BLOCKCHAIN

The foundation behind Bitcoin

Sourav Sen Gupta
Indian Statistical Institute, Kolkata

CRYPTOGRAPHY

Backbone of Blockchain Technology

Component 1 : Cryptographic Hash Functions

HASH FUNCTIONS

$$h : \{0,1\}^* \rightarrow \{0,1\}^n$$

Map *variable-length* input to *constant-length* output.

HASH FUNCTIONS

$$h : \{0,1\}^* \rightarrow \{0,1\}^n$$

Finding the pre-image of a *given* output is not *easy*.

HASH FUNCTIONS

$$h : \{0,1\}^* \rightarrow \{0,1\}^n$$

Finding a colliding twin of a *given* input is not *easy*.

HASH FUNCTIONS

$$h : \{0,1\}^* \rightarrow \{0,1\}^n$$

Finding any colliding *pair* of inputs is not *easy*.

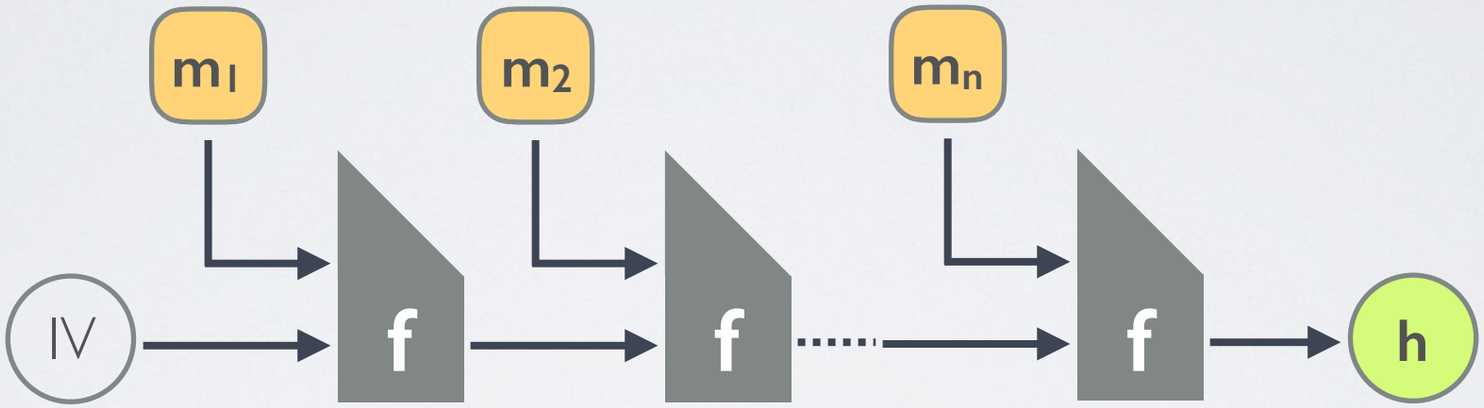
It is of course possible, but not easy.

HASH FUNCTIONS

$$h : \{0,1\}^* \rightarrow \{0,1\}^n$$

Minor input-*mismatch* to major output-*mismatch*.

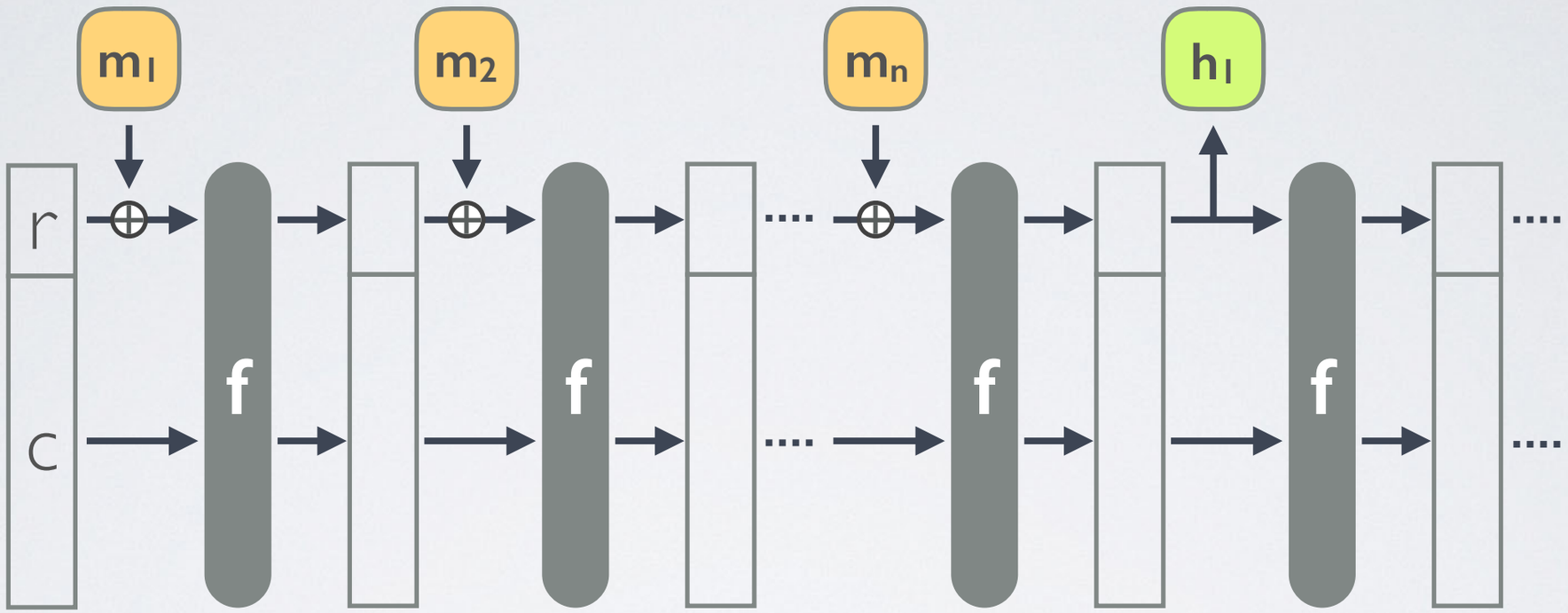
CONSTRUCTIONS



Merkle-Damgard Construction

Example : SHA 256 — used in Bitcoin

CONSTRUCTIONS

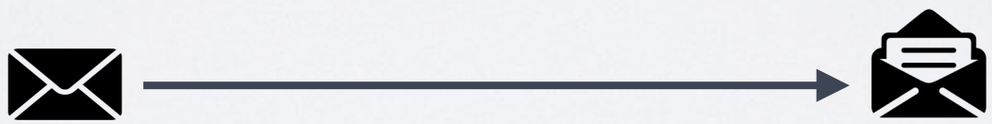


Sponge Construction

Example : SHA 3 — used in Ethereum

APPLICATIONS

commit(x) :
c = h(r || x)



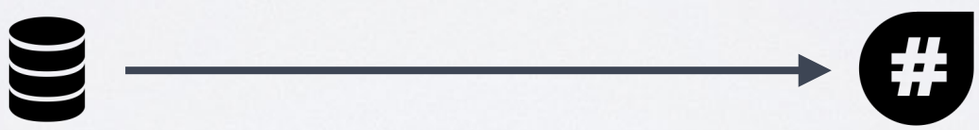
verify(c,r,x) :
h(r || x) == c

Provably secure scheme for Commitment

Random nonce **r** must have a high min-entropy for this scheme to be secure.

APPLICATIONS

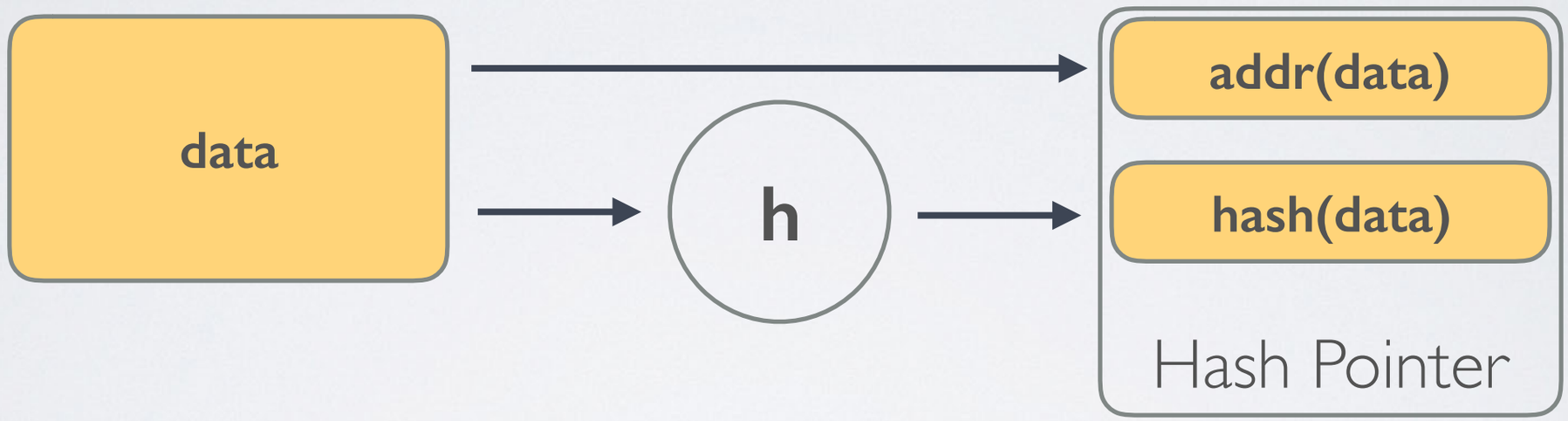
record(x) :
c = h(x)



verify(c,x) :
h(x) == c

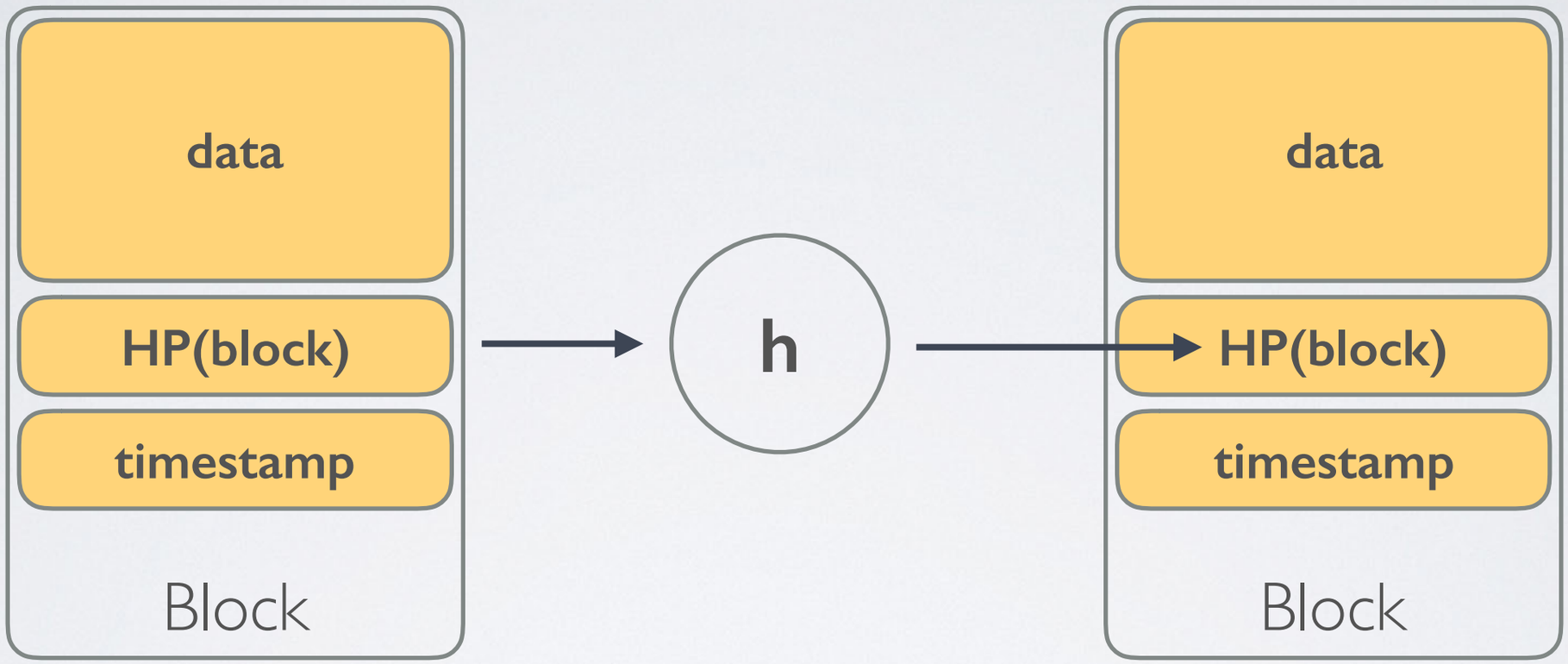
Provably secure scheme for tamper-detection

DATA STRUCTURES



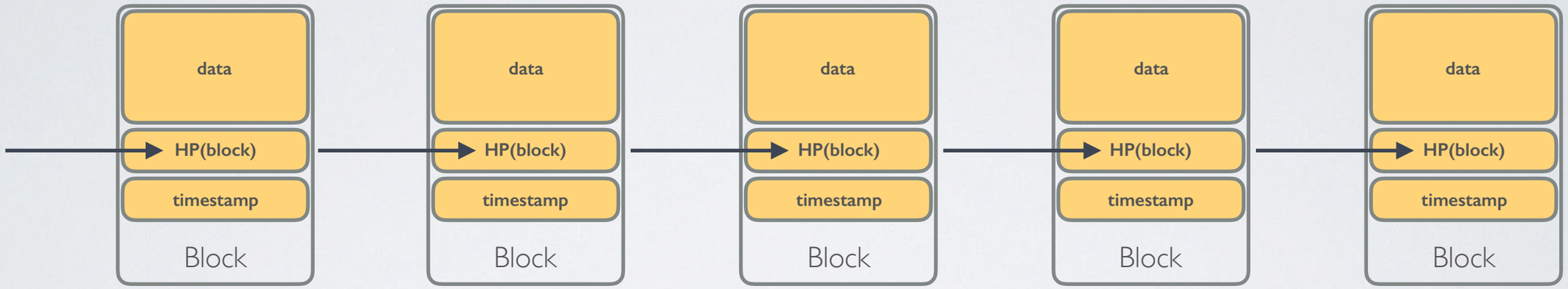
Tamper-evident data pointer = Hash Pointer

DATA STRUCTURES



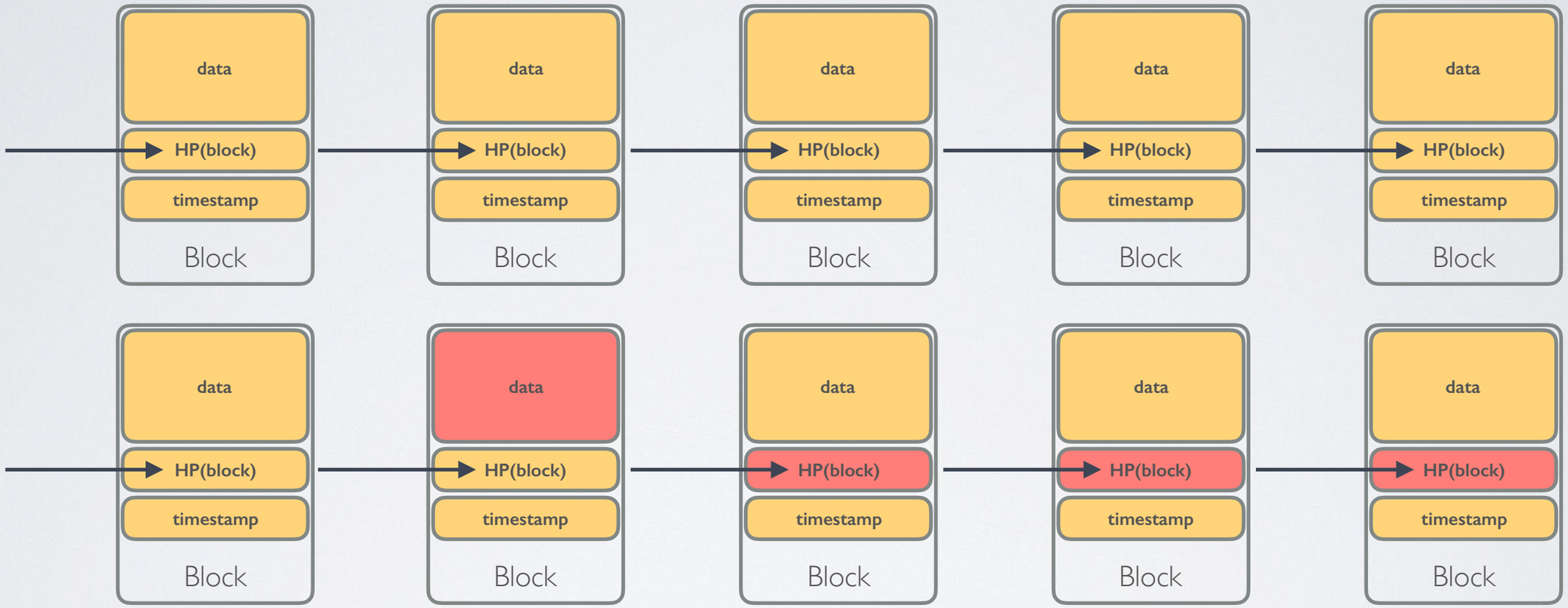
Tamper-evident linked data structure = Block

DATA STRUCTURES



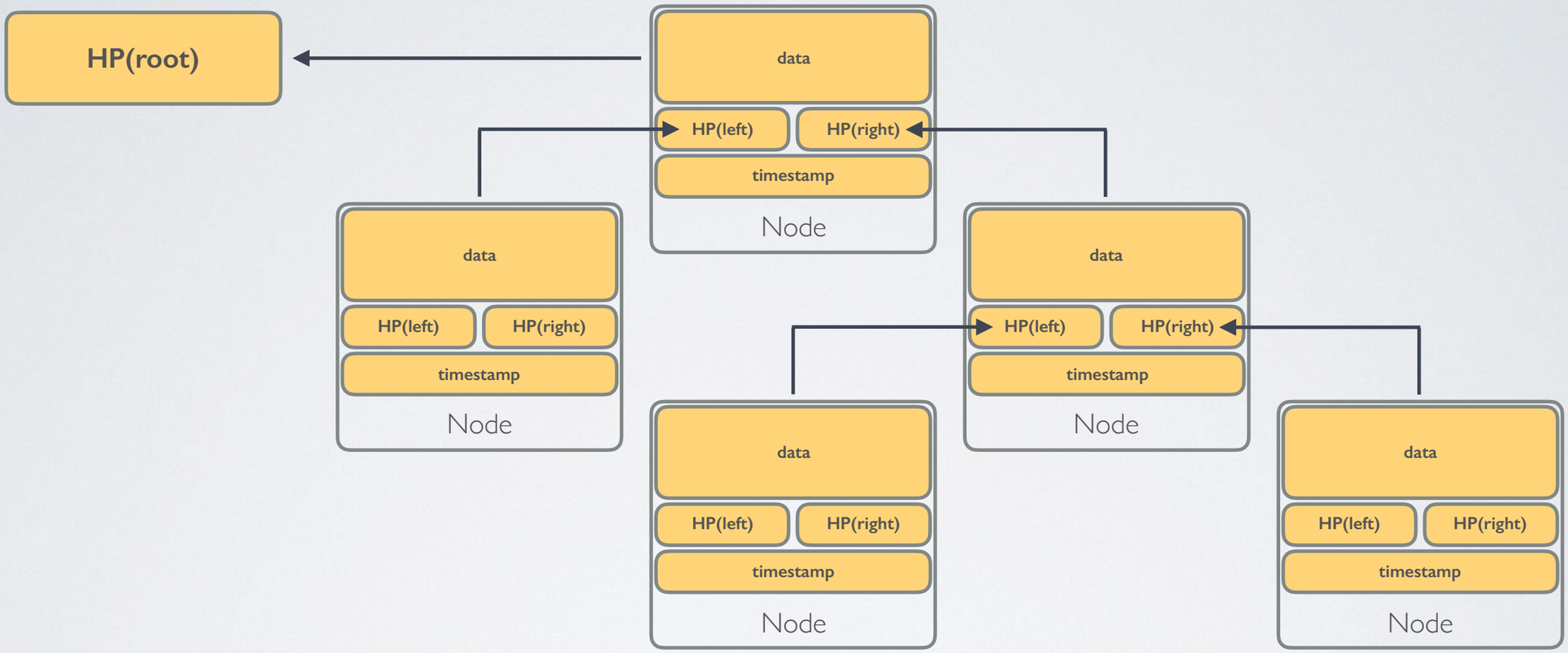
Tamper-evident linked-list = Blockchain

DATA STRUCTURES



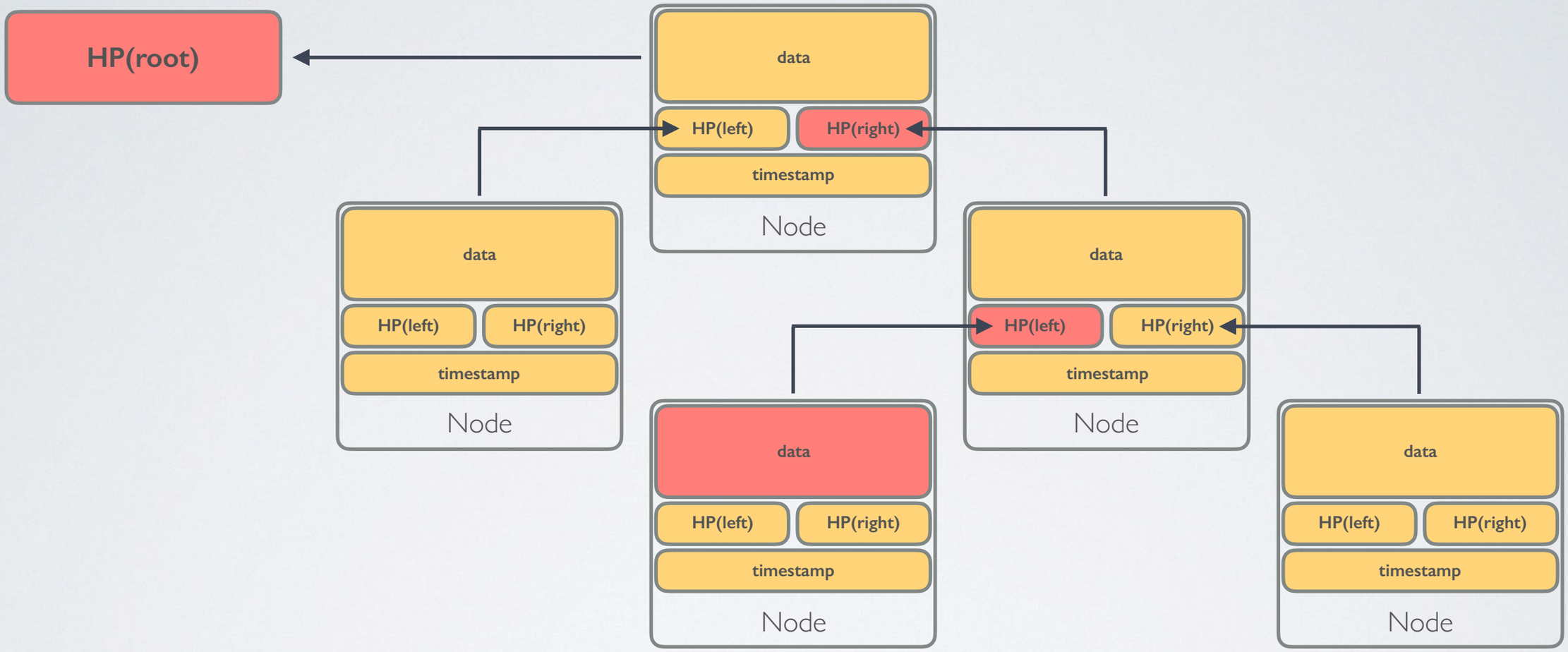
Tamper-evident linked-list = Blockchain

DATA STRUCTURES



Tamper-evident binary-tree = Merkle Tree

DATA STRUCTURES



Tamper-evident binary-tree = Merkle Tree

DATA STRUCTURES

Properties	**Blockchain**	**Merkle Tree**	**Merkle Trie**
Size of Commitment	**O(1)**	**O(1)**	**O(1)**
Append a Block/Node	**O(1)**	**O(log n)**	**O(k)**
Update a Block/Node	**O(n)**	**O(log n)**	**O(k)**
Proof of Membership	**O(n)**	**O(log n)**	**O(k)**
Structural Abstraction	***List of Objects***	***Set of Objects***	***Set of (key, value)***
Used for Construction	***Bitcoin***	***Bitcoin***	***Ethereum***

