

Blockchain and Cryptocurrencies

> Cryptocurrencies
Bitcoin addresses
Blockchain
Mining
Ethereum
Smart Contracts
Blockchain Crypto
Hyperledger

Prof Bill Buchanan OBE
<https://asecuritysite.com/blockchain/>



Block

> Crypt
Bitcoin
Blockchain
Mining
Ethereum
Smart Contracts
Hyperledger

Prof |
<https://>

No	Date	Subject	Lab
2	28 Jan 2022	Ciphers and Fundamentals Unit	Lab Demo
3	4 Feb 2022	Symmetric Key	Lab
4	11 Feb 2022	Hashing and MAC	Lab
5	18 Feb 2022	Asymmetric (Public) Key	Lab
6	25 Feb 2022	Key Exchange	Lab
7	4 Mar 2022	Digital Signatures and Certificates	Lab
8	11 Mar 2022	Revision lecture and Test 1/Coursework	Mini-project/Coursework
9	18 Mar 2022	Test (Units 1-5) 40% of overall mark here	
10	25 Mar 2022	Tunnelling	Lab
11	1 Apr 2022	Blockchain	Lab
12	8 Apr 2022	Future Cryptography	Lab
13	29 Apr 2022		Lab
14	6 May 2022		Lab
15	13 May 2022	Coursework Hand-in - 60% of overall mark	



Blockchain and Cryptocurrencies

> Cryptocurrencies

Bitcoin addresses

Blockchain

Mining

Ethereum

Smart Contracts

Blockchain Crypto

Prof Bill Buchanan OBE

<http://asecuritysite.com/crypto10>

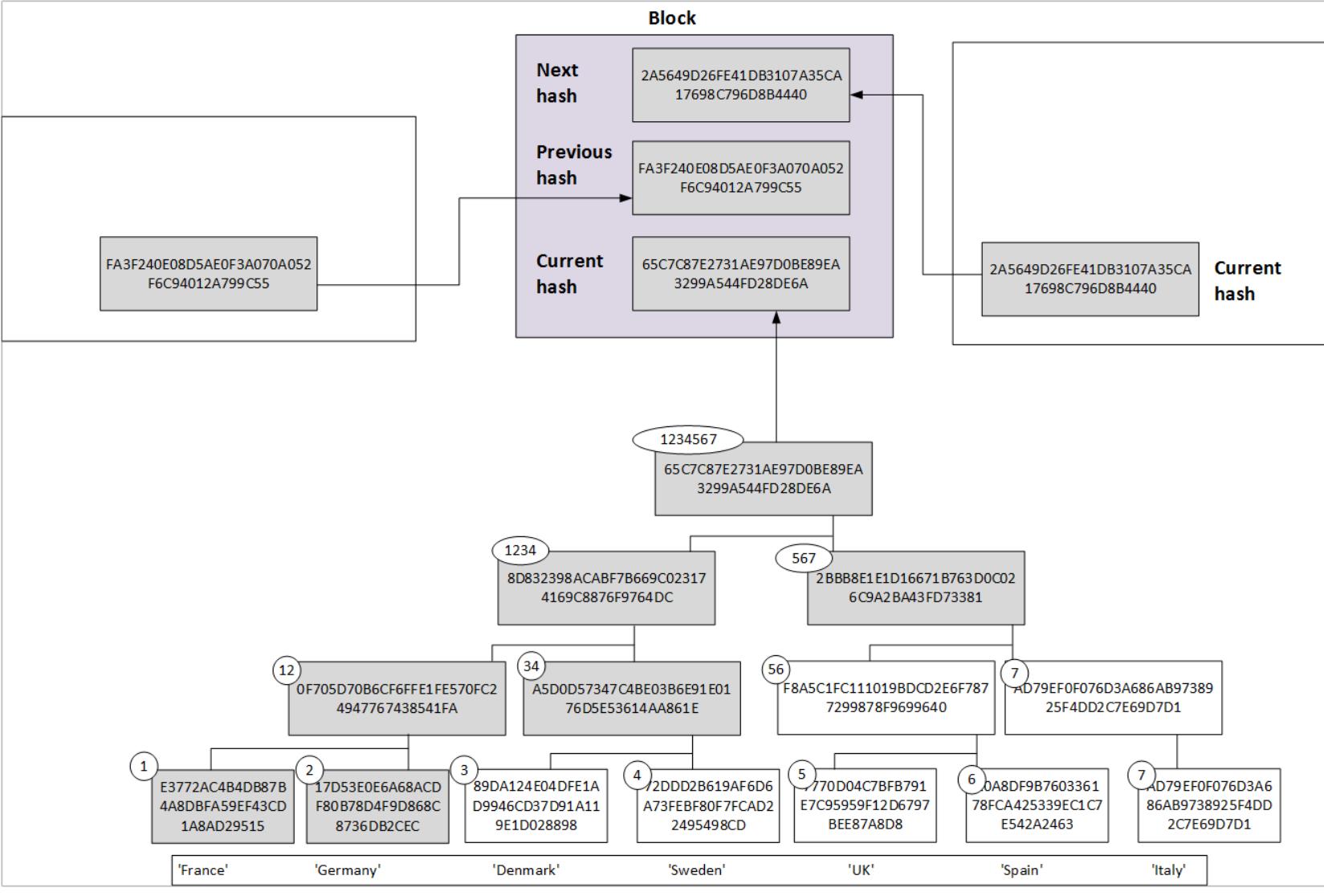
<http://asecuritysite.com/encryption>





ncies





Who is 13 years old?



Who is 13 years old?



Who is 13 years old?



Who is 13 years old?



Who is 13 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



Be Your Own Bank.

Use your Blockchain wallet
to buy bitcoin now.

GET STARTED →



Who is 13 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	0000
Previous Block	0000
Next Block(s)	0000
Merkle Root	4a5e

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 13 years old?

Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshi@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 13 years old?

Rebels with a Cause (Your Privacy)

May/June 1991

Electronic Cash System

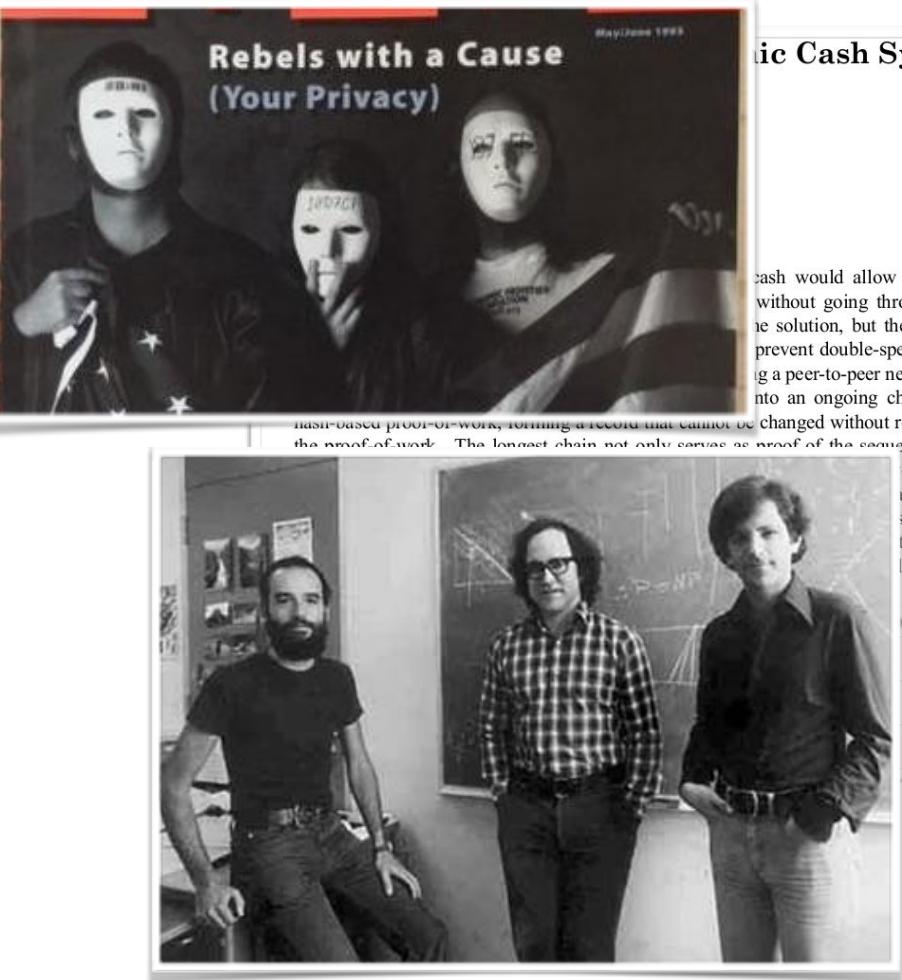
cash would allow online without going through a central authority, but the main problem is how to prevent double-spending. By putting each transaction onto an ongoing chain of transactions based on proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain 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 KWL
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 13 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 13 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 13 years old?



His work was a hotch-potch of
tography methods
sourced in the 1970s
lic key - and also of
ik movement which
the 1990s, and was
ric Hughes, Tim May
nore.

of 5 January 2018,

the blockchain size is
around [385GB](#), and there are 19
million coins in circulation [[here](#)].

Who is 13 years old?



His work was a hotch-potch of
tography methods
sourced in the 1970s
lic key - and also of
ik movement which
the 1990s, and was
ric Hughes, Tim May
nore.

of 5 January 2018,

the blockchain size is
around [385GB](#), and there are 19
million coins in circulation [[here](#)].

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 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 caught?

Published on December 21, 2017

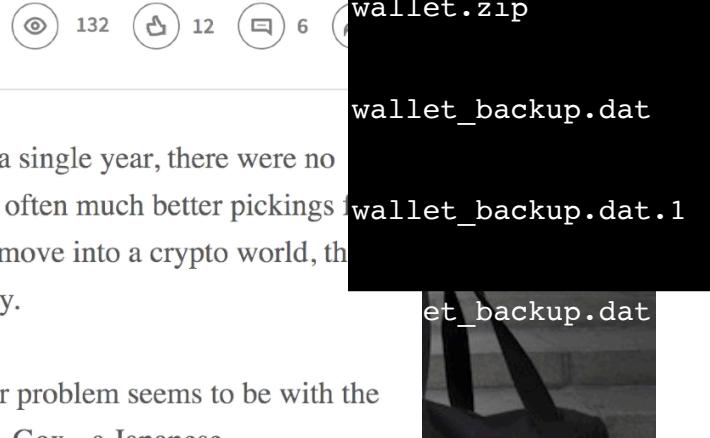
[Edit article](#) | [View stats](#)



Prof Bill Buchanan OBE, PhD, FBCS

Professor at Napier University

[1,194 articles](#)



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.

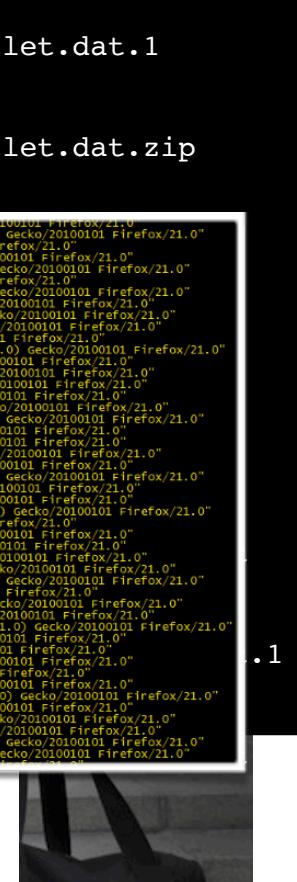
While cryptocurrencies are safe in themselves, the major problem seems to be with the places which hold the wallets. In 2014, for example, Mt. Gox - a Japanese cryptocurrency exchange - filed for bankruptcy after a hacker drained the exchange of 100s of thousands of Bitcoins.

The Most Profitable Crime?

