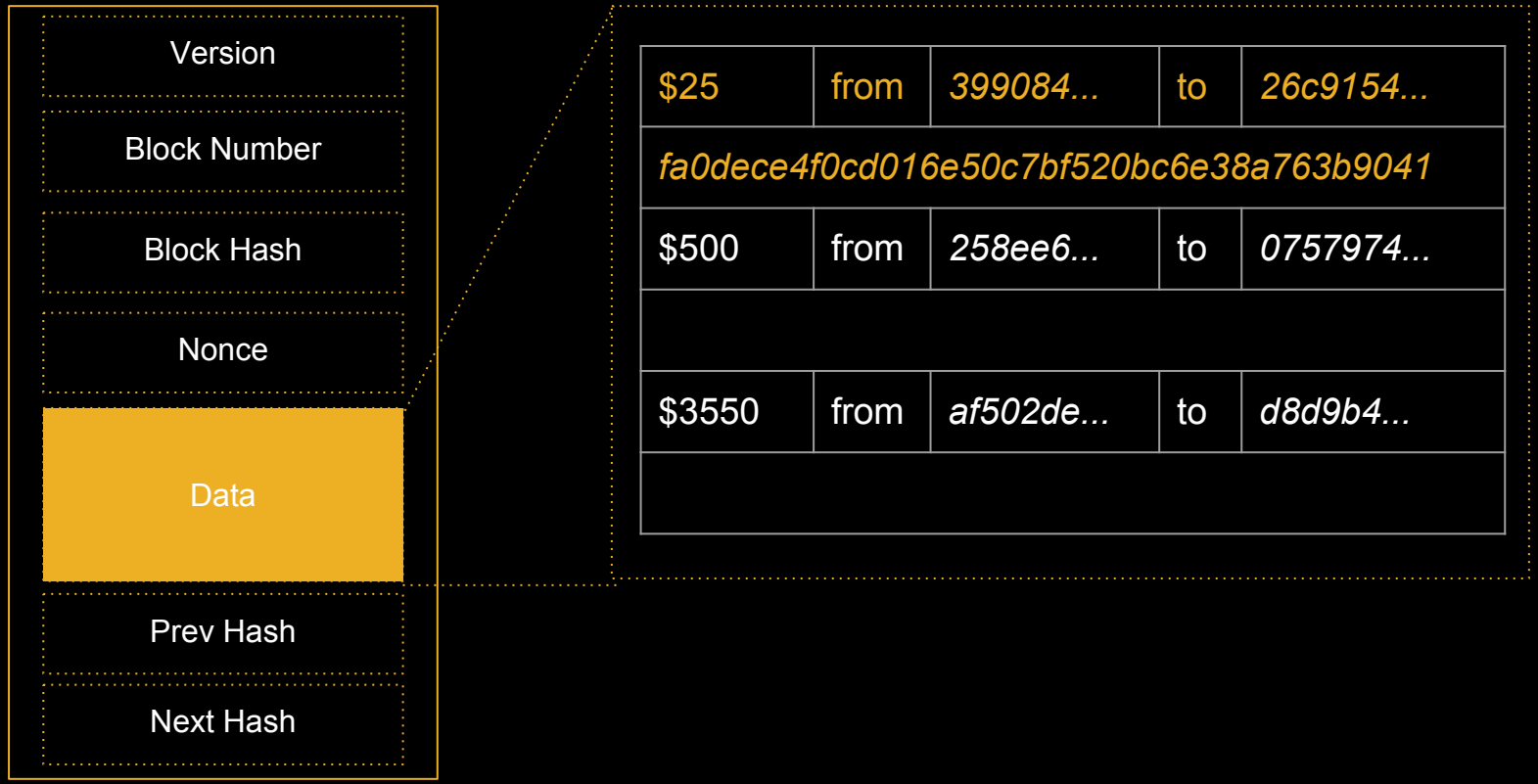
Blockchain


Version
Block Number
Block Hash
Nonce
Data
Prev Hash
Next Hash
$25 from Alice to Bob
$500 from Randy to Ralf
$3550 from Bob to Stefan
$1980 from Kyne to Andreas
$60 from Thomas to Elvira