QUESTIONS

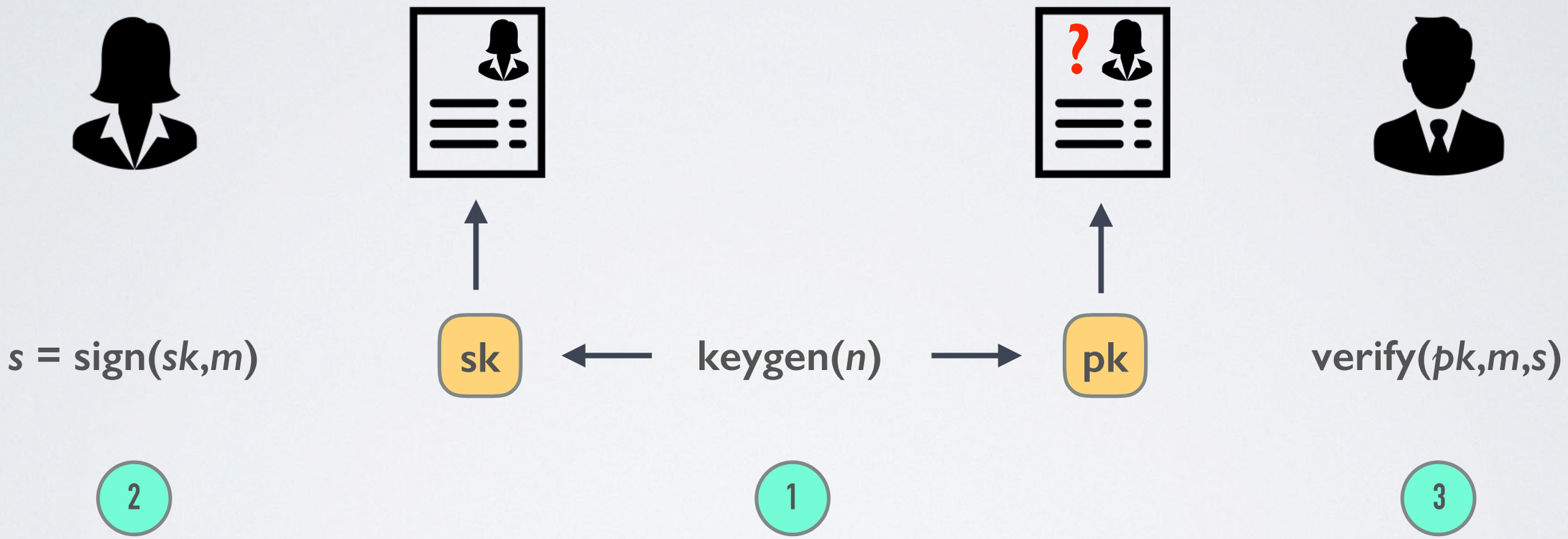
Can any pointer-based data structure be efficiently converted into a Hash-Pointer based data structure?

Will such an exercise be at all useful in any use case?

Do these structures provide any additional advantage?

Component 2 : Digital Signature Schemes

DIGITAL SIGNATURE

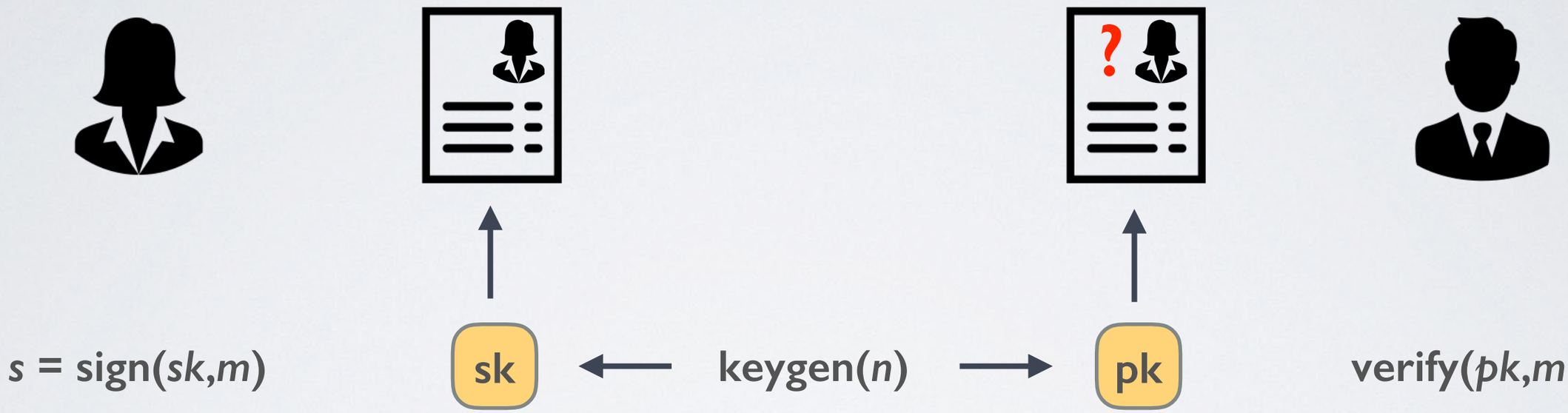


Digital signature as a set of three algorithms

DIGITAL SIGNATURE

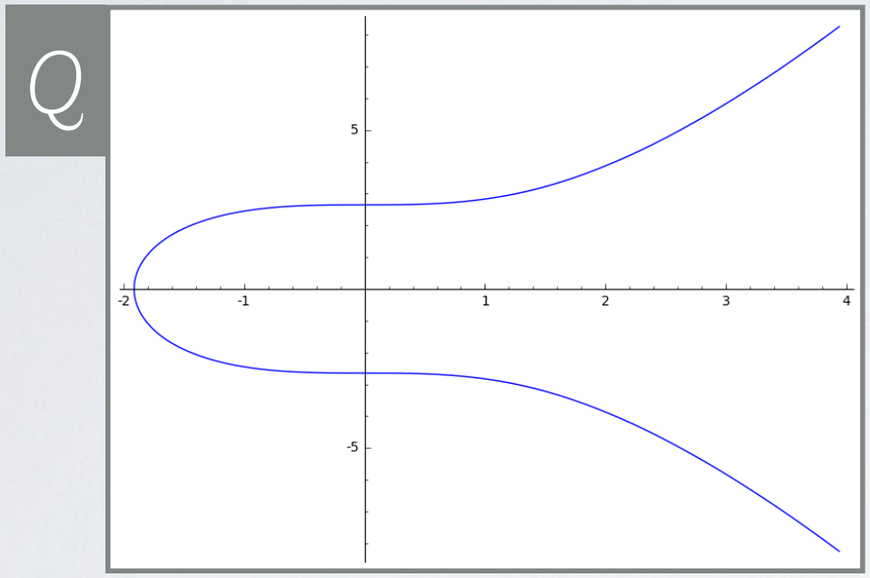
$(sk, pk) = \text{keygen}(n) \longrightarrow \text{verify}(pk, m, \text{sign}(sk, m)) = \text{True}$

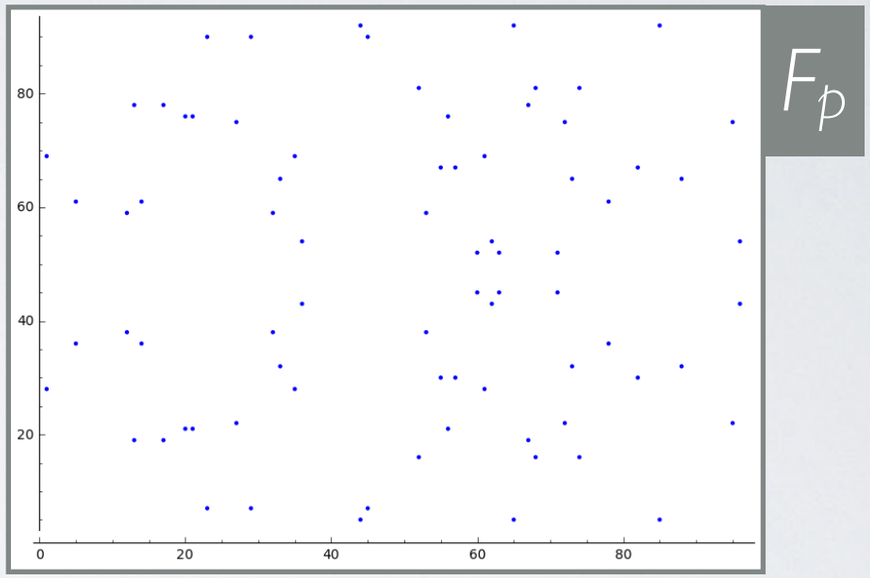
DIGITAL SIGNATURE



Given *pk* and access to sign(m_i) as an oracle, an adversary should not be able to create a valid fresh message-signature pair (*m*,*s*)

CONSTRUCTION





Elliptic Curve Digital Signature Algorithm (ECDSA)

ECDSA on curve $E(F_p)$: { (x,y) in F_p x F_p | $y^2 = x^3 + 7$ }
with base prime $p = 2^{256} - 2^{32} - 2^9 - 2^8 - 2^7 - 2^6 - 2^4 - 1$

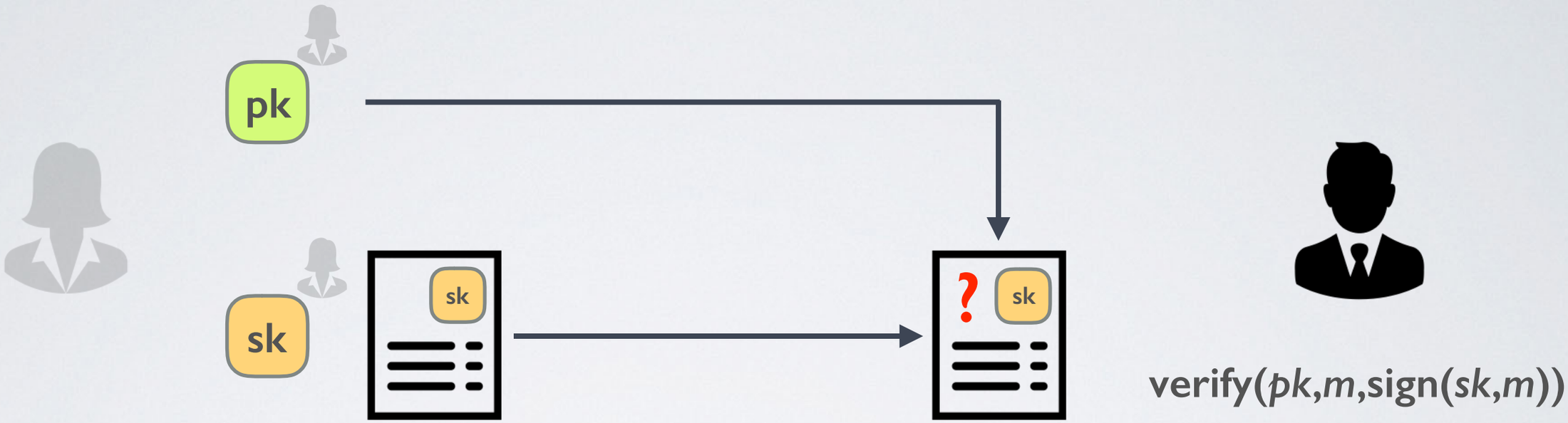
CONSTRUCTION

Elliptic Curve group of size $|E(F_p)| = q \sim p \sim 2^{256}$

Parameters	Format	Range	Bit-size
sk	random	Z_q	256
pk	*sk* x *G*	$E(F_p)$	512
m	hash(*M*)	Z_q	256
Signature	(*r*, *s*)	$Z_q \times Z_q$	512

ECDSA on curve $E(F_p)$: { (x,y) in $F_p \times F_p$ | $y^2 = x^3 + 7$ }
with base prime $p = 2^{256} - 2^{32} - 2^9 - 2^8 - 2^7 - 2^6 - 2^4 - 1$