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

		wallet.dat.1	wallet.dat.zip
112. 92.122.186 -	17/oct/2017:07:49:00 -0400	"GET /\$20copy.wallet.dat HTTP/1.1" 404 283 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10.8; rv:21.0) Gecko/201001 Firefox/21.0"	
112. 92.122.186 -	17/oct/2017:07:57:07 -0400	"GET /didierstevens_walleter.dat.zip HTTP/1.1" 404 283 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10.8; rv:21.0) Gecko/201001 Firefox/21.0"	
112. 92.122.186 -	17/oct/2017:07:57:09 -0400	"GET /wallet.dat HTTP/1.1" 404 275 "Mozilla/5.0 (Macintosh; Intel Mac OS X 10.8; rv:21.0) Gecko/201001 Firefox/21.0"	
112. 92.122.186 -	17/oct/2017:07:57:10 -0400	"GET /bitcoin_wallet.zip HTTP/1.1" 404 283 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10.8; rv:21.0) Gecko/201001 Firefox/21.0"	
112. 92.122.186 -	17/oct/2017:07:57:20 -0400	"GET /backups/bitcoin_wallet.dat HTTP/1.1" 404 291 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10.8; rv:21.0) Gecko/201001 Firefox/21.0"	
112. 92.122.186 -	17/oct/2017:07:57:20 -0400	"GET /wallet.dat HTTP/1.1" 404 275 "Mozilla/5.0 (Macintosh; Intel Mac OS X 10.8; rv:21.0) Gecko/201001 Firefox/21.0"	
112. 92.122.186 -	17/oct/2017:07:57:40 -0400	"GET /didierstevens_walleter.dat.zip HTTP/1.1" 404 291 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10.8; rv:21.0) Gecko/201001 Firefox/21.0"	
112. 92.122.186 -	17/oct/2017:07:57:41 -0400	"GET /wallet.dat HTTP/1.1" 404 286 "Mozilla/5.0 (Macintosh; Intel Mac OS X 10.8; rv:21.0) Gecko/201001 Firefox/21.0"	
112. 92.122.186 -	17/oct/2017:07:57:45 -0400	"GET /bitcoin_wallet.dat.zip HTTP/1.1" 404 287 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10.8; rv:21.0) Gecko/201001 Firefox/21.0"	
112. 92.122.186 -	17/oct/2017:07:58:04 -0400	"GET /home_bitcoin/wallet.dat HTTP/1.1" 404 290 "Mozilla/5.0 (Macintosh; Intel Mac OS X 10.8; rv:21.0) Gecko/201001 Firefox/21.0"	
112. 92.122.186 -	17/oct/2017:07:58:05 -0400	"GET /home/ubuntu_bitcoin/wallet.dat HTTP/1.1" 404 290 "Mozilla/5.0 (Macintosh; Intel Mac OS X 10.8; rv:21.0) Gecko/201001 Firefox/21.0"	
112. 92.122.186 -	17/oct/2017:07:58:25 -0400	"GET /datadir/walleter.dat.zip HTTP/1.1" 404 283 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10.8; rv:21.0) Gecko/201001 Firefox/21.0"	
112. 92.122.186 -	17/oct/2017:07:58:35 -0400	"GET /\$20copyComdat.HTTP/1.1" 404 282 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10.8; rv:21.0) Gecko/201001 Firefox/21.0"	
112. 92.122.186 -	17/oct/2017:07:58:35 -0400	"GET /backup/wallet.tar.gz HTTP/1.1" 404 285 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10.8; rv:21.0) Gecko/201001 Firefox/21.0"	
112. 92.122.186 -	17/oct/2017:07:58:44 -0400	"GET /wallet_backup.dat HTTP/1.1" 404 282 "Mozilla/5.0 (Macintosh; Intel Mac OS X 10.8; rv:21.0) Gecko/201001 Firefox/21.0"	
112. 92.122.186 -	17/oct/2017:07:58:45 -0400	"GET /bitcoin_data/wallet.dat HTTP/1.1" 404 288 "Mozilla/5.0 (Macintosh; Intel Mac OS X 10.8; rv:21.0) Gecko/201001 Firefox/21.0"	
112. 92.122.186 -	17/oct/2017:07:59:16 -0400	"GET /didierstevens_walleter.dat.zip HTTP/1.1" 404 293 "Mozilla/5.0 (Macintosh; Intel Mac OS X 10.8; rv:21.0) Gecko/201001 Firefox/21.0"	
112. 92.122.186 -	17/oct/2017:07:59:20 -0400	"GET /backups/wallet.dat.zip HTTP/1.1" 404 282 "Mozilla/5.0 (Macintosh; Intel Mac OS X 10.8; rv:21.0) Gecko/201001 Firefox/21.0"	
112. 92.122.186 -	17/oct/2017:07:59:37 -0400	"GET /backup/wallet.dat HTTP/1.1" 404 292 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10.8; rv:21.0) Gecko/201001 Firefox/21.0"	
112. 92.122.186 -	17/oct/2017:07:59:37 -0400	"GET /bitcoindata/wallet.dat HTTP/1.1" 404 287 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10.8; rv:21.0) Gecko/201001 Firefox/21.0"	
112. 92.122.186 -	17/oct/2017:08:00:21 -0400	"GET /bitcoin_wallet.dat HTTP/1.1" 404 283 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10.8; rv:21.0) Gecko/201001 Firefox/21.0"	
112. 92.122.186 -	17/oct/2017:08:00:23 -0400	"GET /didierstevens_com_wallet.zip HTTP/1.1" 404 293 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10.8; rv:21.0) Gecko/201001 Firefox/21.0"	
112. 92.122.186 -	17/oct/2017:08:00:28 -0400	"GET /.bitcoin_wallet.dat HTTP/1.1" 404 284 "Mozilla/5.0 (Macintosh; Intel Mac OS X 10.8; rv:21.0) Gecko/201001 Firefox/21.0"	
112. 92.122.186 -	17/oct/2017:08:00:28 -0400	"GET /\$20copyComdat.HTTP/1.1" 404 284 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10.8; rv:21.0) Gecko/201001 Firefox/21.0"	
112. 92.122.186 -	17/oct/2017:08:00:46 -0400	"GET /home/root_bitcoin/wallet.dat HTTP/1.1" 404 294 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10.8; rv:21.0) Gecko/201001 Firefox/21.0"	
112. 92.122.186 -	17/oct/2017:08:00:50 -0400	"GET /wallet.zip HTTP/1.1" 404 275 "Mozilla/5.0 (Macintosh; Intel Mac OS X 10.8; rv:21.0) Gecko/201001 Firefox/21.0"	
112. 92.122.186 -	17/oct/2017:08:02:47 -0400	"GET /backups/wallet.zip HTTP/1.1" 404 283 "Mozilla/5.0 (Macintosh; Intel Mac OS X 10.8; rv:21.0) Gecko/201001 Firefox/21.0"	
112. 92.122.186 -	17/oct/2017:08:02:49 -0400	"GET /wallet_backup.zip HTTP/1.1" 404 282 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10.8; rv:21.0) Gecko/201001 Firefox/21.0"	
112. 92.122.186 -	17/oct/2017:08:02:50 -0400	"GET /bitcoin_wallet.dat.zip HTTP/1.1" 404 285 "Mozilla/5.0 (Macintosh; Intel Mac OS X 10.8; rv:21.0) Gecko/201001 Firefox/21.0"	
112. 92.122.186 -	17/oct/2017:08:03:55 -0400	"GET /\$20copyComdat.HTTP/1.1" 404 289 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10.8; rv:21.0) Gecko/201001 Firefox/21.0"	
112. 92.122.186 -	17/oct/2017:08:03:55 -0400	"GET /backup/wallet%20-%20copy.dat HTTP/1.1" 404 289 "Mozilla/5.0 (Macintosh; Intel Mac OS X 10.8; rv:21.0) Gecko/201001 Firefox/21.0"	
112. 92.122.186 -	17/oct/2017:08:04:30 -0400	"GET /wallet.tar.gz HTTP/1.1" 404 278 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10.8; rv:21.0) Gecko/201001 Firefox/21.0"	
112. 92.122.186 -	17/oct/2017:08:05:23 -0400	"GET /backup/bitcoin_wallet.dat HTTP/1.1" 404 290 "Mozilla/5.0 (Macintosh; Intel Mac OS X 10.8; rv:21.0) Gecko/201001 Firefox/21.0"	
112. 92.122.186 -	17/oct/2017:08:05:39 -0400	"GET /\$20copyComdat.HTTP/1.1" 404 286 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10.8; rv:21.0) Gecko/201001 Firefox/21.0"	
112. 92.122.186 -	17/oct/2017:08:05:44 -0400	"GET /didierstevens_com_walleter.dat.zip HTTP/1.1" 404 291 "Mozilla/5.0 (Macintosh; Intel Mac OS X 10.8; rv:21.0) Gecko/201001 Firefox/21.0"	
112. 92.122.186 -	17/oct/2017:08:05:45 -0400	"GET /\$20copyComdat.HTTP/1.1" 404 291 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10.8; rv:21.0) Gecko/201001 Firefox/21.0"	
112. 92.122.186 -	17/oct/2017:08:06:23 -0400	"GET /data_wallet.dat HTTP/1.1" 404 280 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10.8; rv:21.0) Gecko/201001 Firefox/21.0"	
112. 92.122.186 -	17/oct/2017:08:06:43 -0400	"GET /Bitcoin/wallet.dat HTTP/1.1" 404 283 "Mozilla/5.0 (Macintosh; Intel Mac OS X 10.8; rv:21.0) Gecko/201001 Firefox/21.0"	
112. 92.122.186 -	17/oct/2017:08:07:13 -0400	"GET /wallet.dat_1 HTTP/1.1" 404 277 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10.8; rv:21.0) Gecko/201001 Firefox/21.0"	
112. 92.122.186 -	17/oct/2017:08:07:28 -0400	"GET /bitcoin_wallet.dat HTTP/1.1" 404 283 "Mozilla/5.0 (Macintosh; Intel Mac OS X 10.8; rv:21.0) Gecko/201001 Firefox/21.0"	
112. 92.122.186 -	17/oct/2017:08:09:16 -0400	"GET /\$20copyComdat.HTTP/1.1" 404 293 "Mozilla/5.0 (Macintosh; Intel Mac OS X 10.8; rv:21.0) Gecko/201001 Firefox/21.0"	
112. 92.122.186 -	17/oct/2017:08:10:38 -0400	"GET /BitcoinData/wallet.dat HTTP/1.1" 404 287 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10.8; rv:21.0) Gecko/201001 Firefox/21.0"	
112. 92.122.186 -	17/oct/2017:08:11:06 -0400	"GET /\$20copyComdatadir/wallet.dat HTTP/1.1" 404 291 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10.8; rv:21.0) Gecko/201001 Firefox/21.0"	
112. 92.122.186 -	17/oct/2017:08:11:20 -0400	"GET /bitcoin_datadir/wallet.dat HTTP/1.1" 404 291 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10.8; rv:21.0) Gecko/201001 Firefox/21.0"	

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.



.1

The Most Profitable Crime?

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

```
112.92.122.186 - - [17/oct/2017:07:57:00 +0000] "GET /backups/coin_wallet.dat HTTP/1.1" 404 283 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10.8; rv:21.0) Gecko/201001 Firefox/21.0"
112.92.122.186 - - [17/oct/2017:07:57:07 -0000] "GET /oldiesetc/coin_wallet.dat HTTP/1.1" 404 283 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10.8; rv:21.0) Gecko/201001 Firefox/21.0"
112.92.122.186 - - [17/oct/2017:07:57:09 +0000] "GET /wallet.dat HTTP/1.1" 404 275 "Mozilla/5.0 (Macintosh; Intel Mac OS X 10.8; rv:21.0) Gecko/201001 Firefox/21.0"
112.92.122.186 - - [17/oct/2017:07:57:10 +0000] "GET /bitcoin_wallet.zip HTTP/1.1" 404 283 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10.8; rv:21.0) Gecko/201001 Firefox/21.0"
112.92.122.186 - - [17/oct/2017:07:57:20 +0000] "GET /backups/bitcoin_wallet.dat HTTP/1.1" 404 291 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10.8; rv:21.0) Gecko/201001 Firefox/21.0"
112.92.122.186 - - [17/oct/2017:07:57:20 +0000] "GET /wallet.tar HTTP/1.1" 404 275 "Mozilla/5.0 (Macintosh; Intel Mac OS X 10.8; rv:21.0) Gecko/201001 Firefox/21.0"
112.92.122.186 - - [17/oct/2017:07:57:21 +0000] "GET /didiesterse_wallet.dat HTTP/1.1" 404 291 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10.8; rv:21.0) Gecko/201001 Firefox/21.0"
112.92.122.186 - - [17/oct/2017:07:57:21 +0000] "GET /didiesterse_wallet.dat HTTP/1.1" 404 286 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10.8; rv:21.0) Gecko/201001 Firefox/21.0"
112.92.122.186 - - [17/oct/2017:07:57:41 -0000] "GET /home/.bitcoin/wallet.dat.zip HTTP/1.1" 404 287 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10.8; rv:21.0) Gecko/201001 Firefox/21.0"
112.92.122.186 - - [17/oct/2017:07:57:45 +0000] "GET /bitcoin_wallet.dat.zip HTTP/1.1" 404 287 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10.8; rv:21.0) Gecko/201001 Firefox/21.0"
112.92.122.186 - - [17/oct/2017:07:58:04 -0000] "GET /wallet.dat.zip HTTP/1.1" 404 279 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10.8; rv:21.0) Gecko/201001 Firefox/21.0"
112.92.122.186 - - [17/oct/2017:07:58:05 +0000] "GET /home/ubuntu/.bitcoin/wallet.dat HTTP/1.1" 404 296 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10.8; rv:21.0) Gecko/201001 Firefox/21.0"
112.92.122.186 - - [17/oct/2017:07:58:29 -0000] "GET /dataadir/wallet.dat HTTP/1.1" 404 283 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10.8; rv:21.0) Gecko/201001 Firefox/21.0"
112.92.122.186 - - [17/oct/2017:07:58:31 -0000] "GET /wallet-20-320conv.dat HTTP/1.1" 404 282 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10.8; rv:21.0) Gecko/201001 Firefox/21.0"
112.92.122.186 - - [17/oct/2017:07:58:31 -0000] "GET /wallet.dat.1 HTTP/1.1" 404 283 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10.8; rv:21.0) Gecko/201001 Firefox/21.0"
112.92.122.186 - - [17/oct/2017:07:58:31 -0000] "GET /wallet.dat.zip HTTP/1.1" 404 283 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10.8; rv:21.0) Gecko/201001 Firefox/21.0"
```



Dimitrios Slamaris

@dim0x69

Follow



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

```
{16e2115b1e00"}], "id":168440}
5 / body: {"jsonrpc":"2.0","method":"eth_sendTransaction","params": [{"from":"0
16e2115b1e00"}], "id":943614}
5 / body: {"jsonrpc":"2.0","method":"eth_sendTransaction","params": [{"from":"0
16e2115b1e00"}], "id":263038}
5 / body: {"jsonrpc":"2.0","method":"eth_sendTransaction","params": [{"from":"0
16e2115b1e00"}], "id":472772}
5 / body: {"jsonrpc":"2.0","method":"eth_sendTransaction","params": [{"from":"0
16e2115b1e00"}], "id":771759}
5 / body: {"jsonrpc":"2.0","method":"eth_sendTransaction","params": [{"from":"0
16e2115b1e00"}], "id":817614}
5 / body: {"jsonrpc":"2.0","method":"eth_sendTransaction","params": [{"from":"0
16e2115b1e00"}], "id":537357}
```



is to be with the
ese

he exchange of

The Most Profitable Crime?

wallet.dat.1

Which is the easiest crime to implement with the largest payoff?

```
112.92.122.186 - - [17/OCT/2017:07:57:00 +0000] "GET /didierstevens_bitcoin_walle...  
112.92.122.186 - - [17/OCT/2017:07:57:07 -0400] "GET /didierstevens_bitcoin_walle...  
112.92.122.186 - - [17/OCT/2017:07:57:09 +0000] "GET /wallet.dat HTTP/1.1"  
112.92.122.186 - - [17/OCT/2017:07:57:10 +0000] "GET /bitcoin_wallet.zip H...  
112.92.122.186 - - [17/OCT/2017:07:57:20 +0000] "GET /backups/bitcoin_walle...  
112.92.122.186 - - [17/OCT/2017:07:57:20 +0000] "GET /wallet.tar.gz H...  
112.92.122.186 - - [17/OCT/2017:07:57:31 +0000] "GET /didierstevens_bitco...  
112.92.122.186 - - [17/OCT/2017:07:57:40 +0000] "GET /didierstevens_bitco...  
112.92.122.186 - - [17/OCT/2017:07:57:41 +0000] "GET /didierstevens_bitco...  
112.92.122.186 - - [17/OCT/2017:07:57:45 +0000] "GET /home/.bitcoin/walle...  
112.92.122.186 - - [17/OCT/2017:07:57:45 +0000] "GET /bitcoin_wallet.dat.z...  
112.92.122.186 - - [17/OCT/2017:07:58:04 +0000] "GET /wallet.dat.zip HTTP/1.1  
112.92.122.186 - - [17/OCT/2017:07:58:05 +0000] "GET /home/ubuntu/.bitcoin...  
112.92.122.186 - - [17/OCT/2017:07:58:29 +0000] "GET /datadir/wallet.dat.H...  
112.92.122.186 - - [17/OCT/2017:07:58:31 +0000] "GET /wallet20-320conv.d...
```



