Blockchain and Cryptocurrencies

Cryptocurrencies
Bitcoin addresses
Blockchain
Mining
Ethereum
Smart Contracts

Prof Bill Buchanan OBE

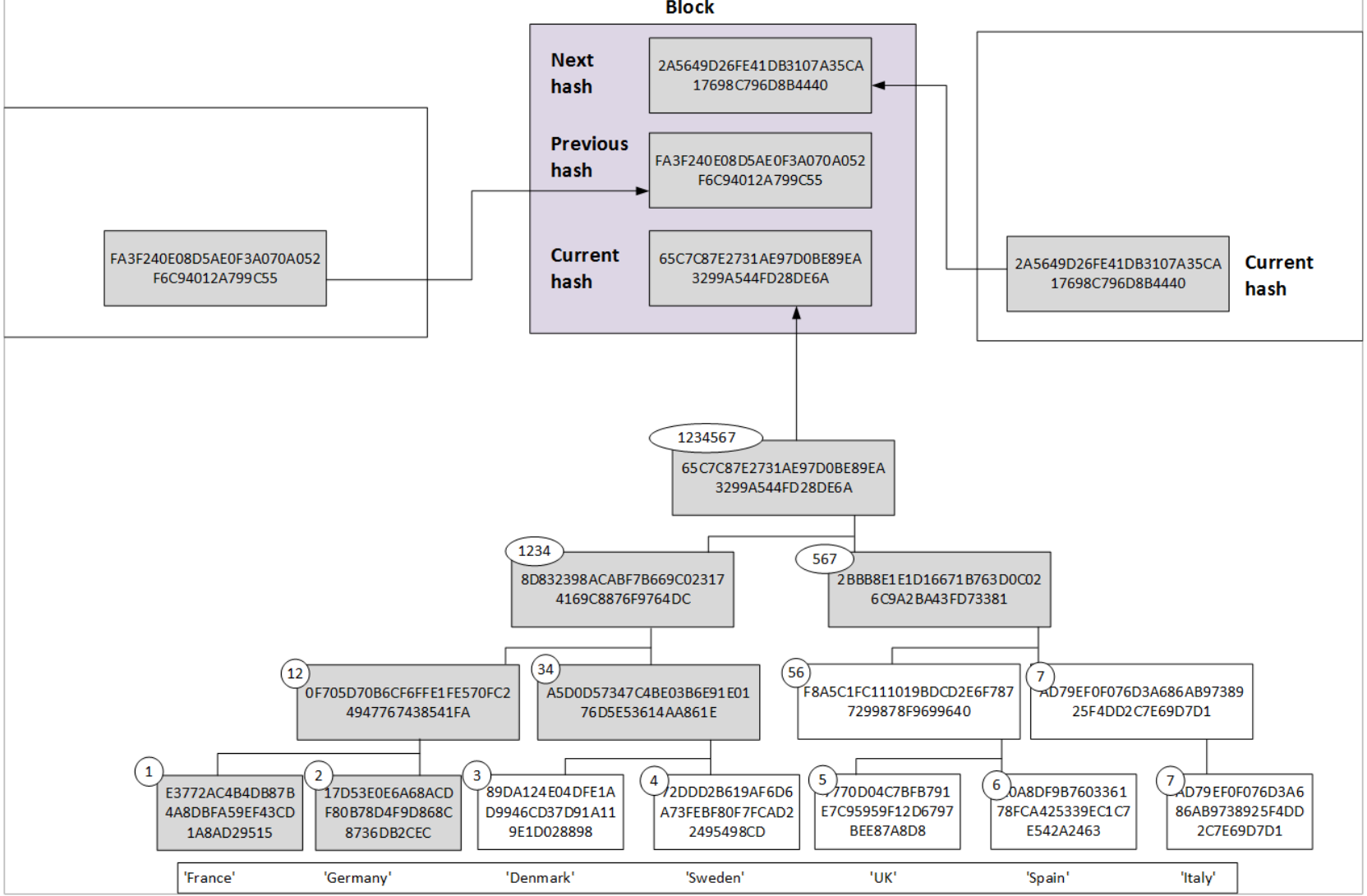
http://asecuritysite.com/ethereum
https://asecuritysite.com/blockchain/

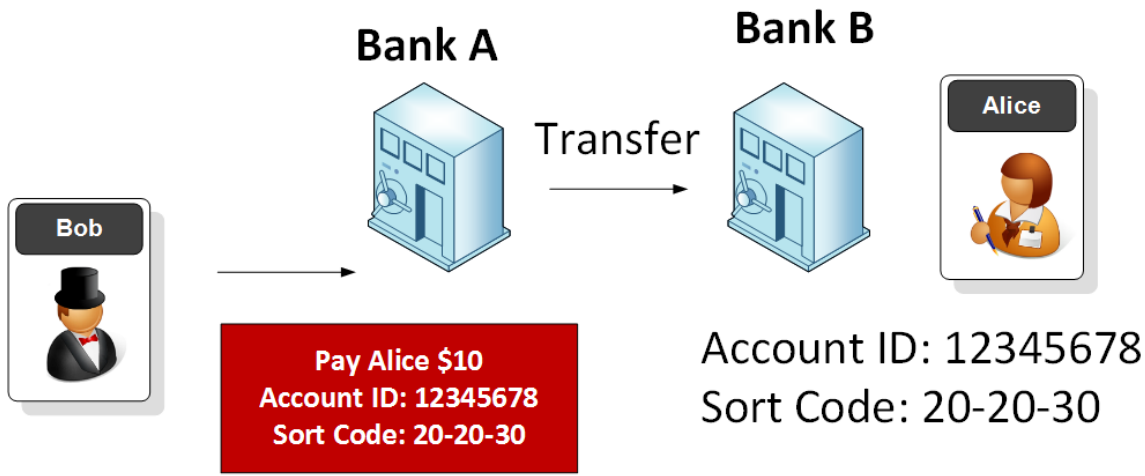
ocurrencies

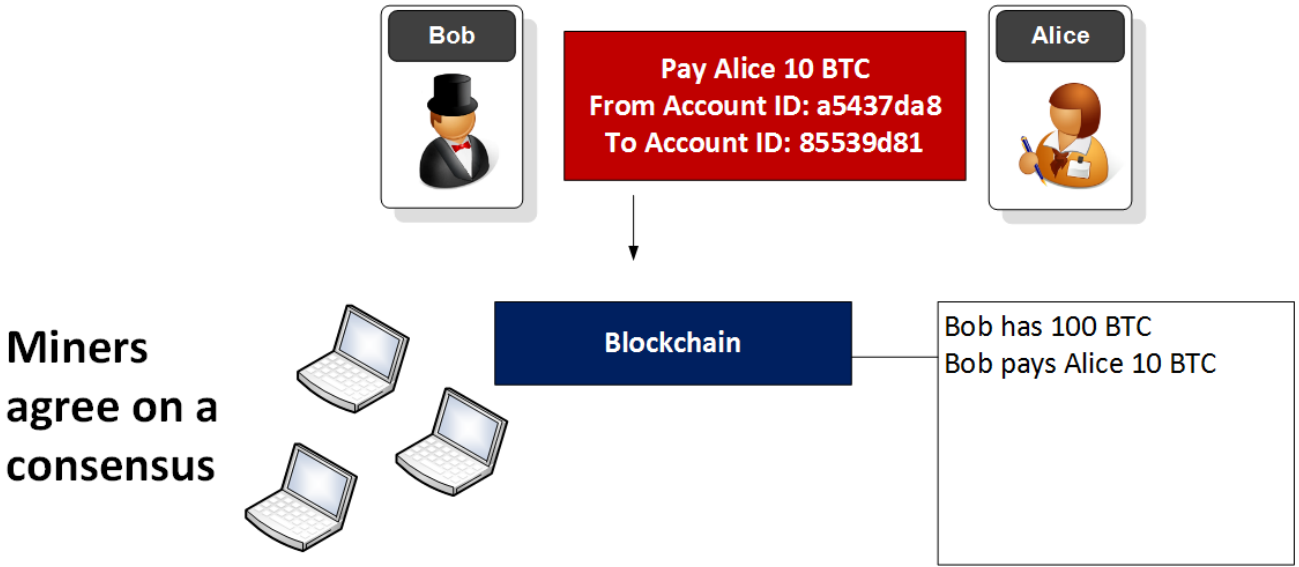
BE

eum

kchain/


Block
Next hash
2A5649D26FE41DB3107A35CA 17698C796D8B4440
Previous hash
FA3F240E08D5AE0F3A070A052 F6C94012A799C55
Current hash
65C7C87E2731AE97D0BE89EA 3299A544FD28DE6A
FA3F240E08D5AE0F3A070A052 F6C94012A799C55
2A5649D26FE41DB3107A35CA 17698C796D8B4440
Current hash
1234567
65C7C87E2731AE97D0BE89EA 3299A544FD28DE6A
1234
8D832398ACABF7B669C02317 4169C8876F9764DC
567
2BBB8E1E1D16671B763D0C02 6C9A2BA43FD73381
12
0F705D70B6CF6FFE1FE570FC2 4947767438541FA
34
A5D0D57347C4BE03B6E91E01 76D5E53614AA861E
56
F8A5C1FC111019BDCD2E6F787 7299878F9699640
7
AD79EF0F076D3A686AB97389 25F4DD2C7E69D7D1
1
E3772AC4B4DB87B 4A8DBFA59EF43CD 1A8AD29515
2
17D53E0E6A68ACD F80B78D4F9D868C 8736DB2CEC
3
89DA124E04DFE1A D9946CD37D91A11 9E1D028898
4
72DDD2B619AF6D6 A73FEBF80F7FCAD2 2495498CD
5
770D04C7BFB791 E7C95959F12D6797 BEE87A8D8
6
0A8DF9B7603361 78FCA425339EC1C7 E542A2463
7
AD79EF0F076D3A6 86AB9738925F4DD 2C7E69D7D1
'France'
'Germany'
'Denmark'
'Sweden'
'UK'
'Spain'
'Italy'


Bank A
Bank B
Transfer
Alice
Bob
Pay Alice $10
Account ID: 12345678
Sort Code: 20-20-30
Account ID: 12345678
Sort Code: 20-20-30


Bob
Pay Alice 10 BTC
From Account ID: a5437da8
To Account ID: 85539d81
Alice
Miners
agree on a
consensus
Blockchain
Bob has 100 BTC
Bob pays Alice 10 BTC

Who is 15 years old?

Who is 15 years old?

Who is 15 years old?

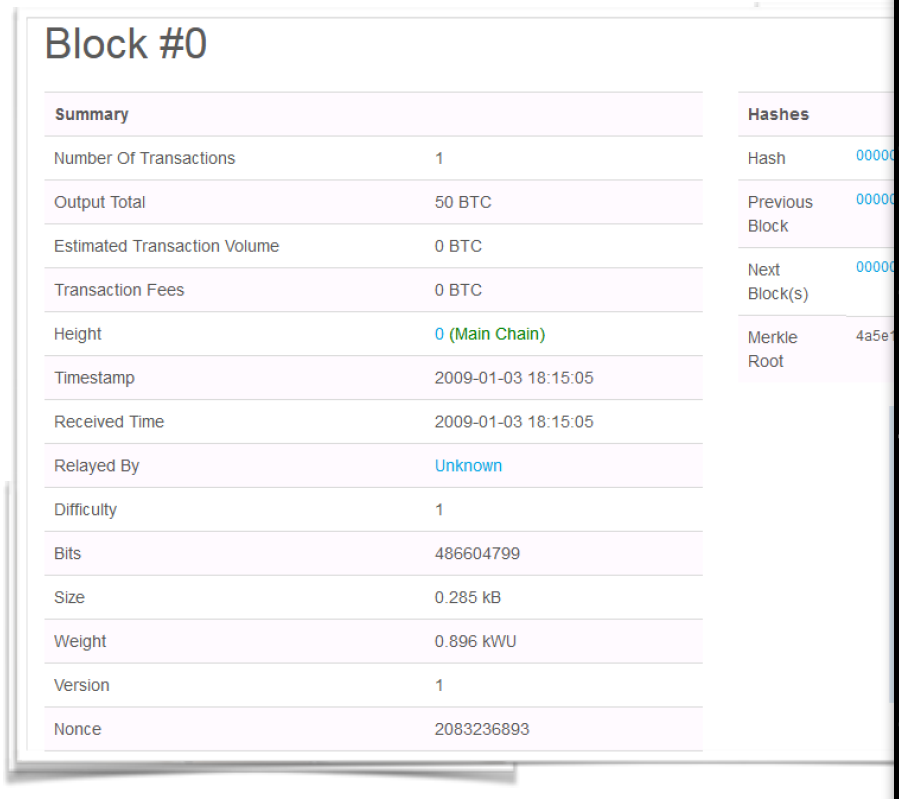
Who is 15 years old?