APPLICATION



Publish the public key *pk* as your Identity

Use the secret key *sk* to prove your identity

BITCOIN

Blockchain in Practice

BITCOIN

Ledger of Transactions

between

Pseudonymous Identities

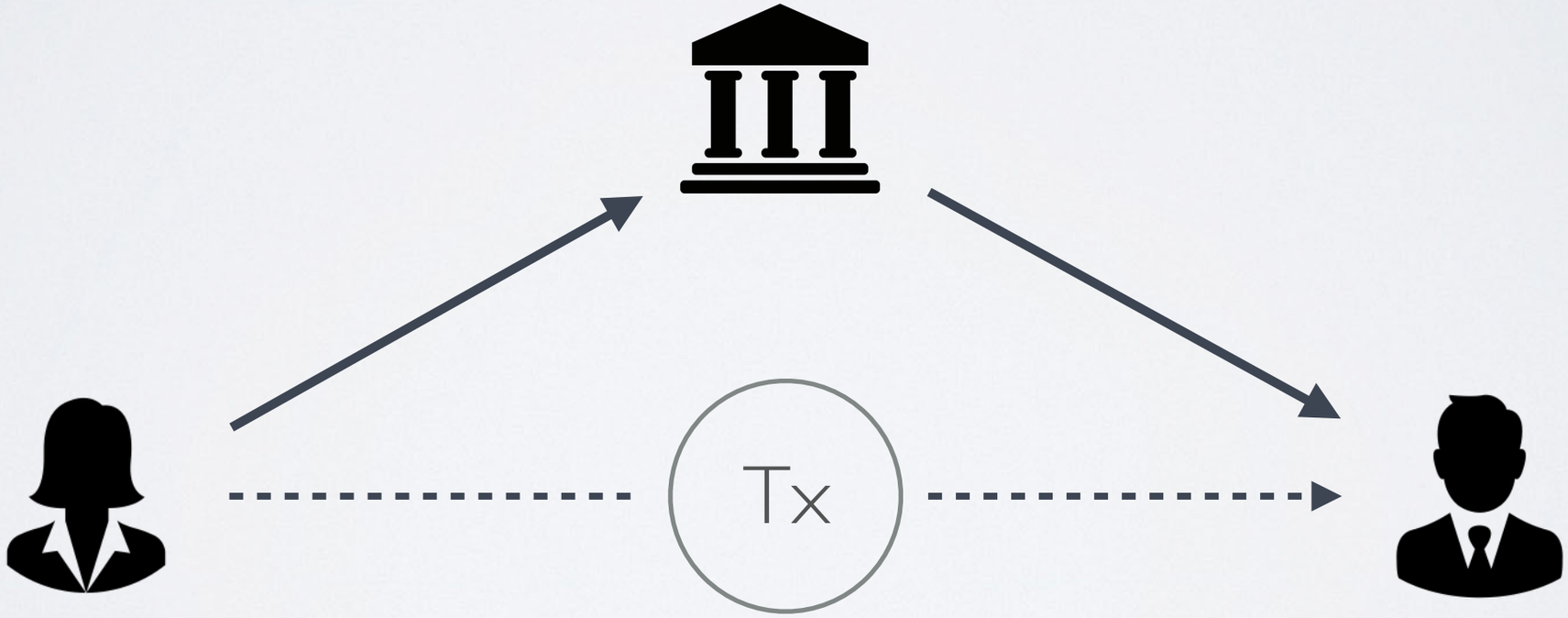
Semi-Decentralised
Tamper-Resistant

Publicly-Verifiable
Eventually-Consistent

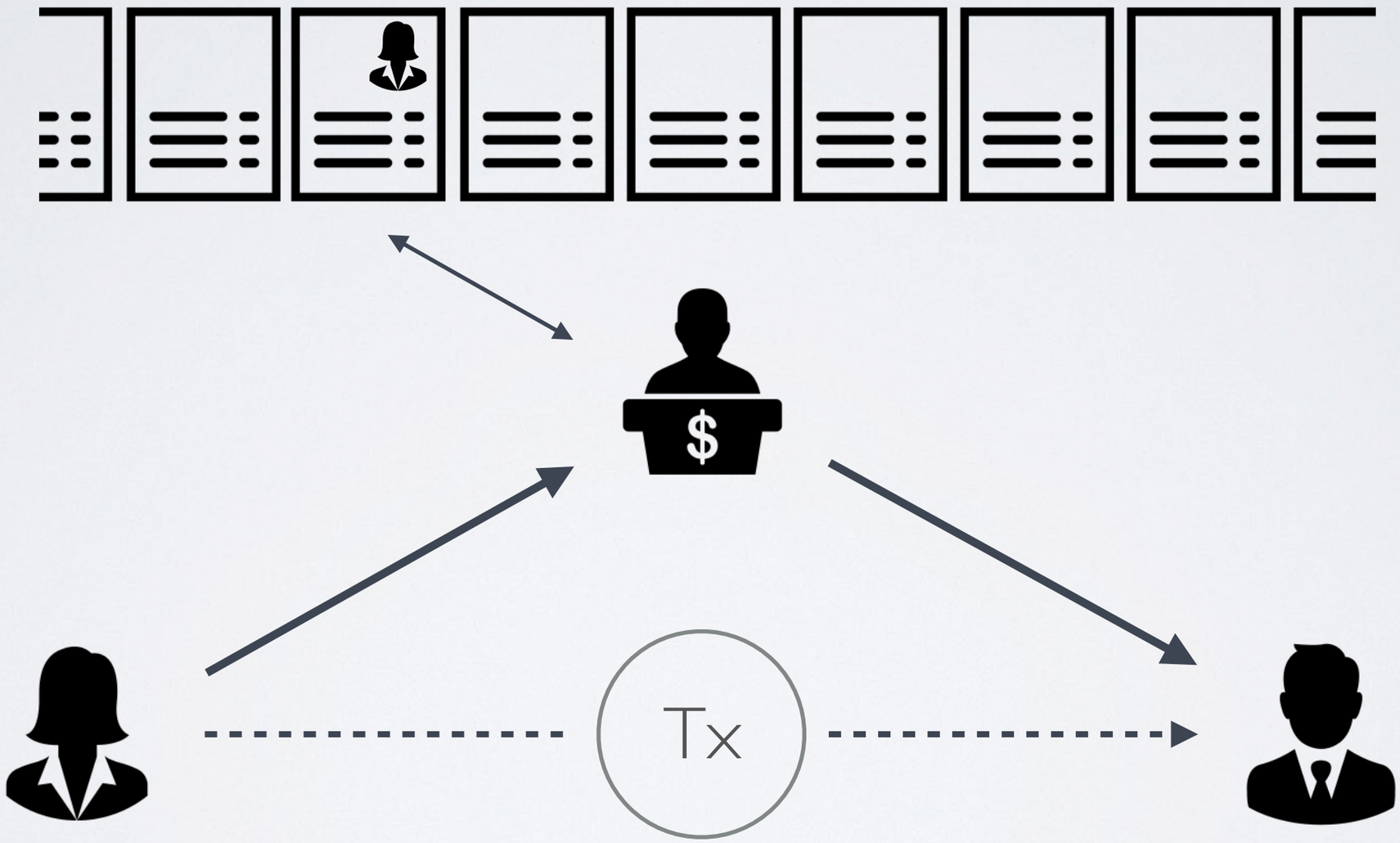
NOT BITCOIN

Economic Transaction

that we are familiar with

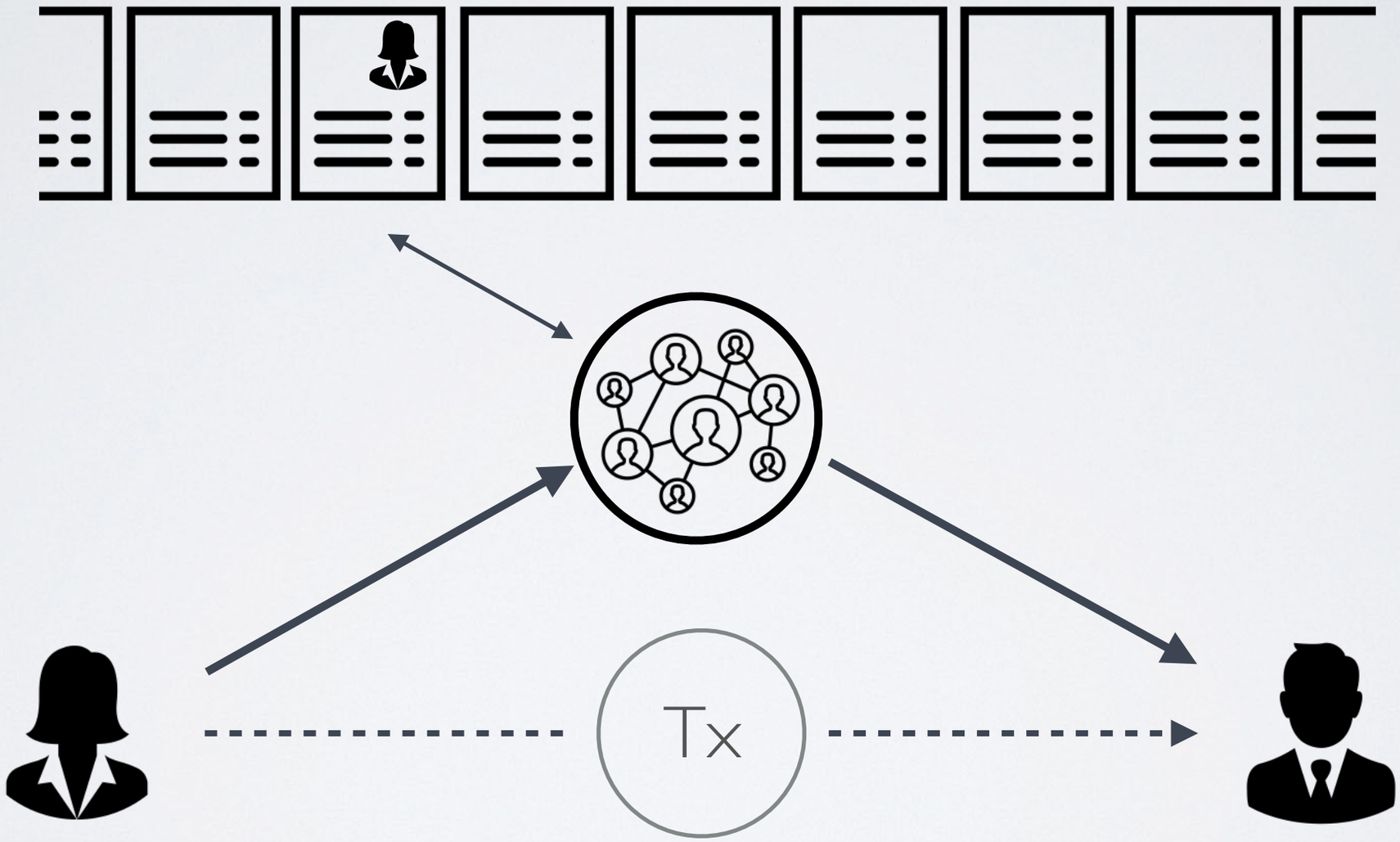


NOT BITCOIN



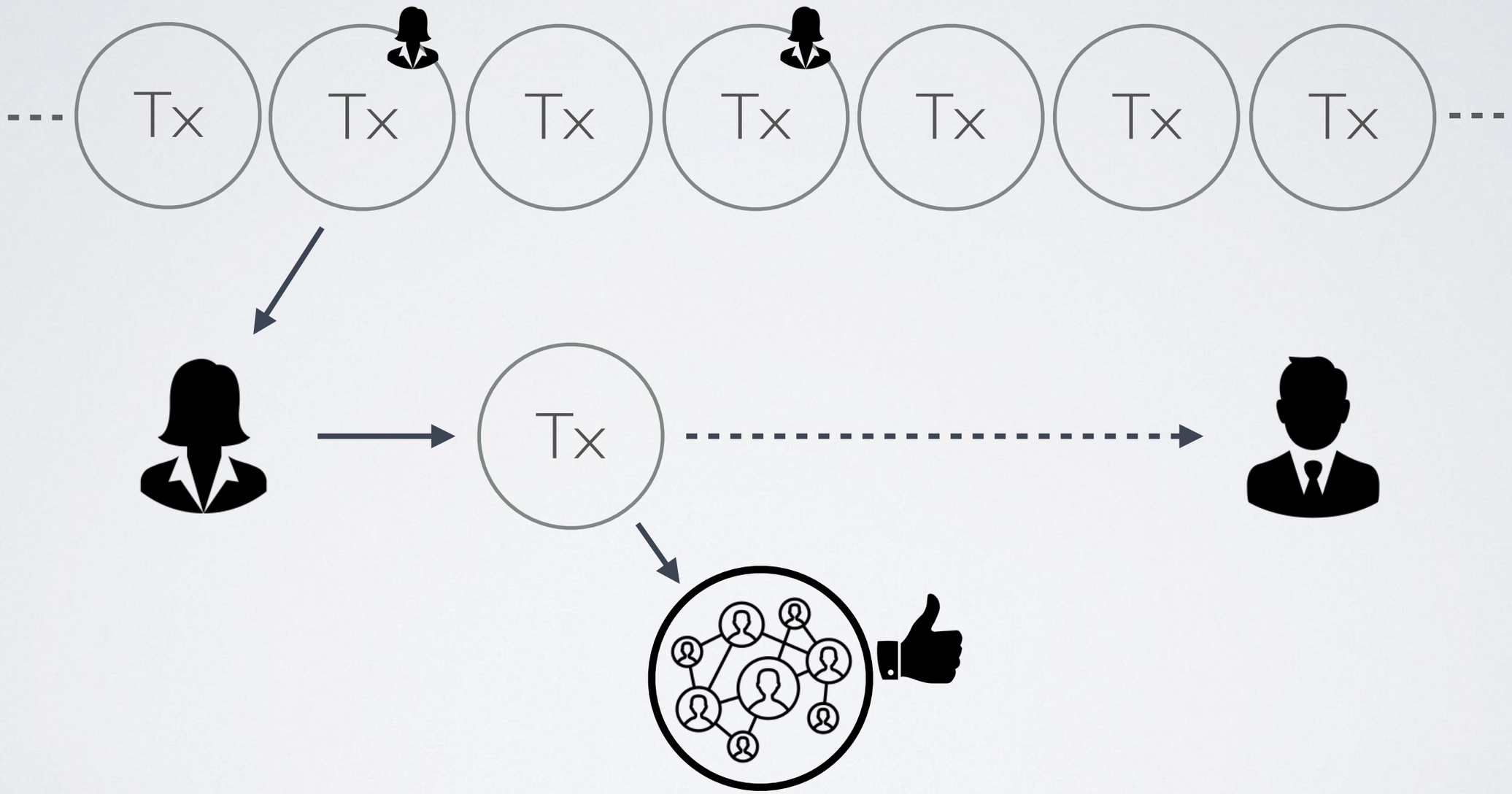
Centralised Account-based Ledger

NOT BITCOIN



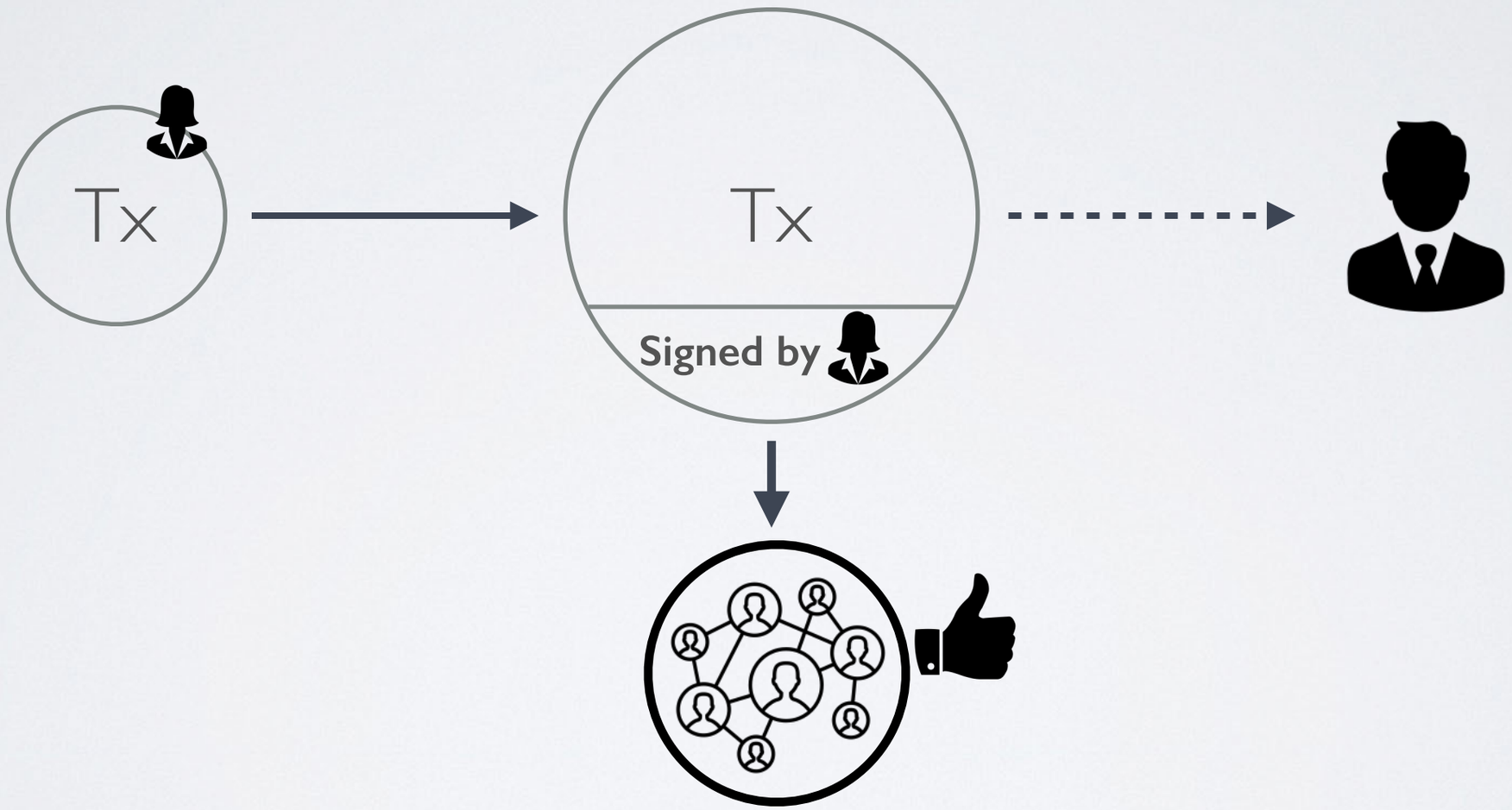
Decentralised Account-based Ledger

NOT BITCOIN YET



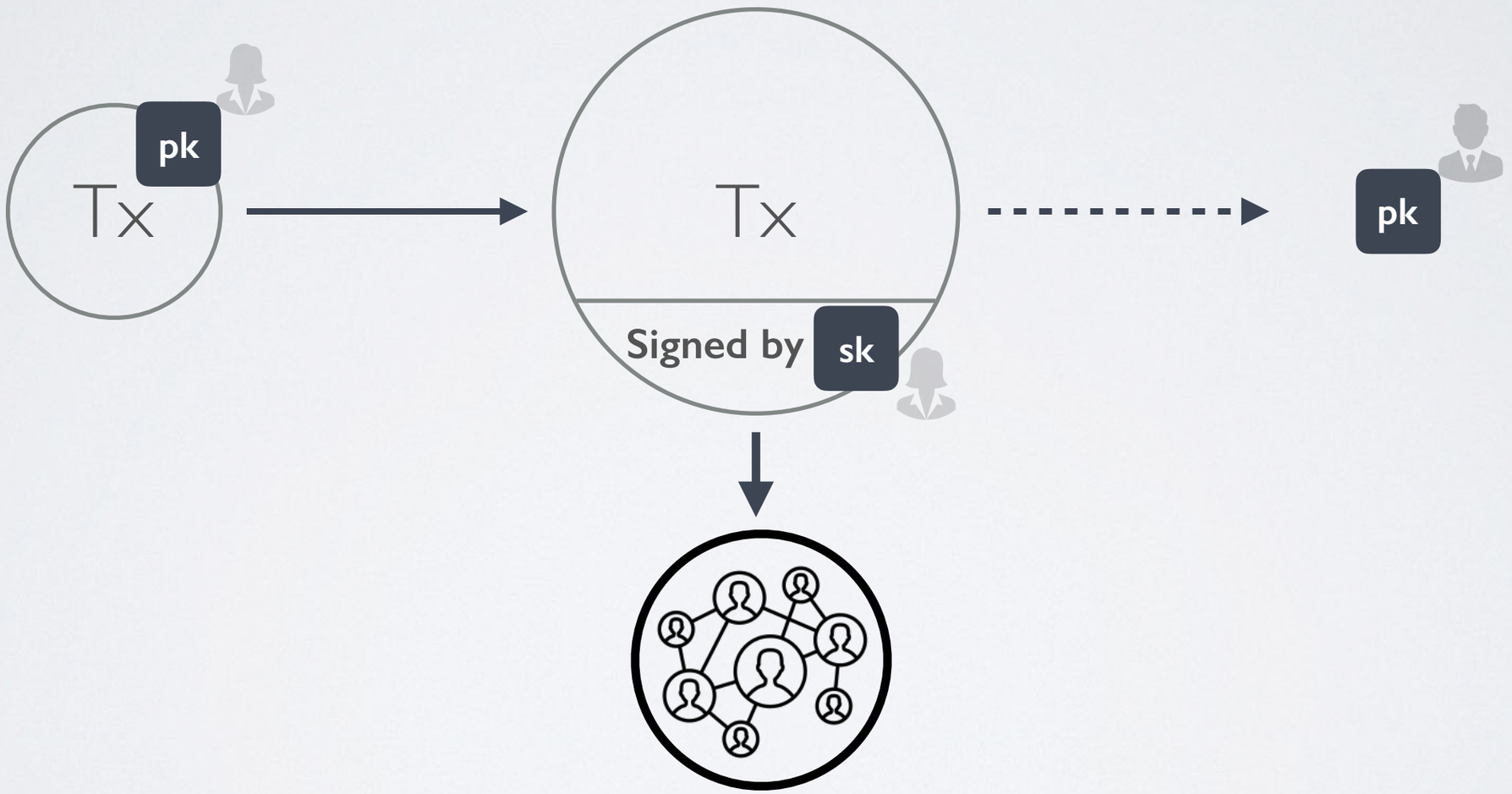
Decentralised Transaction-based Ledger

TRANSACTION



Network <u>verifies</u> the Signature

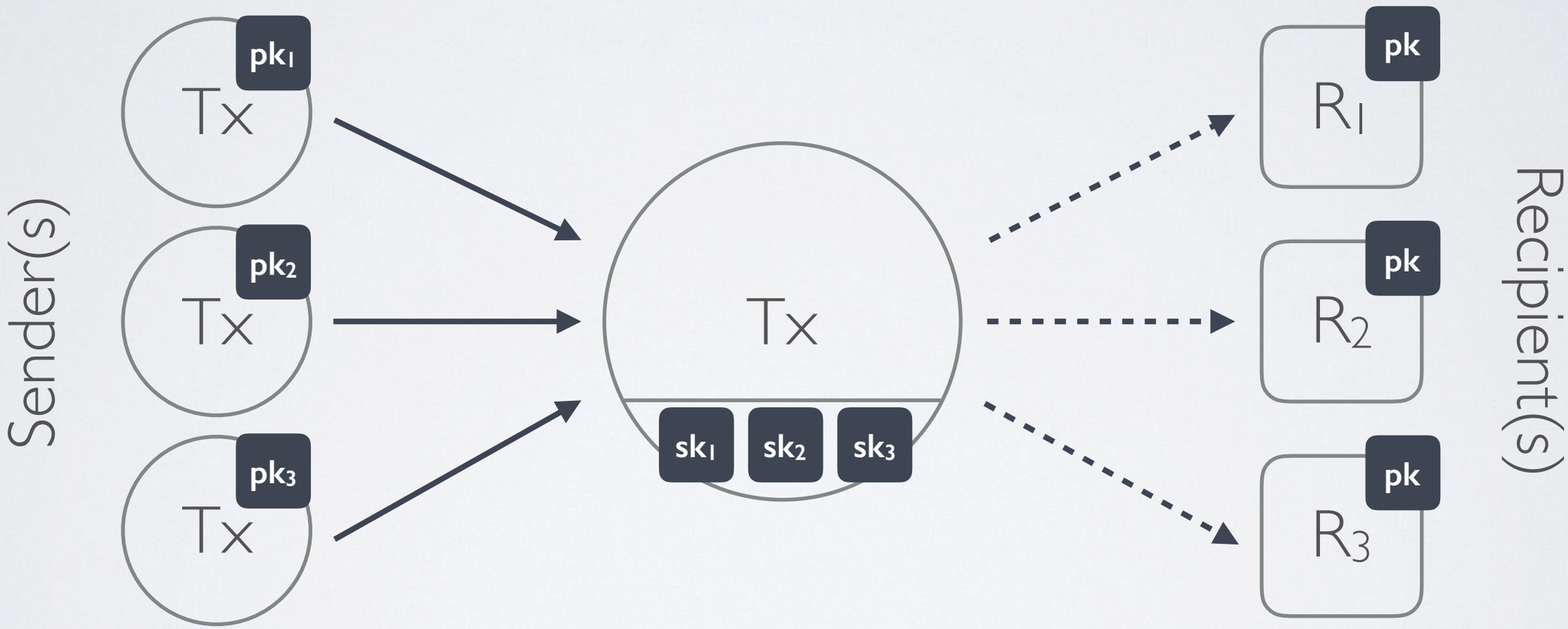
TRANSACTION



Network <u>verifies</u> the Signature

TRANSACTION

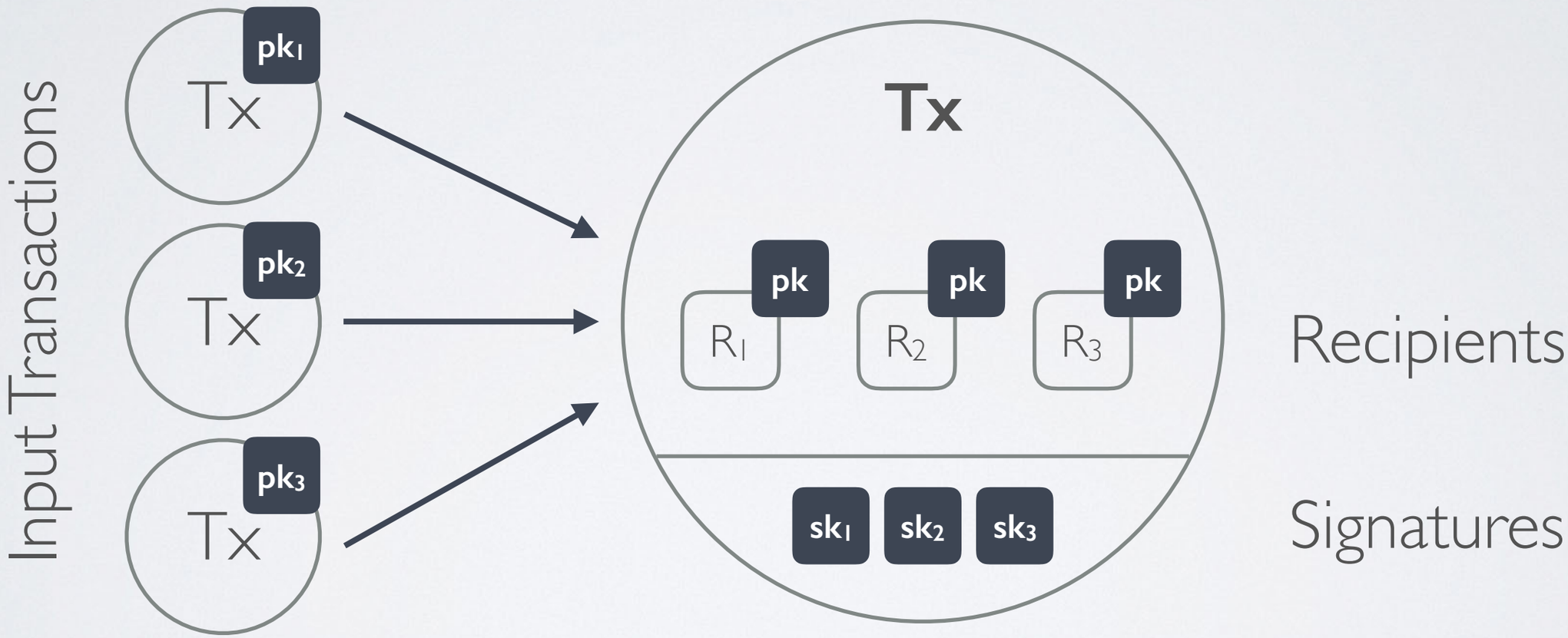
Input : Array of previous Transactions | Output : Array of recipient Addresses



Network verifies the Signature(s)

TRANSACTION

Input : Array of previous Transactions | Output : Array of recipient Addresses



Network verifies the Signature(s)

TRANSACTION

Metadata

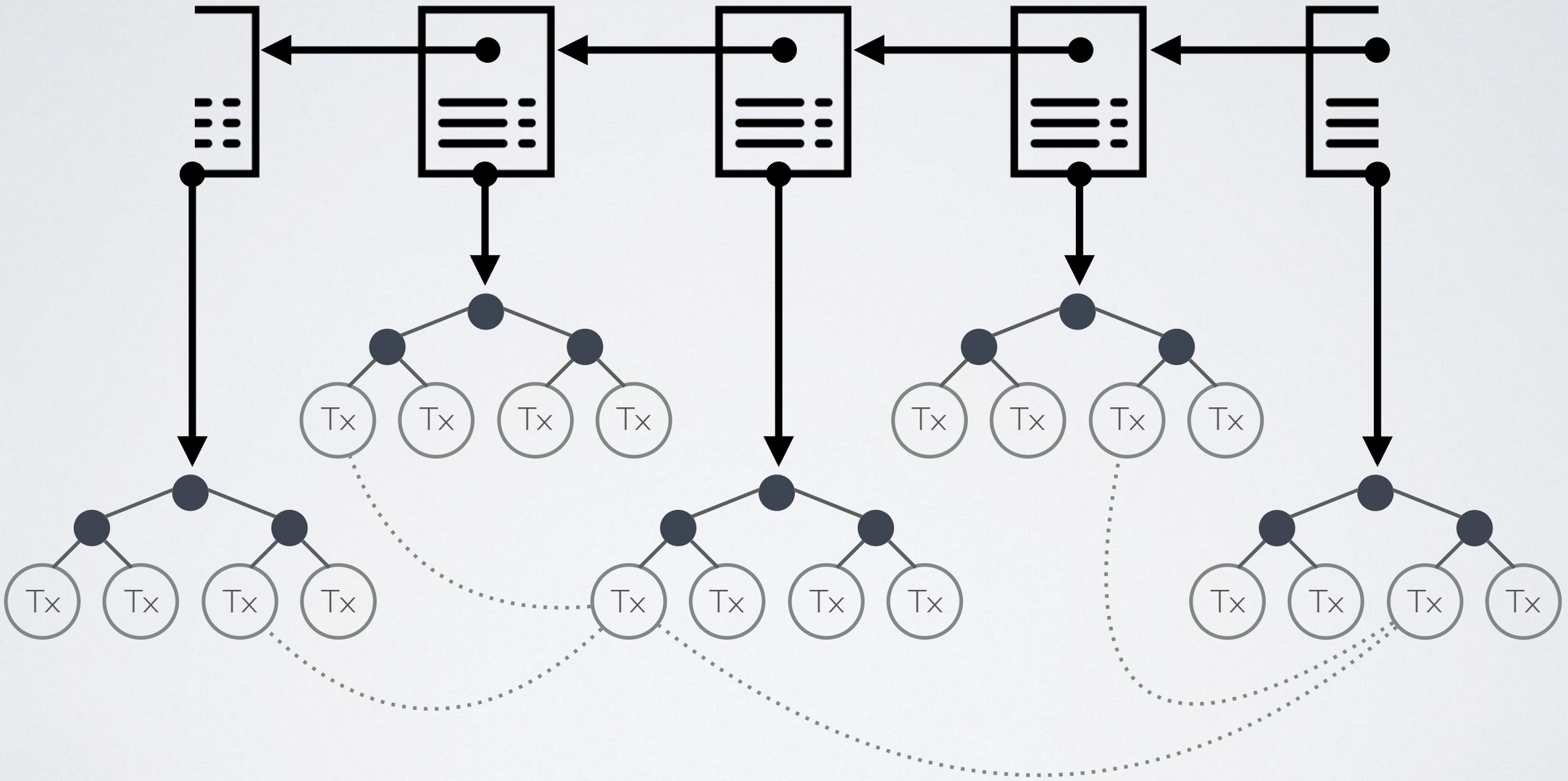
Input(s)

Output(s)


```
"hash":"b6f6991d03df0e2e04dafffcd6bc418aac66049e2cd74b80f14ac86db1e3f0da",
"ver":1,
"vin_sz":1,
"vout_sz":2,
"lock_time":"Unavailable",
"size":258,
"relayed_by":"64.179.201.80",
"block_height, 12200,
"tx_index":"12563028",
"inputs":[

        {
            "prev_out":{
                "hash":"a3e2bcc9a5f776112497a32b05f4b9e5b2405ed9",
                "value":"100000000",
                "tx_index":"12554260",
                "n":"2"
            },
            "script":"76a914641ad5051edd97029a003fe9efb29359fcee409d88ac"
        }

    ],
"out":[

            {
                "value":"98000000",
                "hash":"29d6a3540acfa0a950bef2bfdc75cd51c24390fd",
                "script":"76a914641ad5051edd97029a003fe9efb29359fcee409d88ac"
            },

            {
                "value":"2000000",
                "hash":"17b5038a413f5c5ee288caa64cfab35a0c01914e",
                "script":"76a914641ad5051edd97029a003fe9efb29359fcee409d88ac"
            }

    ]
```