Dimitrios Slamaris

@dim0x69

Bot trying to steal Ethers from
after enumerating "my" account
balance and my client version!

```
{ "id": 168440 },  
 5 / body: {"jsonrpc": "2.0", "method": "eth_sendTransaction"},  
{ "id": 943614 },  
 5 / body: {"jsonrpc": "2.0", "method": "eth_sendTransaction"},  
{ "id": 263038 },  
 5 / body: {"jsonrpc": "2.0", "method": "eth_sendTransaction"},  
{ "id": 472772 },  
 5 / body: {"jsonrpc": "2.0", "method": "eth_sendTransaction"},  
{ "id": 771759 },  
 5 / body: {"jsonrpc": "2.0", "method": "eth_sendTransaction"},  
{ "id": 817614 },  
 5 / body: {"jsonrpc": "2.0", "method": "eth_sendTransaction", "params": [{"from": "0x16e2115b1e00"}]},  
{ "id": 537357 }
```

Transactions	Comments			
The 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...
0xe2ef8c8fc58b0c8...	4505716	12 hrs 40 mins ago	0x2e820b454fdb39...	[IN] 0xcd9da0595a...
0x7e6b86be49c5b2...	4501770	1 day 3 hrs ago	0x8ba912954aedfea...	[IN] 0xcd9da0595a...
0x37819f1ff137cee7...	4494468	2 days 8 hrs ago	0xbfac940ec55e1aa...	[IN] 0xcd9da0595a...
0xd32fbe5771f291b...	4494300	2 days 8 hrs ago	0xbfac940ec55e1aa...	[IN] 0xcd9da0595a...
0x57ddb94fe86a279...	4481415	4 days 10 hrs ago	0x258c827f5acf8c9...	[IN] 0xcd9da0595a...
0x01961c698168b82...	4476889	5 days 4 hrs ago	0x258c827f5acf8c9...	[IN] 0xcd9da0595a...
0x8aeab96ce489f68a...	4463267	7 days 8 hrs ago	0xb093c35549e6eff...	[IN] 0xcd9da0595a...
0x724db32959abbda...	4462970	7 days 10 hrs ago	0x009befef5643f989...	[IN] 0xcd9da0595a...
0xb0c6d757a125d4f...	4462968	7 days 10 hrs ago	0x009befef5643f989...	[IN] 0xcd9da0595a...
0x0dc63df6d875d7c...	4461840	7 days 14 hrs ago	0x009befef5643f989...	[IN] 0xcd9da0595a...
0x231e1d2e23e50e4...	4457742	8 days 6 hrs ago	0xd58b7ae09f88e0f...	[IN] 0xcd9da0595a...
0xa6c1d7d96d160f1...	4457725	8 days 6 hrs ago	0x54160297ff7892b...	[IN] 0xcd9da0595a...
0x3cb8b7b8576a35...	4457650	8 days 6 hrs ago	0x54160297ff7892b...	[IN] 0xcd9da0595a...
0x51029839c261899...	4456959	8 days 9 hrs ago	0xd58b7ae09f88e0f...	[IN] 0xcd9da0595a...

The Most Profitable Crime?

wallet.dat.1

Which is the easiest crime to implement with the largest payoff?

```
112.92.122.186 - - [17/OCT/2017:07:57:00 +0000] "GET /didierstevens_bitcoin_walle...  
112.92.122.186 - - [17/OCT/2017:07:57:07 -0400] "GET /didierstevens_bitcoin_walle...  
112.92.122.186 - - [17/OCT/2017:07:57:09 +0000] "GET /wallet.dat HTTP/1.1"  
112.92.122.186 - - [17/OCT/2017:07:57:10 +0000] "GET /bitcoin_wallet.zip H...  
112.92.122.186 - - [17/OCT/2017:07:57:20 +0000] "GET /backups/bitcoin_walle...  
112.92.122.186 - - [17/OCT/2017:07:57:20 +0000] "GET /wallet.tar.gz H...  
112.92.122.186 - - [17/OCT/2017:07:57:31 +0000] "GET /didierstevens_bitco...  
112.92.122.186 - - [17/OCT/2017:07:57:40 +0000] "GET /didierstevens_bitco...  
112.92.122.186 - - [17/OCT/2017:07:57:41 +0000] "GET /didierstevens_bitco...  
112.92.122.186 - - [17/OCT/2017:07:57:45 +0000] "GET /home/.bitcoin/walle...  
112.92.122.186 - - [17/OCT/2017:07:57:45 +0000] "GET /bitcoin_wallet.dat.z...  
112.92.122.186 - - [17/OCT/2017:07:58:04 +0000] "GET /wallet.dat.zip HTTP/1.1  
112.92.122.186 - - [17/OCT/2017:07:58:05 +0000] "GET /home/ubuntu/.bitcoin...  
112.92.122.186 - - [17/OCT/2017:07:58:29 +0000] "GET /datadir/wallet.dat.H...  
112.92.122.186 - - [17/OCT/2017:07:58:31 +0000] "GET /wallet20-320conv.d...
```



Dimitrios Slamaris

@dim0x69

Bot trying to steal Ethers from
after enumerating "my" account
balance and my client version!

```
{ "id": 168440 },  
 5 / body: {"jsonrpc": "2.0", "method": "eth_sendTransaction"},  
{ "id": 943614 },  
 5 / body: {"jsonrpc": "2.0", "method": "eth_sendTransaction"},  
{ "id": 263038 },  
 5 / body: {"jsonrpc": "2.0", "method": "eth_sendTransaction"},  
{ "id": 472772 },  
 5 / body: {"jsonrpc": "2.0", "method": "eth_sendTransaction"},  
{ "id": 771759 },  
 5 / body: {"jsonrpc": "2.0", "method": "eth_sendTransaction"},  
{ "id": 817614 },  
 5 / body: {"jsonrpc": "2.0", "method": "eth_sendTransaction", "params": [{"from": "0x16e2115b1e00"}]},  
{ "id": 537357 }
```

Transactions	Comments			
The 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...
0xe2ef8c8fc58b0c8...	4505716	12 hrs 40 mins ago	0x2e820b454fdb39...	[IN] 0xcd9da0595a...
0x7e6b86be49c5b2...	4501770	1 day 3 hrs ago	0x8ba912954aedfea...	[IN] 0xcd9da0595a...
0x37819f1ff137cee7...	4494468	2 days 8 hrs ago	0xbfac940ec55e1aa...	[IN] 0xcd9da0595a...
0xd32fbe5771f291b...	4494300	2 days 8 hrs ago	0xbfac940ec55e1aa...	[IN] 0xcd9da0595a...
0x57ddb94fe86a279...	4481415	4 days 10 hrs ago	0x258c827f5acf8c9...	[IN] 0xcd9da0595a...
0x01961c698168b82...	4476889	5 days 4 hrs ago	0x258c827f5acf8c9...	[IN] 0xcd9da0595a...
0x8ae96ce489f68a...	4463267	7 days 8 hrs ago	0xb093c35549e6eff...	[IN] 0xcd9da0595a...
0x724db32959abbda...	4462970	7 days 10 hrs ago	0x009befef5643f989...	[IN] 0xcd9da0595a...
0xb0c6d757a125d4f...	4462968	7 days 10 hrs ago	0x009befef5643f989...	[IN] 0xcd9da0595a...
0x0dc63df6d875d7c...	4461840	7 days 14 hrs ago	0x009befef5643f989...	[IN] 0xcd9da0595a...
0x231e1d2e23e50e4...	4457742	8 days 6 hrs ago	0xd58b7ae09f88e0f...	[IN] 0xcd9da0595a...
0xa6c1d7d96d160f1...	4457725	8 days 6 hrs ago	0x54160297ff7892b...	[IN] 0xcd9da0595a...
0x3cb8b7b8576a35...	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 are physical borders?

What is consent?



Dear 21st Century ...

What is the ownership of something?

What are physical borders?

What is consent?

Who's laws do I comply with?



Dear 21st Century ...

What is the ownership of something?

What are physical borders?

What is consent?

Who's laws do I comply with?

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.

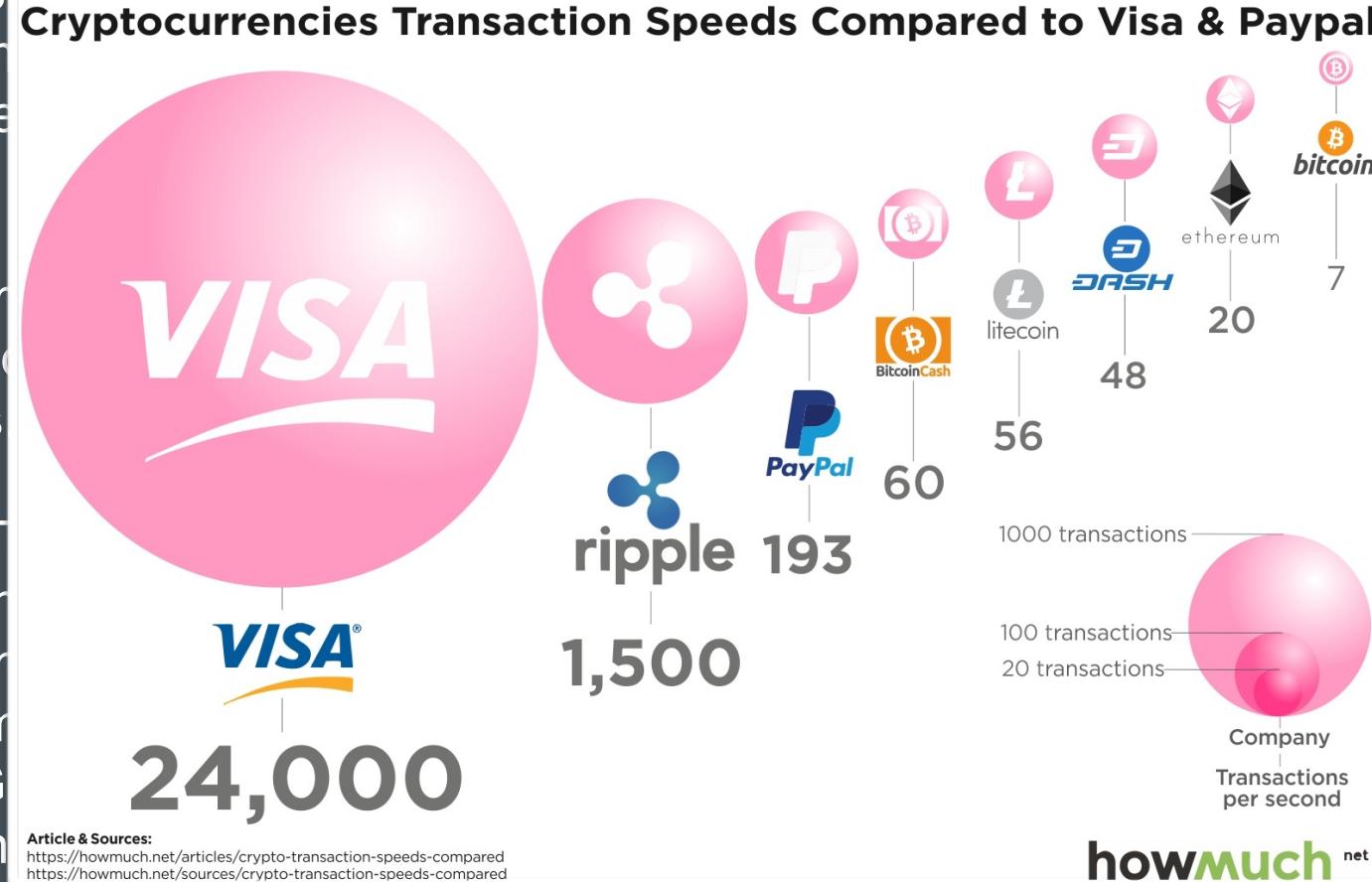


Dear

1st Generation. These cryptocurrencies, such as Bitcoin, Litecoin, Monero and Bitcoin Cash, basically instant and transfer value but have suffered from high transaction fees and long times to confirm times.

2nd Generation. Ethereum, Ripple, Dash, Litecoin, Monero, Lisk, have platform features. This generation adds more logical operations to the Blockchain.

3rd Generation. DAG based distributed system. traditional Blockchain can take some time to confirm blocks. With DAG, it can thus speeds up the confirmation process.



Dear [redacted]
1st Generation. These cryptocurrencies, such as Bitcoin, Litecoin, Monero and Bitcoin Cash, basically instant and transform value but have suffered from [redacted]

Cryptocurrencies Transaction Speeds Compared to Visa & Paypal

	 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

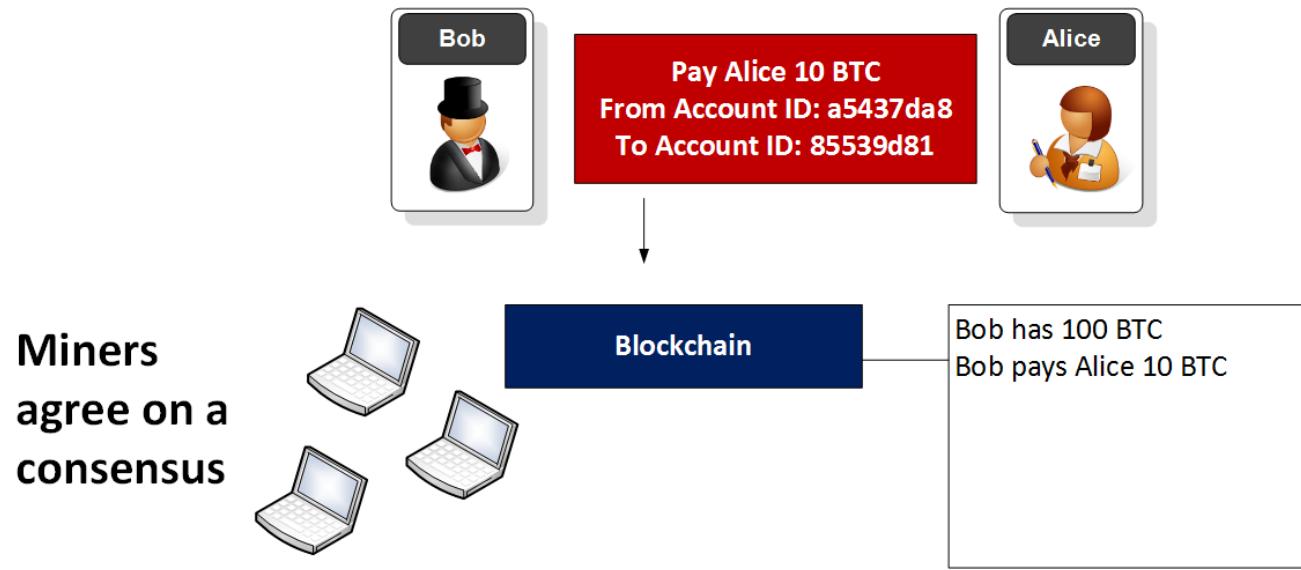
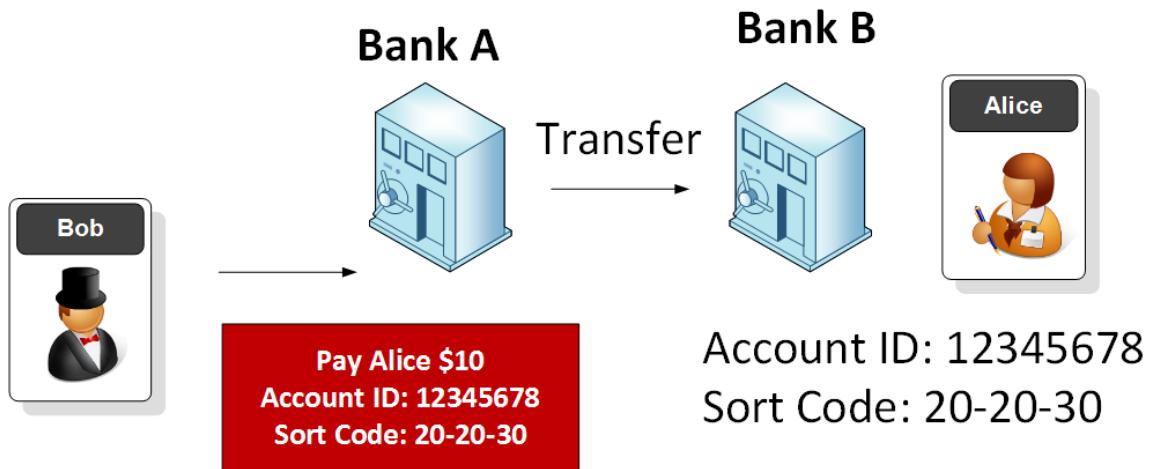
- based on their respective website

thus speeds up th

Article & Sources:

<https://howmuch.net/articles/crypto-transaction-speeds-compared>
<https://howmuch.net/sources/crypto-transaction-speeds-compared>

Payments



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.
- 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.
- Others: Ethereum, Ripple, Litecoin, Monero, Ethereum Classic, Dash, Steem, KiloCoin and Augur.