Block #0

Summary	
Number Of Transactions	1
Output Total	50 BTC
Estimated Transaction Volume	0 BTC
Transaction Fees	0 BTC
Height	0 (Main Chain)
Timestamp	2009-01-03 18:15:05
Received Time	2009-01-03 18:15:05
Relayed By	Unknown
Difficulty	1
Bits	486604799
Size	0.285 kB
Weight	0.896 kWU
Version	1
Nonce	2083236893

Hashes	
Hash	000000000019d6689c085ae165831e934ff763ae46a2a6c172b3f1b60a8ce26f
Previous Block	0000000000000000000000000000000000000000000000000000000000000000
Next Block(s)	00000000839a8e6886ab5951d76f411475428afc90947ee320161bbf18eb6048
Merkle Root	4a5e1e4baab89f3a32518a88c31bc87f618f76673e2cc77ab2127b7afdeda33b

Who is 15 years old?



Block #0

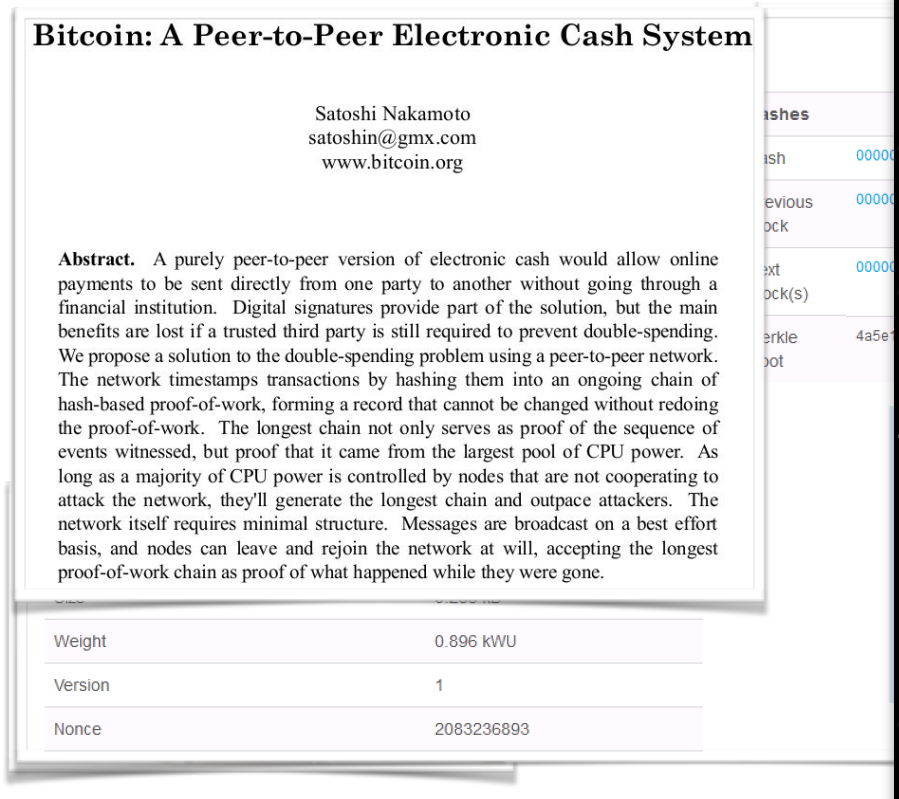
Summary	
Number Of Transactions	1
Output Total	50 BTC
Estimated Transaction Volume	0 BTC
Transaction Fees	0 BTC
Height	0 (Main Chain)
Timestamp	2009-01-03 18:15:05
Received Time	2009-01-03 18:15:05
Relayed By	Unknown
Difficulty	1
Bits	486604799
Size	0.285 kB
Weight	0.896 kWU
Version	1
Nonce	2083236893

Hashes	
Hash	00000
Previous Block	00000
Next Block(s)	00000
Merkle Root	4a5e1

His work was a hotch-potch of differing cryptography methods that could be sourced in the 1970s - such as public key - and also of the cyber punk movement which developed in the 1990s, and was founded by Eric Hughes, Tim May and John Gilmore.

Currently, as of 5 January 2018, the blockchain size is around 385GB, and there are 19 million coins in circulation [here].

Who is 15 years old?



Bitcoin: A Peer-to-Peer Electronic Cash System

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

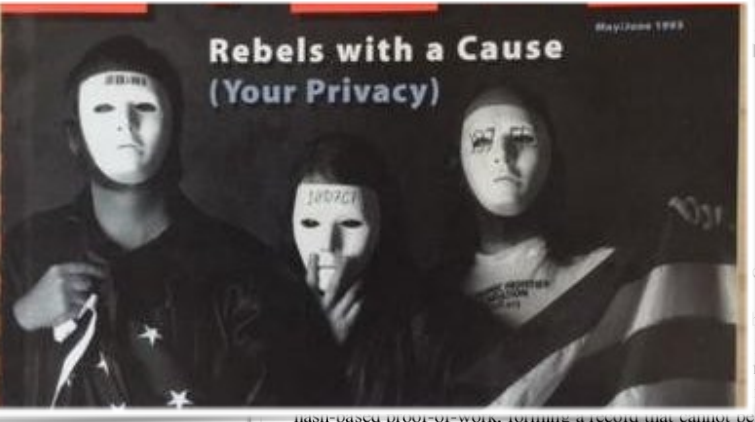
Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required 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.

Weight	0.896 kWU
Version	1
Nonce	2083236893

His work was a hotch-potch of differing cryptography methods that could be sourced in the 1970s - such as public key - and also of the cyber punk movement which developed in the 1990s, and was founded by Eric Hughes, Tim May and John Gilmore.

Currently, as of 5 January 2018, the blockchain size is around 385GB, and there are 19 million coins in circulation [here].

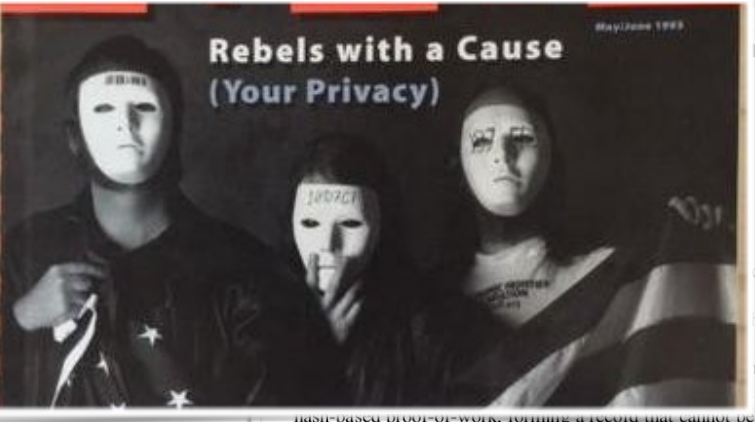
Who is 15 years old?

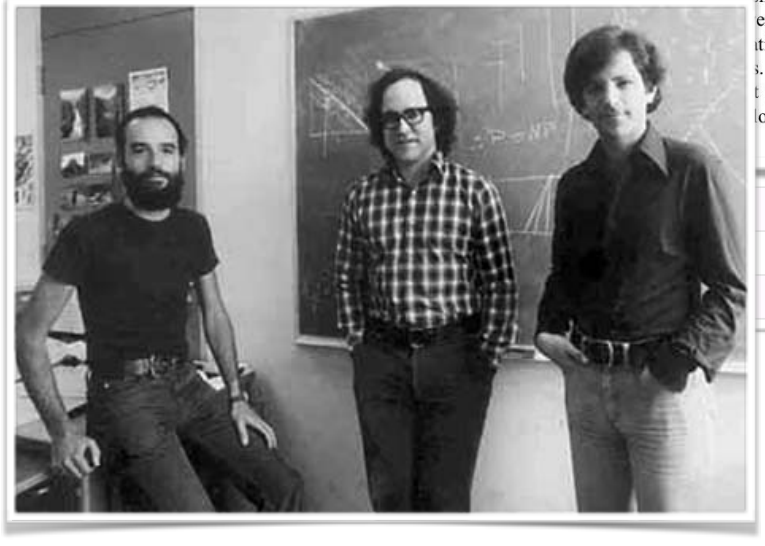


His work was a hotch-potch of differing cryptography methods that could be sourced in the 1970s - such as public key - and also of the cyber punk movement which developed in the 1990s, and was founded by Eric Hughes, Tim May and John Gilmore.

Currently, as of 5 January 2018, the blockchain size is around 385GB, and there are 19 million coins in circulation [here].

Who is 15 years old?





His work was a hotch-potch of differing cryptography methods that could be sourced in the 1970s - such as public key - and also of the cyber punk movement which developed in the 1990s, and was founded by Eric Hughes, Tim May and John Gilmore.

Currently, as of 5 January 2018, the blockchain size is around 385GB, and there are 19 million coins in circulation [here].

Who is 15 years old?

His work was a hotch-potch of differing cryptography methods that could be sourced in the 1970s - such as public key - and also of the cyber punk movement which developed in the 1990s, and was founded by Eric Hughes, Tim May and John Gilmore.

Currently, as of 5 January 2018, the blockchain size is around 385GB, and there are 19 million coins in circulation [here].

Who is 15 years old?

His work was a hotch-potch of
differing cryptography methods
rced in the 1970s
ey - and also of
ovement which
1990s, and was
lughes, Tim May
.

January 2018,
e is
around 385GB, and there are 19 million coins in circulation [here].

The Most Profitable Crime?

The Most Profitable Crime?

Which is the easiest crime to implement, with the largest potential return, and with virtually no chance of being caught?

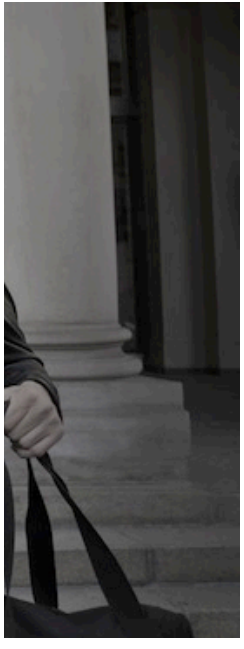
Published on December 21, 2017 Edit article | View stats

Prof Bill Buchanan OBE, PhD, FBCS
Professor at Napier University
1,194 articles

132 12 6 3

I remember hearing that, in the UK, for the first time in a single year, there were no actual physical bank robberies. Why? Because there are often much better pickings for criminals if they can hack their way into a bank. As we move into a crypto world, the opportunities for cyber criminals will increase by the day.

While cryptocurrencies are safe in themselves, the major problem seems to be with the places which hold the wallets. In 2014, for example, Mt. Gox - a Japanese cryptocurrency exchange - filed for bankruptcy after a hacker drained the exchange of 100s of thousands of Bitcoins.



The Most Profitable Crime?

Which is the easiest crime to implement with the largest potential return, and with virtually no chance of being caugh

Published on December 21, 2017 Edit article | View stats

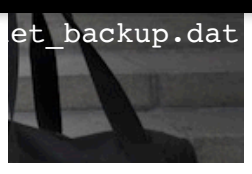
Prof Bill Buchanan OBE, PhD, FBCS
Professor at Napier University
1,194 articles

132 12 6

I remember hearing that, in the UK, for the first time in a single year, there were no actual physical bank robberies. Why? Because there are often much better pickings f criminals if they can hack their way into a bank. As we move into a crypto world, th opportunities for cyber criminals will increase by the day.

While cryptocurrencies are safe in themselves, the major problem seems to be with the places which hold the wallets. In 2014, for example, Mt. Gox - a Japanese cryptocurrency exchange - filed for bankruptcy after a hacker drained the exchange of 100s of thousands of Bitcoins.

```
wallet.dat.1
wallet.dat.zip
wallet.tar
wallet.tar.gz
wallet.zip
wallet_backup.dat
wallet_backup.dat.1
```



The Most Profitable Crime?