Data obtained from blockchain.info

LEDGER



Decentralised Transaction-based Ledger

BLOCK


```
"hash":"0000000000000bae09a7a393a8acded75aa67e46cb81f7acaa5ad94f9eacd103",
"ver":1,
"prev_block":"00000000000007d0f98d9edca880a6c124e25095712df8952e0439ac7409738a",
"mrkl_root":"935aa0ed2e29a4b81e0c995c39e06995ecce7ddbebb26ed32d550a72e8200bf5",
"time":1322131230,
"bits":437129626,
"nonce":2964215930,
"n_tx":22,
"size":9195,
"block_index":818044,
"main_chain":true,
"height":154595,
"received_time":1322131301,
"relayed_by":"108.60.208.156",
"tx":[--Array of Transactions--]
```


Data obtained from blockchain.info

BLOCK

Block #432480

Summary	
Number Of Transactions	30
Output Total	61.8094689 BTC
Estimated Transaction Volume	11.5927698 BTC
Transaction Fees	0.00834728 BTC
Height	432480 (Main Chain)
Timestamp	2016-10-02 04:37:37
Received Time	2016-10-02 04:37:37
Relayed By	AntPool
Difficulty	241,227,200,229.99
Bits	402951892
Size	13.123 KB
Version	536870912
Nonce	1448113972
Block Reward	12.5 BTC

Hashes	
Hash	00000000000000000fde8ecc312a3d0a4fab5161269dfd8317896aeffdbab39
Previous Block	00000000000000000003781c1129ddaa2098278fe92383058425022498db13ac1b
Next Block(s)	00000000000000000358a68107974fe63cf1569cc4ba31f16e479950d04f5a7c
Merkle Root	6c200c34de7b060ddcb7c4e993b951ed643c023983b2d5755370fca9da08d86a

Network Propagation (Click To View)

Data obtained from blockchain.info

BLOCK

Transactions

d0bcae91a49d02cb71760e8aebd8d34340598454a167d19c1bdf65a86da85d11		**2016-10-02 04:37:37**
No Inputs (Newly Generated Coins)	→	1EFg9XXX1U99pNJJTeQwuuEpbHFW4XS8uL 12.50834728 BTC

12.50834728 BTC

d58bf9d6e19ca676e66811e2a407aaaf8a926157a6431bf04272919d449bed34		**2016-10-02 04:37:21**
1QCRjVTjgK8LqcMQFWfd5GSEcfE1NtrW79	→	13VArUeQJnjGKwGAfdRBdve1oke6zAcx6k 0.02782028 BTC 1EtY5A1ueGTuJZvHPJrsUgsKQwHRySYKuh 0.62616966 BTC

0.65398994 BTC

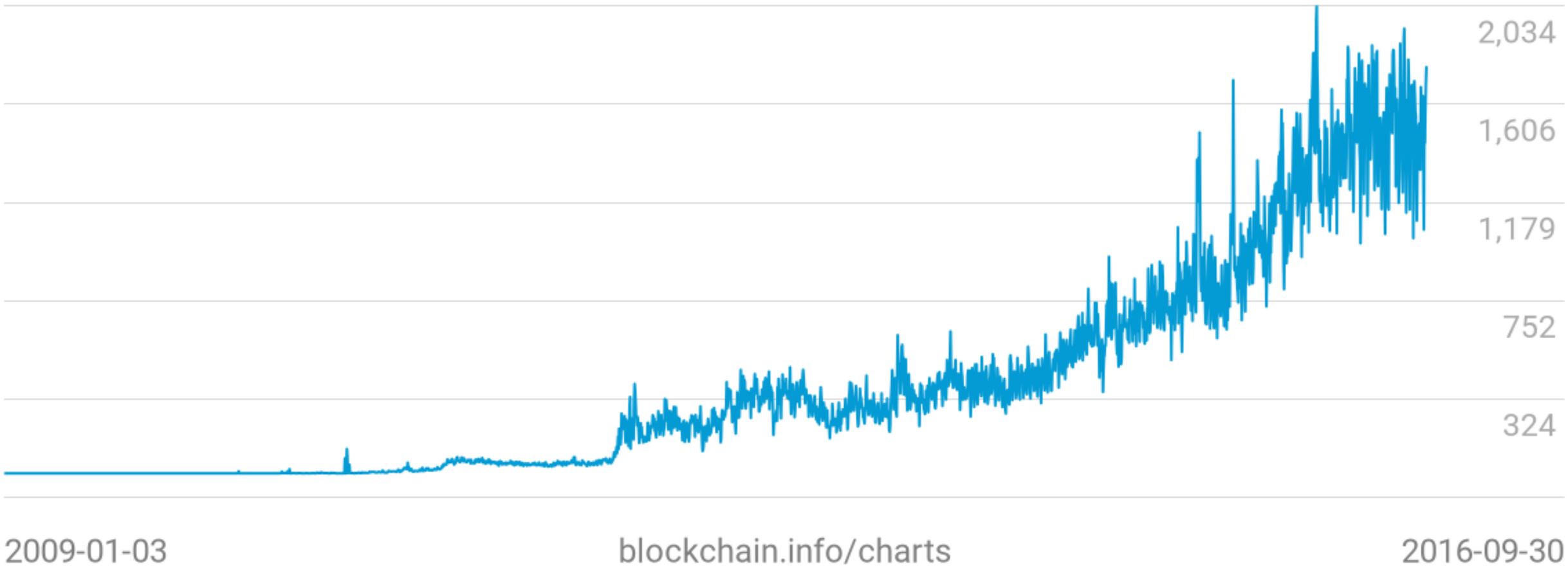
a03feb6c19c3d975f4bd5f779295d34048993d419fce64b6f0173f397dabd52d		**2016-10-02 04:37:37**
1NMSgX56XiSGp9aHzSSFp5EwxyZ3R5ABpC	→	19JDWh5ZSqKE6HbQsUECHWHwht2QbJTsAW 0.34 BTC 1GhXx4CGcNh6QEJTx2NwTLK1oFszjwa4aB 15.7935 BTC

16.1335 BTC

BLOCK

Average Number Of Transactions Per Block

1,767

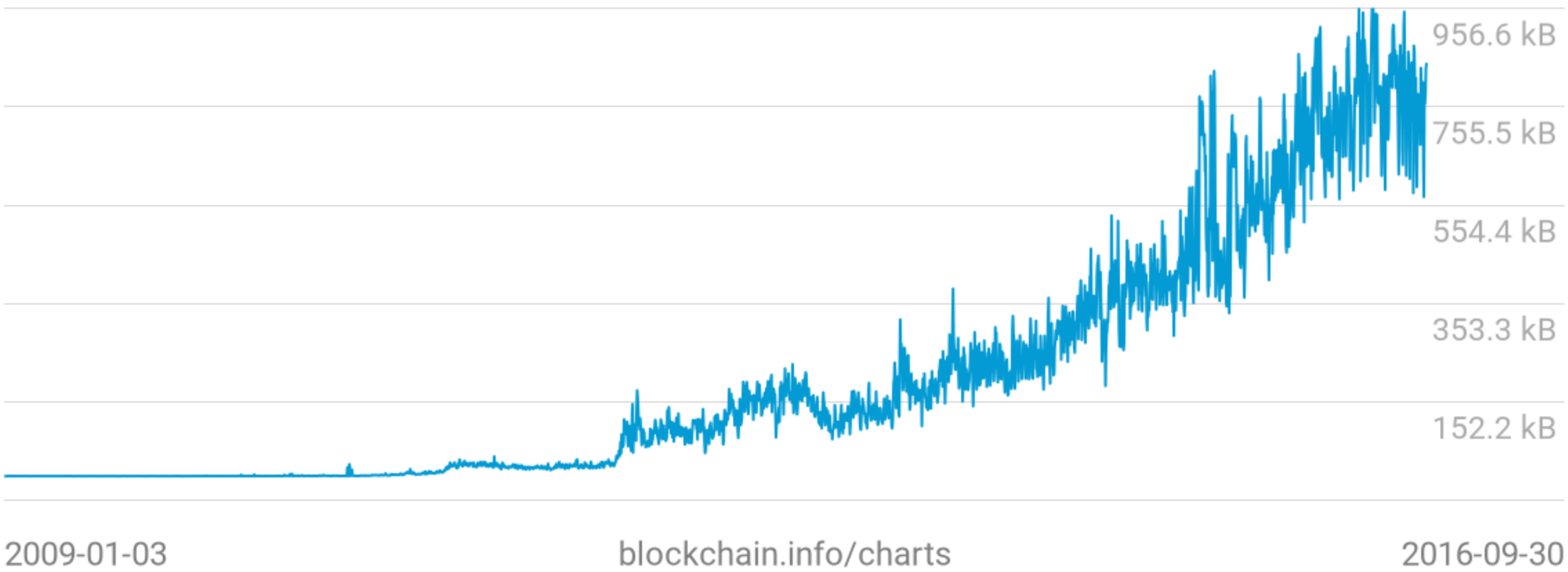


Data obtained from blockchain.info

BLOCK

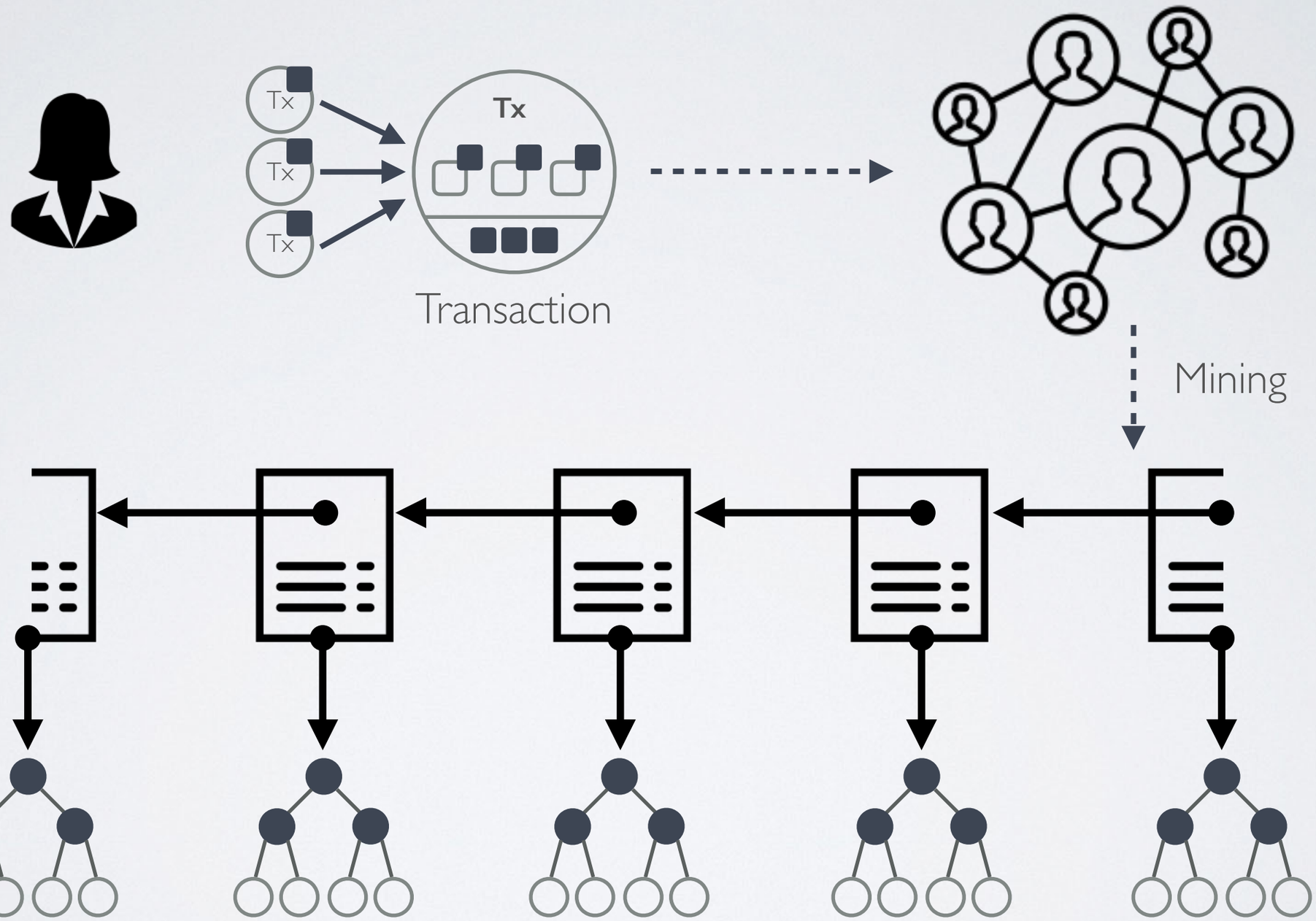
Average Block Size

843.4 kB

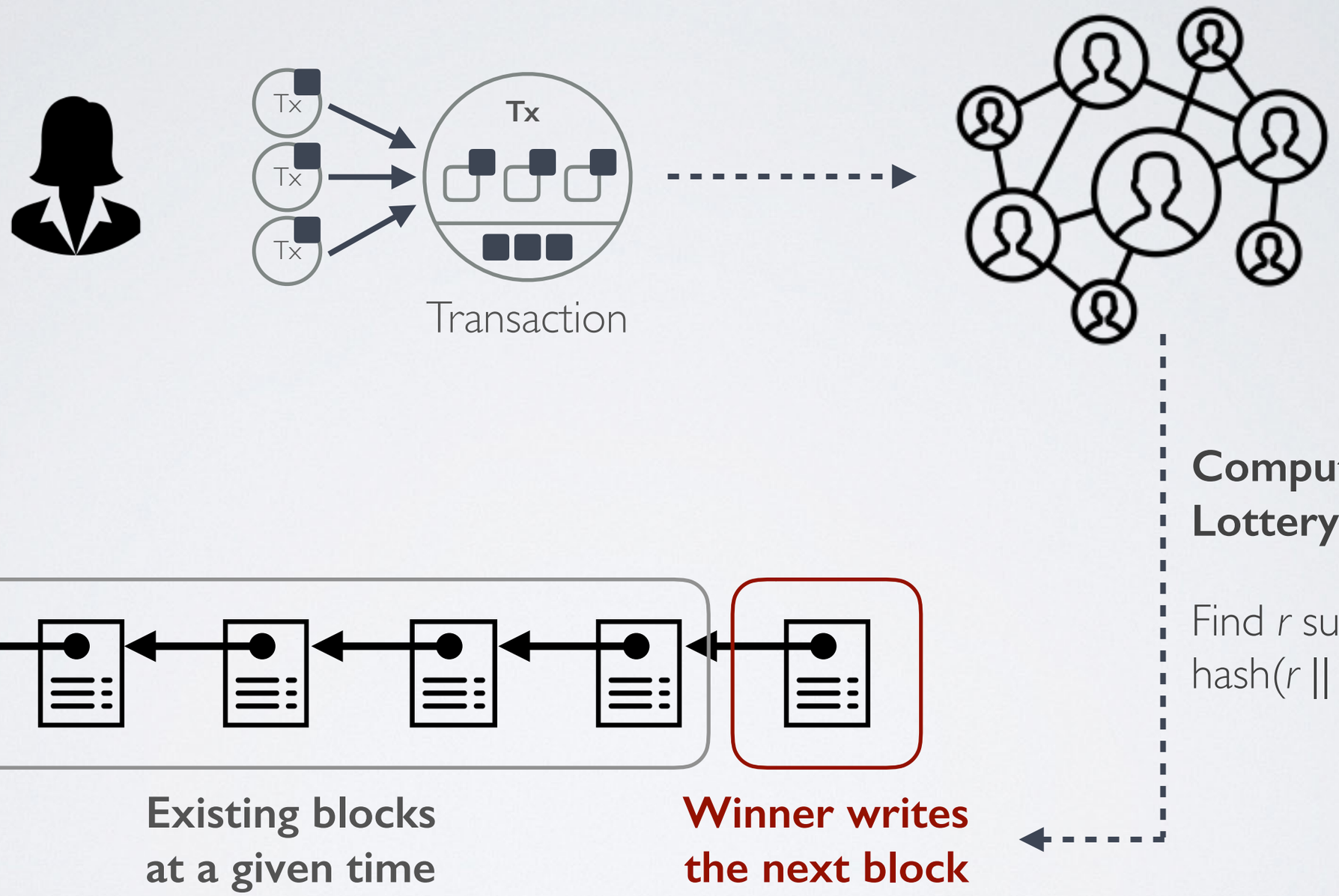


Data obtained from blockchain.info

BITCOIN



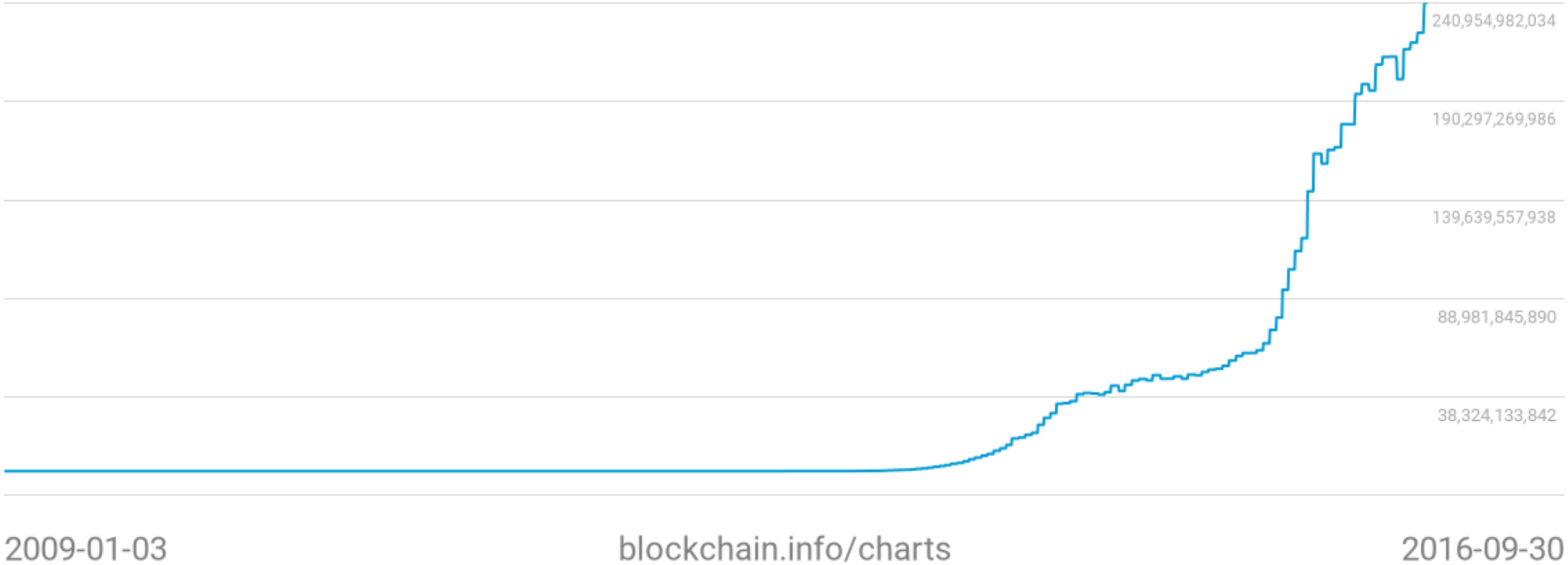
MINING


Tx
Tx
Tx
Tx
Transaction
Computational
Lottery (Puzzle)
Find r such that
hash(r || m) < C
Existing blocks
at a given time
Winner writes
the next block

MINING

Difficulty

241,227,200,229

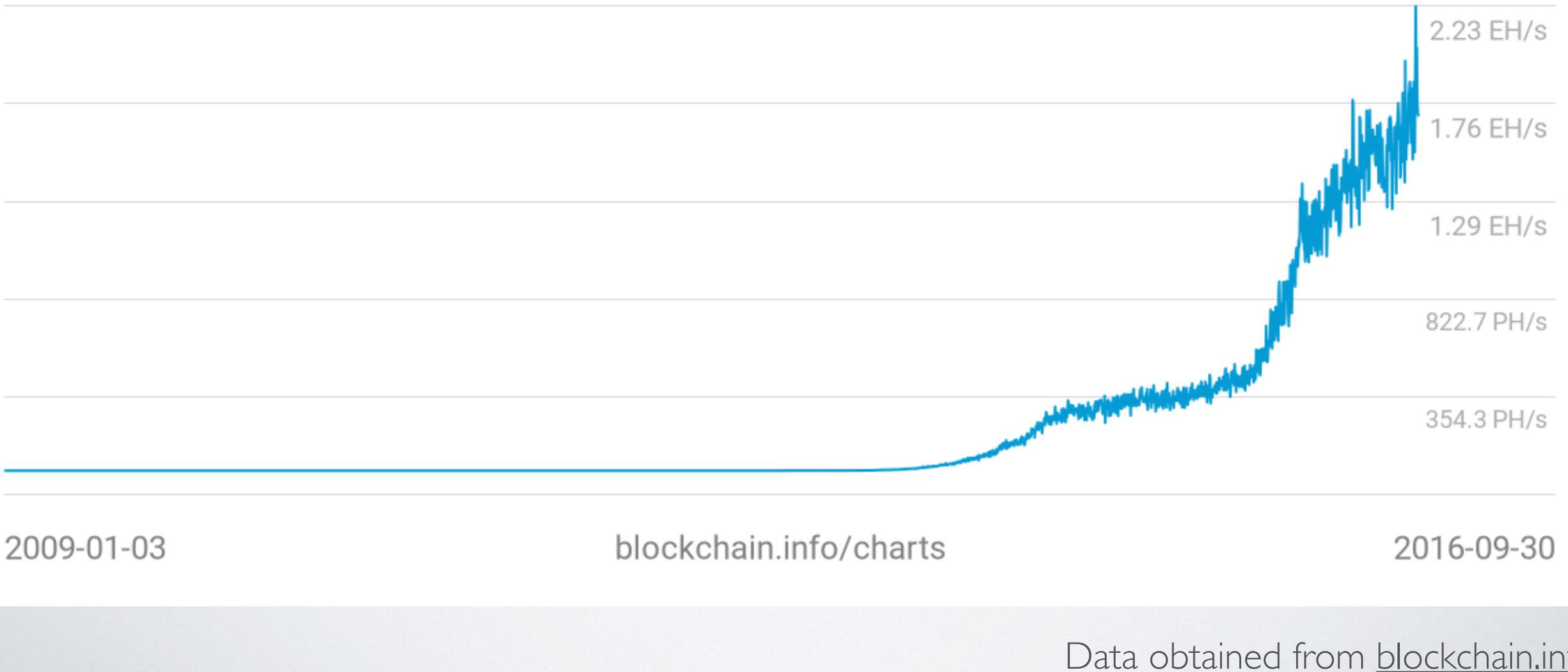


Data obtained from blockchain.info

MINING

Hash Rate

1.70 EH/s



Data obtained from blockchain.info

MINING

Transactions

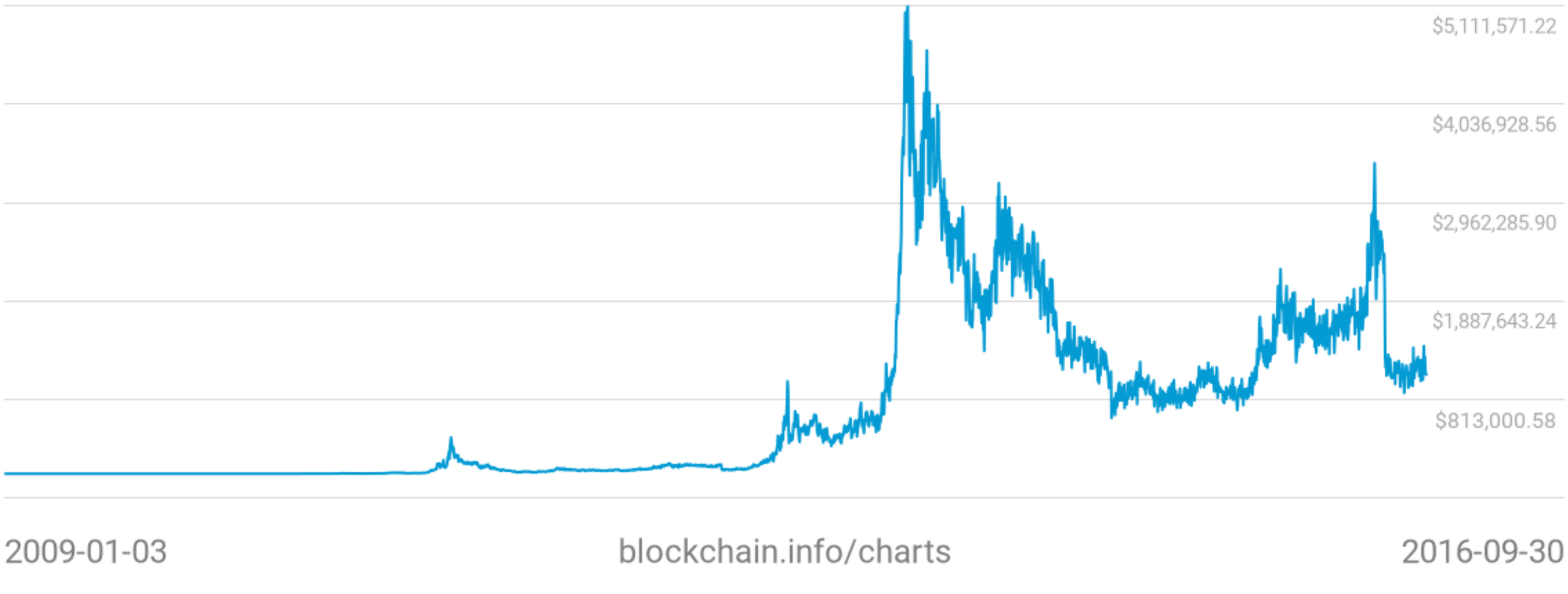
d0bcae91a49d02cb71760e8aebd8d34340598454a167d19c1bdf65a86da85d11			2016-10-02 04:37:37
No Inputs (Newly Generated Coins)	→	1EFg9XXX1U99pNJJTeQwuuEpbHFW4XS8uL	12.50834728 BTC
			12.50834728 BTC
d58bf9d6e19ca676e66811e2a407aaaf8a926157a6431bf04272919d449bed34			2016-10-02 04:37:21
1QCRjVTjgK8LqcMQFWfd5GSEcfE1NtrW79	→	13VArUeQJnjGKwGAfdRBdve1oke6zAcx6k	0.02782028 BTC
		1EtY5A1ueGTuJZvHPJrsUgsKQwHRySYKuh	0.62616966 BTC
			0.65398994 BTC
a03feb6c19c3d975f4bd5f779295d34048993d419fce64b6f0173f397dabd52d			2016-10-02 04:37:37
1NMSgX56XiSGp9aHzSSFp5EwxyZ3R5ABpC	→	19JDWh5ZSqKE6HbQsUECHWHwht2QbJTsAW	0.34 BTC
		1GhXx4CGcNh6QEJTx2NwTLK1oFszjwa4aB	15.7935 BTC
			16.1335 BTC