Genesis Record

Big accounts

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

Summary		Transactions	
Address	3D2oetdNuZUqQHPJmcMDDHYoqkyNVsFk9r	No.	3493
Hash 160	7c6775e20e3e938d2d7e9d79ac310108ba501ddb	Transactions	
Tools	Related Tags - Unspent Outputs	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		Transactions	
Address	3EDzR4QKeGJyCZWXML1kAGqj8gHNQ798sF	No. Transactions	1
Hash 160	897d25262f68b8a8d4e2adf2ab082ce0f58a69d1	Total Received	2,034.668943 BTC
Tools	Related Tags - Unspent Outputs	Final Balance	2,034.668943 BTC

Request Payment

Donation Button



e3a9cbc0c5ec55db3ac02029d8cbaf1370e04e8603d9e5000106091c66c308d

2017-11-14 08:03:03

3Qk9qheSn4Y5wUCmSAT4ggbhHbRRgRdVaW	→	1LAGK834p9y4h34jWgGjHsSRNUgKWB9Cho	0.009 BTC
		1GANFvqWMg1zmVGU2WKUAuGDS5PGj3KBNx	0.01718 BTC
		3Mfly7hJB44kYTHrgCuJ7JgpzL1tSqWg	15.6262 BTC
		37K7vhCNe8VmLnhdjBRRBZB1EL5zZhI94Zg8	0.31678 BTC
		1FKjowv879X5RGDeU21zzxirVbgNoeGaJr	0.169 BTC
		3BazbNWURUzdk58myGn1V9F6HPabtUjZwN	0.01265 BTC
		3HCJDcEjzHyip6TJ3kwQQajGxJW6scbzGB	13,067.17305362 BTC
			13,083.32386362 BTC

Genesis Record

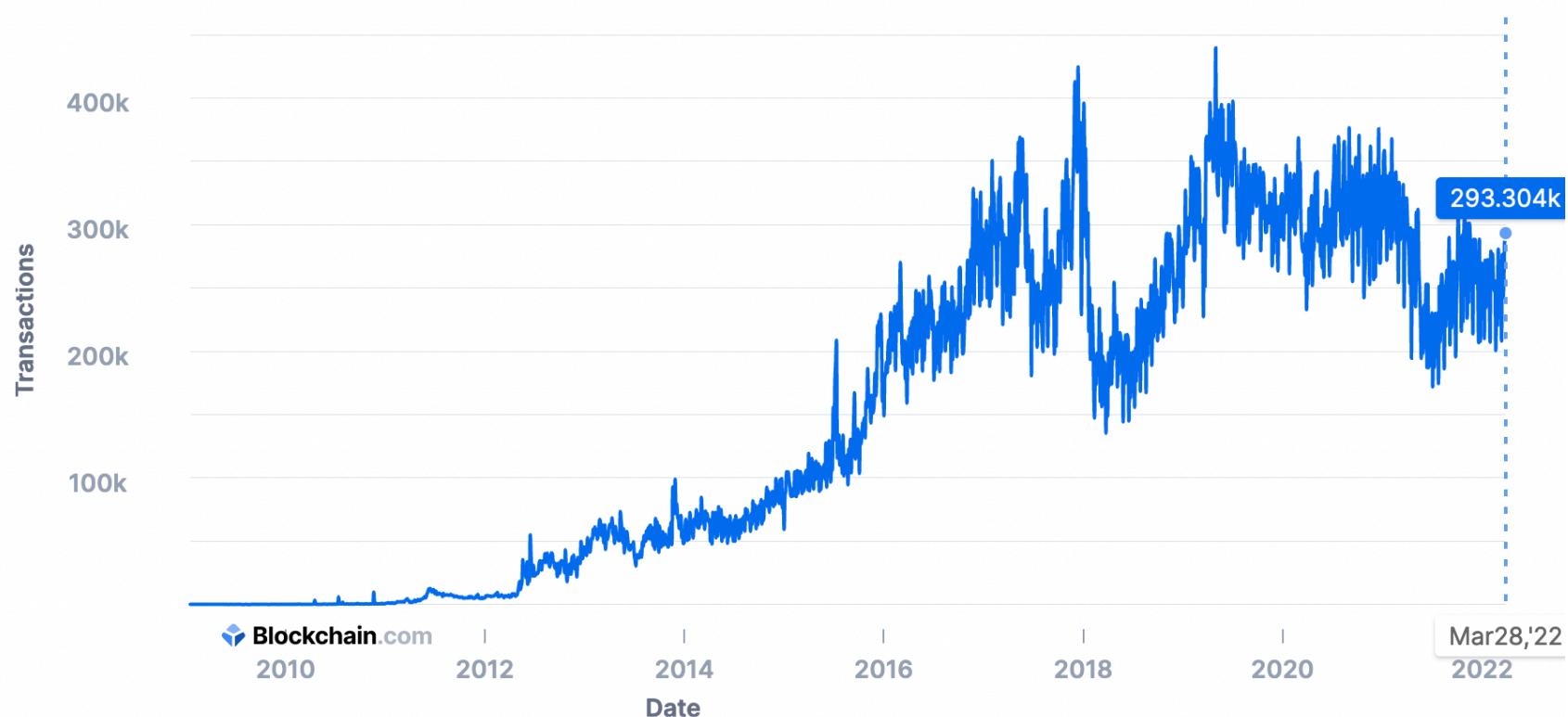
Summary

Hash	4410c8d14ff9f87ceeed1d65cb58e7c7b2422b2d7529afc675208... 	2019-09-06 04:13
	1PfceCKGraSPEvx6nfjw5ZCLLy8Ct23Qd5 \$0.04  	37XuVSEpWW4trkfmvWzegTHQt7BdktSKUs \$588,282,890.50 
	1PfceCKGraSPEvx6nfjw5ZCLLy8Ct23Qd5 \$0.04 	
	1JCe8z4jJVNXSjohjM4i9Hh813dLCNx2Sy \$31.12 	
	1JCe8z4jJVNXSjohjM4i9Hh813dLCNx2Sy \$0.04 	
	1PfceCKGraSPEvx6nfjw5ZCLLy8Ct23Qd5 \$0.05 	
	1KKIEAkpnQR2FH5kpkGP6442ZDkd6ZdrRS \$0.05 	
	15NQthxeLSwMtEaXJFM7YUCf59LzmFjkeH \$0.05 	
	15K8LDNMqvcVyPk9oubtQ6yYtdGdpENPXq \$620,624.45 	
	1JCe8z4jJVNXSjohjM4i9Hh813dLCNx2Sy \$0.41 	
	1PfceCKGraSPEvx6nfjw5ZCLLy8Ct23Qd5 \$0.05 	
	Load more inputs... (82 remaining)	
Fee	\$406.79 (480.115 sat/B - 120.029 sat/WU - 13611 bytes)	\$588,282,890.50

Bitcoin transactions

Confirmed Transactions Per Day

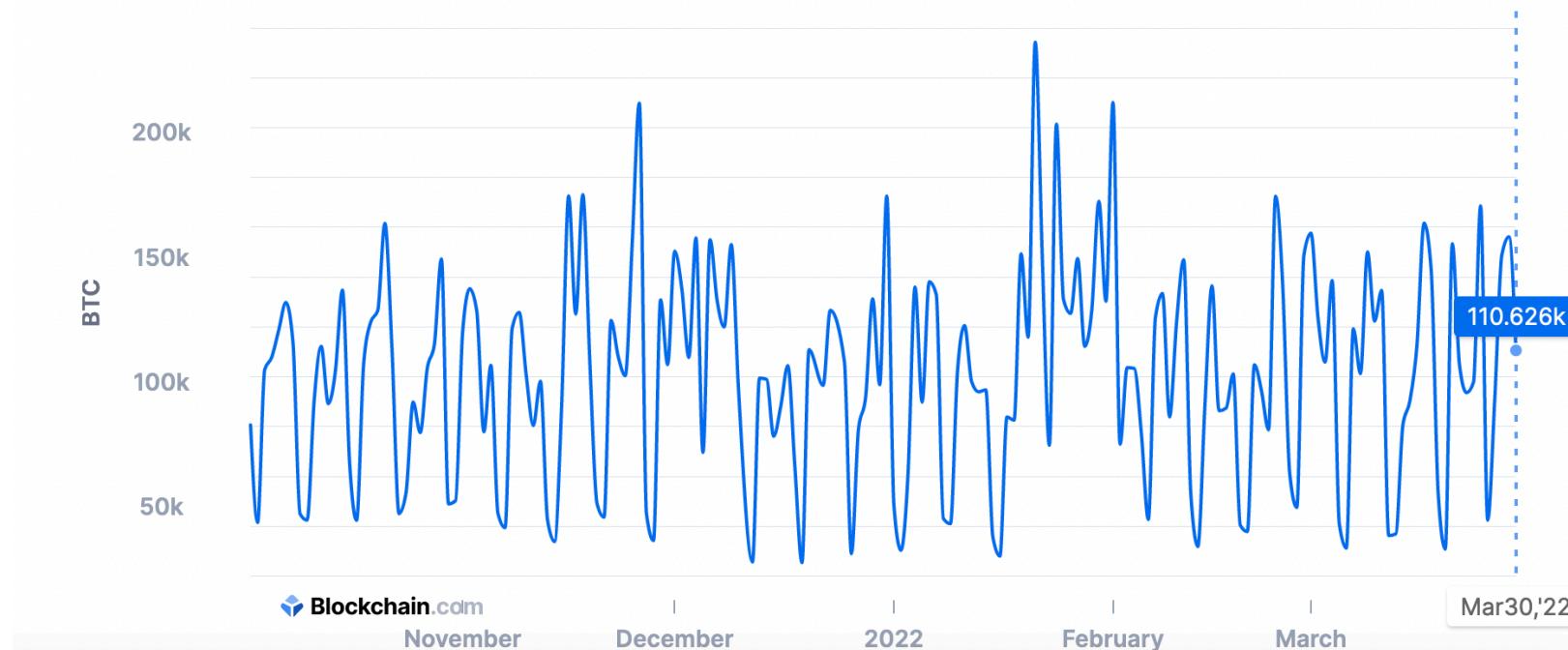
The total number of confirmed transactions per day.



Transaction value

Estimated Transaction Value (BTC)

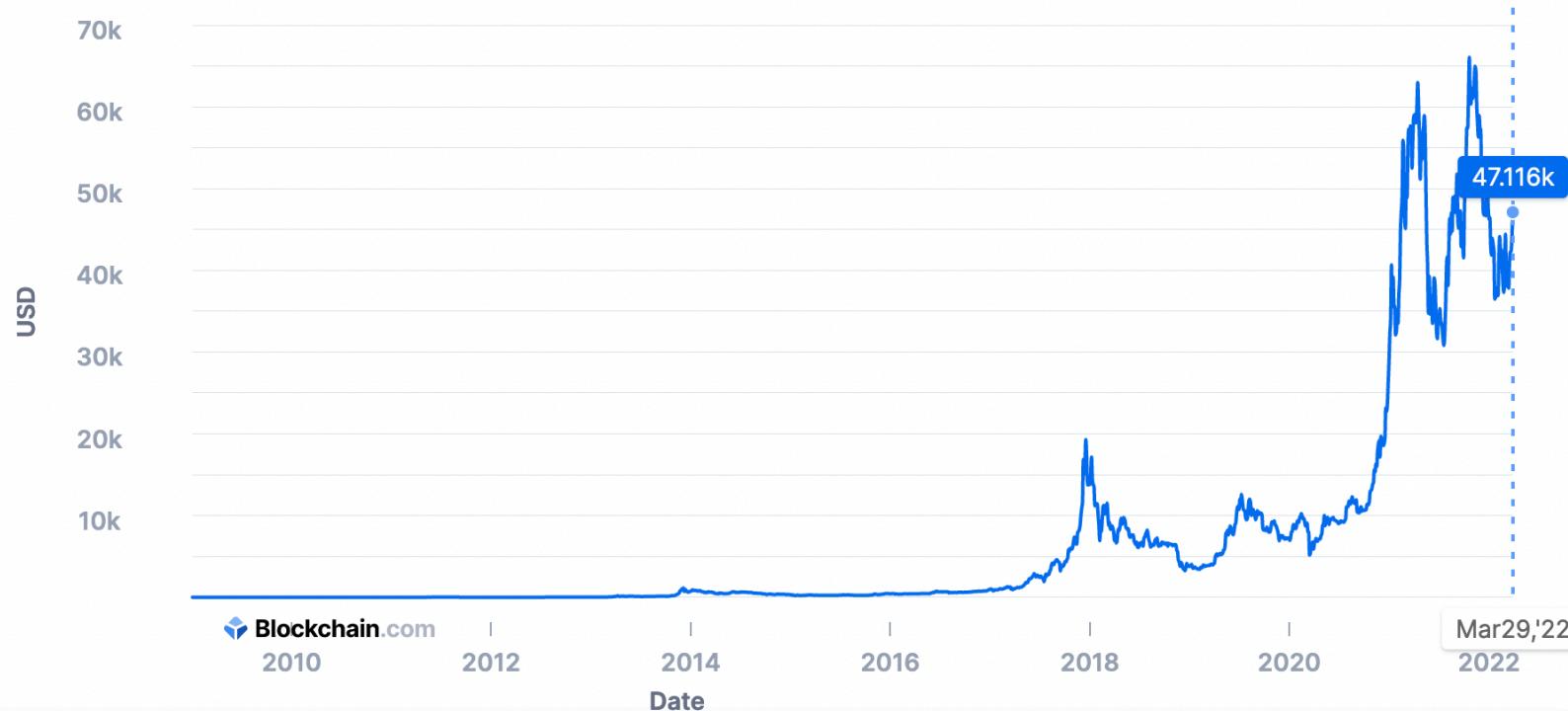
The total estimated value in BTC of transactions on the blockchain. This does not include coins returned as change.