Which is the easiest crime to implement with the largest potential return, and

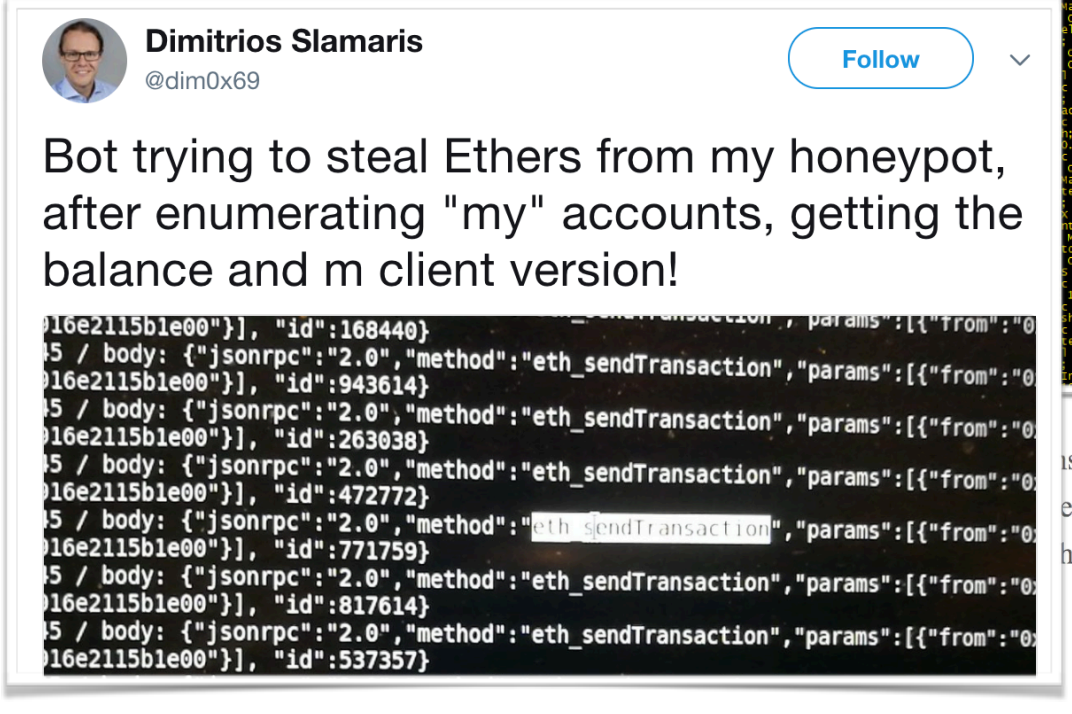
While cryptocurrencies are safe in themselves, the major problem seems to be with the places which hold the wallets. In 2014, for example, Mt. Gox - a Japanese cryptocurrency exchange - filed for bankruptcy after a hacker drained the exchange of 100s of thousands of Bitcoins.

The Most Profitable Crime?

Which is the easiest crime to implement with the largest potential return, and

wallet.dat.1

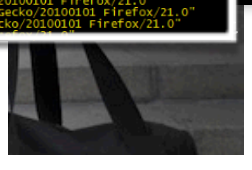
wallet.dat.zip



Dimitrios Slamaris
@dim0x69

Follow

Bot trying to steal Ethers from my honeypot, after enumerating "my" accounts, getting the balance and m client version!



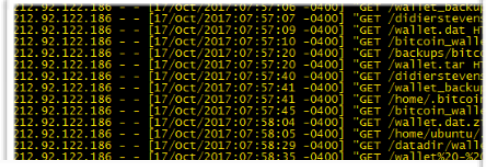
is to be with the
ese
he exchange of

The Most Profitable Crime?

Which is the easiest crime to implement
with the largest potential return, and

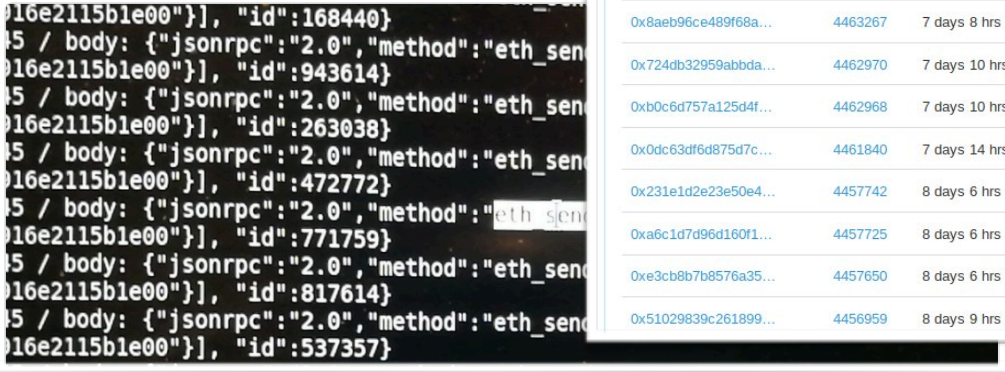
wallet.dat.1

wallet.dat.zip



Dimitrios Slamaris
@dim0x69

Bot trying to steal Ethers fr
after enumerating "my" acc
balance and m client versio



Transactions | Comments

Latest 25 txns from a total Of 81 transactions

TxHash	Block	Age	From		To
0xb435f8eb66f5a90...	4508126	3 hrs 23 mins ago	0x4f6462305a43cec...	IN	0xcd9da0595a
0x35d861310c18f8f...	4506352	10 hrs 8 mins ago	0x51017155a53d140...	IN	0xcd9da0595a
0xe2ef8c8fcf58b0c8...	4505716	12 hrs 40 mins ago	0x2e820b454dfdb39...	IN	0xcd9da0595a
0x7e6b86be4e9c5b2...	4501770	1 day 3 hrs ago	0x8ba912954aedfea...	IN	0xcd9da0595a
0x37819f1ff137cee7...	4494468	2 days 8 hrs ago	0xfbac940ec55e1aa...	IN	0xcd9da0595a
0xd32fbe5771f291b...	4494300	2 days 8 hrs ago	0xfbac940ec55e1aa...	IN	0xcd9da0595a
0x57ddb94fe86a279...	4481415	4 days 10 hrs ago	0x258c827f5acf8c9...	IN	0xcd9da0595a
0x01961c698168b82...	4476889	5 days 4 hrs ago	0x258c827f5acf8c9...	IN	0xcd9da0595a
0x8aeb96ce489f68a...	4463267	7 days 8 hrs ago	0xb093c35549e6eff...	IN	0xcd9da0595a
0x724db32959abbda...	4462970	7 days 10 hrs ago	0x009befe5643f989...	IN	0xcd9da0595a
0xb0c6d757a125d4f...	4462968	7 days 10 hrs ago	0x009befe5643f989...	IN	0xcd9da0595a
0x0dc63df6d875d7c...	4461840	7 days 14 hrs ago	0x009befe5643f989...	IN	0xcd9da0595a
0x231e1d2e23e50e4...	4457742	8 days 6 hrs ago	0xd58b7ae09f88e0f...	IN	0xcd9da0595a
0xa6c1d7d96d160f1...	4457725	8 days 6 hrs ago	0x54160297ff7892b...	IN	0xcd9da0595a
0xe3cb8b7b8576a35...	4457650	8 days 6 hrs ago	0x54160297ff7892b...	IN	0xcd9da0595a
0x51029839c261899...	4456959	8 days 9 hrs ago	0xd58b7ae09f88e0f...	IN	0xcd9da0595a

Dear 21st Century …

Dear 21st Century …

What is the ownership of something?

Dear 21st Century …

What is the ownership of something?

Dear 21st Century …

What is the ownership of something?

What is consent?

Dear 21st Century …

What is the ownership of something?

What is consent?

What are physical borders?

Dear 21st Century …

What is the ownership of something?

What is consent?

Who's laws do I comply with?

What are physical borders?

Dear 21st Century …

What is the ownership of something?

What is consent?

Who's laws do I comply with?

What are physical borders?

Why does fiat currency exist?

Dear 21st Century …

What is the ownership of something?

What is consent?

What are my rights to privacy?

Who's laws do I comply with?

What are physical borders?

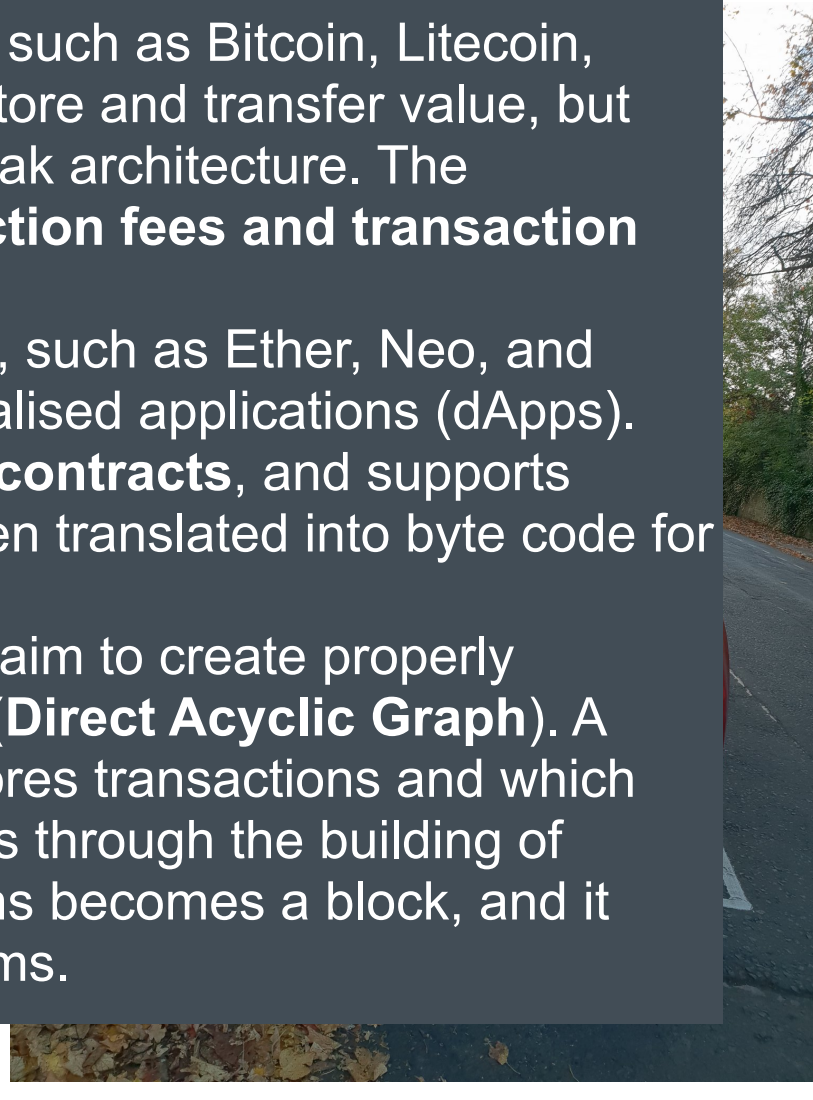
Why does fiat currency exist?

Dea

1st Generation. These cryptocurrencies, such as Bitcoin, Litecoin, Monero and Bitcoin Cash, basically just store and transfer value, but have suffered from poor scaling and a weak architecture. The overheads involve relatively **high transaction fees and transaction times**.

2nd Generation. These cryptocurrencies, such as Ether, Neo, and Lisk, have platforms that support decentralised applications (dApps). This generation adds **coding and smart contracts**, and supports logical operations. A high-level code is then translated into byte code for the Blockchain.

3rd Generation. These cryptocurrencies aim to create properly distributed systems, and many use DAG (**Direct Acyclic Graph**). A traditional Blockchain just sequentially stores transactions and which can take some time to create a consensus through the building of blocks. With DAG, each of the transactions becomes a block, and it thus speeds up the consensus mechanisms.

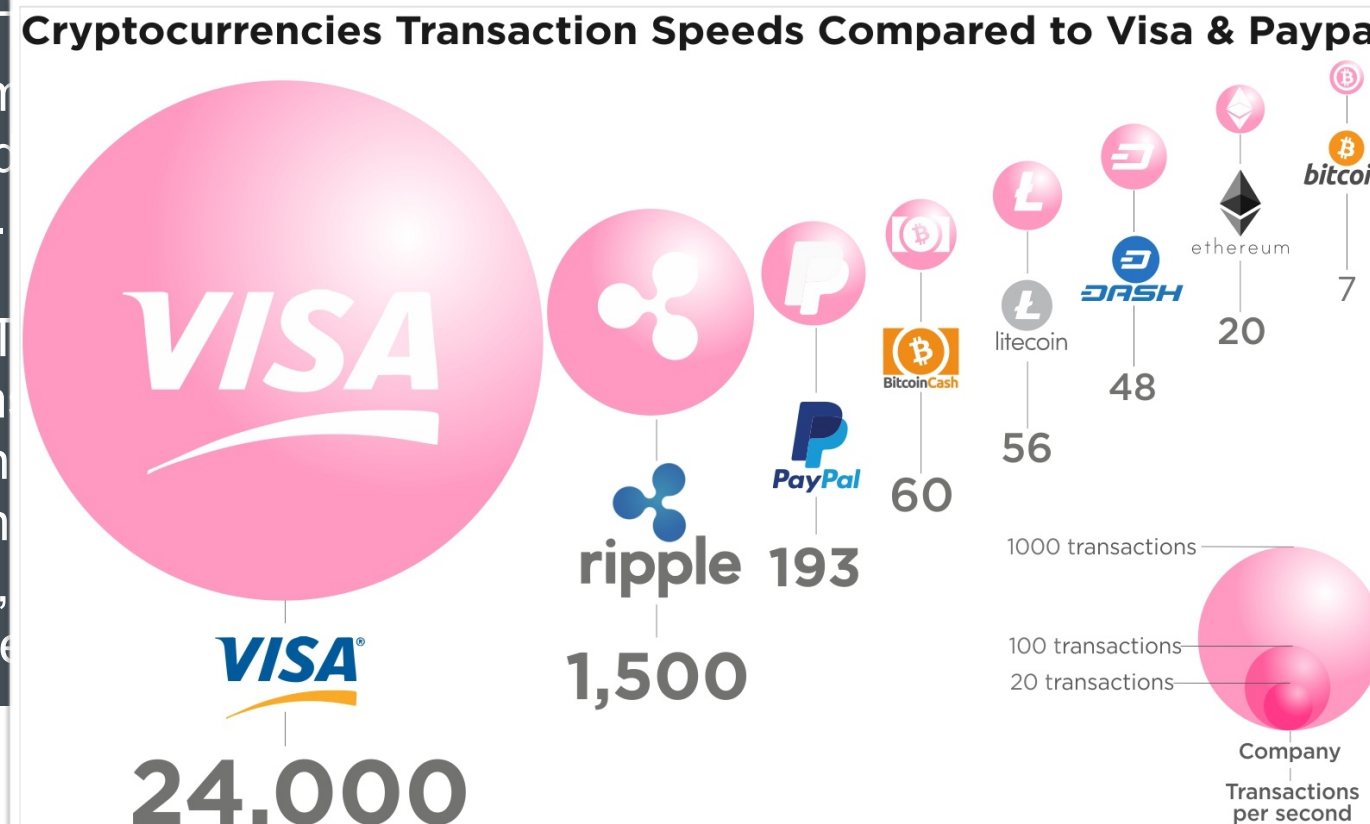


Dea

1st Generation. These cryptocurrencies, such as Bitcoin, Litecoin, Monero and Bitcoin Cash, basically just store and transfer value, but have suffered from poor scaling and a weak architecture. The overheads involve relatively **high transaction fees and transaction times**.