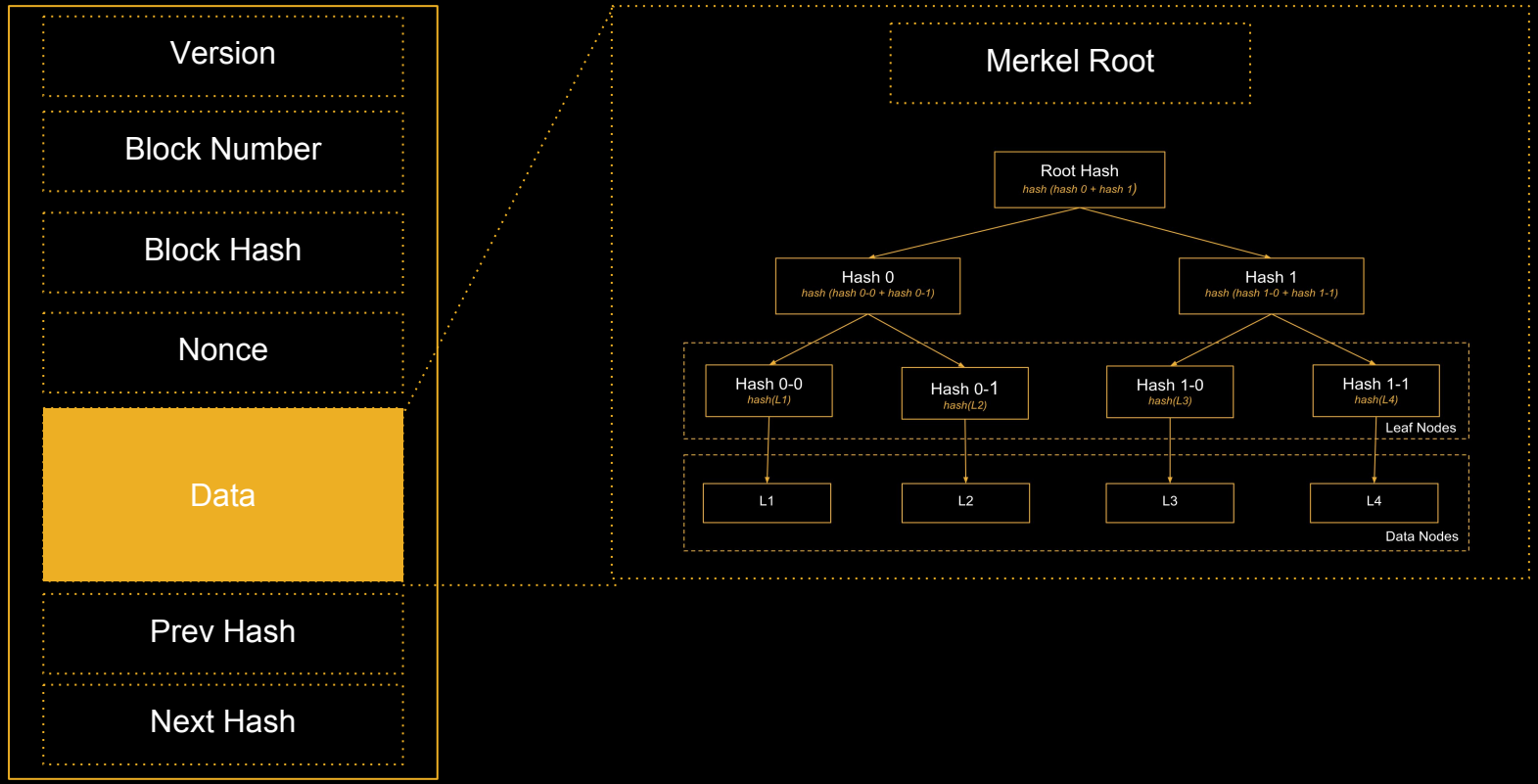
Blockchain

$25	from	*399084...*	to	*26c9154...*
$500	from	*258ee6...*	to	*0757974...*
$3550	from	*af502de...*	to	*d8d9b4...*
$1980	from	*038189...*	to	*cd016e...*
$60	from	*17c89c...*	to	*aaac54...*