Bitcoin value

Market Price (USD)

The average USD market price across major bitcoin exchanges.



Types

#	Name	Price	24h %	7d %	Market Cap	Volume(24h)	Circulating Supply	Last 7 Days	More
1	Bitcoin BTC Buy	\$46,459.89	-1.47%	+5.76%	\$883,013,010,050	\$32,852,256,547 706,853 BTC	18,999,012 BTC		⋮
2	Ethereum ETH Buy	\$3,354.37	-0.78%	+7.75%	\$403,257,532,992	\$16,134,073,440 4,808,610 ETH	120,187,142 ETH		⋮
3	Tether USDT	\$1.00	+0.01%	-0.02%	\$81,960,944,399	\$90,555,594,996 90,525,541,240 USDT	81,933,743,051 USDT		⋮
4	BNB BNB Buy	\$434.06	-1.10%	+4.76%	\$71,630,352,530	\$2,712,377,199 6,252,363 BNB	165,116,761 BNB		⋮
5	USD Coin USDC	\$1	+0.03%	-0.00%	\$51,606,757,536	\$4,820,220,296 4,822,970,227 USDC	51,636,199,146 USDC		⋮
6	Solana SOL Buy	\$125.20	+1.95%	+23.37%	\$40,707,254,351	\$4,025,840,669 32,166,876 SOL	325,255,100 SOL		⋮
7	XRP XRP	\$0.8238	-4.36%	-2.36%	\$39,671,905,046	\$2,392,585,832 2,902,181,779 XRP	48,121,609,012 XRP		⋮
8	Cardano ADA	\$1.17	-0.93%	+0.18%	\$39,535,932,858	\$1,645,078,214 1,403,875,139 ADA	33,739,133,347 ADA		⋮
9	Terra LUNA Buy	\$104.72	-3.56%	+11.36%	\$37,213,241,216	\$2,460,573,785 23,455,582 LUNA	354,737,682 LUNA		⋮
10	Avalanche AVAX Buy	\$97.58	+0.58%	+10.83%	\$26,096,693,493	\$2,519,204,078 25,801,523 AVAX	267,280,626 AVAX		⋮

Blockchain and Cryptocurrencies

Cryptocurrencies

> Bitcoin addresses

Blockchain

Mining

Ethereum

Smart Contracts

Blockchain Crypto

Prof Bill Buchanan OBE

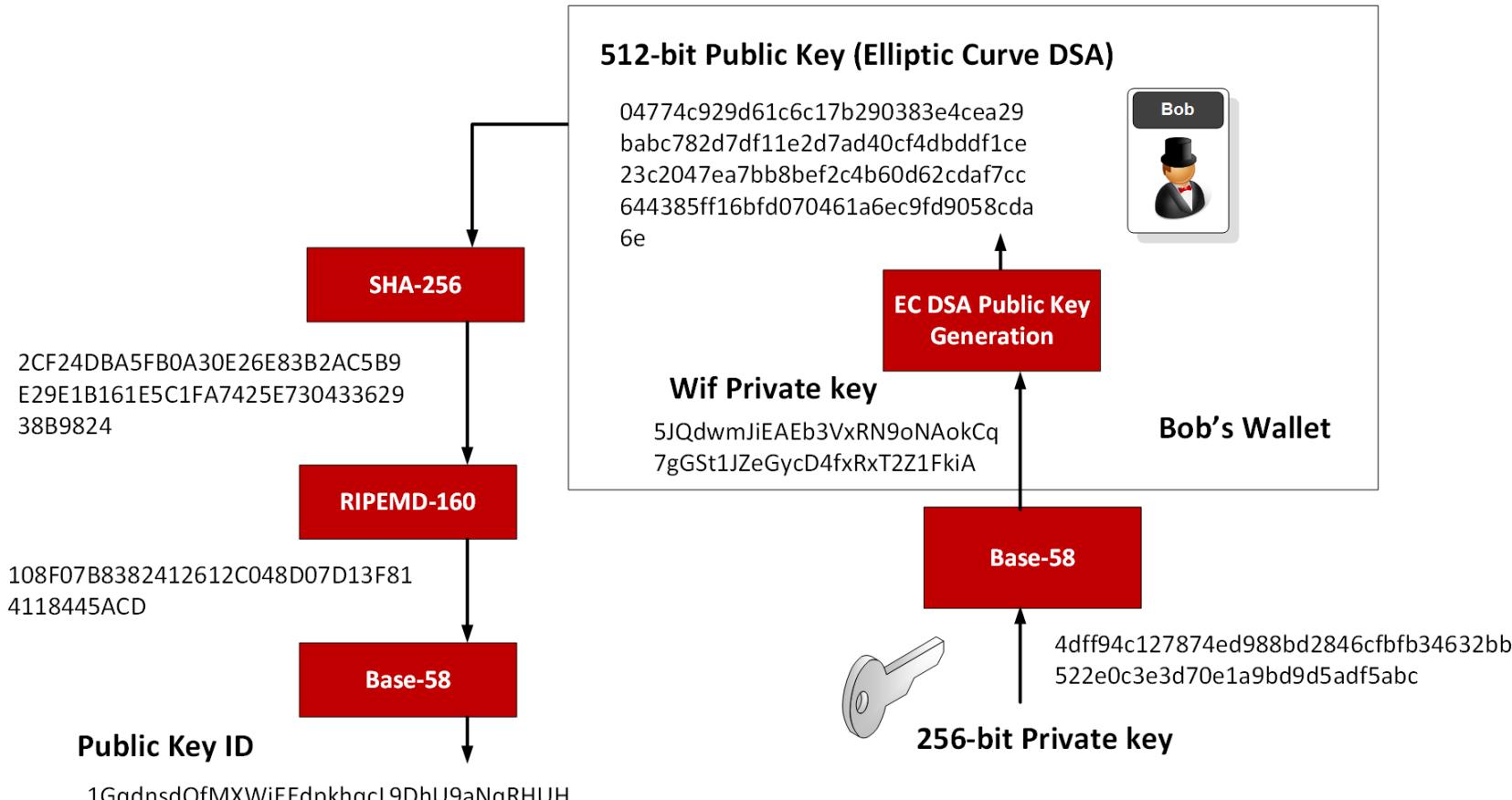
<https://asecuritysite.com/blockchain>



Bitcoin Wallet and Addresses

P2PKH - Public key hash - 17VZNX1SN5NtKa8UQFxwQbFeFc3iqRYhem

P2SH - Pay to script hash - 3EktnHQD7RiAE6uzMj2ZifT9YgRrkSgzQX -
Sender proves a script.

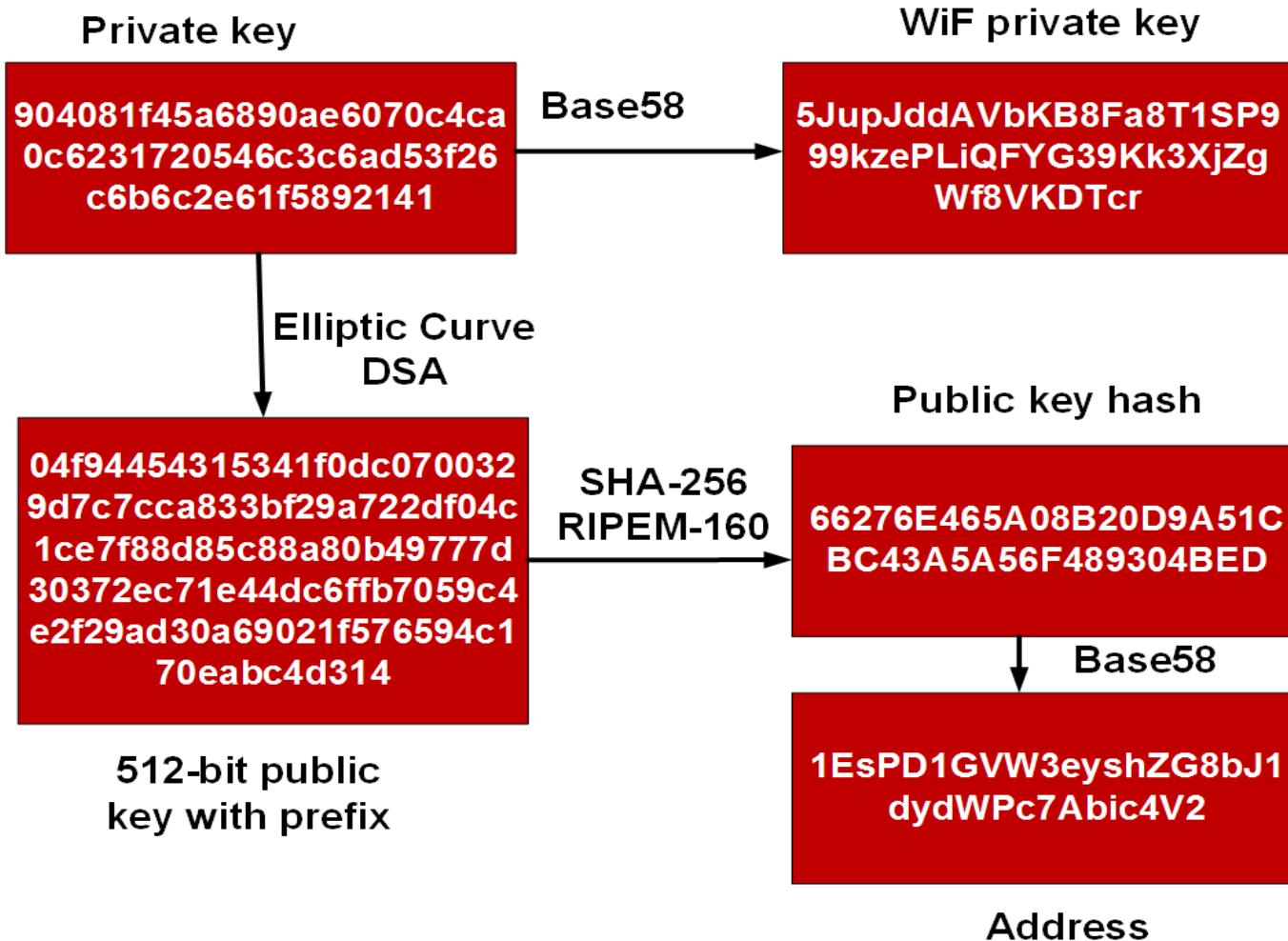


Summary	
Address	1JyvJ5TcN2hzu7dDEeVuuikgyHtpwU8NE6
Hash 160	c53deb8dda6fb0c388da19fbcf63270cc4f4cbfd
Tools	Related Tags - Unspent Outputs

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

[Request Payment](#) [Donation Button](#)





Private key:

4c0333a50b7724c71b89df148d83f64d49d896e21701007eeb8cada52744aca2

Public key:

0489fc7b8c3f655a10840d35c76ebb5596694045e49e940fb1e7a759da4edf0fafc45bb
bea6f5a56abf14c145c529c8eda9d3ad606f3a0bf4ca01ce991d4987b97

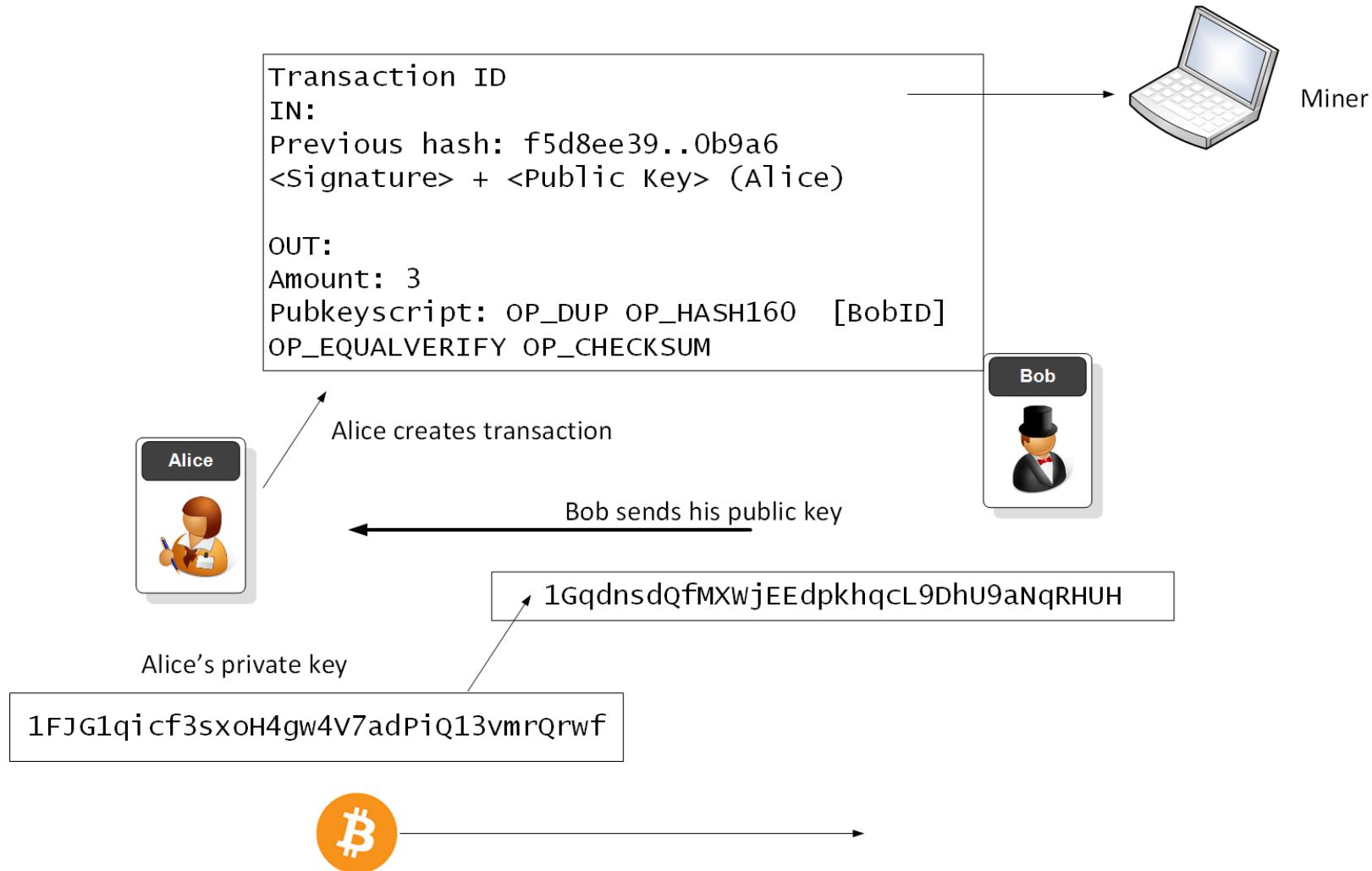
Wif: 5JPmDetQXXvc5aT5efyrg7BxHbH4135owRzq9DD7n2eWQCta5MN