2nd Generation. T
Lisk, have platform
This generation ac
logical operations.
the Blockchain.

3rd Generation. T
distributed system
traditional Blockch
can take some tim
blocks. With DAG,
thus speeds up the



Dea

1st Generation. These cryptocurrencies, such as Bitcoin, Litecoin, Monero and Bitcoin Cash, basically just store and transfer value, but

	Heat Ledger	Bitcoin	Ethereum	Waves	Steem	Bitshares	Ardor
Operational	✓	✓	✓	✓	✓	✓	✓
Consensus Mechanism	POS/POP	POW	POW	DPOS/LPOS	POW	DPOS	POS
Block Target Time	25 second	10 minutes	15 second	1- 30 second	2 second	2 second	1 minute
Actual TPS max	1000 tps	2000 tps	2000 tps	1000 tps	1000 tps	100,000 tps	800 tps
Blockchain Size		90.9 Gb.	75 Gb.	--	--	--	--
Expected Blockchain Growth Rate		4.4 Gb./month	187 Mb./month	--	--	--	--
Current Total Available Supply	*25,000,000 HEAT*	*16,032,800 BTC*	*86,746,437 ETH*	*100,000,000 WAVES*	*225,967,998 STEEM*	*2,557,560,000 BTS*	*998,999,495 ARDR*
Decentralized Application	✓	✓	✓	✓	✓	✓	✓
Multi Signature	✓	✓	✗	✗	✗	✗	✓
Asset to Asset Exchange	✓	✗	✗	✓	✗	✓	✓
Sidechain	✓	✓	✓	✗	✗	✓	✓
Smart Contracts	✗	✗	✓	✗	✗	✓	✗
Language Used	Java	C/C++	C/C++	*Javascript*	*Python*	*C++*	*Java*

- based on thier respective we

blocks. With DAG,
thus speeds up the

VISA

24,000

1,500

100 transactions
20 transactions

Company

Transactions per second

History

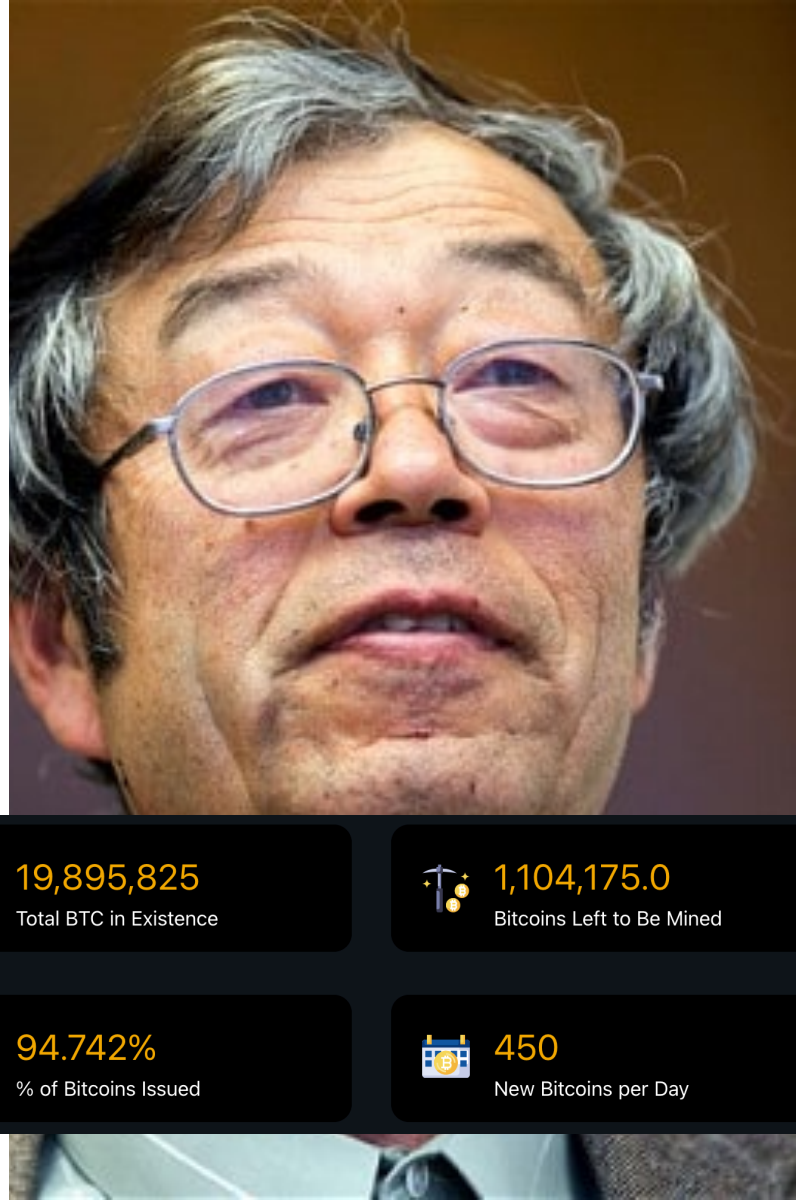
- Bitcoin was created in 2009 by someone known as Satoshi Nakamoto.
- Does not require the support of a central government or organisation to regulate it, nor a broker to manage payments.
- The Bitcoin currency is instead created when users *mine* for it, using their computers to perform complex calculations through special software.
- Bitcoin (BTC) divisible to the 8th decimal place.
- BTC can be split into 100,000,000 units.
- 0.00000001 bitcoin is one Satoshi.
- Was Satoshi from the UK? [here]

History

- Bitcoin designed to limit the number of bitcoins that can ever be created. [21 million]
- Each transaction then has a reward, and the reward reduces over time, which should reduce the supply of the coins.
- In April 2020, the reward for a successful mining process was reduced from 12.5 BTC to 6.25 BTC. This reward will continue to reduce until the currency is forked (and where new parameters are used), or when we reach a saturation level.
- On 20 April 2024, it halved again. Block here and here.
- Others: Ethereum, Ripple, Litecoin, Monero, Ethereum Classic, Dash, Steem, KiloCoin and Augur.

History

- Bitcoin designed to limit the number of bitcoins that can ever be created. [21 million]
- Each transaction then has a reward, and the reward reduces over time, which should reduce the supply of the coins.
- In April 2020, the reward for a successful mining process was reduced from 12.5 BTC to 6.25 BTC. This reward will continue to reduce until the currency is forked (and where new parameters are used), or when we reach a saturation level.
- On 20 April 2024, it halved again. Block here and here.
- Others: Ethereum, Ripple, Litecoin, Monero, Ethereum Classic, Dash, Steem, KiloCoin and Augur.



History

- Bitcoin was created in 2009 by someone known as Satoshi Nakamoto.
- Does not require the support of a central government or organisation to regulate it, nor a broker to manage payments.
- The Bitcoin currency is instead created when users *mine* for it, using their computers to perform complex calculations through special software.
- Bitcoin (BTC) divisible to the 8th decimal place.
- BTC can be split into 100,000,000 units.
- 0.00000001 bitcoin is one Satoshi.

History

- Bitcoin designed to limit the number of bitcoins that can ever be created.
- Each transaction then has a reward, and the reward reduces over time, which should reduce the supply of the coins.
- In 2016, the reward for a successful mining process was reduced from 25 BTC to 12.5 BTC. This reward will continue to reduce until the currency is forked (and where new parameters are used), or when we reach a saturation level.
- Others: Ethereum, Ripple, Litecoin, Monero, Ethereum Classic, Dash, Steem, KiloCoin and Augur.

Genesis Record

Summary	
Height	0 (Main chain)
Hash	000000000019d6689c085ae165831e934ff763ae46a2a6c172b3f1b60a8ce26f
Previous Block	0000000000000000000000000000000000000000000000000000000000000000
Next Blocks	00000000839a8e6886ab5951d76f411475428afc90947ee320161bbf18eb6048
Time	2009-01-03 18:15:05
Difficulty	1
Bits	486604799
Number Of Transactions	1
Output Total	50 BTC
Estimated Transaction Volume	0 BTC
Size	0.285 KB
Version	1
Merkle Root	4a5e1e4baab89f3a32518a88c31bc87f618f76673e2cc77ab2127b7afdeda33b
Nonce	2083236893
Block Reward	50 BTC
Transaction Fees	

4a5e1e4baab89f3a32518a88c31bc87f618f76673e2cc77ab2127b7afdeda33b 2009-01-03 18:15:05

No Inputs (Newly Generated Coins) → 1A1zP1eP5QGefi... (Genesis of Bitcoin) 50 BTC

50 BTC

Big accounts

Bitcoin Address Addresses are identifiers which you use to send bitcoins to another person.

Summary	
Address	3D2oetdNuZUqQHPJmcMDDHYoqkyNVsFk9r
Hash 160	7c6775e20e3e938d2d7e9d79ac310108ba501ddb
Tools	Related Tags - Unspent Outputs

Transactions	
No. Transactions	3493
Total Received	1,210,471.32658275 BTC
Final Balance	180,773.05403806 BTC

Bitcoin Address Addresses are identifiers which you use to send bitcoins to another person.

Summary	
Address	3EDzR4QKeGJyCZWXMF1kAGqi8gHNQ798sF
Hash 160	897d25262f68b8a8d4e2adf2ab082ce0f58a69d1
Tools	Related Tags - Unspent Outputs

Transactions	
No. Transactions	1
Total Received	2,034.668943 BTC
Final Balance	2,034.668943 BTC

Request Payment

Donation Button

e3a9cbec0c5ec55db3ac02029d8cbaf1370e04e8603d9e5000106091c66c308d 2017-11-14 08:03:03

3Qk9qheSn4Y5wUCmSAT4ggbhHbRRgRdVaW	1LAGK834p9y4h34jWgGjHsSRNUgKWB9Cho	0.009 BTC
	1GANRvqWMg1zmVGU2WKUAuGDS5PGj3KBNx	0.01718 BTC
	3Mfiy7hJB44kY7YHRgCuJ7JgpzuL1tSqWg	15.6262 BTC
	37kTvhCNe8WmLnhdjBRRZBtEL5zzH94Zq8	0.31678 BTC
	1FKjowv879X5RGDeU21zzxinVbgNoeGaHr	0.169 BTC
	3BazbNWURUzdk58myGn1V9F6HPabtUjZwN	0.01265 BTC
	3HCJDcEjzHyip6TJ3kwQQaJGxJW6scbzGB	13,067.17305362 BTC

13,083.32386362 BTC

Genesis Record

Summary	
Address	3EDzR4QKeGJyCZWXMF1kAGqi8gHNQ798sF
Hash 160	897d25262f68b8a8d4e2adf2ab082ce0f58a69d1
Tools	Related Tags - Unspent Outputs

Transactions	
No. Transactions	1
Total Received	2,034.668943 BTC
Final Balance	2,034.668943 BTC

Request Payment

Donation Button

Transactions (Oldest First)

Filter

67079f670818b0e44ed70399bcdc4664a8595fb6f90f8538b7821c7ac889bbe8			2017-11-13 19:10:37
3HomPY371CsvvjyaCZj7ExLf1TcSQ82HuG	→	3EDzR4QKeGJyCZWXMF1kAGqi8gHNQ798sF	2,034.668943 BTC

1 Confirmation

12,801,546.94 USD @2017-11-13T19:10:37Z

Bitcoin transactions and valuation

Bitcoin BTC

Find out more about various crypto assets and their risks here.