Data obtained from blockchain.info

MINING

Miners Revenue

$1,084,454.00

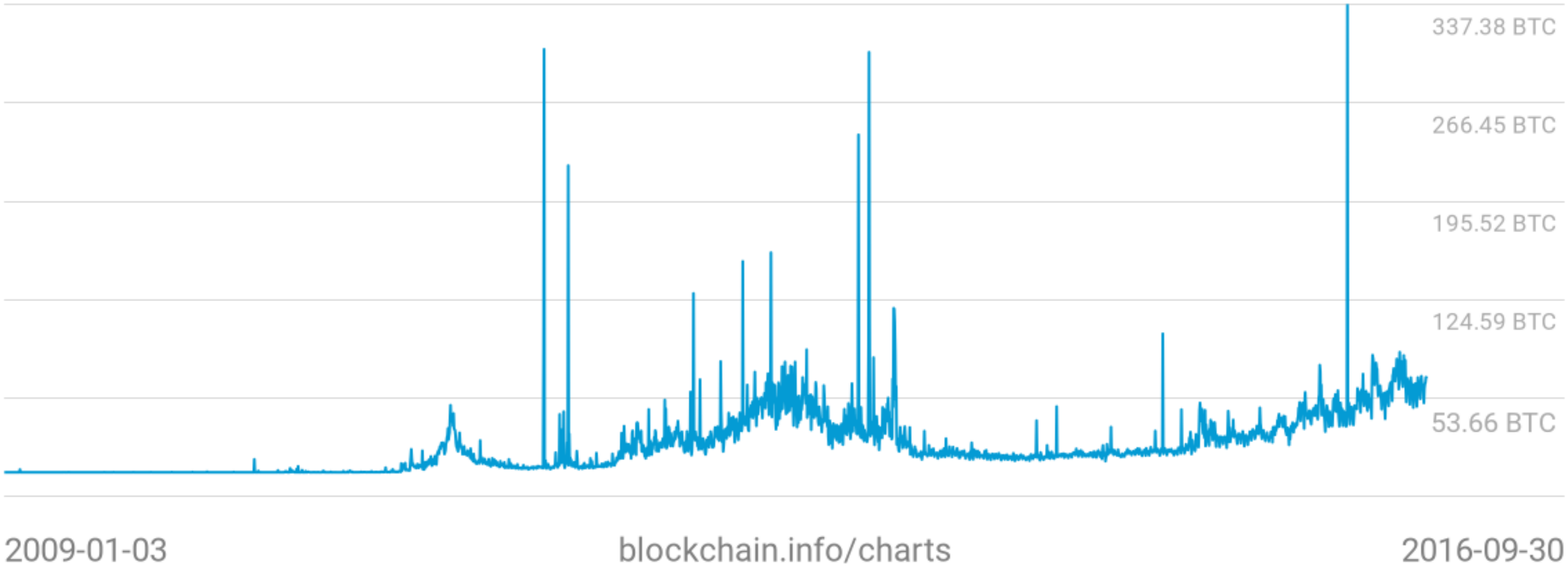


Data obtained from blockchain.info

MINING

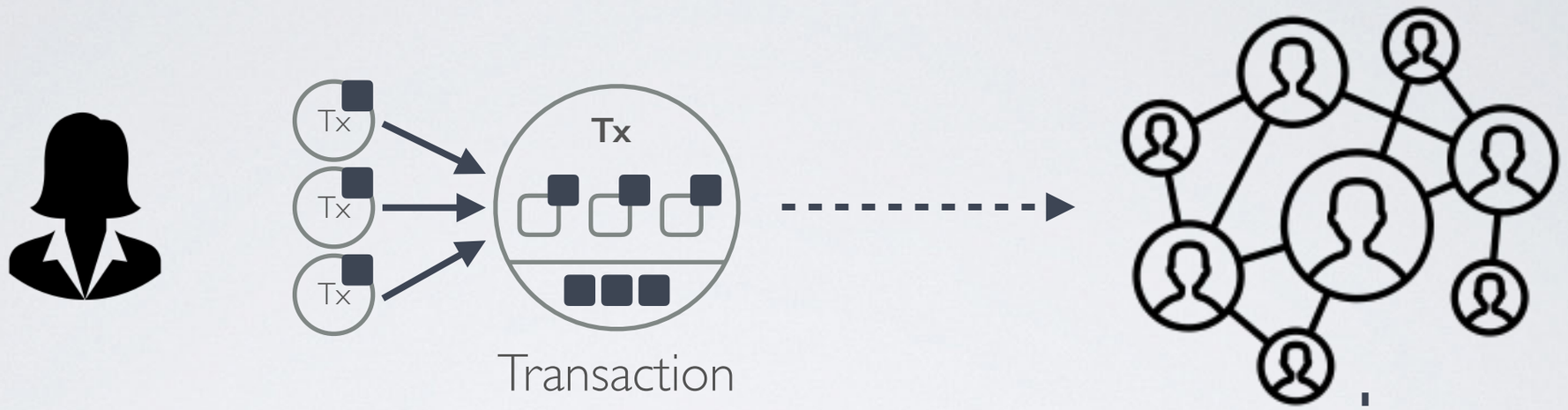
Total Transaction Fees

68.45 BTC



Data obtained from blockchain.info

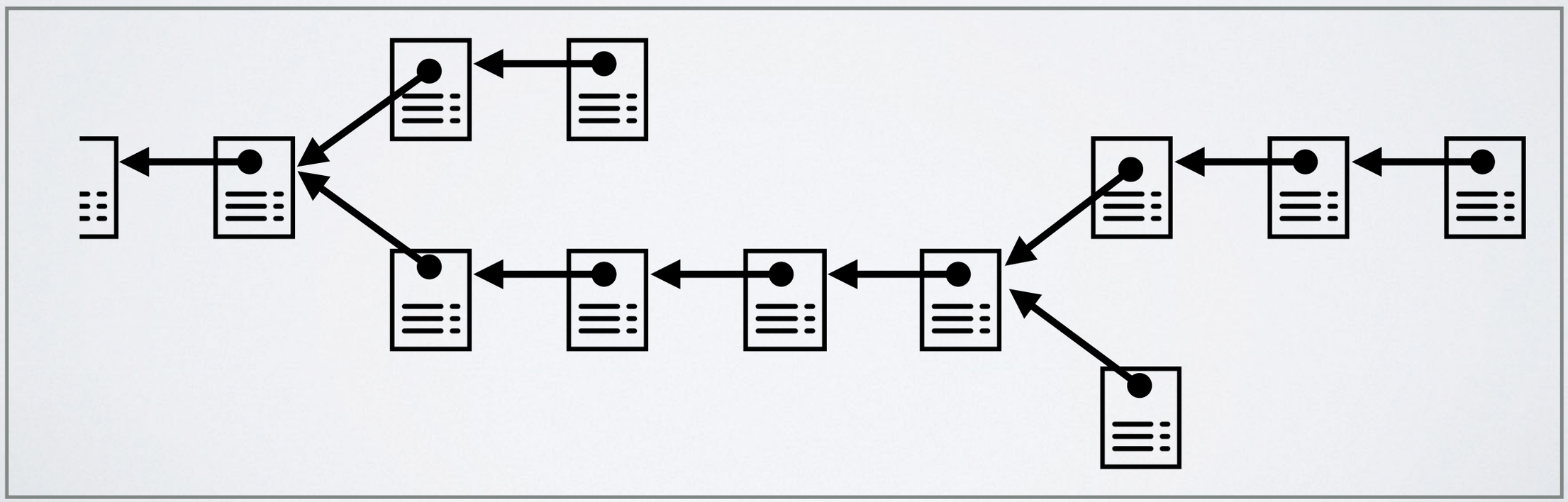
BITCOIN



BITCOIN

Framework — Decentralised peer-to-peer collaborative network

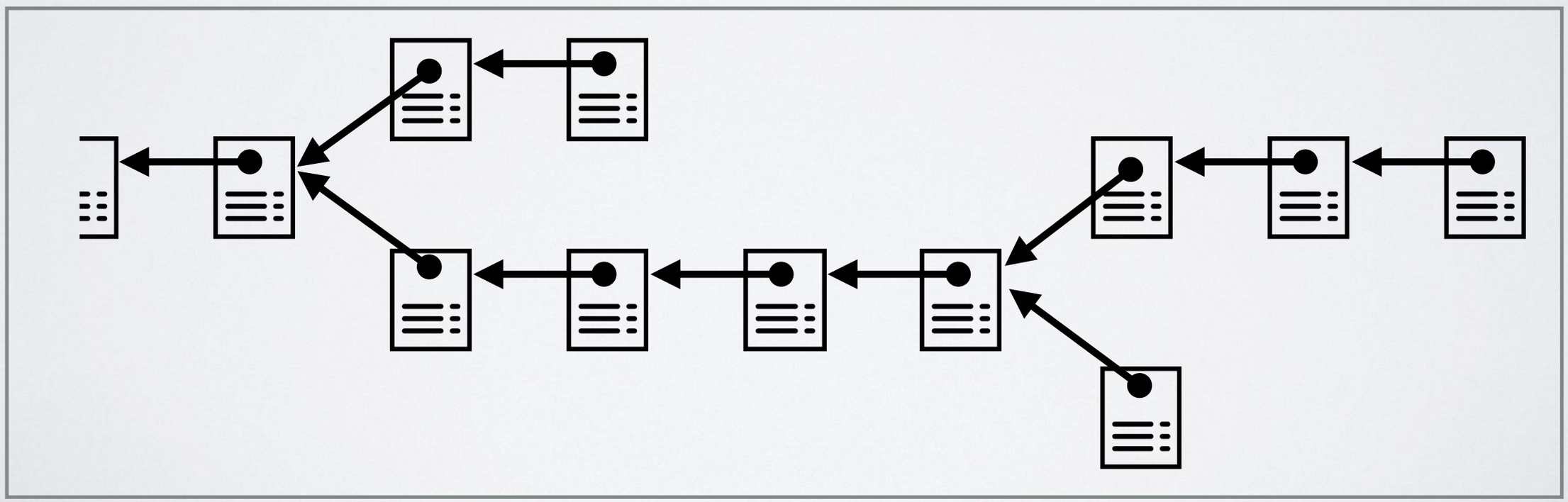
Goal : All peers should agree on a sequence of transactions



BITCOIN

Publicly-Verifiable

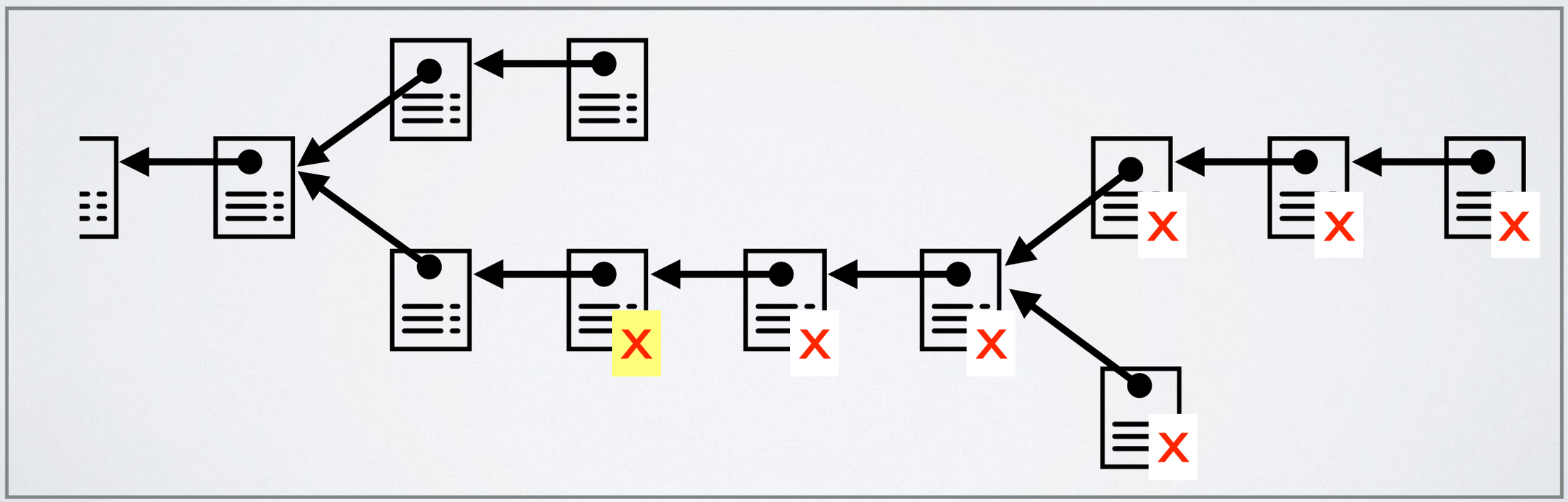
as the complete ledger and the hash function is public



BITCOIN

Tamper-Evident / Tamper-Resistant

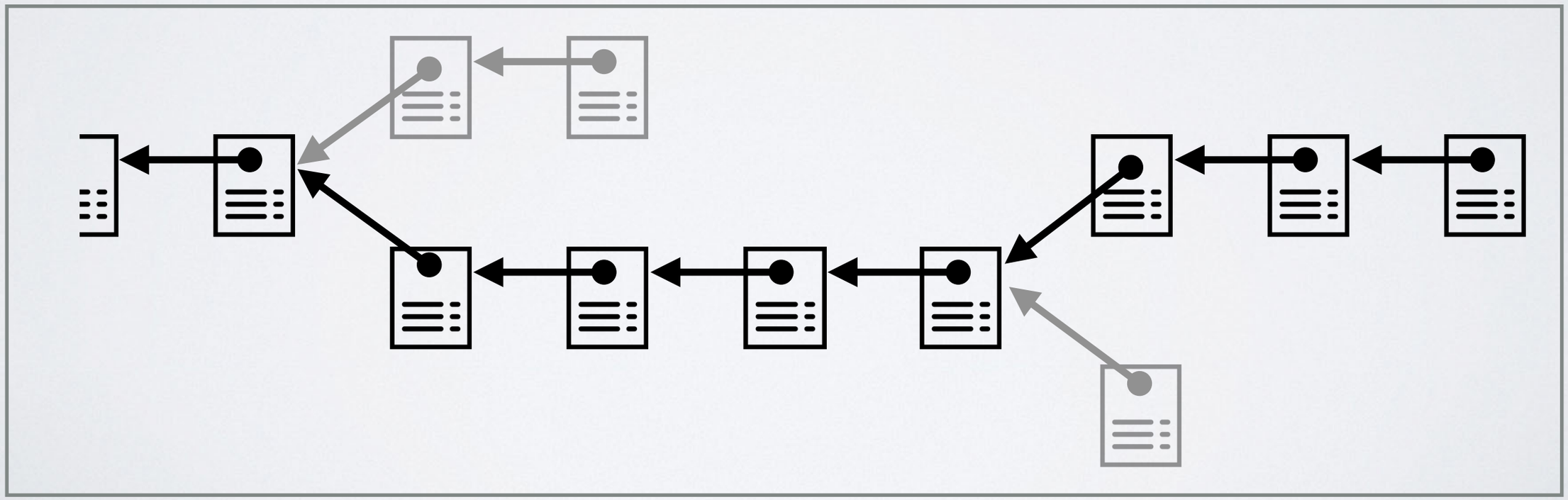
as the ledger is connected through a chain of hash pointers



BITCOIN

Eventually-Consistent

as the longest chain eventually sustains as the main chain



BITCOIN

b6e399ae67749b84eeb2b532c04f8d8c0093c4ea07f95adc0f4f56dd9900e861

1MCcSazqZC3B5ctd4uLeNyWZZaJHKAb7Av (0.0035 BTC - Output)	1LtTV7jAcDjhgKjQN1TBcJxVd7JHNbjXJ2 - (Unspent)	0.0001144 BTC
	1PLfBoLYC9hycWP28GyRnceuKWg4LmTjER - (Unspent)	0.00325 BTC
	Unconfirmed Transaction!	0.0033644 BTC

0002edc4b6b8e8044c75ab34f978aa225533f5e3d58ddd99929e2092e6026f6e — 2016-06-05 20:19:02

13vHWR3iLsHeYwT42RnuKYNBoVPrKKZgRv	13vHWR3iLsHeYwT42RnuKYNBoVPrKKZgRv	565.41197403 BTC
	1MQJTEsVf3XM6QbxDpSZ9hSCTQHt1QnGn4	0.52572306 BTC
		565.93769709 BTC

ca3f5a0220810210d8581a8e6ac0ec54ee436d8045db501efd3ca7a3ef791818 — 2016-06-05 20:26:25

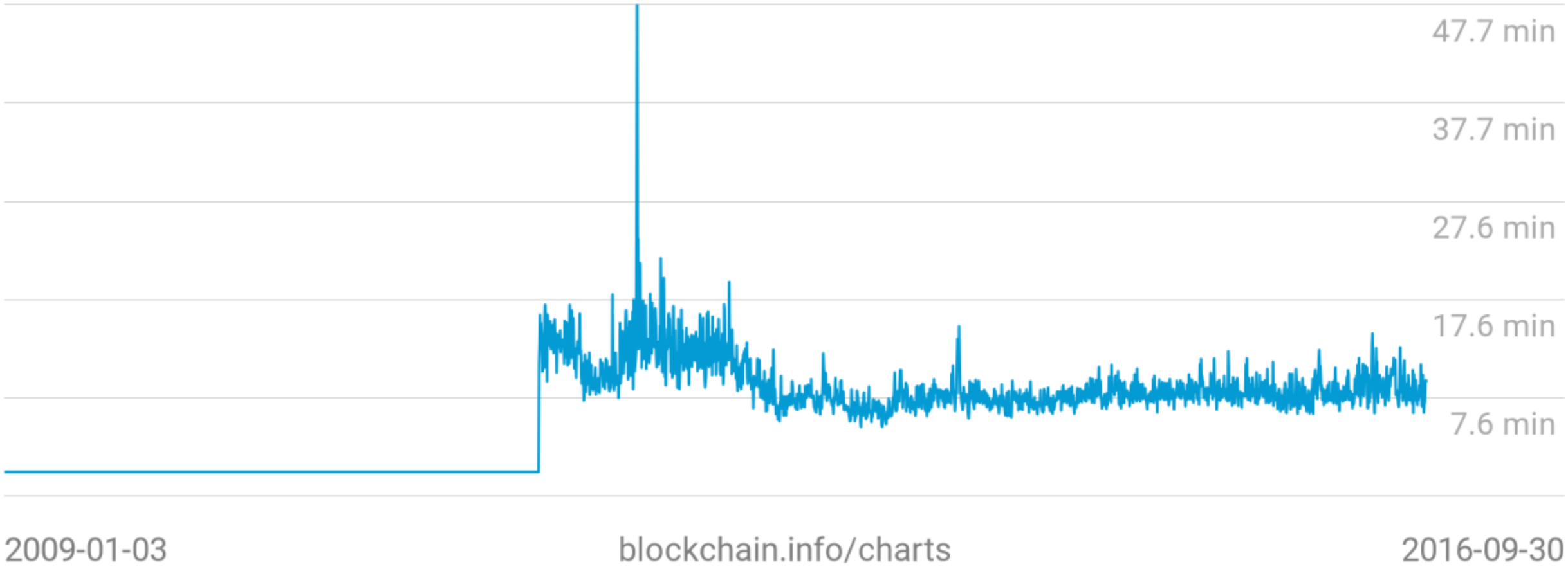
1FpvD2SVLjoAhNWsPdTTJjFyJhYxTKn8U	14gyaggU787pgQtgbMWR6ciXjD6QaMvpP4	0.009 BTC
	31vCz9jSspkwbqopejqS3jt3kaTmue9CoZ	0.044593 BTC
	1PL12AqN2ittA4CAmguuNH1E5mpgBpdF6D	0.02609 BTC
	19QRNiDNnkMN1yv4AhyAXP5kLdL2wRgJmr	80.0186079 BTC
	1FTKnmp3YE4XD7m7VxU8yoot7khyz6ZJGm	0.009 BTC
	1GGWhkSMwHoSdRZHgfLcjja6Db5ers4EBZ	0.01121 BTC
		80.1185009 BTC