Address: 16RAf9CjnstWCfBJGfrzSSMfTeHJVt8QWw

Signed:

4830450220264c4dce5f1cf0dff8d32d21c5d5cf6baed428b12ae6f8594924246a611e9
ee602210096ef8e7054ec7a39f0a35d8de3fd50090b1d125c0e795af8cf3d577b67640
7ca01410489fc7b8c3f655a10840d35c76ebb5596694045e49e940fb1e7a759da4edf0f
afc45bbbea6f5a56abf14c145c529c8eda9d3ad606f3a0bf4ca01ce991d4987b97

Bitcoin transaction



Blockchain and Cryptocurrencies

Cryptocurrencies
Bitcoin addresses
> Blockchain
Mining
Ethereum
Smart Contracts
Blockchain Crypto

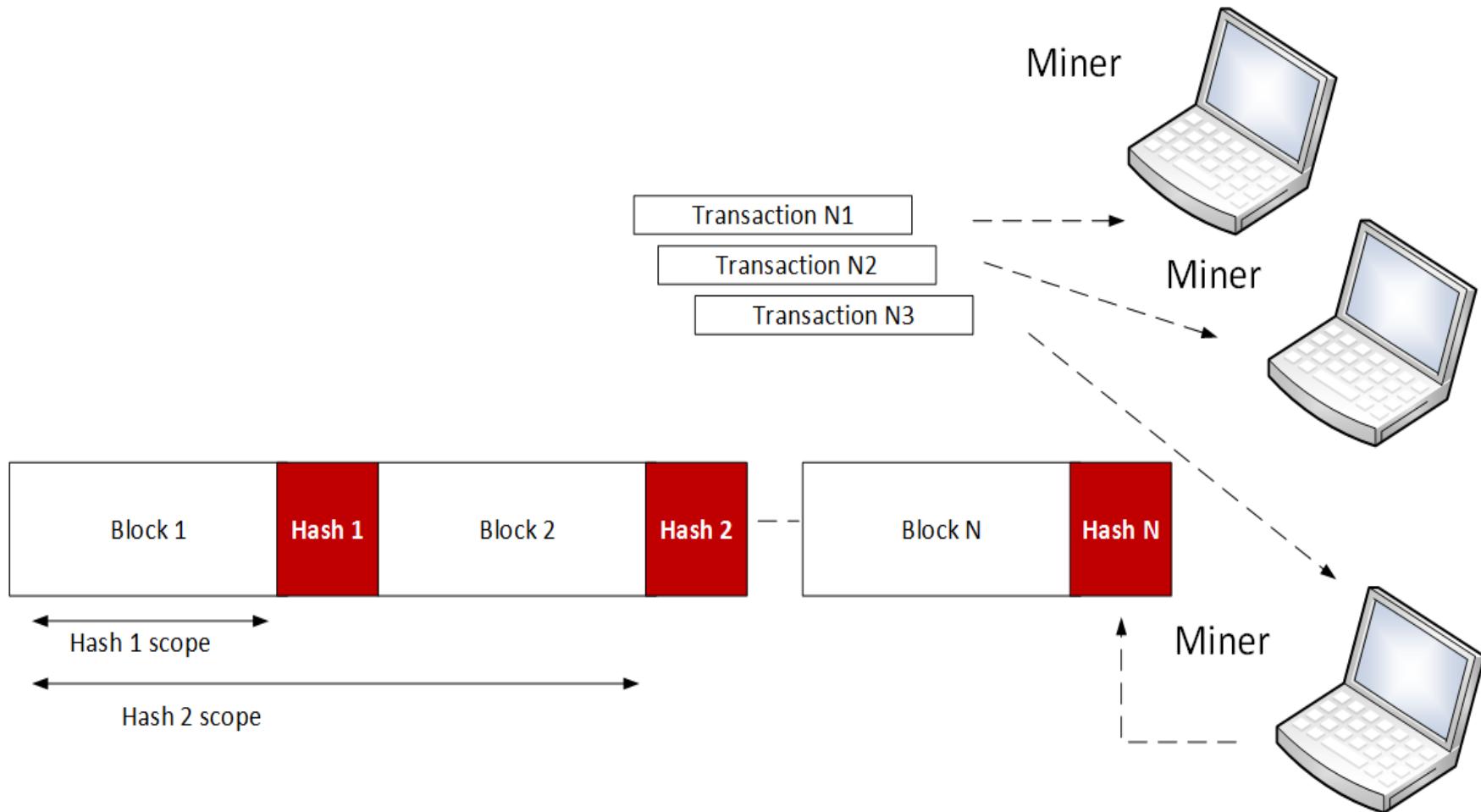
Prof Bill Buchanan OBE

<http://asecuritysite.com/crypto10>

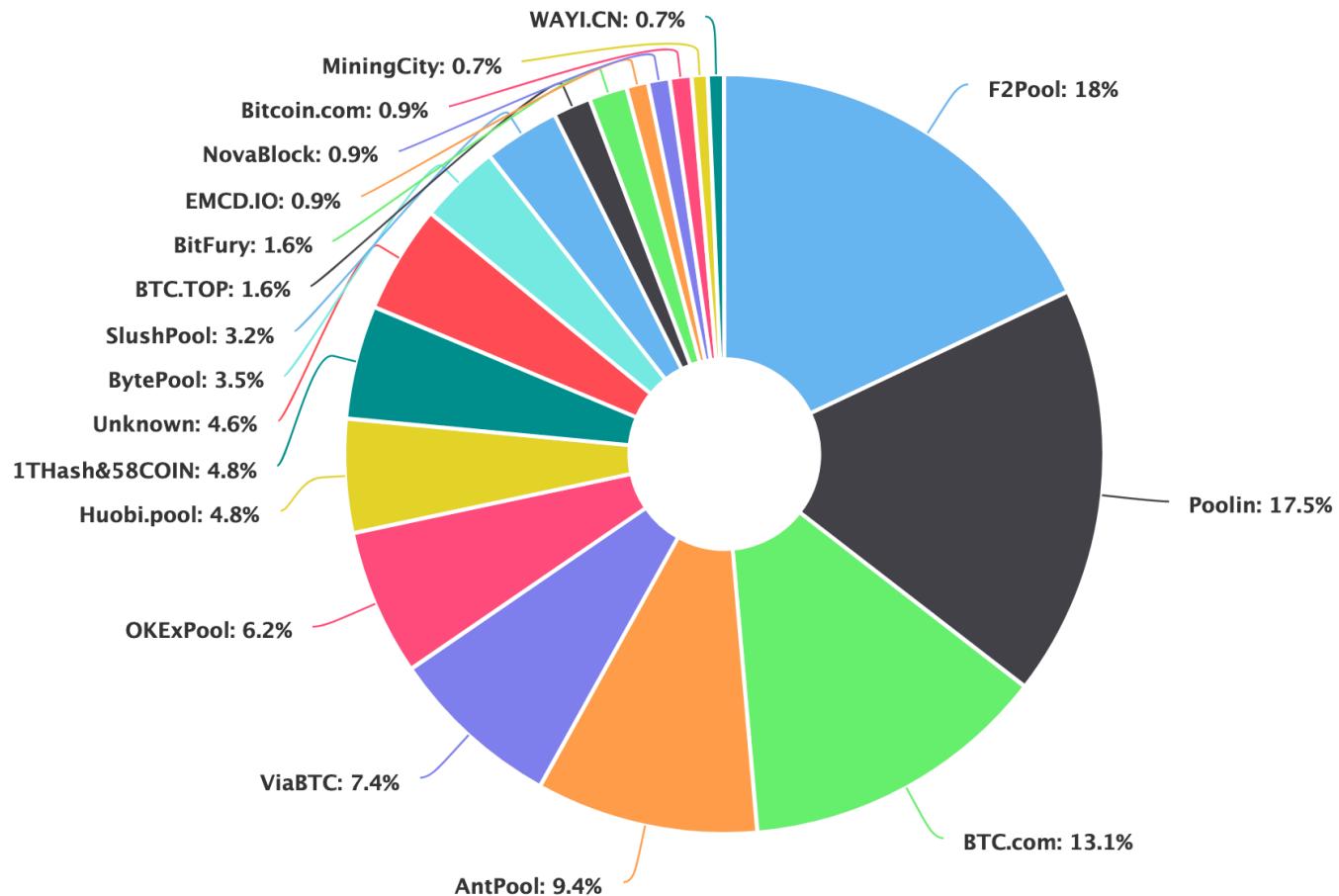
<http://asecuritysite.com/encryption>



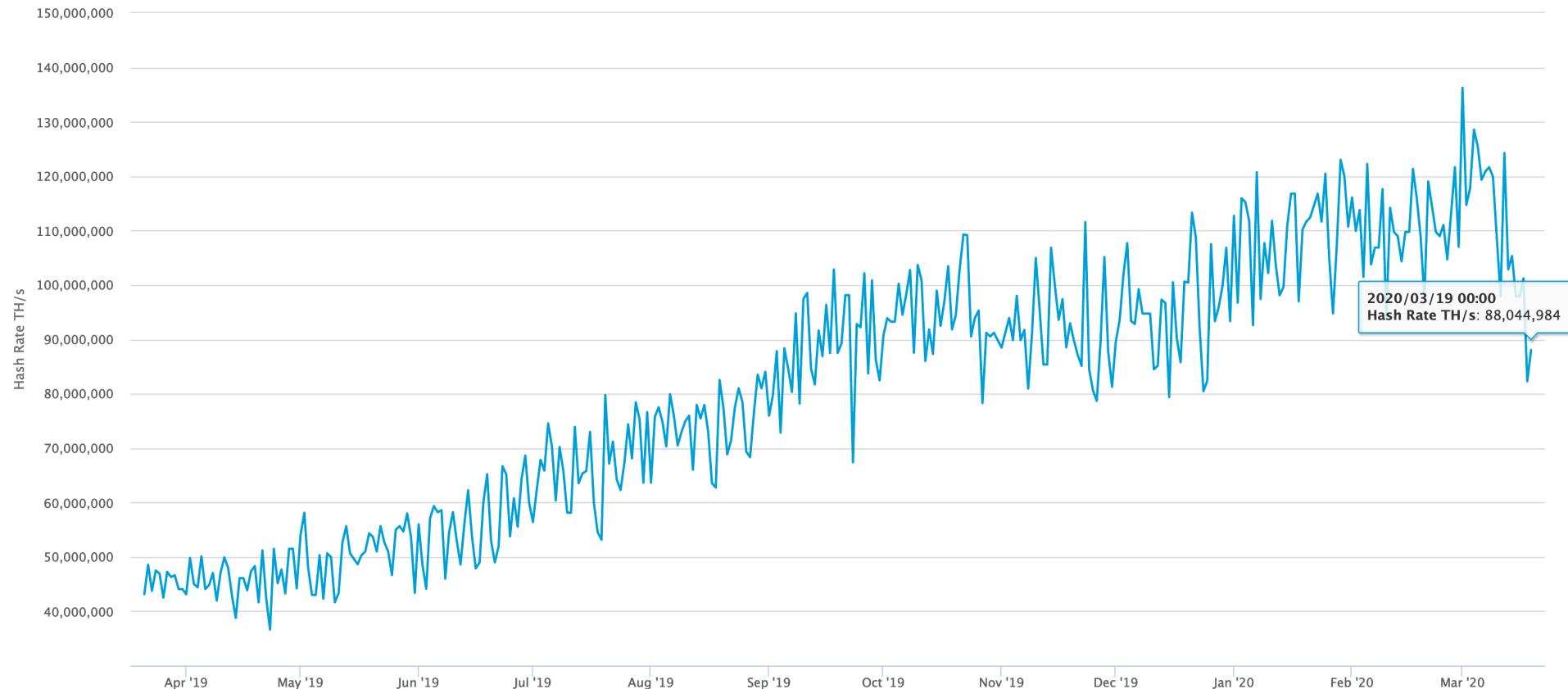
Mining process



Successful miners



Hash Rate TH/s



Mining Processes

- Hash
- 0000000000000000d98e57b83834a2d1f438
7a93d06861bcf3ea5fc498bd55
- Previous Block
- 000000000000000012138e05f0779765277a9
d2ab7e4a2a70882790abf98a0c

Blocks

Block #475370

Summary	
Number Of Transactions	1937
Output Total	10,443.01703436 BTC
Estimated Transaction Volume	555.96160374 BTC
Transaction Fees	0.87013657 BTC
Height	475370 (Main Chain)
Timestamp	2017-07-11 21:44:58
Received Time	2017-07-11 21:44:58
Relayed By	AntPool
Difficulty	708,659,466,230.33
Bits	402754864
Size	998.17 KB
Version	0x20000000
Nonce	1203121562
Block Reward	12.5 BTC

Hashes	
Hash	0000000000000000d98e57b83834a2d1f4387a93d06861bcf3ea5fc498bd55
Previous Block	000000000000000012138e05f0779765277a9d2ab7e4a2a70882790abf98a0c
Next Block(s)	000000000000000010e3117695c04d66d31cfa8489b70579dcc2f12c5a2daae
Merkle Root	140d91abab9501d50ace079ba12c80125f48c2b5fe7d9da685ea3ee8ea767e82

Blockchain and Cryptocurrencies

Cryptocurrencies

Bitcoin addresses

Blockchain

Mining

> Ethereum

Smart Contracts

Blockchain Crypto

Prof Bill Buchanan OBE

<https://asecuritysite.com/blockchain>



Crypto Kitties

Crypto Kitties

 CryptoKitties

[Sign in](#) [Marketplace](#)

Search

[For Sale](#) [Siring](#) [Gen 0](#) [All Kitties](#)

Sort by [Youngest first](#)

98,387 Kitties [Filter Kitties](#)

New

For sale ⚡ 0.2360



Kitty 465397 · Gen 0 · Fast
♥ 0

New

For sale ⚡ 0.2311



Kitty 465351 · Gen 0 · Fast
♥ 1

New

For sale ⚡ 0.2302



Kitty 465348 · Gen 0 · Fast
♥ 3

New

For sale ⚡ 0.1976



Kitty 465331 · Gen 3 · Swift
♥ 6

Crypto Kitties

 CryptoKitties

[Sign in](#) [Marketplace](#)

Search

[For Sale](#) [Siring](#) [Gen 0](#) [All Kitties](#)

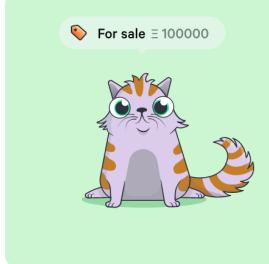
Sort by [Youngest first](#)



For sale ⚡ 117911

Kitty 117911 · Gen 0 · Fast

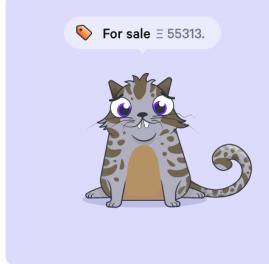
9 hearts



For sale ⚡ 100000

Kitty 118472 · Gen 0 · Brisk

5 hearts



For sale ⚡ 55313.