Price History

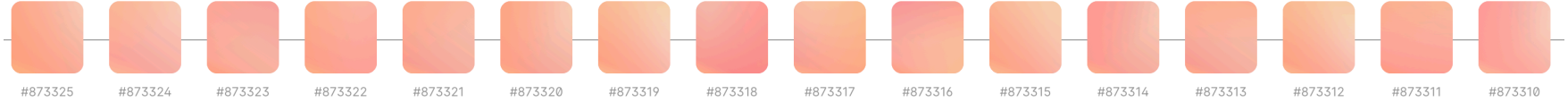
$102,488.85 • 05:53

Vol 139,422,106,974 BTC

1D 1W 1M 1Y MAX USD

Real-time data is obtained from multiple sources and may sometimes be delayed due to system performance issues. Past performance is not indicative of future results. Find out more about various crypto assets and their risks here.

Blockchain

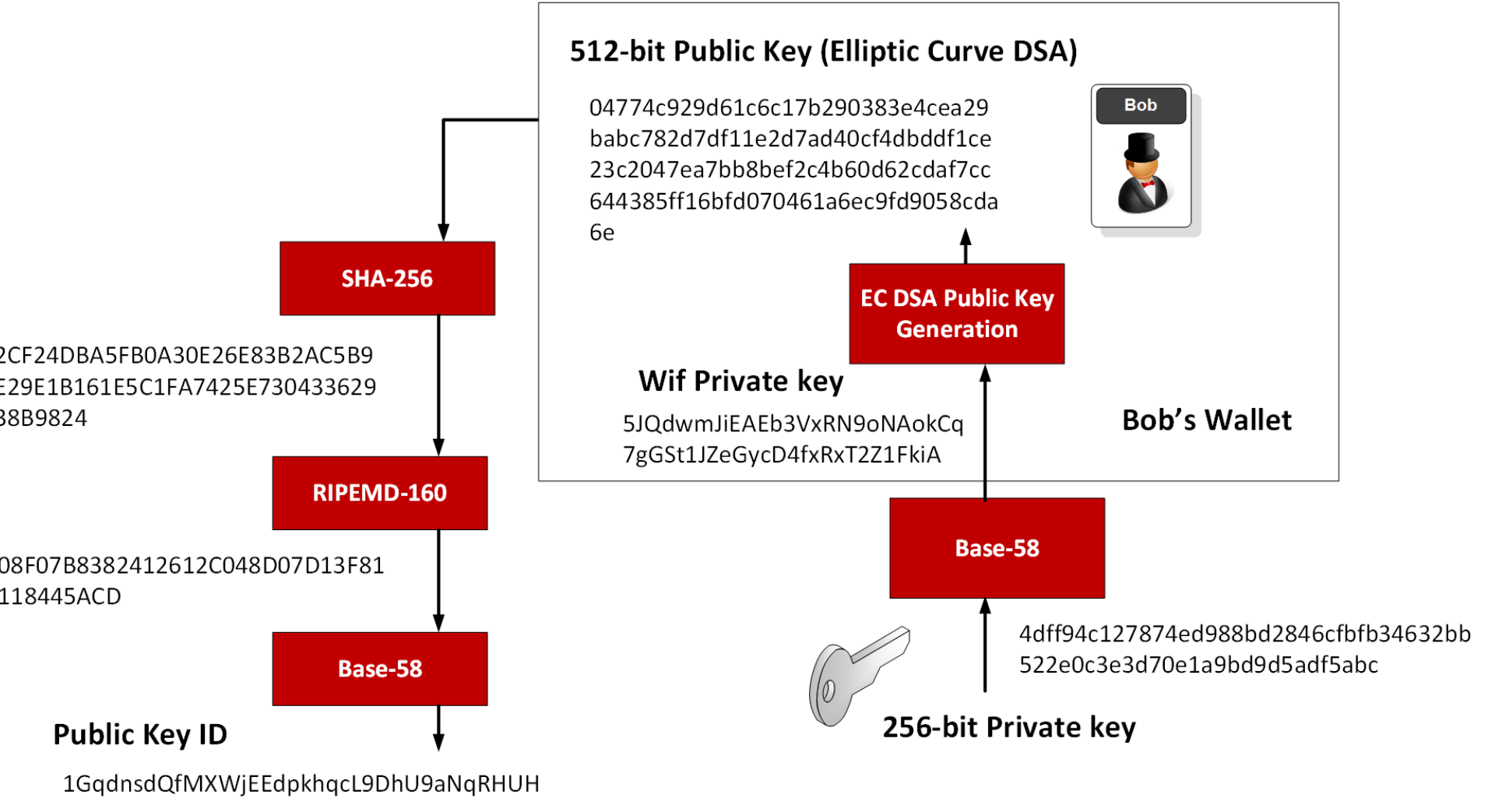


Bitcoin trading volume

Blockchain and Cryptocurrencies

Cryptocurrencies
Bitcoin addresses
Blockchain
Mining

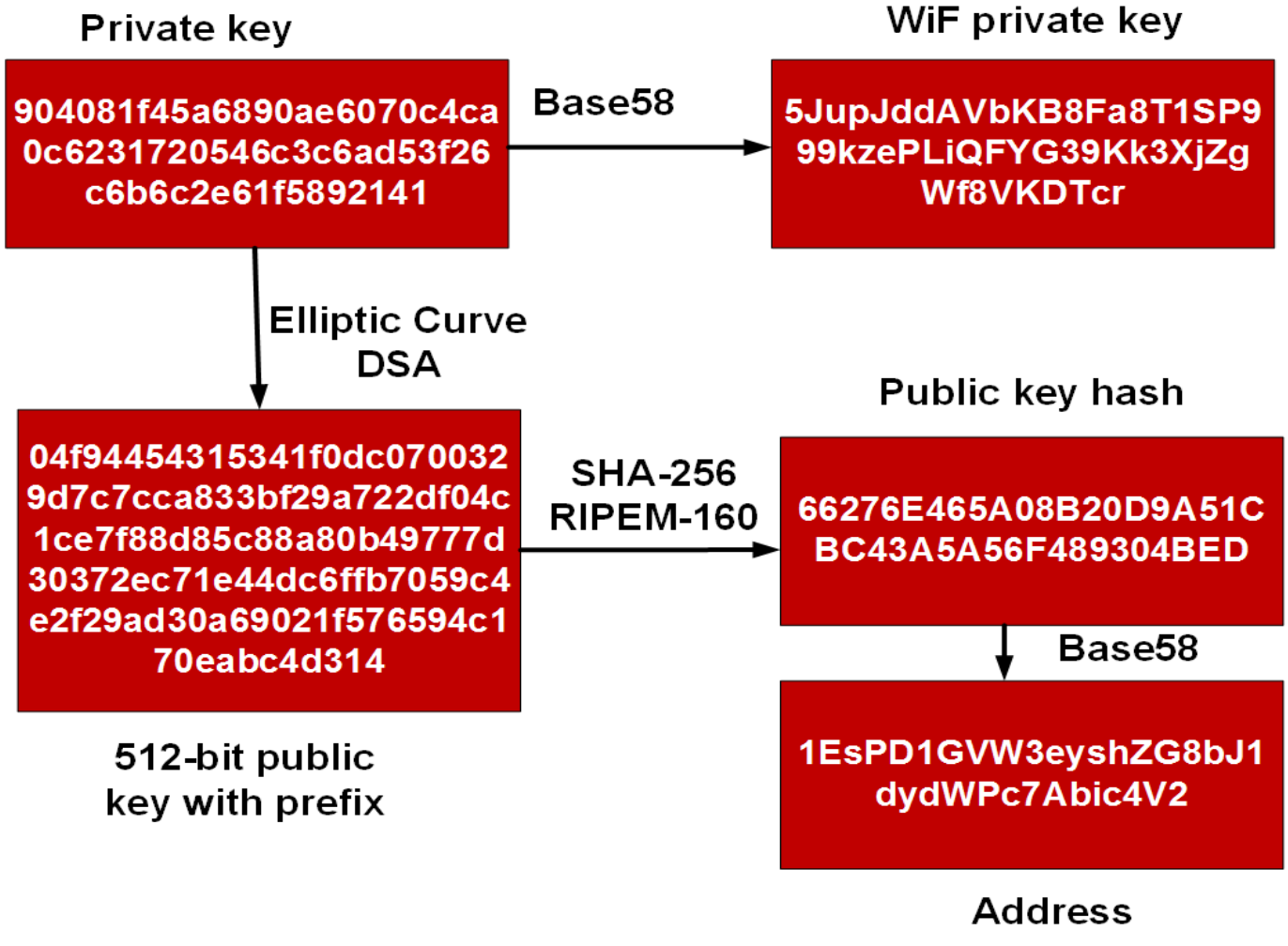
Bitcoin Wallet and Addresses



Summary	
Address	1JyvJ5TcN2hzu7dDEeVuuikgyHtpwU8NE6
Hash 160	c53deb8dda6fb0c388da19fbcf63270cc4f4cbfd
Tools	Related Tags - Unspent Outputs

Transactions	
No. Transactions	20
Total Received	0.64531495 BTC
Final Balance	0 BTC

Request Payment | Donation Button


Private key
904081f45a6890ae6070c4ca0c6231720546c3c6ad53f26c6b6c2e61f5892141
Base58
WiF private key
5JupJddAVbKB8Fa8T1SP999kzePLiQFYG39Kk3XjZgWf8VKDTcr
Elliptic Curve DSA
04f94454315341f0dc0700329d7c7cca833bf29a722df04c1ce7f88d85c88a80b49777d30372ec71e44dc6ffb7059c4e2f29ad30a69021f576594c170eabc4d314
512-bit public key with prefix
SHA-256 RIPEM-160
Public key hash
66276E465A08B20D9A51CBC43A5A56F489304BED
Base58
1EsPD1GVW3eyshZG8bJ1dydWPc7Abic4V2
Address

Private key:
4c0333a50b7724c71b89df148d83f64d49d896e21701007eeb8cada52744aca2

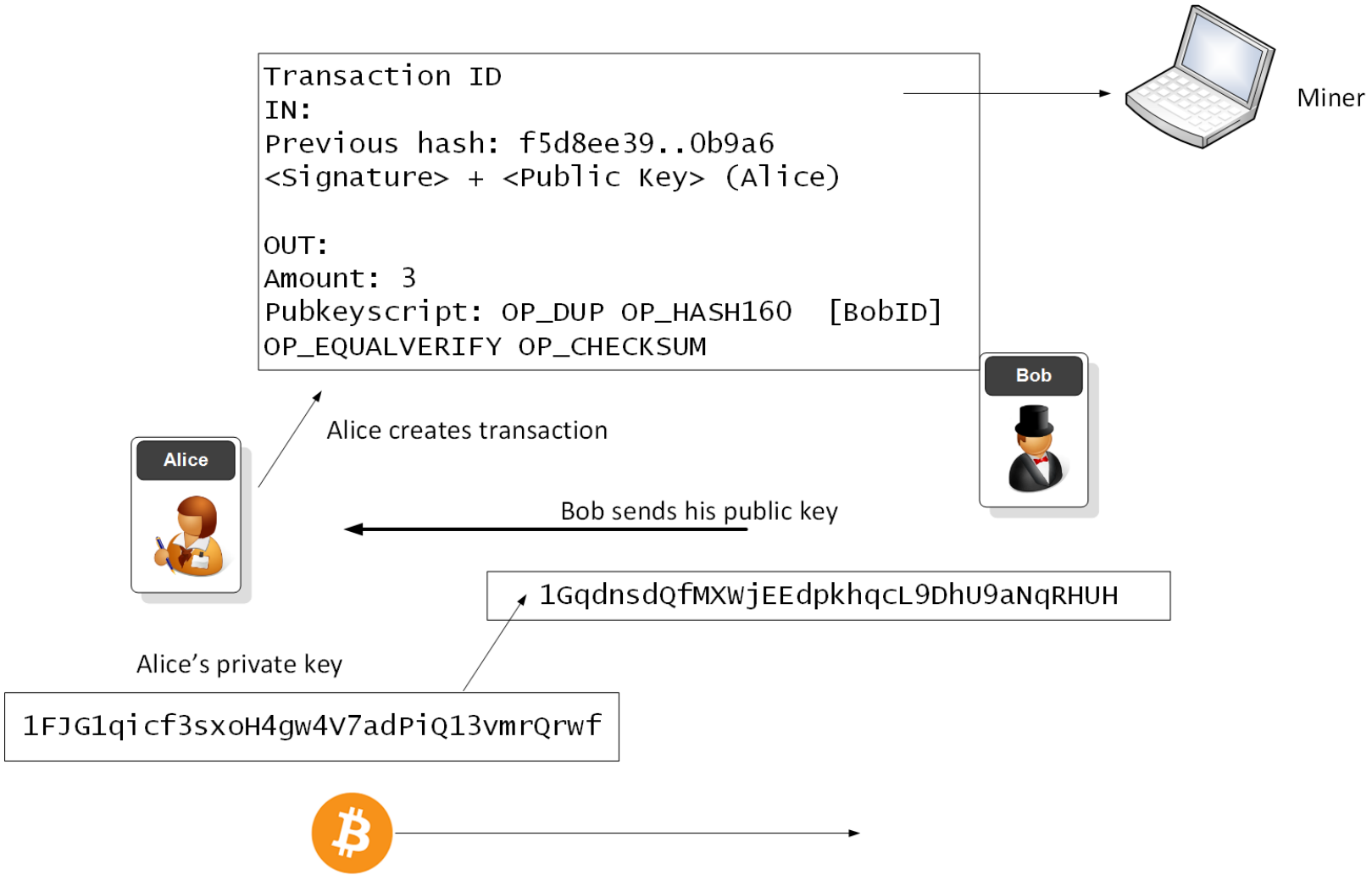
Public key:
0489fc7b8c3f655a10840d35c76ebb5596694045e49e940fb1e7a759da4edf0fafc45b
bbea6f5a56abf14c145c529c8eda9d3ad606f3a0bf4ca01ce991d4987b97