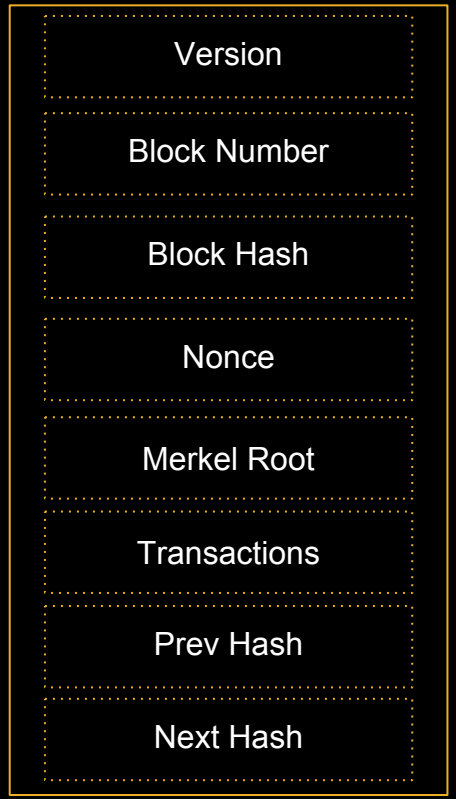
Blockchain


Version
Block Number
Block Hash
Nonce
Data
Prev Hash
Next Hash
$25 from 399084... to 26c9154...
fa0dece4f0cd016e50c7bf520bc6e38a763b9041
$500 from 258ee6... to 0757974...
$3550 from af502de... to d8d9b4...

Blockchain


Version
Block Number
Block Hash
Nonce
Data
Prev Hash
Next Hash
Merkel Root
Root Hash
hash (hash 0 + hash 1)
Hash 0
hash (hash 0-0 + hash 0-1)
Hash 1
hash (hash 1-0 + hash 1-1)
Hash 0-0
hash(L1)
Hash 0-1
hash(L2)
Hash 1-0
hash(L3)
Hash 1-1
hash(L4)
Leaf Nodes
L1
L2
L3
L4
Data Nodes

Blockchain

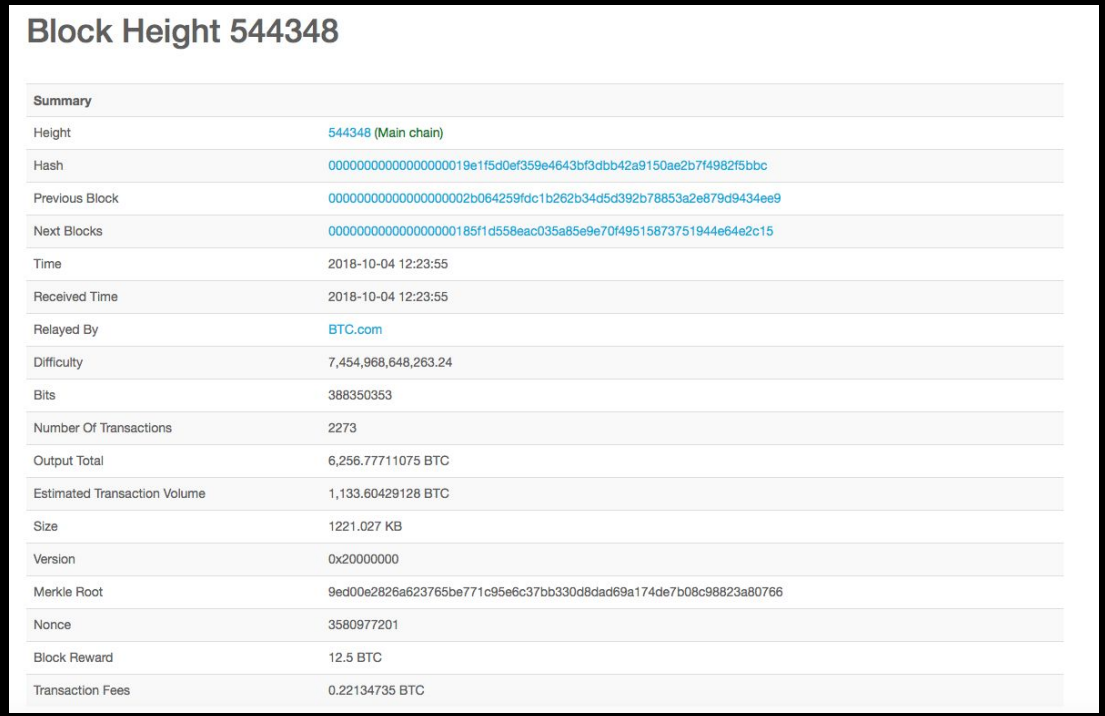

Version
Block Number
Block Hash
Nonce
Merkel Root
Transactions
Prev Hash
Next Hash