Kitty 430720 · Gen 0 · Fast

6 hearts



For sale ⚡ 14467.

Kitty 110005 · Gen 0 · Swift

0 hearts

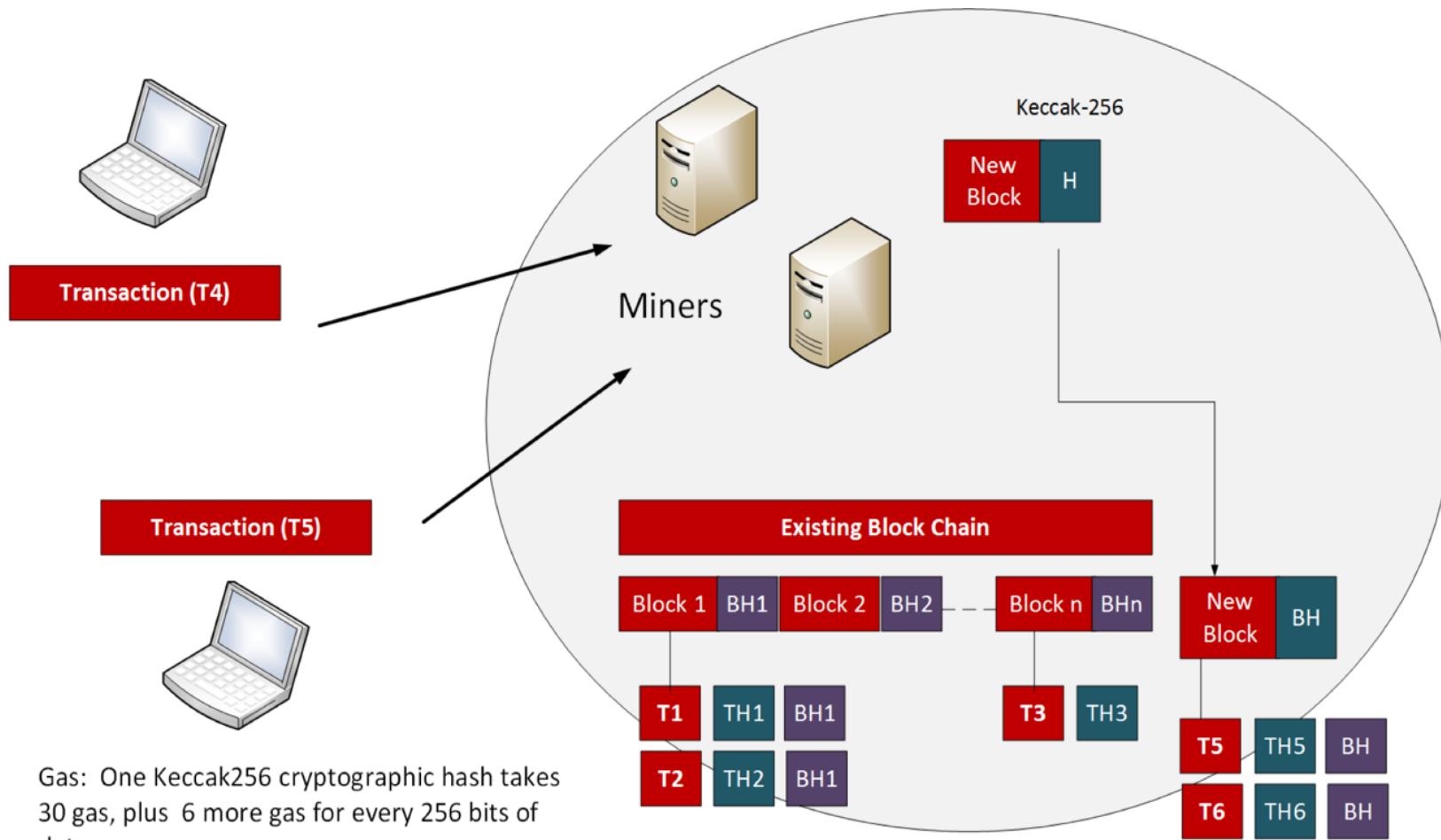
Crypto Kitties



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

- 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.

Gas



Hash	0x5a0b54d5dc17e0aadc383d2db43b0a0d3e029...
Nonce	6,036,880
Number of Transactions	6,036,967
Final Balance	72.518651614514882353 ETH
Total Sent	3038257.557250117417771999 ETH
Total Received	672.358829141229772024 ETH
Total Fees	305.4663511648 ETH

Transactions

Standard

Internal

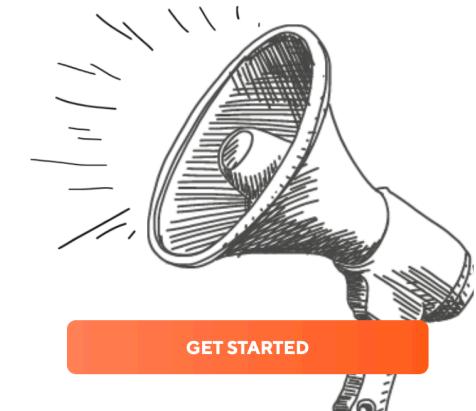
Hash	0x3bcab6d3db3e64147ac881aa9928e1bdc...	2020-03-20 07:00
	0x5a0b54d5dc17e0aadc383d2db43b0a0d...	→ 0x8fd00f170fdf3772c5ebcd90bf257316c691
Fee	0.00012600 ETH (21000 GAS - 6000000000 WEI)	-98.512346513586285551 ETH



Enjoy Our Lowest
Crypto Credit Line™
Rates Ever

from

5.9% APR



Blockchain and Cryptocurrencies

Cryptocurrencies

Bitcoin addresses

Blockchain

Mining

Ethereum

> Smart Contracts

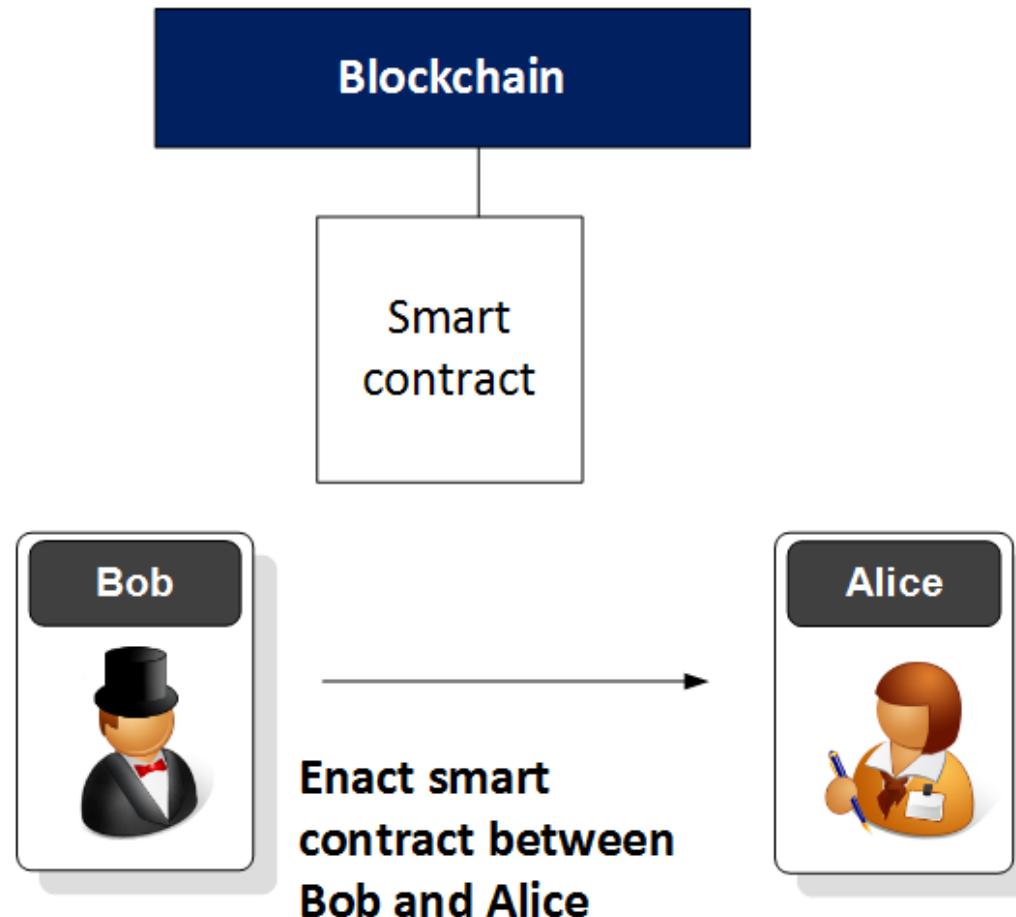
Blockchain Crypto

Prof Bill Buchanan OBE

<https://asecuritysite.com/blockchain>



Smart Contract



The image shows a Solidity code editor interface with the following details:

- File Explorer:** On the left, under the "Workspaces" section, there is a workspace named "zo1". Inside "zo1", there are several folders: ".deps", "contracts", "scripts", "tests", "artifacts", and a folder named "adding". The "adding" folder contains sub-files: "artifacts", "maths.sol", and "verifier.sol". Other files visible in "zo1" include "README.txt", "main.zok", and "verification_key.json".
- Code Editor:** The main area displays two Solidity contracts:
 - maths.sol:** A contract named "mymath" with four functions: `sqrt`, `sqr`, `mul`, and `sub`.
 - `sqrt(uint x) view returns (uint y)`: Calculates the square root of `x` using an iterative algorithm.
 - `sqr(uint a) view returns (uint)`: Returns the square of `a`.
 - `mul(uint a, uint b) view returns (uint)`: Returns the product of `a` and `b`.
 - `sub(uint a, uint b) view returns (uint)`: Returns the difference between `a` and `b`.
 - verifier.sol:** A contract with one function `add` that adds two uints and returns the result.
- Status Bar:** At the bottom, the status bar shows the message "Execution cost: infinite gas - FunctionDefinition.sol" and "1 reference(s)".

Compile with Solidity

SOLIDITY COMPILER

COMPILER 0.8.13+commit.abaa5c0e

Include nightly builds

LANGUAGE Solidity

EVM VERSION default

COMPILER CONFIGURATION

Auto compile

Enable optimization 200

Hide warnings

[Compile maths.sol](#)

CONTRACT mymath (maths.sol)

```
pragma solidity ^0.8.0;

contract mymath {

    function sqrt(uint x) public view returns (uint y) {
        uint z = (x + 1) / 2;
        y = x;
        while (z < y) {
            y = z;
            z = (x / z + z) / 2;
        }
    }

    function sqr(uint a) public view returns (uint) {
        uint c = a * a;
        return c;
    }

    function mul(uint a, uint b) public view returns (uint) {
        uint c = a * b;
        return c;
    }

    function sub(uint a, uint b) public view returns (uint) {
        return a - b;
    }

    function add(uint a, uint b) public view returns (uint) {
        uint c = a + b;
        return c;
    }
}
```

Etherscan Ropsten Testnet Network

All Filters Search by Address / Txn Hash / Block / Token / Ens

Home Blockchain Tokens Misc Ropsten

Contract 0x0895A540Cff8E7829284F1D9c55daF624D6e2Df9

Contract Overview

Balance: 0 Ether

More Info

My Name Tag: Not Available

Contract Creator: 0xbb15b38e4ef6af154b8... at txn 0xce641d9aac54b17f30...

Transactions Contract Events

Latest 1 from a total of 1 transactions

Txn Hash	Method ⓘ	Block	Age	From ↴	To ↴	Value	Txn Fee
0xce641d9aac54b17f30...	0x60806040	12106559	2 mins ago	0xbb15b38e4ef6af154b8...	IN Contract Creation	0 Ether	0.000758827502

[Download CSV Export]

Blockchain and Cryptocurrencies

Cryptocurrencies

Bitcoin addresses

Blockchain

Mining

Ethereum

Smart Contracts

> Blockchain Crypto

Prof Bill Buchanan OBE

<https://asecuritysite.com/blockchain>



Merkle Trees

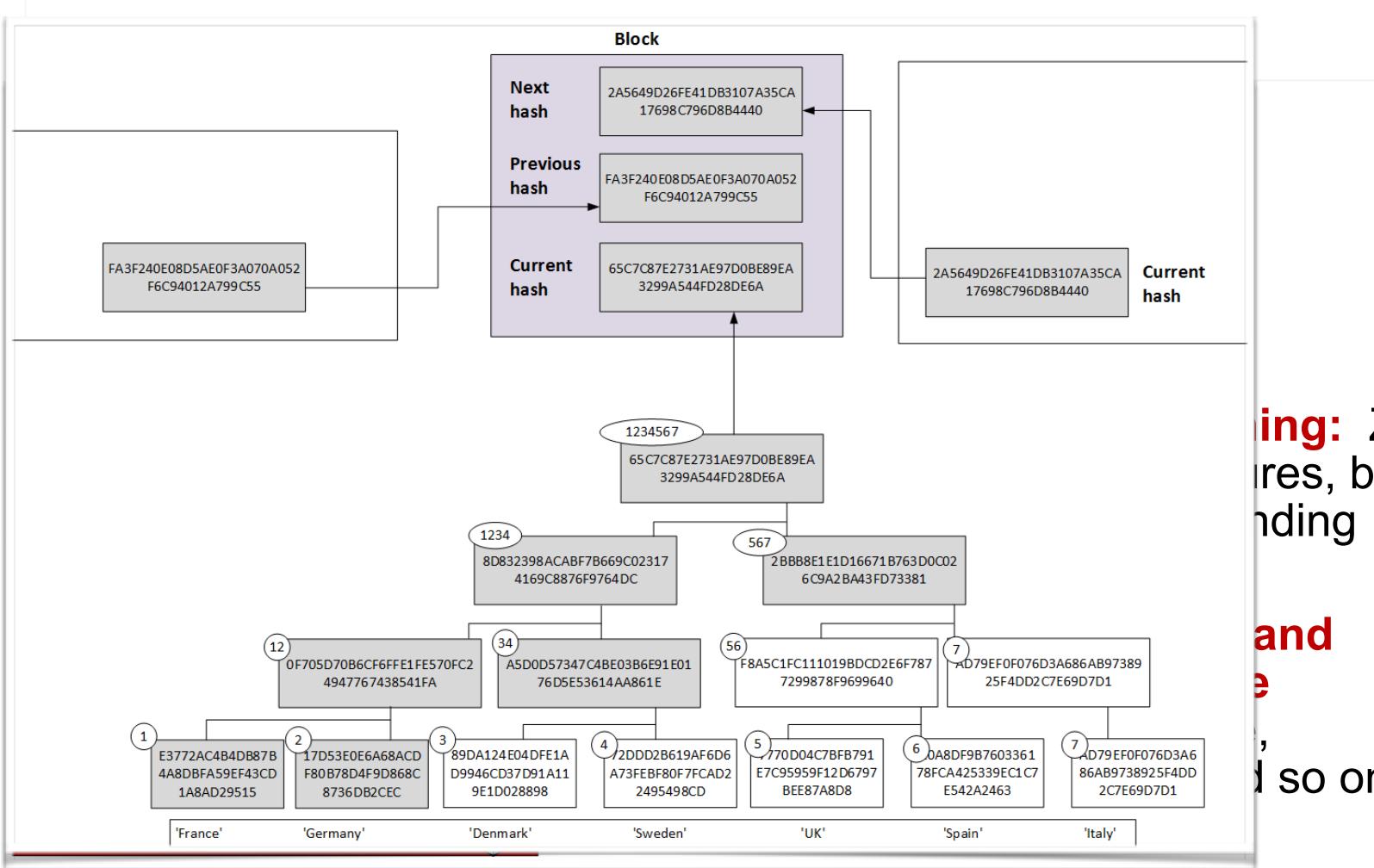
- **Sovereign ID, ZKP and signing:** Zero-knowledge proof, ring signatures, bullet proofs, stealth addresses, blinding factors, and so on.
- **Homomorphic, Distributed and Privacy Preserving Machine Learning:** Meet in the middle, homomorphic encryption, and so on.