Wif: 5JPmDetQXXvc5aT5efyrg7BxHbH4135owRzq9DD7n2eWQCta5MN

Address: 16RAf9CjnstWCfBJGfrzSSMfTeHJVt8QWw

Signed:
4830450220264c4dce5f1cf0dff8d32d21c5d5cf6baed428b12ae6f8594924246a611e
9ee602210096ef8e7054ec7a39f0a35d8de3fd50090b1d125c0e795af8cf3d577b676
407ca01410489fc7b8c3f655a10840d35c76ebb5596694045e49e940fb1e7a759da4e
df0fafc45bbbea6f5a56abf14c145c529c8eda9d3ad606f3a0bf4ca01ce991d4987b97

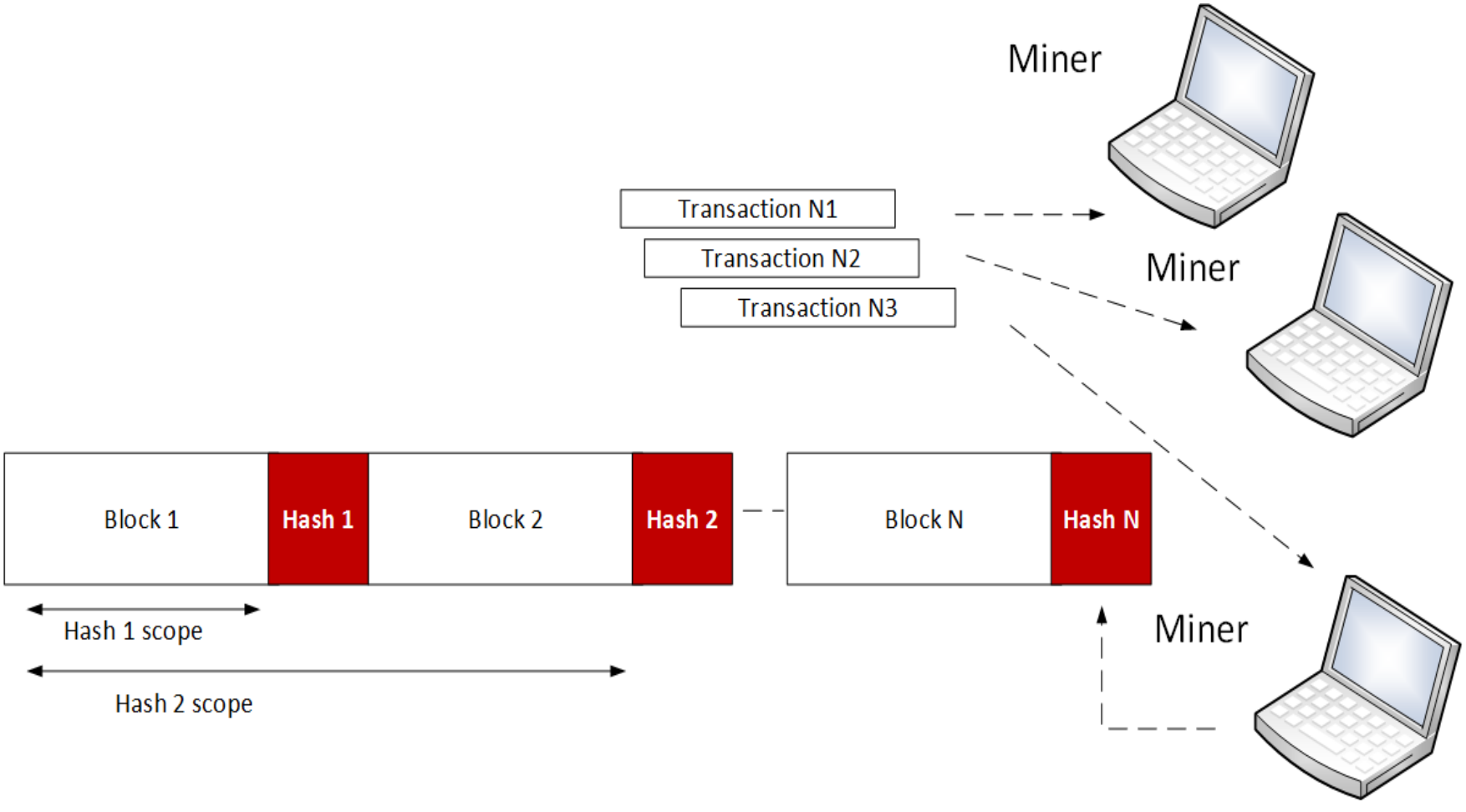
Bitcoin transaction



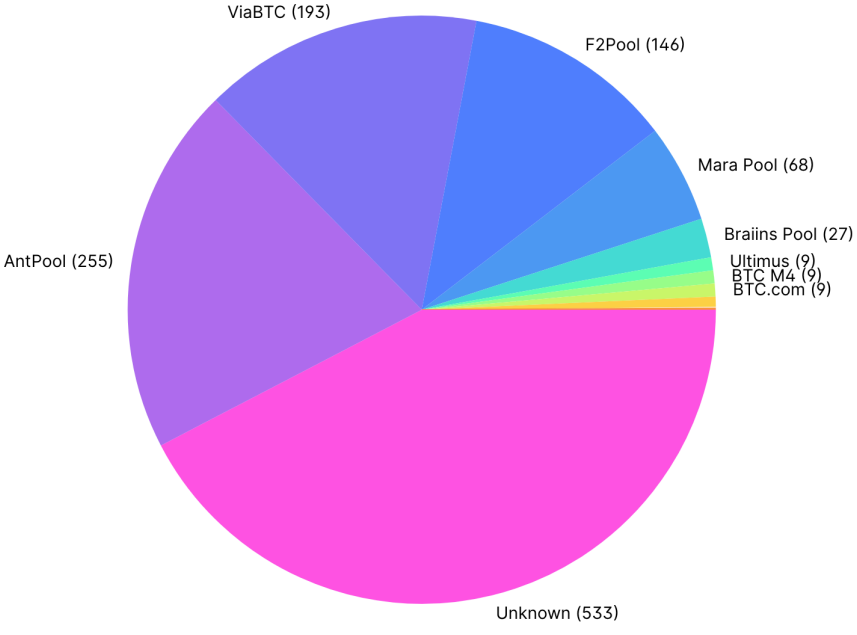
Blockchain and Cryptocurrencies

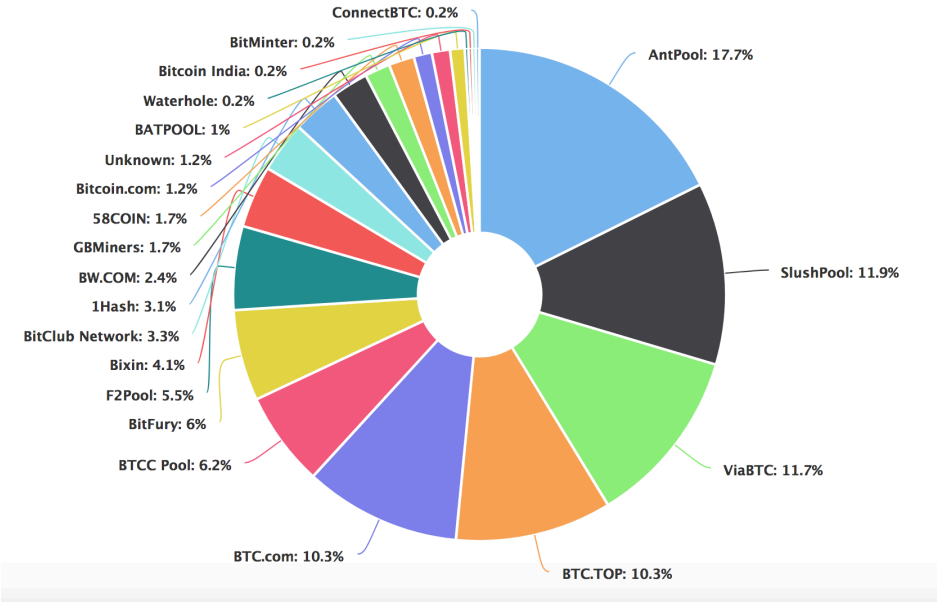
Cryptocurrencies
Bitcoin addresses
Blockchain
Mining

Mining process

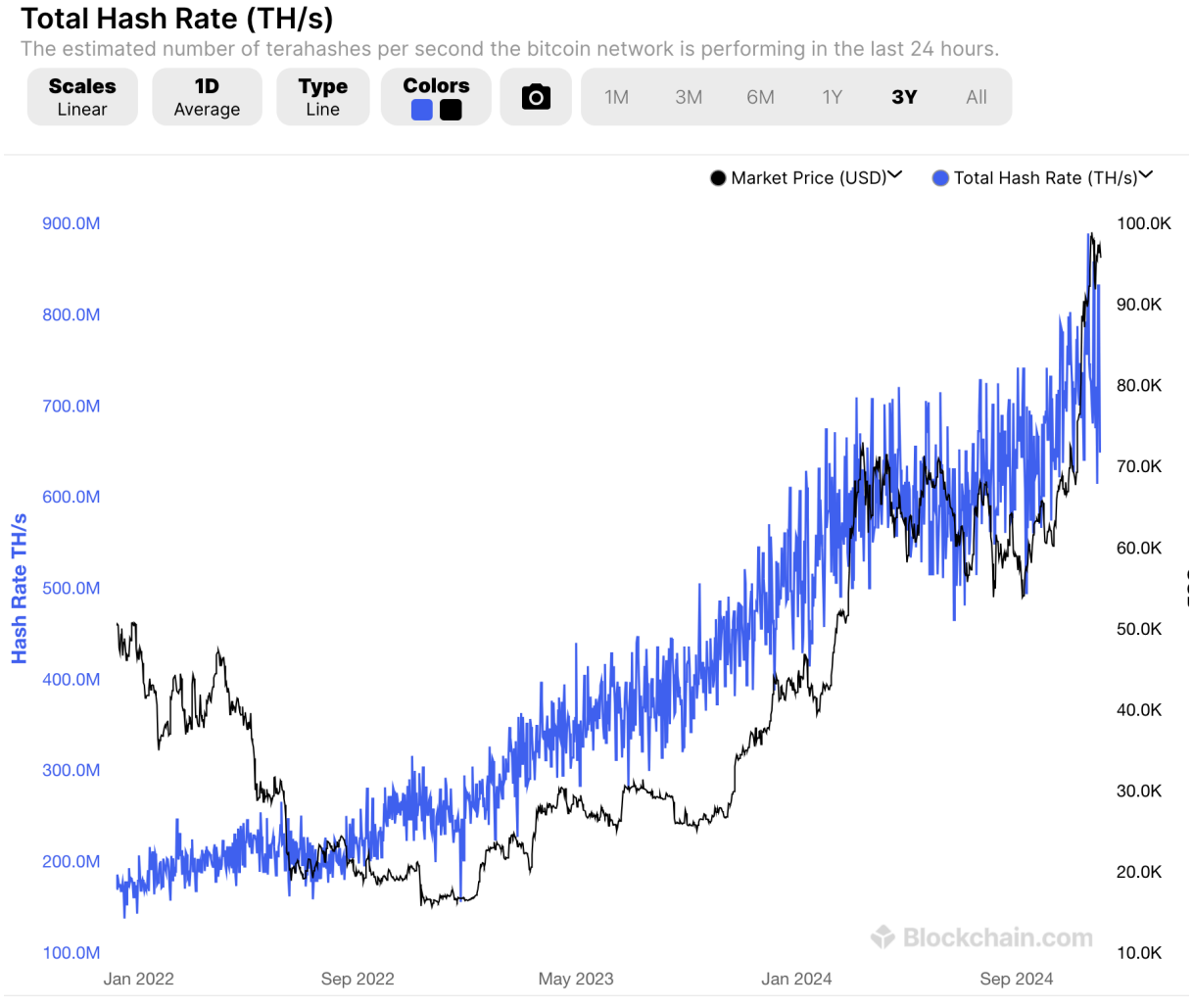


Successful miners (2024 and 2018)





Hash Rate TH/s



Mining Processes

- Hash
- 00000000000000000d98e57b83834a2d1f4387a93d06861bcf3ea5fc498bd55
- Previous Block
- 00000000000000000012138e05f0779765277a9d2ab7e4a2a70882790abf98a0c

Blocks

Bitcoin Block 873,315

Mined on December 05, 2024 04:35:01 • All Blocks

Unknown

Coinbase Message • -QgSpiderPool/78/cK"qN

A total of 9,202.42 BTC ($945,821,846) were sent in the block with the average transaction being 3.1429 BTC ($323,026). Unknown earned a total reward of 3.13 BTC $321,700. The reward consisted of a base reward of 3.13 BTC $321,700 with an additional 0.0954 BTC ($9,805.18) reward paid as fees of the 2,928 transactions which were included in the block.