Data obtained from blockchain.info

BITCOIN

Median Confirmation Time

9.3 min

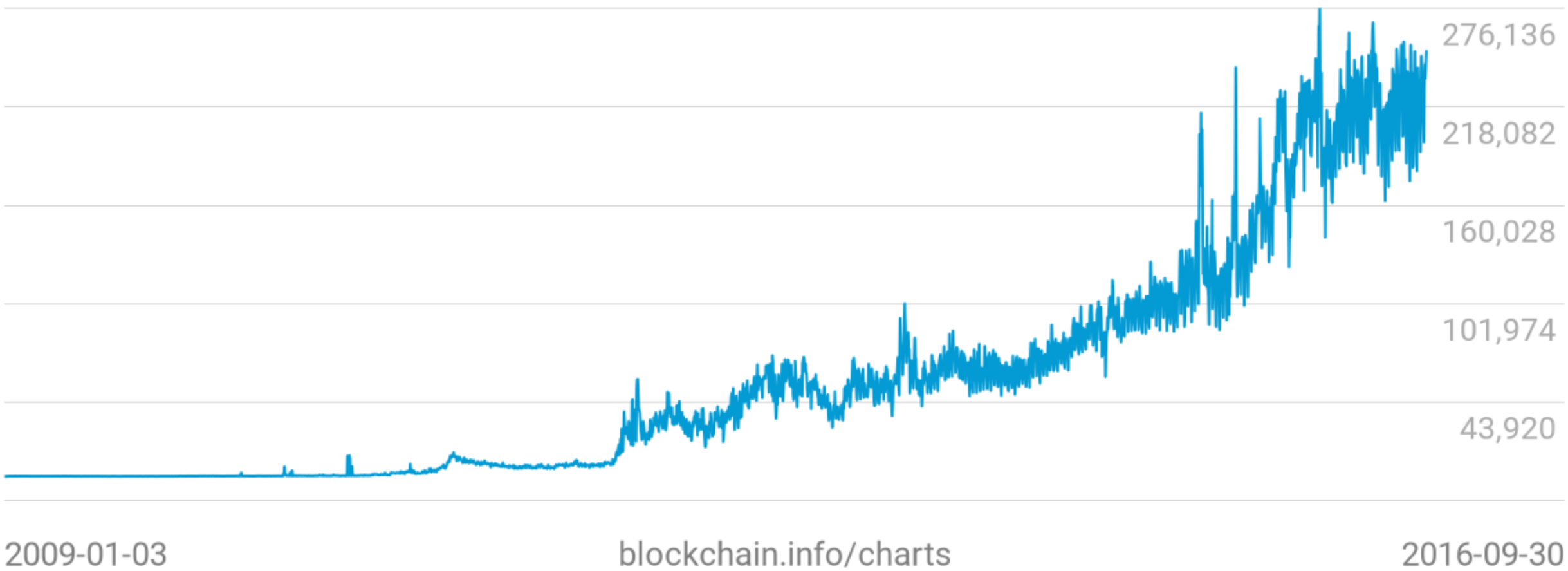


Data obtained from blockchain.info

BITCOIN

Confirmed Transactions Per Day

250,943

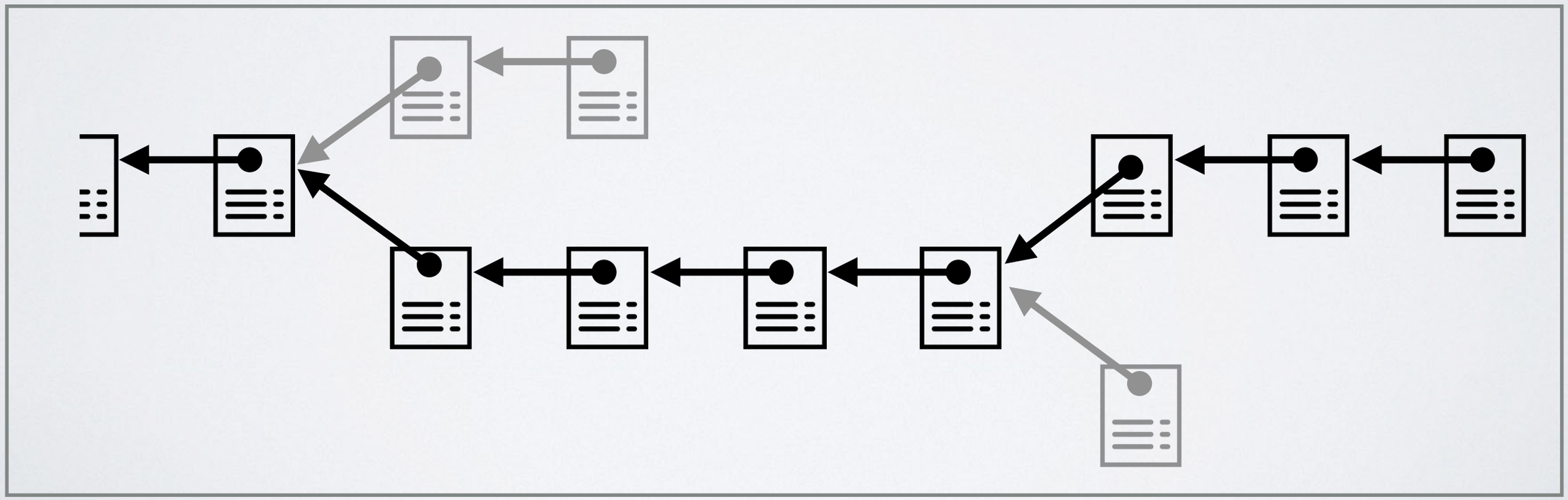


Data obtained from blockchain.info

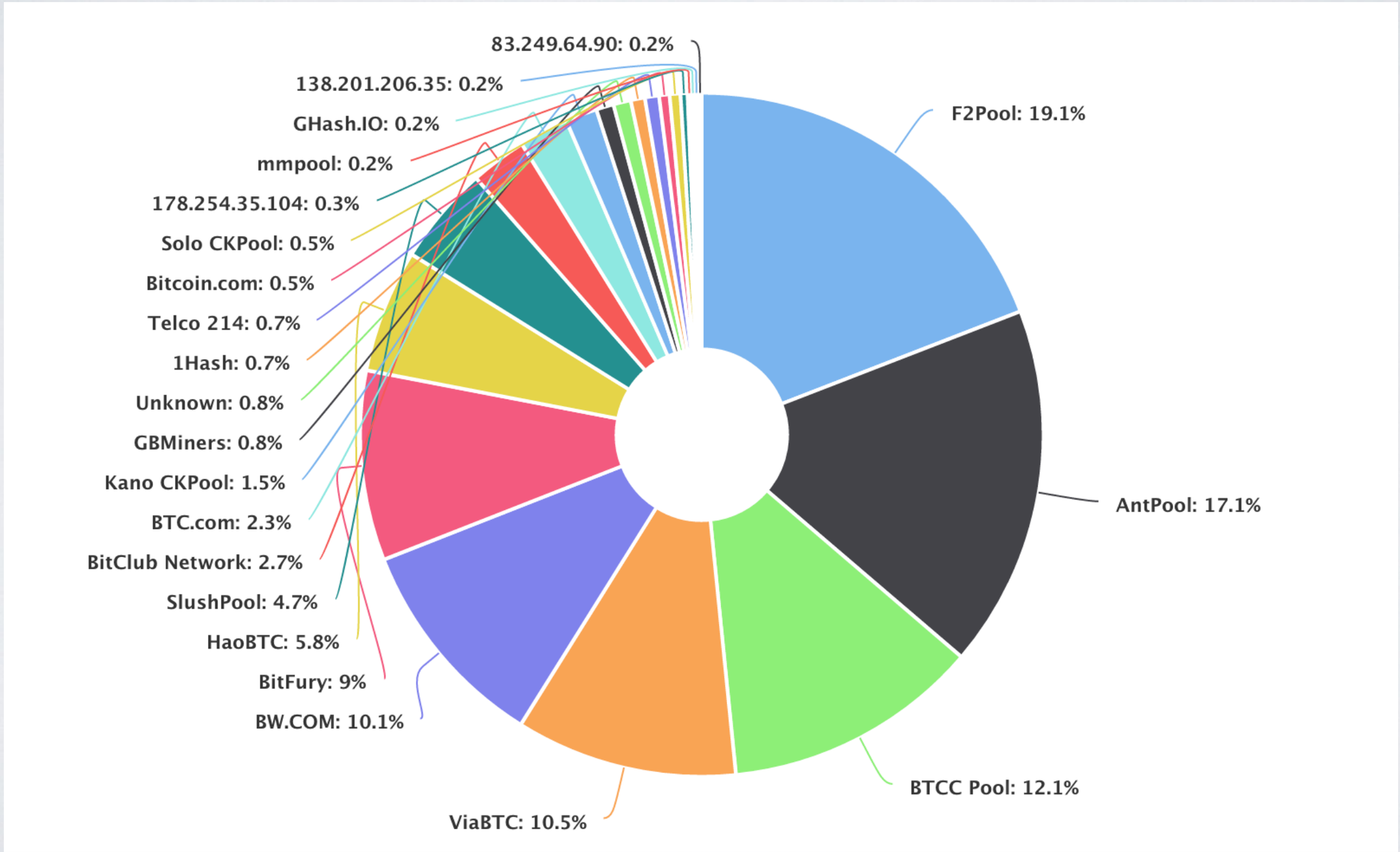
BITCOIN

Semi-Decentralised

as the mining is dominated by computational power



BITCOIN



Data obtained from blockchain.info

BITCOIN

Relayed By	count
F2Pool	115
AntPool	103
BTCC Pool	73
ViaBTC	63
BW.COM	61
BitFury	54
HaoBTC	35
SlushPool	28

Data obtained from blockchain.info

Robin Yao (BW), Wang Chun (F2Pool), Marshall Long (FinalHash), Pan Zhibiao (Bitmain)
Liu Xiang Fu (Avalon), Sam Cole (KnCMiner) and Alex Petrov (BitFury)

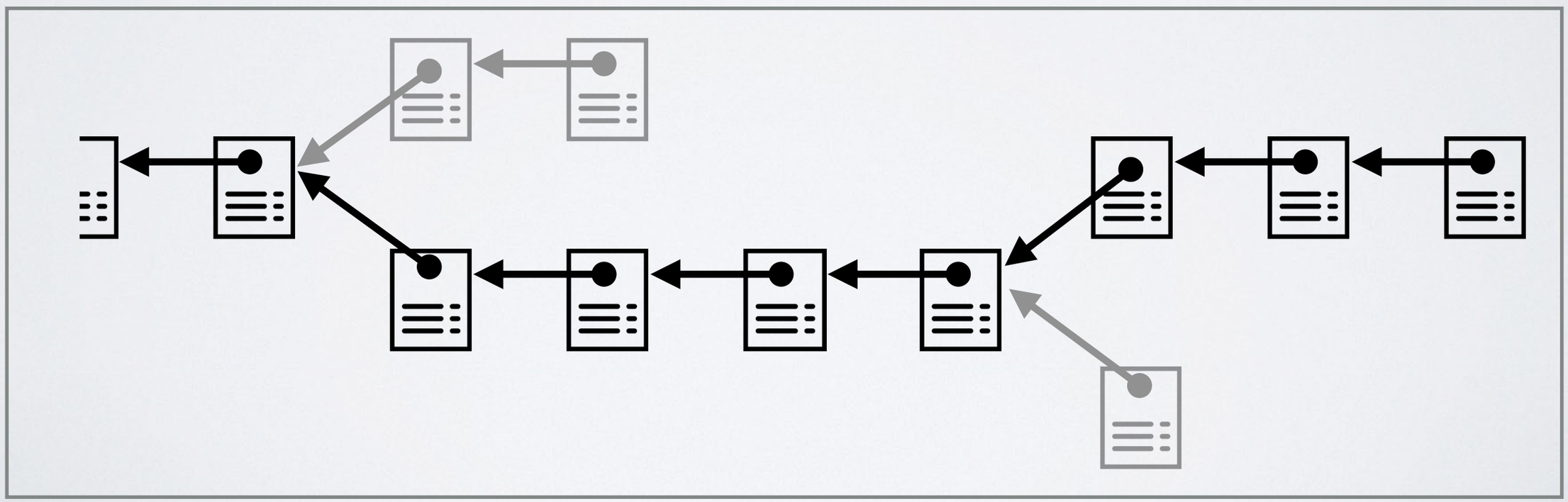
BITCOIN

Semi-Decentralised

Tamper-Resistant

Publicly-Verifiable

Eventually-Consistent



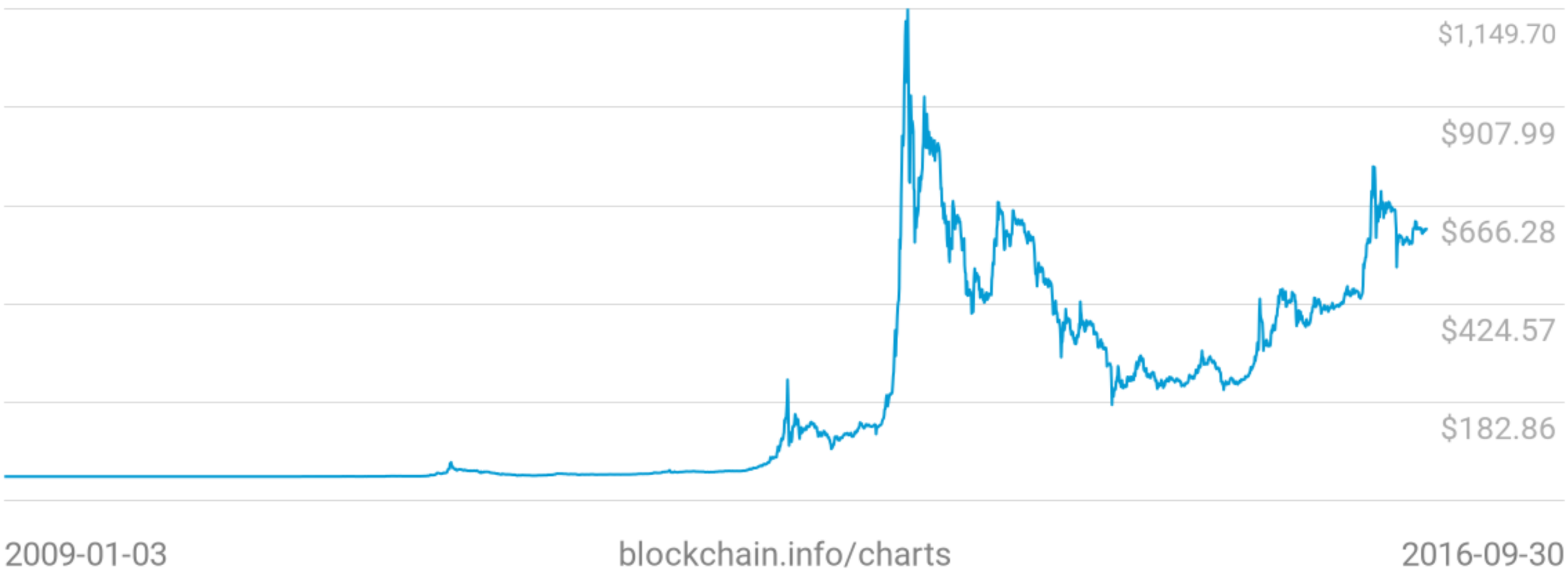
ECONOMICS

The success story of Bitcoin

BITCOIN

Market Price (USD)

$609.40

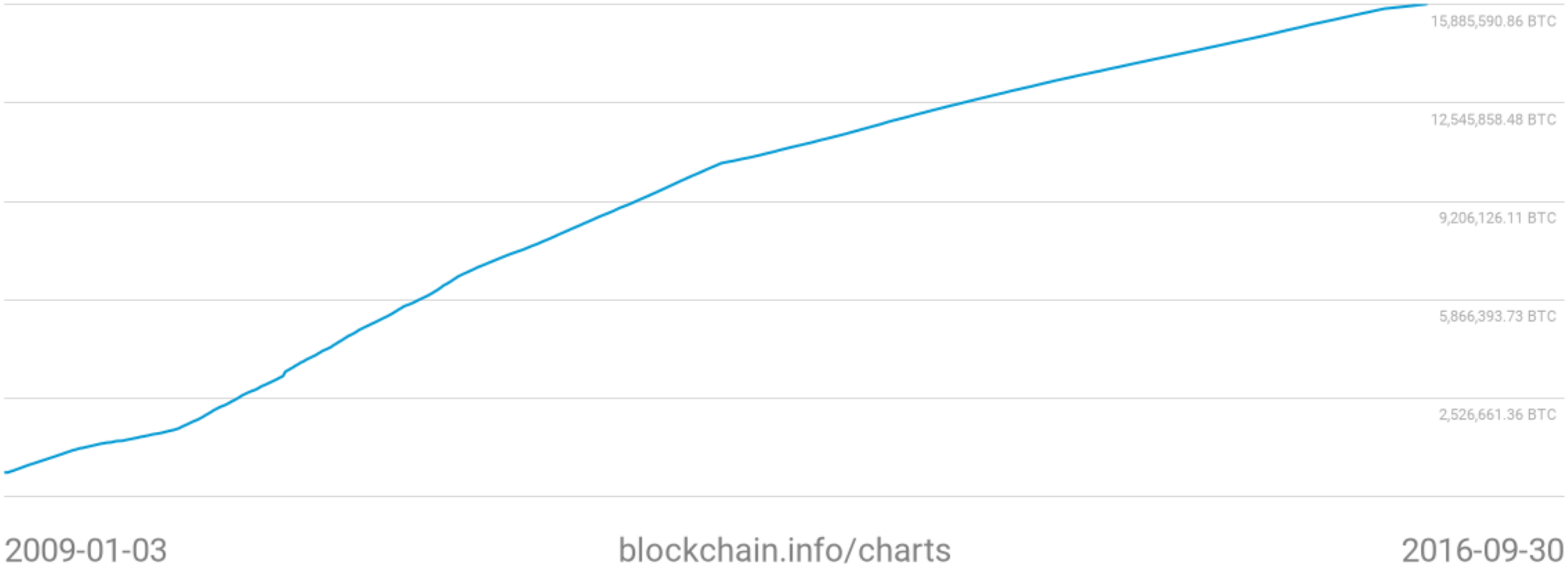


Data obtained from blockchain.info

BITCOIN

Bitcoins in circulation

15,903,537.50 BTC

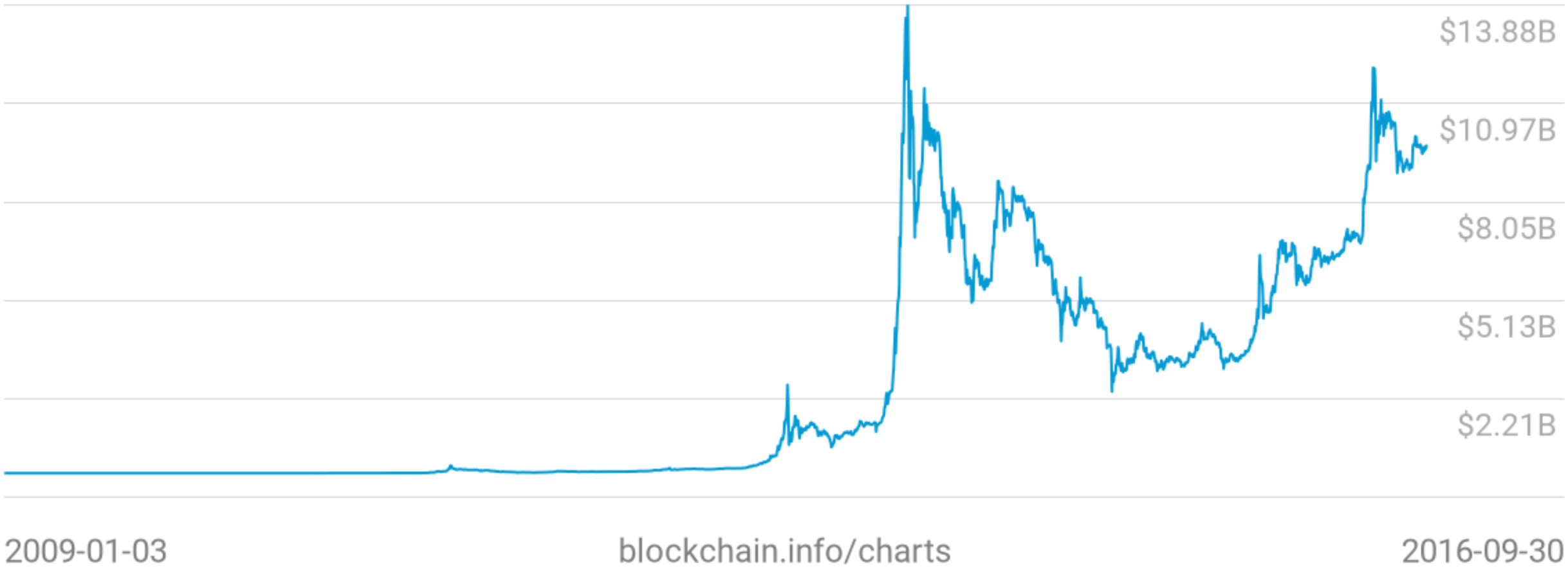


Data obtained from blockchain.info

BITCOIN

Market Capitalization

$9.72B

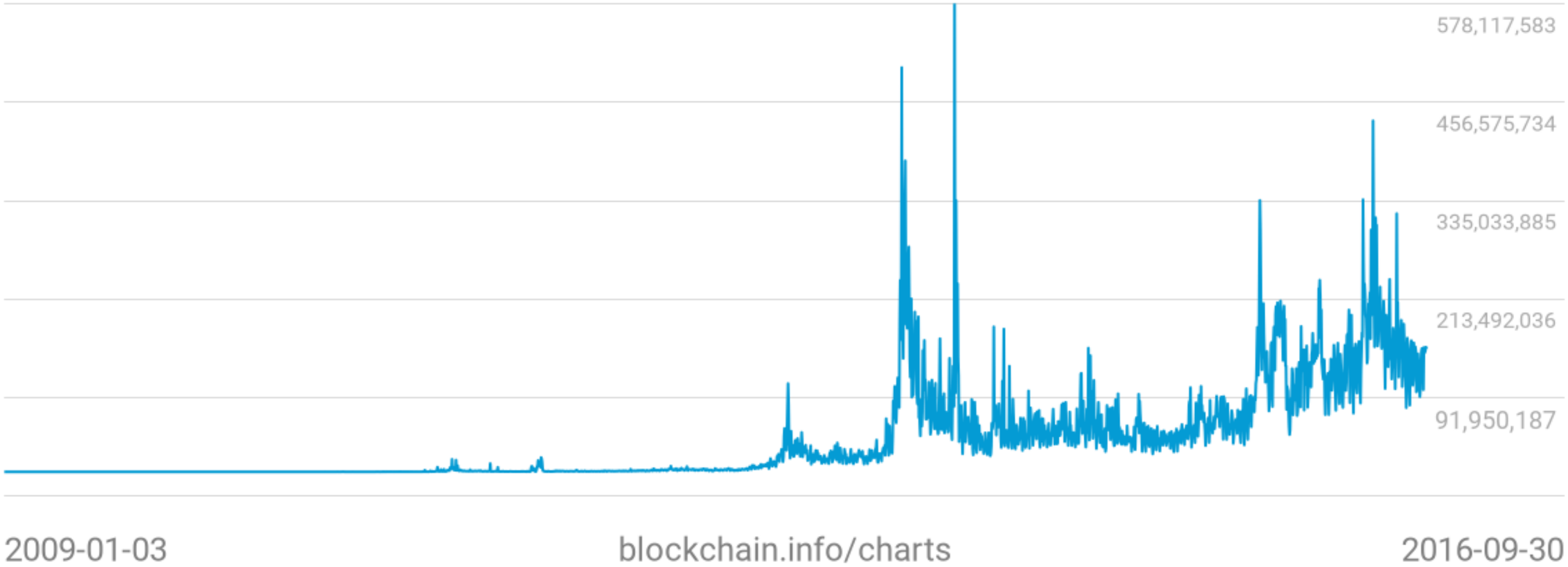


Data obtained from blockchain.info

BITCOIN

Estimated USD Transaction Value

153,295,466

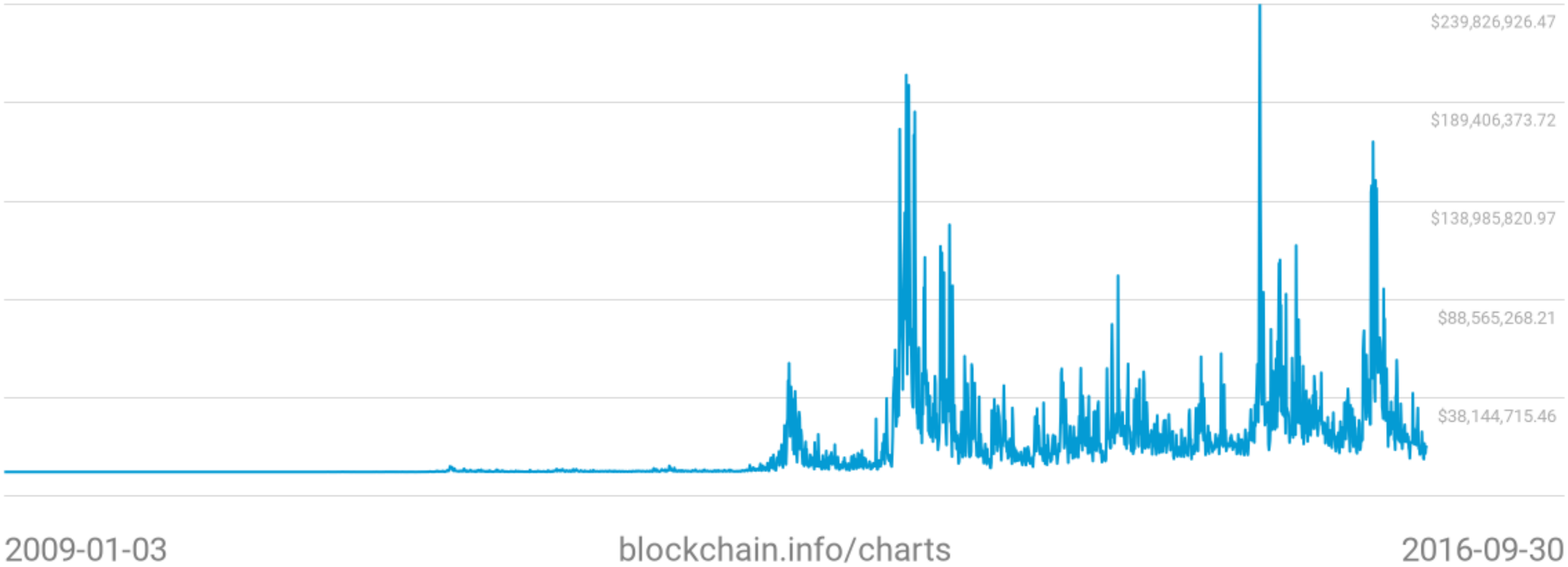


Data obtained from blockchain.info

BITCOIN

USD Exchange Trade Volume

$12,885,196.89



Data obtained from blockchain.info

BITCOIN

29a3efd3ef04f9153d47a990bd7b048a4b2d213daaa5fb8ed670fb85f13bdbcf — **2011-11-16 05:59:08**