Blockchain

Height	Time	Relayed By	Hash	Size (kB)
544348 (Main Chain)	2018-10-04 12:23:55	BTC.com	00000000000000000019e1f5d0ef359e4643bf3dbb42a9150ae2b7f4982f5bbc	1,221.03
544347 (Main Chain)	2018-10-04 12:21:06	AntPool	00000000000000000002b064259fdc1b262b34d5d392b78853a2e879d9434ee9	2.44
544346 (Main Chain)	2018-10-04 12:11:43	BTC.TOP	00000000000000000000838e13f0780c3ac4cdd57ea3131e1be8a8e8503402ae8	1,083.62
544345 (Main Chain)	2018-10-04 12:10:00	Unknown	00000000000000000001996bec34ada885e2faeb3ebd0f1a4f6ed9d751b967c35	1,252.57
544344 (Main Chain)	2018-10-04 11:59:50	BTC.com	00000000000000000003fc7999c5fd58007c751b5c0138bde7057e1aa510ab59	1,234.4
544343 (Main Chain)	2018-10-04 11:33:15	BitClub Network	00000000000000000002480327819bb106416bfa2de483fb8c5827b791347e2f7	1,347.75
544342 (Main Chain)	2018-10-04 11:28:12	BTC.TOP	00000000000000000002434e4b5c067faab0cc4b81dc38c5007f5d5a769134048	1,229.99
544341 (Main Chain)	2018-10-04 11:20:12	F2Pool	00000000000000000008479af506f2063c027c1352519cf925f7a309ad2527af	1,240.19
544340 (Main Chain)	2018-10-04 10:59:05	AntPool	00000000000000000013e0163a26b48ebe579940b812c326a68f0eb131d36f28	360.07
544339 (Main Chain)	2018-10-04 10:27:58	BTC.com	00000000000000000001a1b15abd1acdc5d3481c2b43131f1273f5a1fffe6b5d5	325.94
544338 (Main Chain)	2018-10-04 10:24:45	BTC.com	00000000000000000010d5a230192eb761a174978ff0e4a270000e820c84c564	774.29
544337 (Main Chain)	2018-10-04 10:15:53	Unknown	00000000000000000025a7d35b0e65e2b1478b7ee4776f8874ea479f77d08e8b	232.92
544336 (Main Chain)	2018-10-04 10:14:38	ViaBTC	00000000000000000001da5b2166332a5765ffd3dd754a66e0e24e0b082e369bf	1,238.44
544335 (Main Chain)	2018-10-04 09:58:12	Unknown	00000000000000000002378f63158ca6b61b74b56ea45e269220de7aa0ae5ac1d	764.45
544334 (Main Chain)	2018-10-04 09:54:13	AntPool	00000000000000000012f639eefaa05cc251302e7d54a069d41c24ba7f4c209	0.29
544333 (Main Chain)	2018-10-04 09:50:05	Unknown	00000000000000000185b631e00d4f812ca4720e926268fd0f043da2ace1380	48.79
544332 (Main Chain)	2018-10-04 09:49:44	SlushPool	00000000000000000b2000610441b7a060d68227bad455f18eb7b241cba4d8	1,098.24
544331 (Main Chain)	2018-10-04 09:36:20	Unknown	00000000000000000001c305882cb0e1304c384cdd1981429ebb7795a526f83c8	1,000.02
544330 (Main Chain)	2018-10-04 09:33:31	BTC.TOP	00000000000000000001e33179821296c4910fd774ddec06649711eb21451e3a8	1,196.88
544329 (Main Chain)	2018-10-04 09:19:37	SlushPool	00000000000000000001ed58a4e8acad8567aef7806c30e6ce31df397e902302f	1,189.16