Details

Hash	00000-804b5	Depth	12
Capacity	154.19%	Size	1,616,840
Distance	1h 29m 1s	Version	0×29eda000
BTC	9,202.4233	Merkle Root	04-10
Value	$945,821,846	Difficulty	103,919,634,711,492.17
Value Today	$944,934,917	Nonce	3,974,483,494
Average Value	3.1429041349 BTC	Bits	386,053,475
Median Value	0.01087175 BTC	Weight	3,993,224 WU
Input Value	9,202.52 BTC	Minted	3.13 BTC
Output Value	9,205.64 BTC	Reward	3.22039370 BTC
Transactions	2,928	Mined on	05 Dec 2024, 04:35:01
Witness Tx's	2,721	Height	873,315
Inputs	8,182	Confirmations	12
Outputs	8,051	Fee Range	1-275 sat/vByte
Fees	0.09539370 BTC	Average Fee	0.00003258
Fees Kb	0.0000590 BTC	Median Fee	0.00001272
Fees kWU	0.0000239 BTC	Miner	Unknown

Blockchain and Cryptocurrencies

Cryptocurrencies
Bitcoin addresses
Blockchain
Mining
Ethereum
Smart Contracts

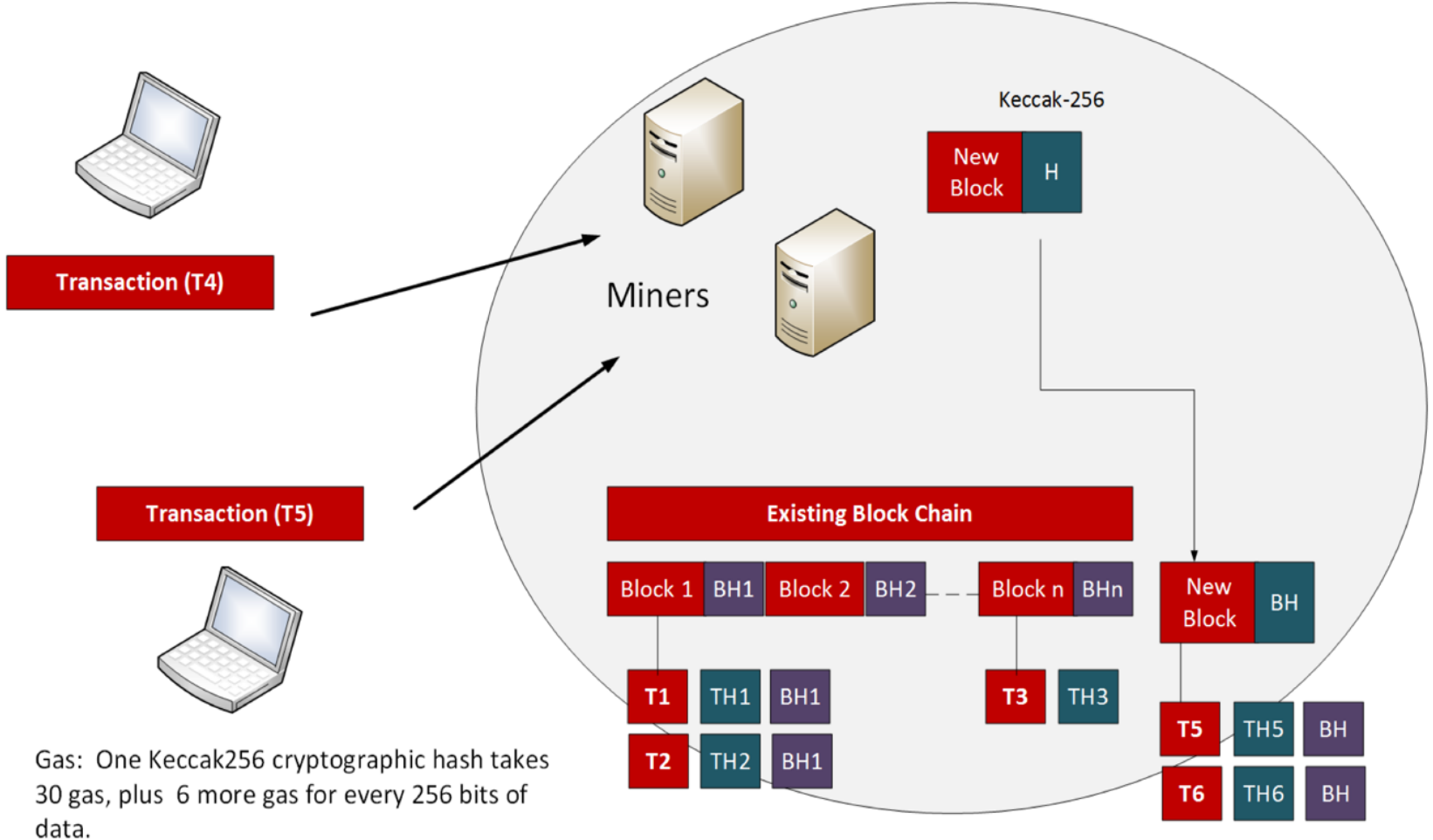
Prof Bill Buchanan OBE

http://asecuritysite.com/ethereum
https://asecuritysite.com/blockchain/

History

- Ethereum was created by Vitalik Buterinin in 2015 and which built on the Bitcoin/ Blockchain concept by included the concept of smart contracts.
- After a hack, in 2016, the Ethereum currency split into two: Ethereum (ETH) and Ethereum Classic (ETC).

Ethereum setup



Gas: One Keccak256 cryptographic hash takes 30 gas, plus 6 more gas for every 256 bits of data.

Gas

- Within Ethereum applications we define the concept of *gas*. This is basically the unit that is used to measure the amount of work that is required to perform a single Keccak-256 hash, and where 30 gas are consumed for a single hash and 6 more gas for each 256 bits of data hashed. In this way there is a motivation to keep contracts small, as they will be less costly.

Gas

- Gas thus provides a way to define the fee that miners receive in performing operations on the blockchain.
- This differs from Bitcoin which only charges for the number of kiloBytes in a transaction. When it comes to the actual payment of the transaction fees, there is a payment of ether to the miners who create the blocks.

Gas

- Ethereum transactions thus have a fee associated with them. If the fee is too low, then the miners will not process the transaction.
- When gas is consumed it is paid to the miner, and cannot be recovered back.
- If the transaction fee is set too high, there are likely to be many eager miners who are keen to profit from the high fee, and your transaction is likely to be prioritized.

Gas

- Overall, though, miners only charge for the work they have done, and they will return back any excess gas which they have not used. A miner can decide whether it needs to change the use of gas according to the price of gas varying. This overcomes the changes in transaction fees that happen in Bitcoin.

Gas

In Ethereum, just like Bitcoin, there is a block limit, so you'll end up paying more if you overspill into another block (which means you should be efficient with your code and data).

The gas price per transaction aims to overcome denial of service and infinite loops, and where 0.00001 Ether or 1 Gas is used to execute a line of code. If there is not enough Ether, no transaction will be performed. It also aims to make code designers efficient and not use waste bandwidth and CPU utilization.

Blockchain and Cryptocurrencies

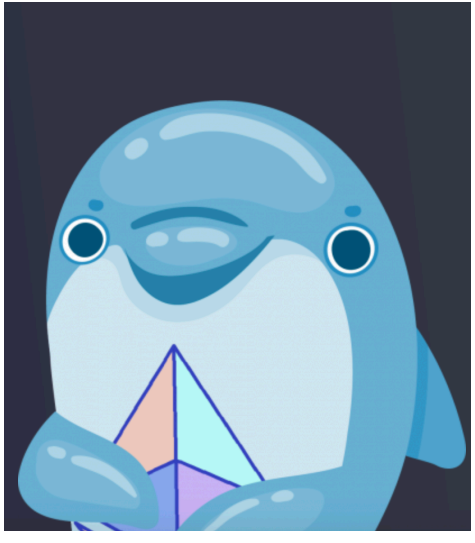
Cryptocurrencies
Bitcoin addresses
Blockchain
Mining
Ethereum
Smart Contracts

Prof Bill Buchanan OBE

http://asecuritysite.com/ethereum
https://asecuritysite.com/blockchain/

Digital Wallet

METAMASK



20:59

Networks

POPULAR | CUSTOM NETWORKS

A malicious network provider can lie about the state of the blockchain and record your network activity. Only add custom networks you trust.

Network Name

sepolia

RPC Url

https://rpc.sepolia.org/

Chain ID

11155111

Symbol

SepoliaEth

Block Explorer URL

https://sepolia.etherscan.io

Add

21:06

sepolia

Account 2

$0

0xbB15...2233

Receive | Send | Swap

Tokens | NFTs

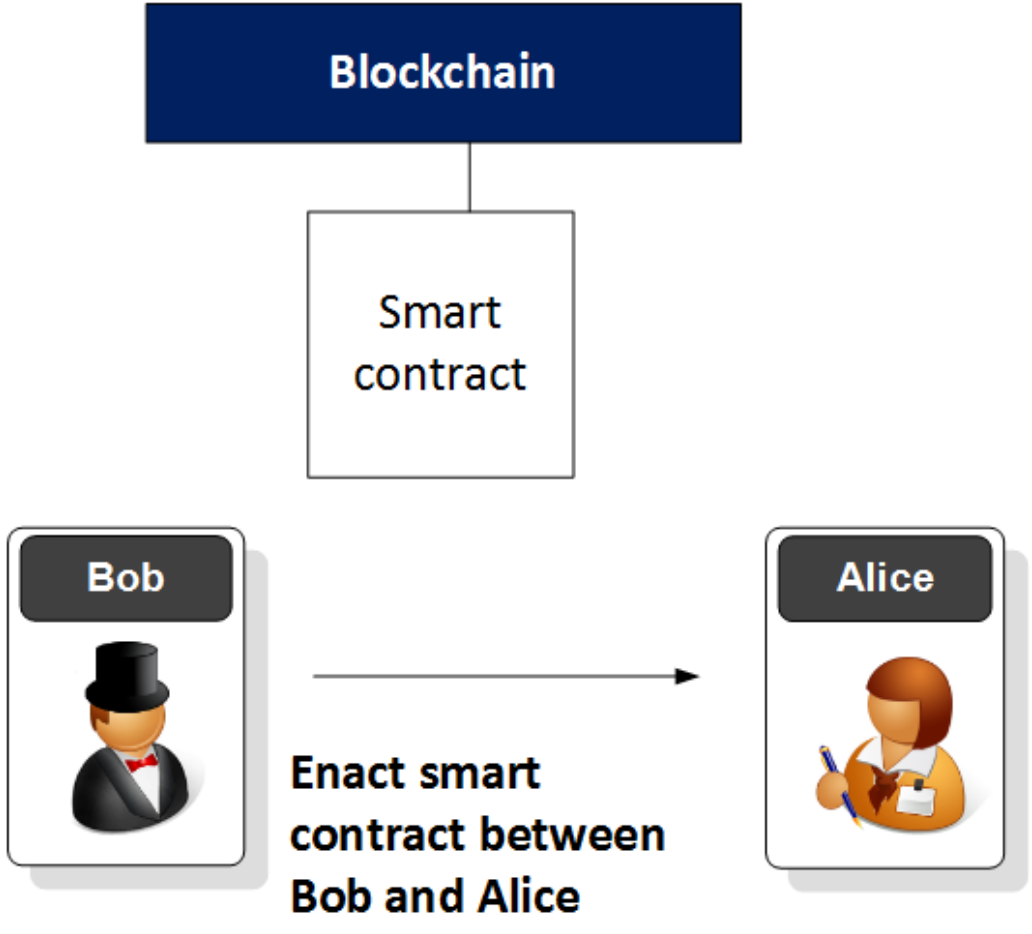
S 8.94274 SEPOLIAETH

Don't see your token?