1QF76AaXFWmMqeiKsRQvQNnz4AhJ91tkwB	1P3S1grZYmcqYDuaEDVDYobJ5Fx85E9fE9	50,000 BTC
1H8PAUxZti5fwzbbeK5gwDdXvEZouSsNuV	1M8s2S5bgAzSSzVTeL7zruvMPLvzSkEAuv	500,000 BTC
1LJY4ey9FVKKuodaDr84sdZDXLy5o8nFDY		
132vQw4XpVdayQarsyQEfrjGTKrhwMogGb		
1GNBnkXohjwf42vzRG5NmkQHFX6iAZb2Sa		
1NW9JSKTUpLAWRhpcQdAkhuCVbnMXXtcKU		
14NCi5KdQa5zhgnRsHhBGJiAPfGzyNij2q		
1Q7ZR5avdc12myfmi36rjtAHBZ8U9ybvs9		
1N6Nb9NnCqU3wKWKPnkHp19PcpSXMMo3pW		
1U5EGSHJeyZd4AHjcSCVZmcgepgKzB72V		

550,000 BTC

78083b6b42f0fd47bf9cdcd2137ef53ae2ec96ef8342fba60008b25826151c1b — **2011-11-29 09:20:46**

1MFxDTacY2xRxmXwWTttZGg6pYADVnjXMs	14AkYsDCYuUu5RwqCjtQomotECqS42uBU8	49.72 BTC
16WHtA31tcqWHSgzVDLe97pNxyk5BGmWWz	1Am1SkVAzckv6bhK1h8tRrjapLb6JFwkrN	466,406.60114432 BTC
1ADdwmHmdieyPv3Jzz6uBenJRojQbWgnTB		
1MBzBLnPPDVPneGcKtRqLbZNoyDsuEpyJz		

466,456.32114432 BTC

Data obtained from blockchain.info

SECURITY

The threat from Bitcoin

BITCOIN

Transactions : Completely transparent and public

Identities : Opaque and pseudonymous addresses

~ 170 Million bitcoin addresses

~ 150 Million bitcoin transactions

~ 80 GB of compressed raw data

~ 80% of transactions have < 2 inputs

~ 90% of transactions have < 3 outputs

BITCOIN

1c3bb3f8846bd6291eb29c6b9e3fc4ec675d3b8aac41964981ec320f4b2cd150 — **2016-06-05 19:33:17**

39xLaGRNXyLrU9Ud6SA95C9DV4eiCNFfcU	→	12vK6bWP4vXxdmqgQ8KBsLm1dzcDZSp6AU	0.05217392 BTC
		39xLaGRNXyLrU9Ud6SA95C9DV4eiCNFfcU	0.60656824 BTC
			0.65874216 BTC

eb049c23e04e7770d7d1e9cf91a67502475ce99ed5d22424dac3c6f5f63e4037 — **2016-06-05 20:18:22**

16QpfGvJSTtrSfR7wtuBJ9SWuQZzqTMKFD	→	1A6pEE4eTrtBaNqFJAeFsU2zYkvbjqAv6w	33.1490177 BTC
		14tDfmLiykLDRmXaLUPr7GSFwgZDQ1eS4h	0.06517962 BTC
			33.21419732 BTC

0002edc4b6b8e8044c75ab34f978aa225533f5e3d58ddd99929e2092e6026f6e — **2016-06-05 20:19:02**

13vHWR3iLsHeYwT42RnuKYNBoVPrKKZgRv	→	13vHWR3iLsHeYwT42RnuKYNBoVPrKKZgRv	565.41197403 BTC
		1MQJTEsVf3XM6QbxDpSZ9hSCTQHt1QnGn4	0.52572306 BTC
			565.93769709 BTC

ca3f5a0220810210d8581a8e6ac0ec54ee436d8045db501efd3ca7a3ef791818 — **2016-06-05 20:26:25**

1FpvD2SVLjoAhNWsPdTTJjFyJhYxTKn8U	→	14gyaggU787pgQtgbMWR6ciXjD6QaMvpP4	0.009 BTC
		31vCz9jSspkwbqopejqS3jt3kaTmue9CoZ	0.044593 BTC
		1PL12AqN2ittA4CAmguuNH1E5mpgBpdF6D	0.02609 BTC
		19QRNiDNnkMN1yv4AhyAXP5kLdL2wRgJmr	80.0186079 BTC
		1FTKnmp3YE4XD7m7VxU8yoot7khyz6ZJGm	0.009 BTC
		1GGWhkSMwHoSdRZHgfLcjja6Db5ers4EBZ	0.01121 BTC
			80.1185009 BTC

BITCOIN

Identities : Opaque and pseudonymous addresses

Anyone can create arbitrarily many identities

All identities "look" the same on the network

~ 170 Million bitcoin addresses

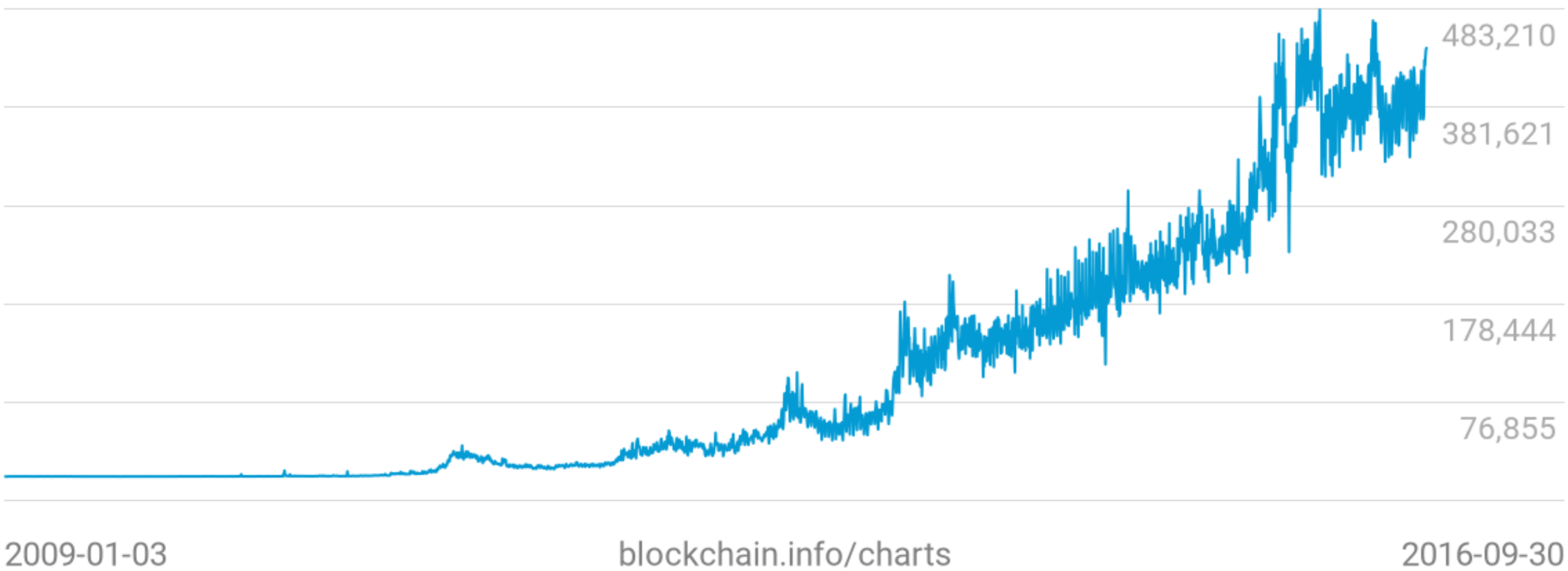
~ 150 Million bitcoin transactions

Provides "anonymity" of Bitcoin transactions.

BITCOIN

Number Of Unique Addresses Used

442,960



Data obtained from blockchain.info

BITCOIN

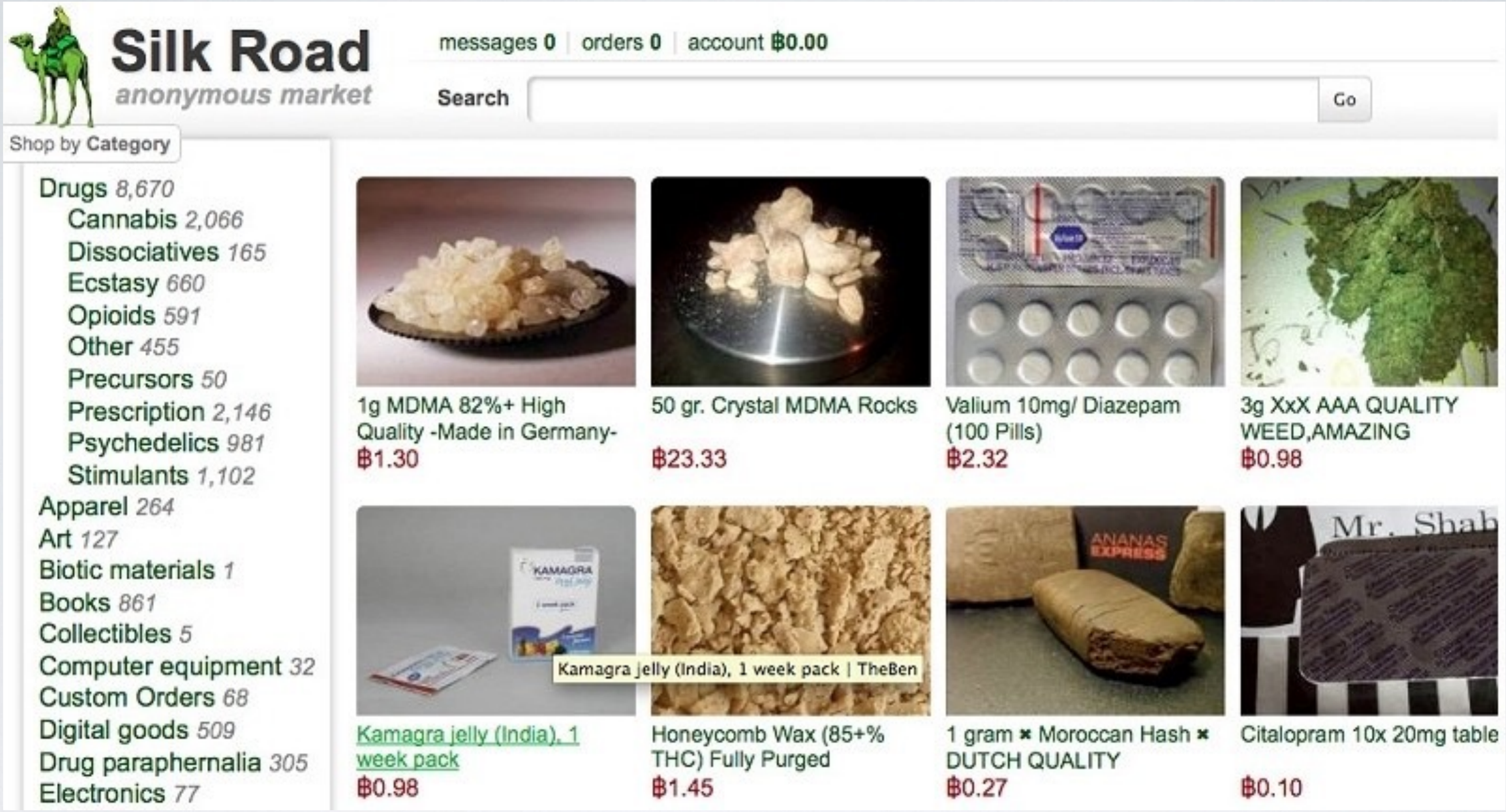

```
"hash160":"660d4ef3a743e3e696ad990364e555c271ad504b",
"address":"1AJbsFZ64EpEfS5UAjAfcUG8pH8Jn3rn1F",
"n_tx":17,
"n_unredeemed":2,
"total_received":1031350000,
"total_sent":931250000,
"final_balance":100100000,
"txs":[--Array of Transactions--]
```


Data obtained from blockchain.info

BITCOIN

17BymcHaGRbXGnEzR2m9woUYNf9FBPPJ2P	253774
1MEe2mebed8wopvy8xyjjHcEQHUPVJn2UC	253660
1KumbRsTcA6UNqU2MHEfqEFnAZYU3w3izR	253650
1Po4J4SNyJuGnMGYJfGTXLEvGgAZKiddr7	253602
1KYXrw4Ftkmomfs4iyVXUSqQeRX75Unoi8	253565
1LuckyP83urTUEJ… (LuckyBit promo)	253316
1Lsqcv4cg5zUctNi2qwNxMkrv1GeBboSUJ	252971
1GUkazUBpXWdSJ9HbgTapAH7uybpi3Cs6K	252889
14wXrm49HxggbdQ6RGfWY8qghGEWhLA28K	252800
12ucu9bHLe2w2ahjibVtp3xmdcGkgUmX4A	252645
1changemCPo732F6oYUyhbyGtFcNVjprq	227930
1HWqsgnSd12Gv8SpoUMi1Cj8hp79BTSpW7	219384
1LuckyB5VGzdZL… (LuckyBit blue)	192587

Data obtained from blockchain.info



Dark Marketplaces to buy-and-sell Drugs

Desert Eagle IMI, Kal.44

New and unused!

Product	Price	Quantity
Desert Eagle IMI, Kal.44	1250 EUR = 2.413 ฿	1 X Buy now
Ammo, 50 Rounds	45 EUR = 0.087 ฿	1 X Buy now

Passports

Product	Price	Quantity
Lithuanian Passport	2650 EUR = 5.117 ฿	1 X Buy now
Netherlands Passport	3150 EUR = 6.082 ฿	1 X Buy now
Denmark Passport	3150 EUR = 6.082 ฿	1 X Buy now

Dark Marketplaces to buy-and-sell Guns and Fake ID

BITCOIN

Identities : Opaque and pseudonymous addresses

Anyone can create arbitrarily many identities

All identities "look" the same on the network

~ 170 Million bitcoin addresses

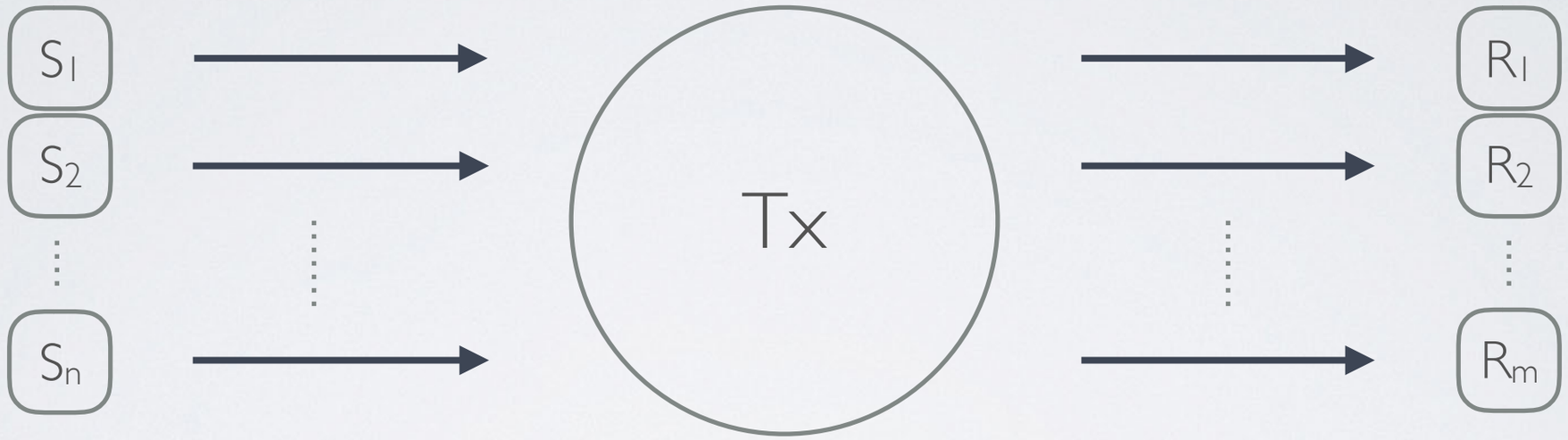
~ 150 Million bitcoin transactions

Is it still possible to trace transactions and identities?

DE-ANONYMIZATION

Potential solution to the threat from Anonymity

TRANSACTION

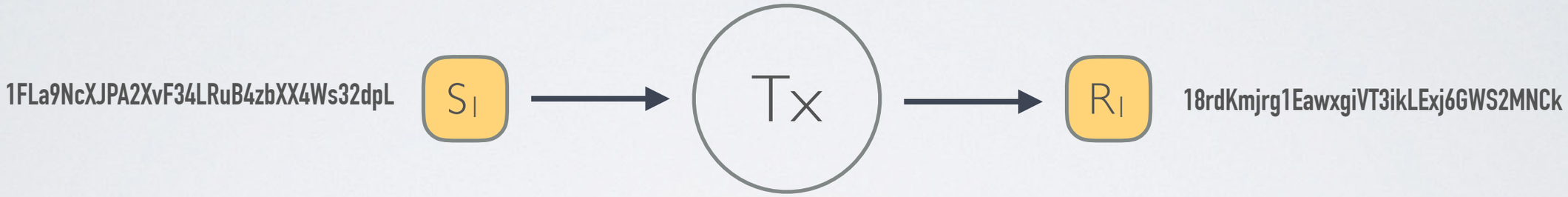


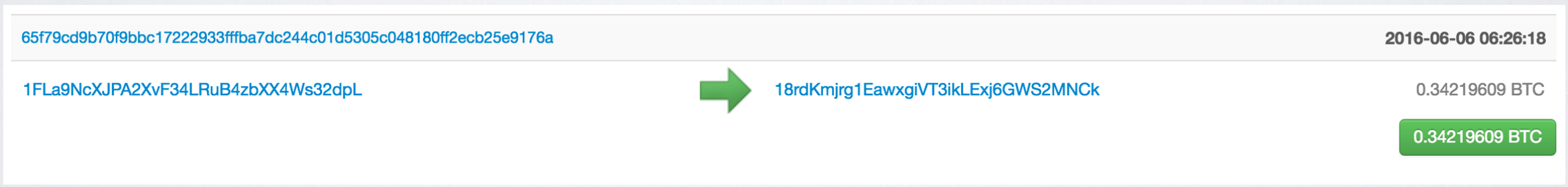
4d46ed1da4abf81d5738dee0d7cded7e6ff73af24d22ecfc87336009e90f9576 **2016-06-06 06:23:37**

1PHwjVTfRVskjYkxVUsqWpYTbmbrqb4i6u		
1CH8bx2QBnAsd3jwzFjEyfyejAc7UFJG4P		
1JpgXweQM4vvfVUAKYdbmojdbVyp3WW7XB		
1CHx2VPEyfAhJ2QYrtKU7nEb3Hx112eBzt	1Cv33AXyMsjefJYgcW7pc9L3RLK7WMcWvz	0.1449276 BTC
1ABaG1VFRt59eVS8kSxcYJgW34Kh2oxBRF	1Patod8dD83wn6j1jQvpEJ3xdgjvw73ELp	0.09517317 BTC
18R6Fnau61jd494LstD1Bfid9VH4LDJojA	1HtqDMWgn6186e8t3EesZQiw7gNbaPJfJH	0.13542628 BTC
1Mib8Nagj9uH53NmTe8us3kMuzmXrDVxkU		
1HtqDMWgn6186e8t3EesZQiw7gNbaPJfJH		
1MPnMC5VFfHD7EpkPbpSf6D1V3aWjzmR2X		

0.37552705 BTC

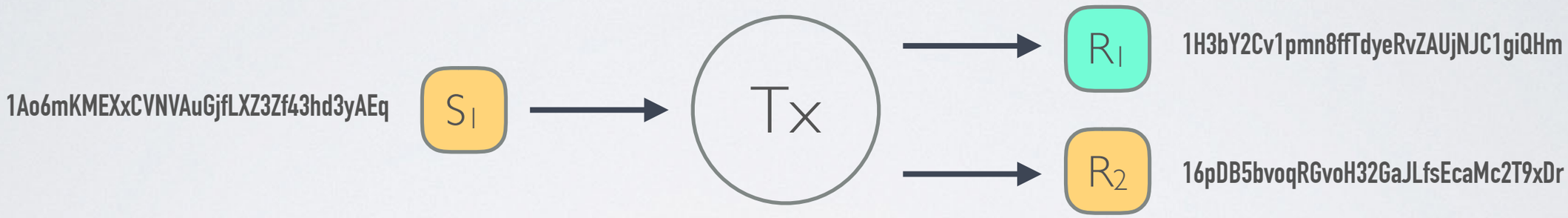
EXAMPLE #1





Note : Single recipient with an exact match of input to output — highly unlikely.