Source: https://www.blockchain.com

Blockchain

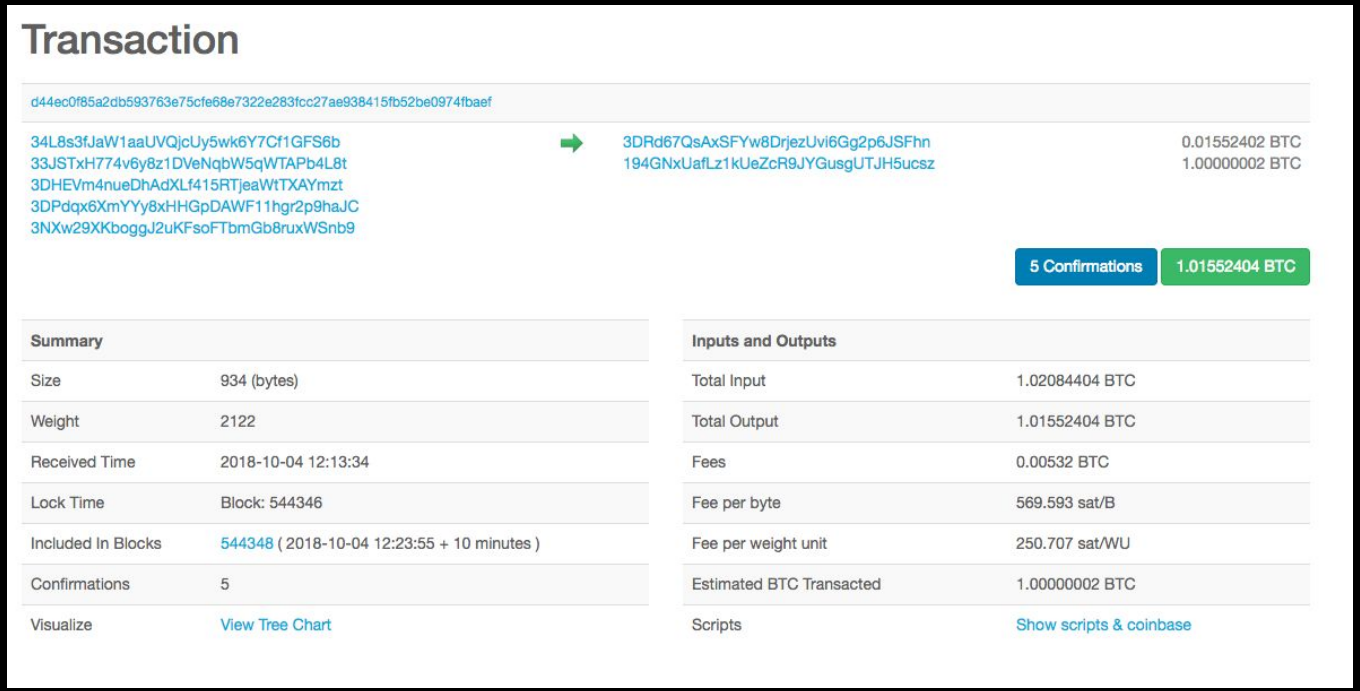


Block Height 544348

Summary	
Height	544348 (Main chain)
Hash	000000000000000000019e1f5d0ef359e4643bf3dbb42a9150ae2b7f4982f5bbc
Previous Block	000000000000000000002b064259fdc1b262b34d5d392b78853a2e879d9434ee9
Next Blocks	000000000000000000185f1d558eac035a85e9e70f49515873751944e64e2c15
Time	2018-10-04 12:23:55
Received Time	2018-10-04 12:23:55
Relayed By	BTC.com
Difficulty	7,454,968,648,263.24
Bits	388350353
Number Of Transactions	2273
Output Total	6,256.77711075 BTC
Estimated Transaction Volume	1,133.60429128 BTC
Size	1221.027 KB
Version	0x20000000
Merkle Root	9ed00e2826a623765be771c95e6c37bb330d8dad69a174de7b08c98823a80766
Nonce	3580977201
Block Reward	12.5 BTC
Transaction Fees	0.22134735 BTC

Source: https://www.blockchain.com

Blockchain



Transaction

d44ec0f85a2db593763e75cfe68e7322e283fcc27ae938415fb52be0974fbaef

34L8s3fJaW1aaUVQjcUy5wk6Y7Cf1GFS6b 33JSTxH774v6y8z1DVeNqbW5qWTAPb4L8t 3DHEVm4nueDhAdXLf415RTjeaWtTXAYmzt 3DPdqx6XmYYy8xHHGpDAWF11hgr2p9haJC 3NXw29XKboggJ2uKFsoFTbmGb8ruxWSnb9	→	3DRd67QsAxSFYw8DrjezUvi6Gg2p6JSFhn 194GNxUafLz1kUeZcR9JYGusgUTJH5ucsz	0.01552402 BTC 1.00000002 BTC

5 Confirmations | 1.01552404 BTC

Summary	
Size	934 (bytes)
Weight	2122
Received Time	2018-10-04 12:13:34
Lock Time	Block: 544346
Included In Blocks	544348 (2018-10-04 12:23:55 + 10 minutes)
Confirmations	5
Visualize	View Tree Chart

Inputs and Outputs	
Total Input	1.02084404 BTC
Total Output	1.01552404 BTC
Fees	0.00532 BTC
Fee per byte	569.593 sat/B
Fee per weight unit	250.707 sat/WU
Estimated BTC Transacted	1.00000002 BTC
Scripts	Show scripts & coinbase