Import tokens

Wallet | Browser

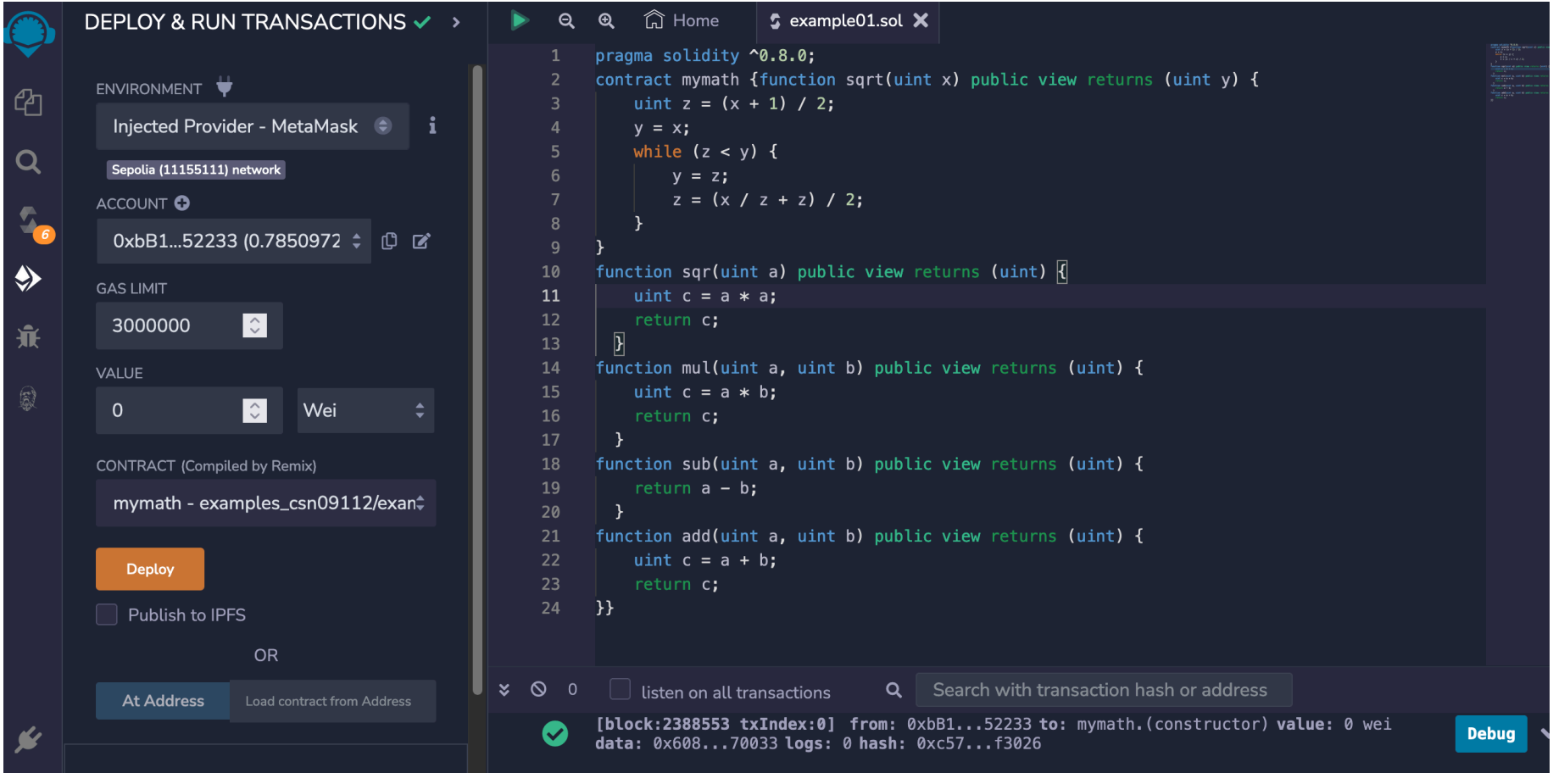
Smart Contract



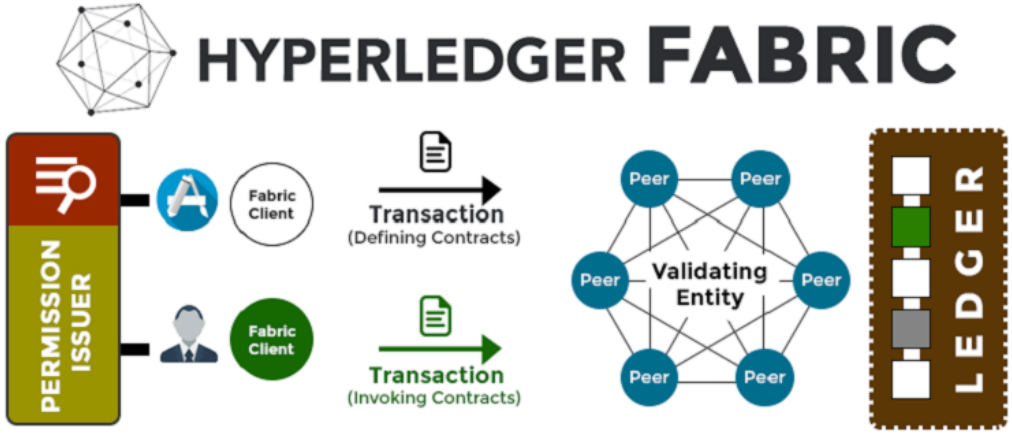
```
pragma solidity ^0.4.0;
contract test2{
   uint a ;
   function test2() {
      a = 1;
   }
   function val() returns(uint){
      return a;
   }
}

contract test3 is test2{
    uint b = a++;
    function show() returns(uint){
       return b;
    }
}
```

Compile with Solidity



Hyperledger Fabric



Key features:

•Private and permissioned.
•Peers: Docker components, and provide multiagency approach for consensus.
•All users log on through valid membership service provider.
•Assets have key-pairs (binary or JSON).
•Chaincode: Smart contracts to handle transactions.
•Privacy: Channels and private data.

101 Blockchains | HYPERLEDGER VS ETHEREUM

Enterprise blockchain is getting traction across major industries. The momentum is underscored by the potential of the technology to revolutionize operations as well as making them affordable, fast, trusted and transparent. To this end, Hyperledger and Ethereum are blazing the trail by establishing frameworks where developers can customize blockchain technology for various use cases.

HYPERLEDGER

Apparently, Hyperledger is quite popular within the enterprise blockchain ecosystem. The community boasts over 260 high-profile partners that include IBM, SAP and many more. Hyperledger is managed by the Linux Foundation which created the ecosystem in December 2015. The platform is open source and supports a modular architecture. On Hyperledger, there are two types of nodes; the validating nodes and the non-validating nodes. The validating nodes validate transactions, maintain the ledger and run the consensus which is BFT consensus protocol.

VS

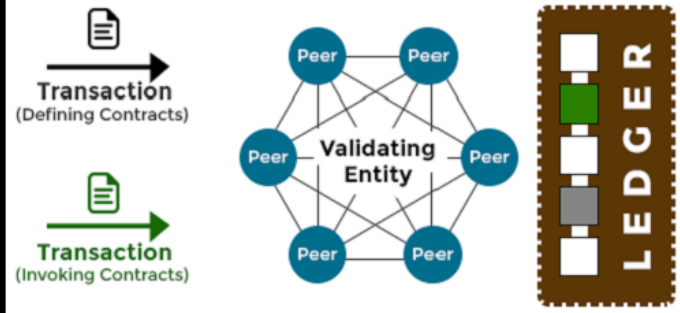
ETHEREUM

This ecosystem is quite generic and serves a wide range of purposes. It relies on the PoW consensus to validate transactions. Further, it is clear that Ethereum is ideal for B2C applications since users do not require permission to participate in transactions. Also, the platform has a native cryptocurrency to facilitate transactions alongside smart contracts.

Is ideal for B2B transactions since participation is permissioned	USABILITY	Is generic in purpose and supports both public and private platforms hence ideal for B2C transactions
Does not have a consensus mechanism Users create their own consensus algorithms due to the pluggable nature of the architecture	CONSENSUS	Uses Proof Of Work consensus mechanism
Does not have any in-built cryptocurrency/token	TOKENS	Comes with Ether (ETH)
Ledger is not public	NATURE OF TRANSACTIONS	All participants can access the ledger of transactions
Written in Go, Java, Node.js	SMART CONTRACT LANGUAGE	Written in Solidity
Accenture, AirBus, American Express, Cisco, Daimler, J.P. Morgan, Intel, IBM, SAP etc.	PARTNERS	IC3, Microsoft, Accenture, J.P. Morgan, Consensys, Intel, Santander, CME Group etc.

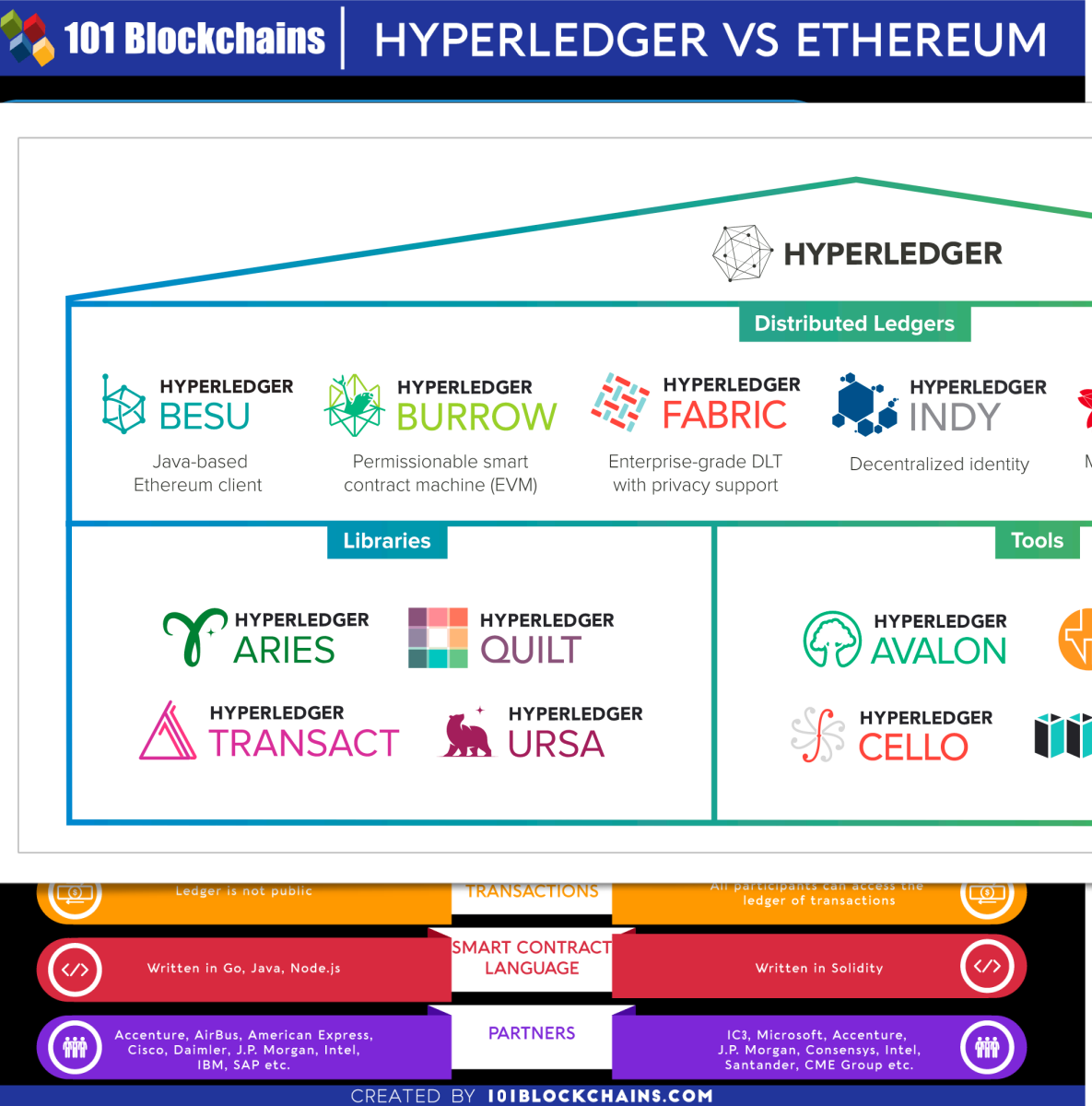
CREATED BY 101BLOCKCHAINS.COM

ERLEDGER FABRIC



Key features:

- Private and permissioned.
- Peers: Docker components, and provide multiagency approach for consensus.
- All users log on through valid membership service provider.
- Assets have key-pairs (binary or JSON).
- Chaincode: Smart contracts to handle transactions.
- Privacy: Channels and private data.



•Chaincode: Smart contracts to handle transactions.
•Privacy: Channels and private data.

Blockchain and Cryptocurrencies

Cryptocurrencies
Bitcoin addresses
Blockchain
Mining
Ethereum
Smart Contracts

Prof Bill Buchanan OBE

http://asecuritysite.com/ethereum
https://asecuritysite.com/blockchain/