EXAMPLE #2



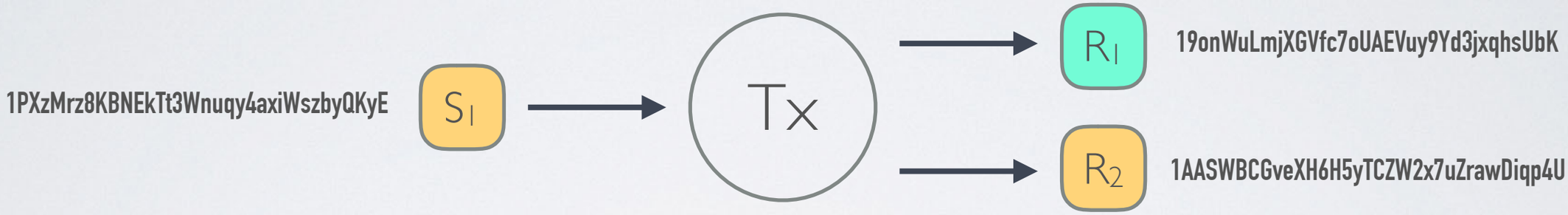
92677f7abff5911131bae9205ca92ffa9741399459a284ab89f56753192aa8fd **2016-06-06 06:16:33**

1Ao6mKMEXxCVNVAuGjfLXZ3Zf43hd3yAEq	→	1H3bY2Cv1pmn8ffTdyeRvZAUjNJC1giQHm	1 BTC
		16pDB5bvoqRGvoH32GaJLfsEcaMc2T9xDr	0.0000831 BTC

1.0000831 BTC

Note : Nice complete denomination along with a random change.

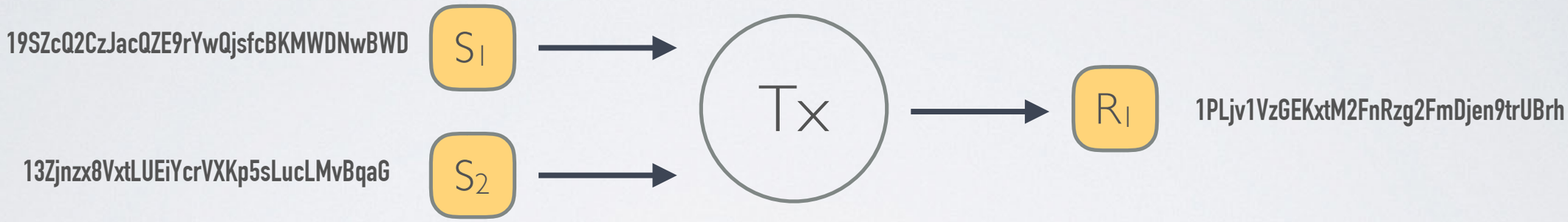
EXAMPLE #3



0727e245d41ae282b3748c4df221eb7bcfbd01bb1f1a63123211d6626c8e2ca3			2016-06-06 06:19:32
1PXzMrz8KBNEkTt3Wnuqy4axiWszbyQKyE	→	19onWuLmjXGVfc7oUAEVuy9Yd3jxqhsUbK	0.01121504 BTC
		1AASWBCGveXH6H5yTCZW2x7uZrawDiqp4U	0.24519446 BTC
			0.2564095 BTC

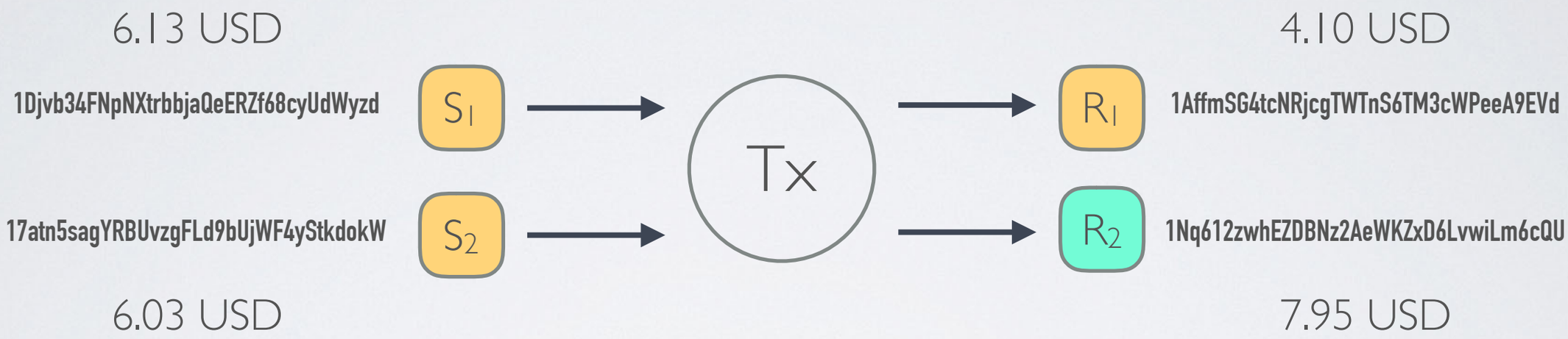
Note : 0.01121504 BTC = 6.50 USD at the time of transaction.

EXAMPLE #4



Note : Two arbitrary inputs exactly match up to a desired output — highly unlikely.

EXAMPLE #5



f367a951551aef2b0864f20a07af61aaa07e3b4e331ab40ab639316a8d33ceda — **2016-06-06 06:22:59**

1Djvb34FNpNXtrbbjaQeERZf68cyUdWyzd	1AffmSG4tcNRjcgTWTnS6TM3cWPeeA9EVd	0.00707248 BTC
17atn5sagYRBUvzgFLd9bUjWF4yStkdokW	1Nq612zwhEZDBNz2AeWKZxD6LvwiLm6cQU	0.01370618 BTC
		0.02077866 BTC

Note : Two input transactions coupled for a payment plus some random change.

CLUSTERING

1PXzMrz8KBNEkTt3Wnuqy4axiWszbyQKyE

1Djvb34FNpNXtrbbjaQeERZf68cyUdWyzd

1FLa9NcXJPA2XvF34LRuB4zbXX4Ws32dpL

17atn5sagYRBUvzgFLd9bUjWF4yStkdokW

19onWuLmjXGVfc7oUAEVuy9Yd3jxqhsUbK

1AASWBCGveXH6H5yTCZW2x7uZrawDiqp4U

1AffmSG4tcNRjcgTWTnS6TM3cWPeeA9EVd

1Ao6mKMEXxCVNVAuGjfLXZ3Zf43hd3yAEq

19SZcQ2CzJacQZE9rYwQjsfcBKMWDNwBWD

13Zjnzx8VxtLUEiYcrVXKp5sLucLMvBqaG

18rdKmjrg1EawxgiVT3ikLExj6GWS2MNCk

16pDB5bvoqRGvoH32GaJLfsEcaMc2T9xDr

1H3bY2Cv1pmn8ffTdyeRvZAUjNJC1giQHm

1PLjv1VzGEKxtM2FnRzg2FmDjen9trUBrh

1Nq612zwhEZDBNz2AeWKZxD6LvwiLm6cQU

IDENTIFICATION

1PXzMrz8KBNEkTt3Wnuqy4axiWszbyQKyE

1Djvb34FNpNXtrbbjaQeERZf68cyUdWyzd

1FLa9NcXJPA2XvF34LRuB4zbXX4Ws32dpL

17atn5sagYRBUvzgFLd9bUjWF4yStkdokW

19onWuLmjXGVfc7oUAEVuy9Yd3jxqhsUbK

1AASWBCGveXH6H5yTCZW2x7uZrawDiqp4U

1AffmSG4tcNRjcgTWTnS6TM3cWPeeA9EVd

1Ao6mKMEXxCVNVAuGjfLXZ3Zf43hd3yAEq

19SZcQ2CzJacQZE9rYwQjsfcBKMWDNwBWD

13Zjnzx8VxtLUEiYcrVXKp5sLucLMvBqaG

18rdKmjrg1EawxgiVT3ikLExj6GWS2MNCk

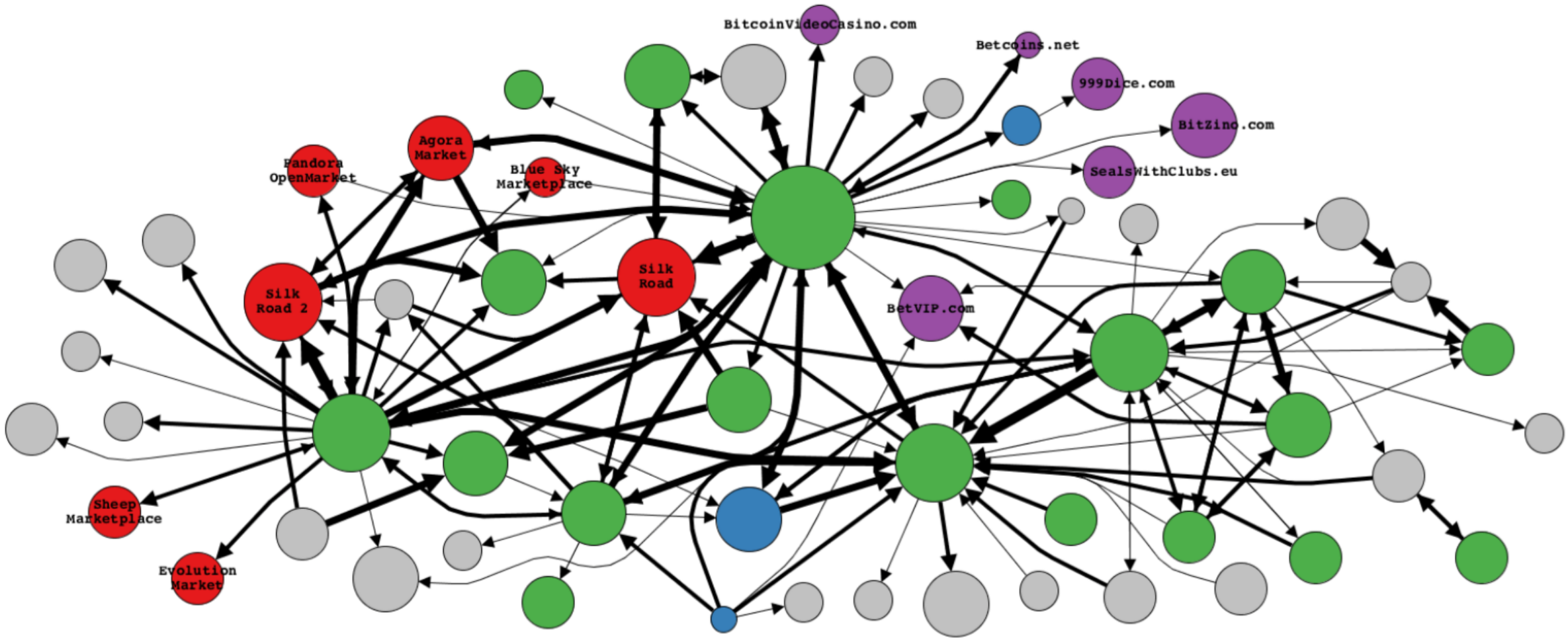
16pDB5bvoqRGvoH32GaJLfsEcaMc2T9xDr

1H3bY2Cv1pmn8ffTdyeRvZAUjNJC1giQHm

1PLjv1VzGEKxtM2FnRzg2FmDjen9trUBrh

1Nq612zwhEZDBNz2AeWKZxD6LvwiLm6cQU

CLUSTERING



The Unreasonable Effectiveness of Address Clustering — Harrigan and Fretter, May 2016

DE-ANONYMIZATION

Passive : Analytics on 80 GB of Bitcoin blockchain data

- Clustering of Bitcoin Addresses with suitable definition of Metrics
- Identification of the Clusters using known and/or leaked Addresses

Active : Injecting and tracking marked Bitcoin transactions

- Registering on Dark Marketplaces, Exchanges, and Mining Pools
- Using Addresses leaked from all these sources for Identification

Elliptic (https://www.elliptic.co/) does something similar in the UK.

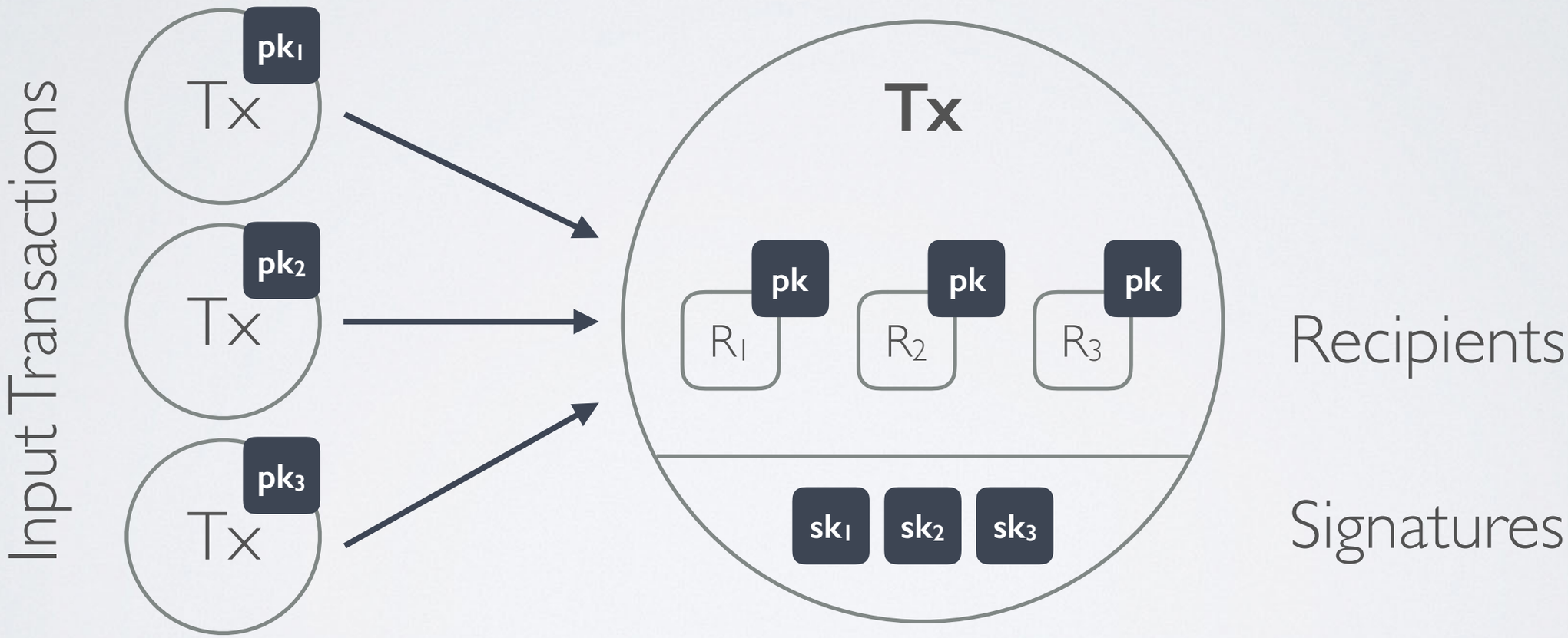
We should try to build our own tool for de-anonymization.

BLOCKCHAIN

Versatile Toolkit for Protocols

TRANSACTION

Input : Array of previous Transactions | Output : Array of recipient Addresses



Network verifies the Signature(s)

TRANSACTION

Metadata

Input(s)

Output(s)


```
"hash":"b6f6991d03df0e2e04dafffcd6bc418aac66049e2cd74b80f14ac86db1e3f0da",
"ver":1,
"vin_sz":1,
"vout_sz":2,
"lock_time":"Unavailable",
"size":258,
"relayed_by":"64.179.201.80",
"block_height, 12200,
"tx_index":"12563028",
"inputs":[

        {
            "prev_out":{
                "hash":"a3e2bcc9a5f776112497a32b05f4b9e5b2405ed9",
                "value":"100000000",
                "tx_index":"12554260",
                "n":"2"
            },
            "script":"76a914641ad5051edd97029a003fe9efb29359fcee409d88ac"
        }

    ],
"out":[

            {
                "value":"98000000",
                "hash":"29d6a3540acfa0a950bef2bfdc75cd51c24390fd",
                "script":"76a914641ad5051edd97029a003fe9efb29359fcee409d88ac"
            },

            {
                "value":"2000000",
                "hash":"17b5038a413f5c5ee288caa64cfab35a0c01914e",
                "script":"76a914641ad5051edd97029a003fe9efb29359fcee409d88ac"
            }

    ]
```


Data obtained from blockchain.info

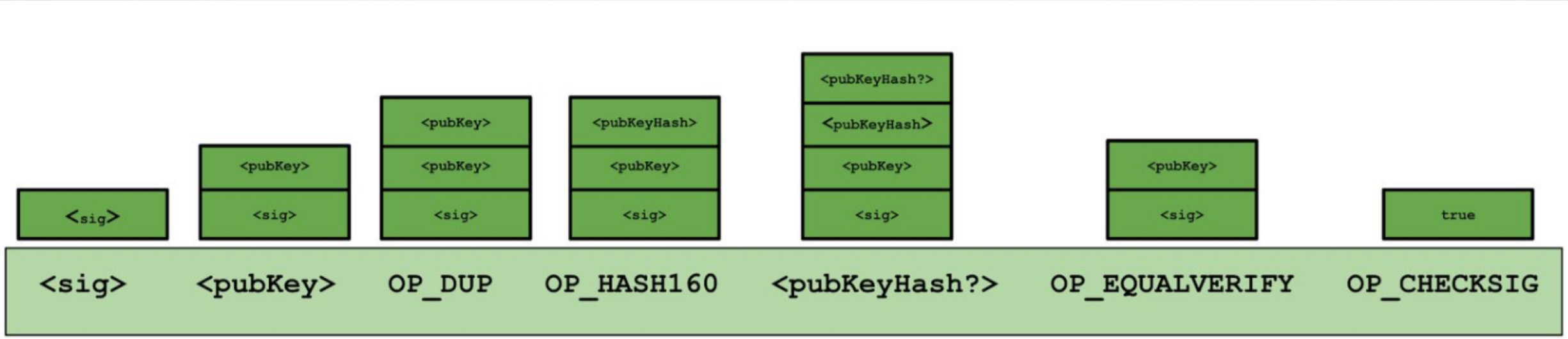
BITCOIN SCRIPT

Input Scripts

3044022019aca6d0972a86fa6cb6b31501d62fbec0972c28d1c8784330b67fb69814e10402202ec7cd22a5a185f12b9de141f51a5016060d131900f931a2c4d7d5bdcdd7a73501 0218a843aa5728fb06d5a114385e4869e8f2497b013df03dd1fa094b46271ac1bb	OK

Output Scripts

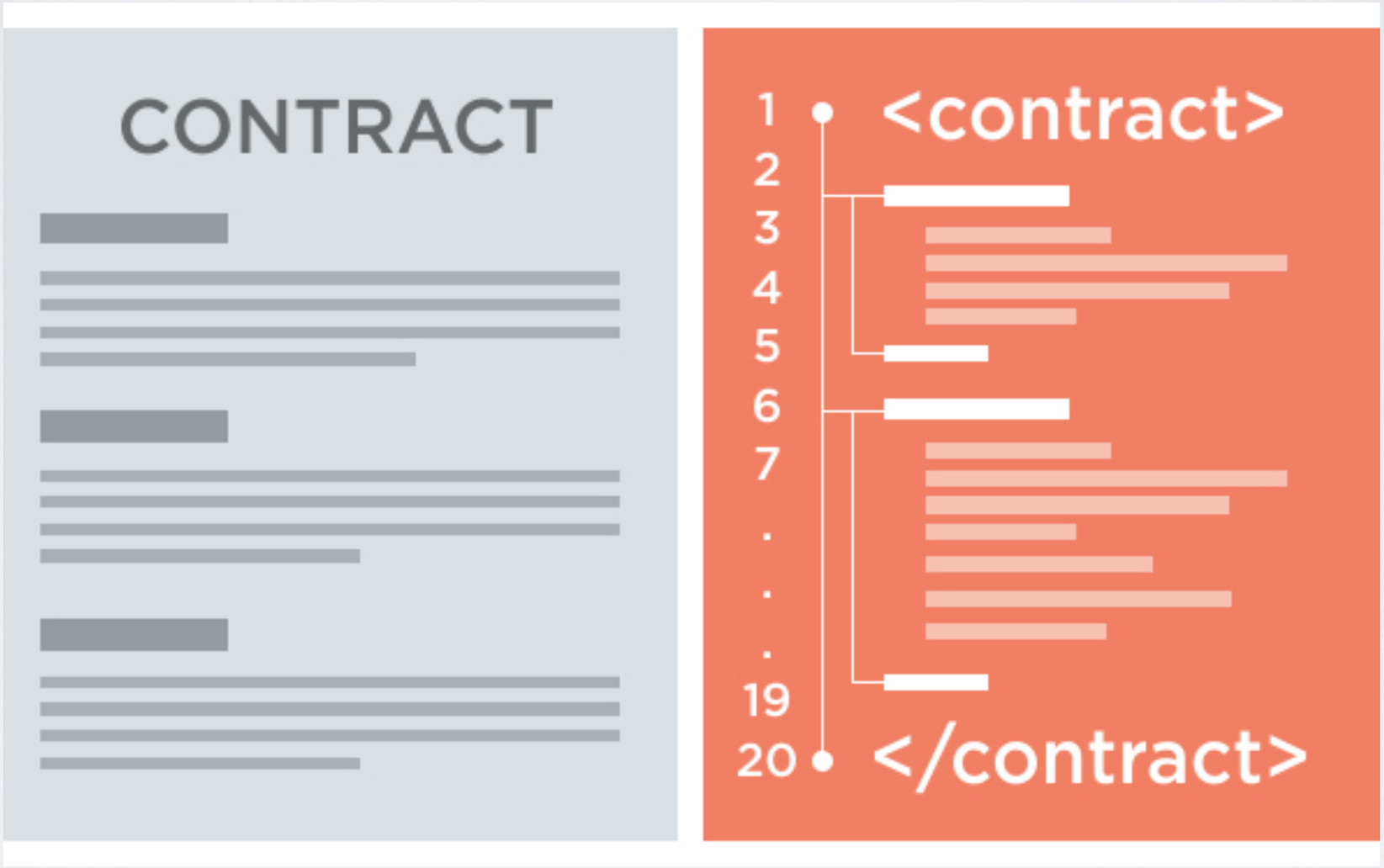
OP_DUP OP_HASH160 da25b659ae06c721144123b4d4f9a27badb50643 OP_EQUALVERIFY OP_CHECKSIG	OK
OP_DUP OP_HASH160 f50a8bf743344862f7e03aa077712cf0f864b17e OP_EQUALVERIFY OP_CHECKSIG	OK



Data obtained from blockchain.info

POTENTIAL

With a powerful Scripting Language



Developing “Smart Contracts” on Blockchain

Smart Contracts

BitShares

Ripple

BitGold

Proof of Space

ZeroCoin

Zcash

ADePT

Smart Properties

RSCoin

Proof of Existence

OpenBazaar

Bitcoin-NG

OneName

BigchainDB

Ethereum

Factom

BitHealth

Retricoin

Namecoin

Proof of Commitment

SpaceMint

BitNation

Perma-Coin

Proof of Stake

GHOST

Proof of Retrievability

"Bitcoin is an idea with disruptive ramifications."

Thank you for listening!