Source: https://www.blockchain.com

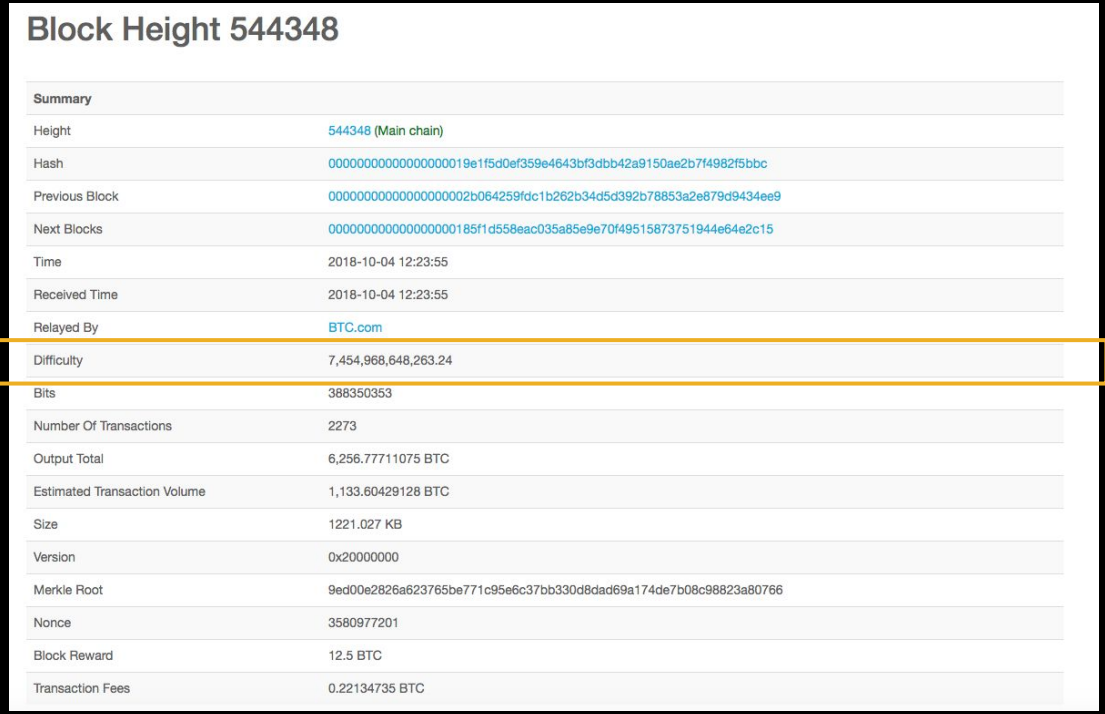
Mining

The cryptographic puzzle that miners solve is to identify the value of nonce so that the hash output of the block being mined starts with a specific number of leading zeroes.

The number of leading zeroes to achieve is called the difficulty of the Blockchain network at the time of mining.

The difficulty is decided by the Blockchain network itself. The difficulty is adjusted periodically as a function of how much hashing power has been deployed by the network of miners.

Mining



Block Height 544348

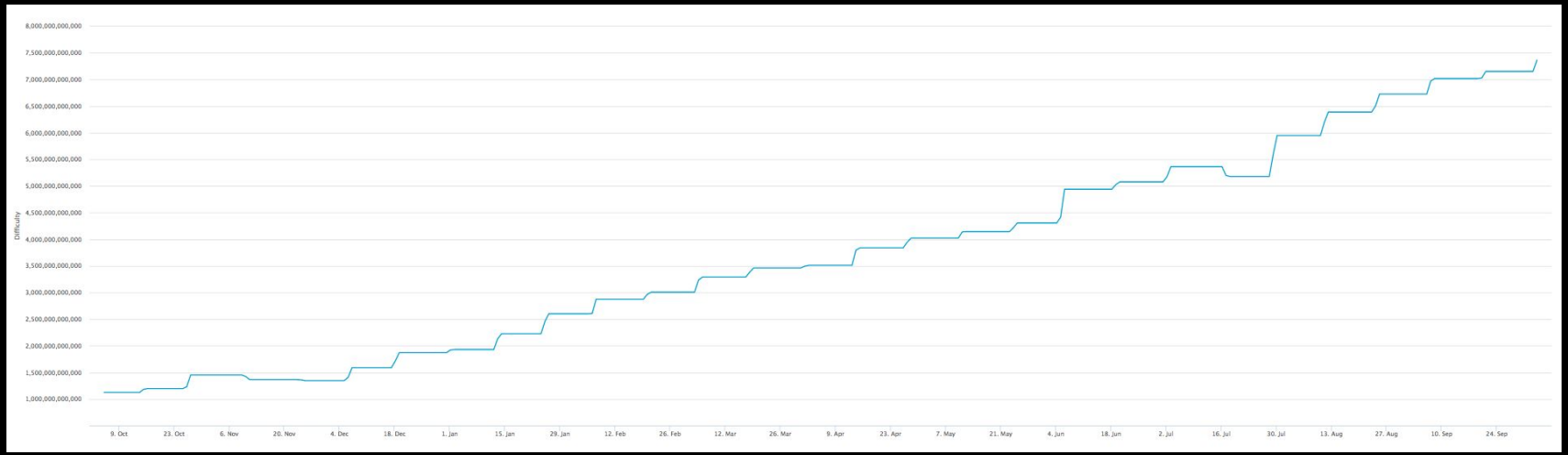
Summary	
Height	544348 (Main chain)
Hash	000000000000000000019e1f5d0ef359e4643bf3dbb42a9150ae2b7f4982f5bbc
Previous Block	000000000000000000002b064259fdc1b262b34d5d392b78853a2e879d9434ee9
Next Blocks	000000000000000000185f1d558eac035a85e9e70f49515873751944e64e2c15
Time	2018-10-04 12:23:55
Received Time	2018-10-04 12:23:55
Relayed By	BTC.com
Difficulty	7,454,968,648,263.24
Bits	388350353
Number Of Transactions	2273
Output Total	6,256.77711075 BTC
Estimated Transaction Volume	1,133.60429128 BTC
Size	1221.027 KB
Version	0x20000000
Merkle Root	9ed00e2826a623765be771c95e6c37bb330d8dad69a174de7b08c98823a80766
Nonce	3580977201
Block Reward	12.5 BTC
Transaction Fees	0.22134735 BTC

Mining

Duration	Number of Blocks Mined
10 minutes	1
1 Hour	6
1 Day	144
2 Weeks	2016
365 Days	52560
4 years	210240

The block generation difficulty calibrates every 2016 blocks, to keep the block generation within average of a single block every 10 minutes.

Mining



Source: https://www.blockchain.com/en/charts/difficulty

Years	Years Since Inception	Total Number of Blocks	Mining Reward (BTC)	Total Mined BTC
2008 - 2012	0 - 4	210000	50	10500000
2012 - 2016	4 - 8	420000	25	15750000
2016 - 2020	8 - 12	630000	12.5	18375000
2020 - 2024	12 - 16	840000	6.25	19687500
2024 - 2028	16 - 20	1050000	3.125	20343750
2028 - 2032	20 - 24	1260000	1.5625	20671875
2032 - 2036	24 - 28	1470000	0.78125	20835937.5
2036 - 2040	28 - 32	1680000	0.390625	20917968.75
2040 - 2044	32 - 36	1890000	0.1953125	20958984.38
2044 - 2048	36 - 40	2100000	0.09765625	20979492.19
2048 - 2052	40 - 44	2310000	0.048828125	20989746.09
2052 - 2056	44 - 48	2520000	0.0244140625	20994873.05
2056 - 2060	48 - 52	2730000	0.01220703125	20997436.52
2060 - 2064	52 - 56	2940000	0.006103515625	20998718.26
2064 - 2068	56 - 60	3150000	0.003051757813	20999359.13
2068 - 2072	60 - 64	3360000	0.001525878906	20999679.57
2072 - 2076	64 - 68	3570000	0.0007629394531	20999839.78
2076 - 2080	68 - 72	3780000	0.0003814697266	20999919.89
2080 - 2084	72 - 76	3990000	0.0001907348633	20999959.95
2084 - 2088	76 - 80	4200000	0.00009536743164	20999979.97
2088 - 2092	80 - 84	4410000	0.00004768371582	20999989.99
2092 - 2096	84 - 88	4620000	0.00002384185791	20999994.99
2096 - 2100	88 - 92	4830000	0.00001192092896	20999997.5
2100 - 2104	92 - 96	5040000	0.000005960464478	20999998.75
2104 - 2108	96 - 100	5250000	0.000002980232239	20999999.37
2108 - 2112	100 - 104	5460000	0.000001490116119	20999999.69
2112 - 2116	104 - 108	5670000	0.0000007450580597	20999999.84
2116 - 2120	108 - 112	5880000	0.0000003725290298	20999999.92
2120 - 2124	112 - 116	6090000	0.0000001862645149	20999999.96
2124 - 2128	116 - 120	6300000	0.00000009313225746	20999999.98
2128 - 2132	120 - 124	6510000	0.00000004656612873	20999999.99
2132 - 2136	124 - 128	6720000	0.00000002328306437	21000000
2136 - 2140	128 - 132	6930000	0.00000001164153218	21000000

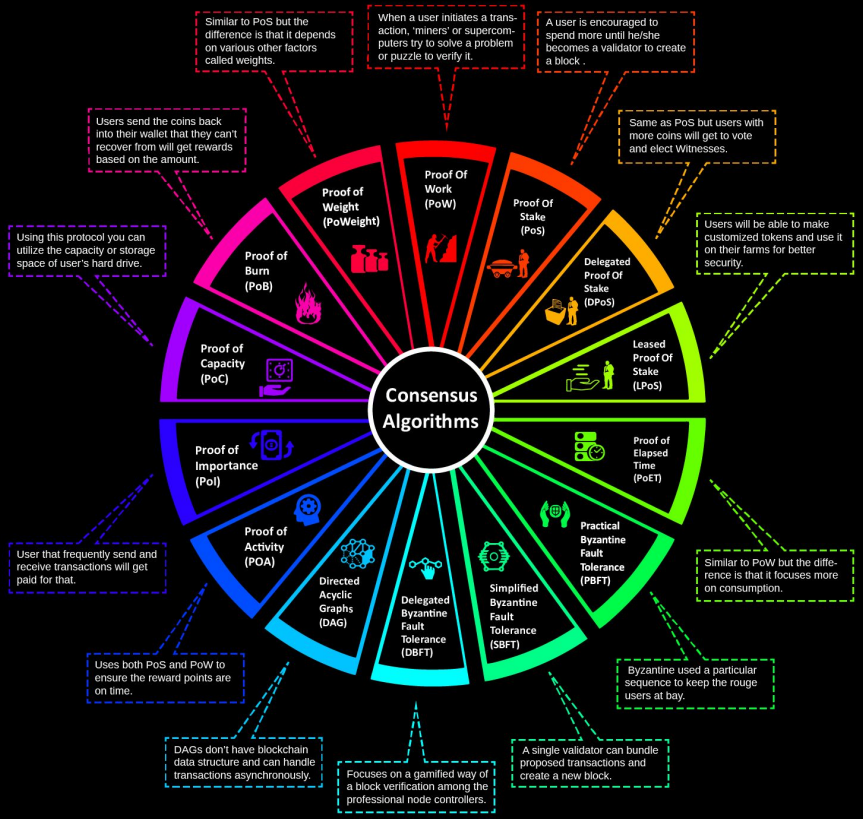
Mining Reward

Current Mining Reward (BTC)	12.5 BTC
Current Mining Reward (USD)	81681.38 USD (Hardware + Power + Network Bandwidth)

Country	Cost of Mining 1 Bitcoin (USD)
Venezuela	531 USD
India	3274 USD
China	3172 USD
United States	4758 USD
Germany	14275 USD

Source: https://www.marketwatch.com/story/heres-how-much-it-costs-to-mine-a-single-bitcoin-in-your-country-2018-03-06

Consensus Algorithms



Source: https://101blockchains.com/consensus-algorithms-blockchain/

War of frameworks

	Etherum	Hyperledger	MultiChain	IOTA (Tangle)	Corda	Ripple	Bitcoin
Description	General Purpose	General Purpose	Payments Blockchain	General Purpose (DAG)	Financial	Payments Blockchain	Payments Blockchain
Mode of Operation	Public or Private	Private	Private		Private	Private	Public
Governance	Etherum Developers	Linux Foundation	Coin Sciences	IOTA Foundation	R3 Consortium	Ripple Labs	Bitcoin Foundation
Consensus	Proof of Work	Configurable	Mining Diversity (Round Robin)	Transaction initiator to validate last 2 transactions	Transaction initiator to validate last 2 transactions	Ripple Protocol (Probabilistic Voting)	Proof of Work
Programming Language	Solidity	Go, Java Rich Tools & Frameworks	Multi-language	Javascript, Abra	Kotlin, Java	-	-
Currency	Ether	-	-	IOTA	-	XRP	BTC
Transactions	45 tps	1000+ tps	10000+tps*	800 - 1000 tps	150 - 1500 tps	1500 tps	10 tps

DAPPS

Source: https://scovan.ca/the-future-is-cryptic/web-3-0/

Applications

Automotive

Vehicle Tracking
Health Monitoring
Fleet Management
Claims Settlement
Usage based Insurance
Vehicle Lifecycle
Ride Sharing
Theft Prevention
Logistics Networks

Finance

Global Payments
Remittance
P2P Lending
Microfinance
Trade Settlement
Insurance
Secondary Market
Multiparty Contracts
Credit History

Legal

Intellectual Property
Title Records
Digital Rights
Escrow/ Custodian Services
Cybersecurity
Wills and Inheritances
Digital Identity

Healthcare

Health databanks
Peer to peer insurance
Drug supply chain integrity
Clinical Trial Provenance

Others...

Music Streaming
Smart Utility Metering
Fine Art Trading

Internet of Things

Smartcities
Connected Cars
Smart homes
Digital Assistants