Merkle Trees

Finance		Applications for financial users, issuers of digital value, and trading and market operations
Value		Instruments that carry monetary or other value.
Governance		Protection of the system from non-technical threats.
Accounting		Framework that contains value within defined and manageable places.
Rights		An authentication concept, with ownership allocated to unit-value, and methods of moving unit-values between unit-identities.
Software Engineering		The tools to move instructions over the net, and hold numbers and information reliably constant on nodes.
Cryptography		Mathematical techniques to state certain truths that could be shared between parties for passing value

ing: Zero-
ires, bullet
nding
and
e
,
d so on.

Merkle Trees

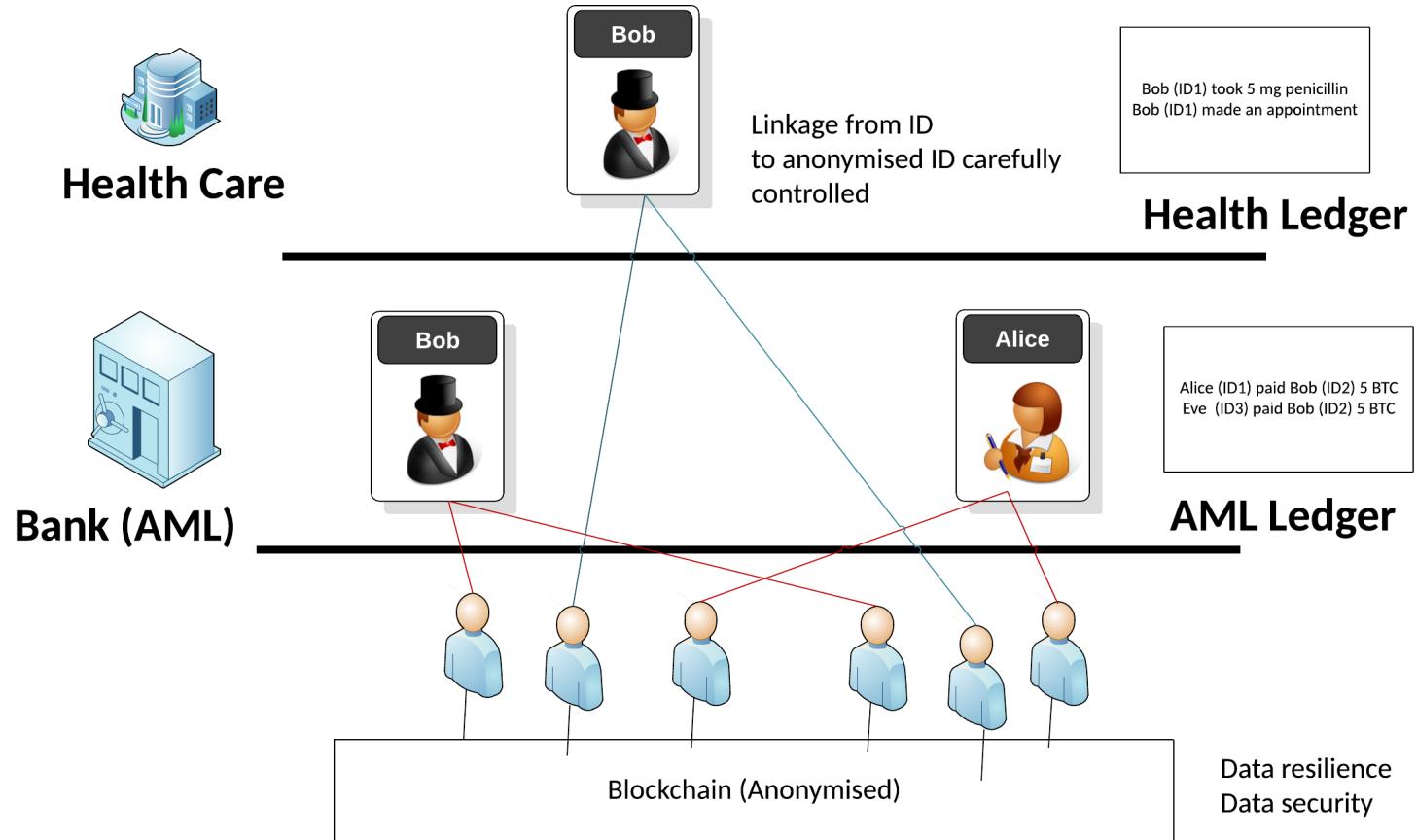


ing: Zero-
ires, bullet
nding

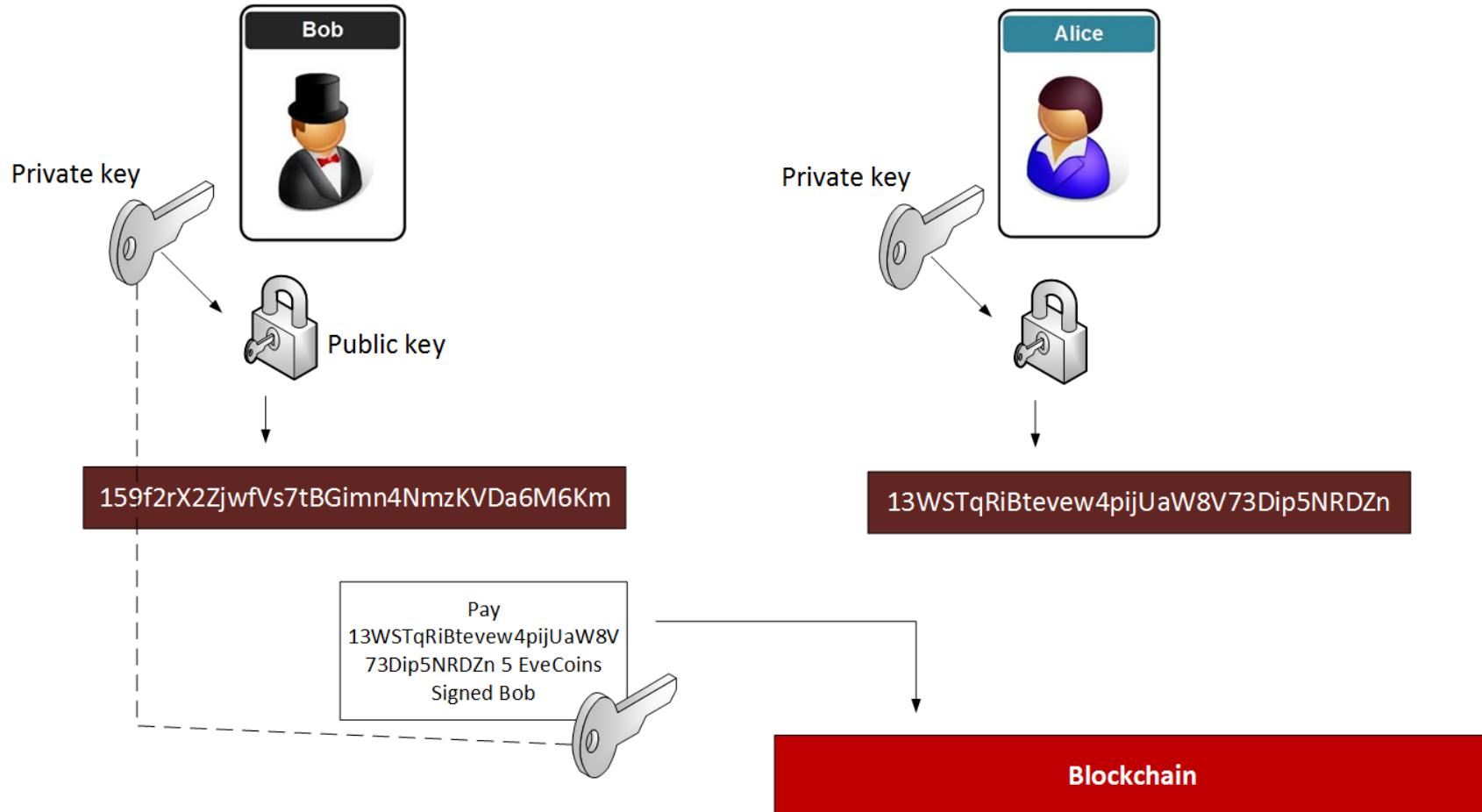
and
e

,
so on.

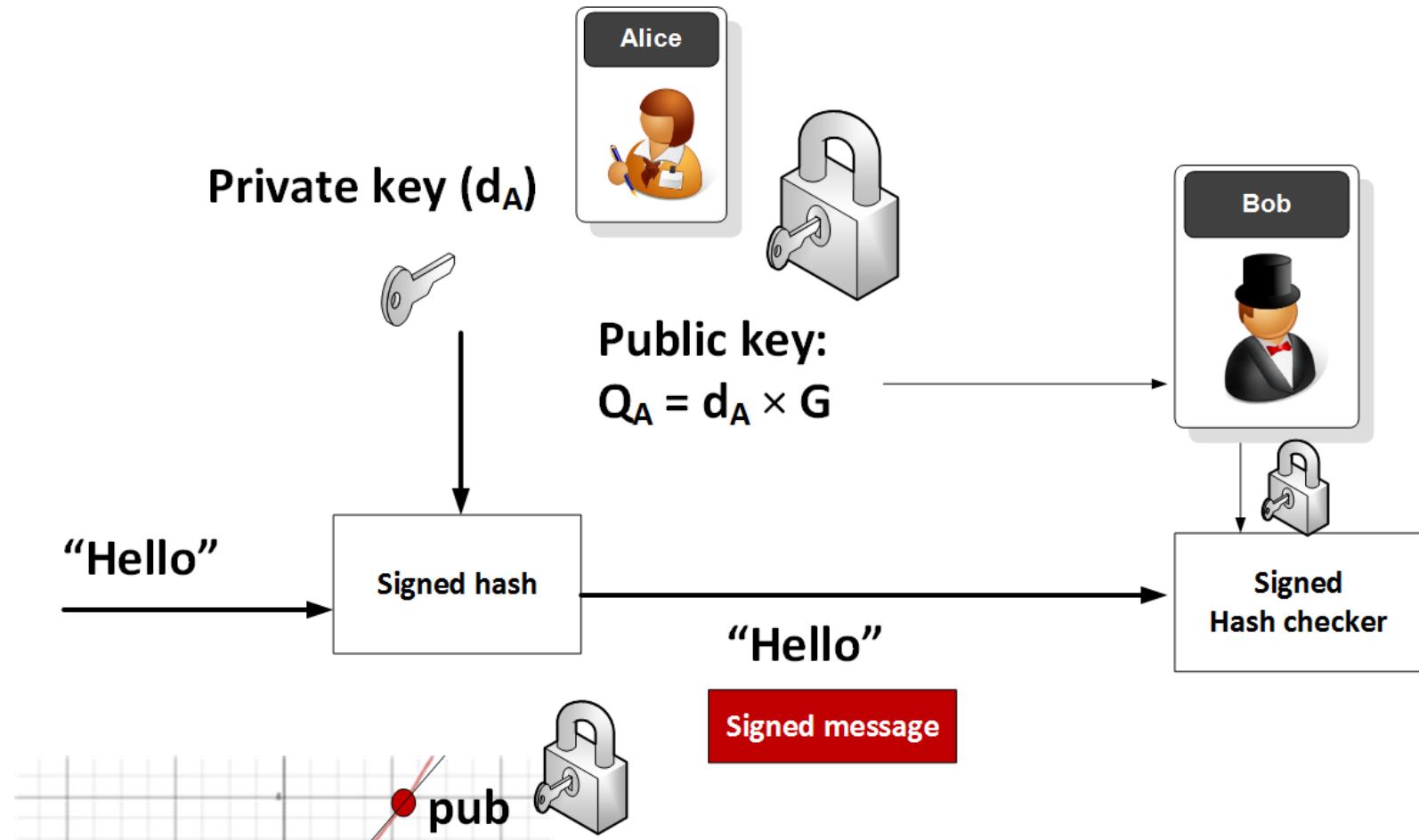
Merkle Trees



Signing



Signing (ECDSA)



Signing (ECDSA)

Message: Hello

Hash (SHA-256): 185f8db32271fe25f561a6fc938b2e264306ec304eda518007d1764826381969

=====Elliptic Curve details =====

N: 115792089237316195423570985008687907852837564279074904382605163141518161494337

G: (55066263022277343669578718895168534326250603453777594175500187360389116729240L,
32670510020758816978083085130507043184471273380659243275938904335757337482424L)

=====Create key pair =====

Private key: 54260937083493926038981685815910187164039687608704947340586607702205641918578

Public key: (51462476226125324693025684915790979951700251074620825319023668376690501350840L,
80137489009097522664481006712918181535677174259818547781755223887788639948939L)

=====Signature generation (r,s) =====

r= 63670406372804074606843871776644737079270928076738594276268091103814128899290

s= 13503713885368555959286645307370967261073993386809582203474575043238647211621

=====Signature verification (v==r) =====

v= 63670406372804074606843871776644737079270928076738594276268091103814128899290

Verified: True

Signing (Schnorr - native multisig)

f0dfd34db8d5ed88fd63b9158e3c607fb43b018cb83d9eb3286b37895e90f21c

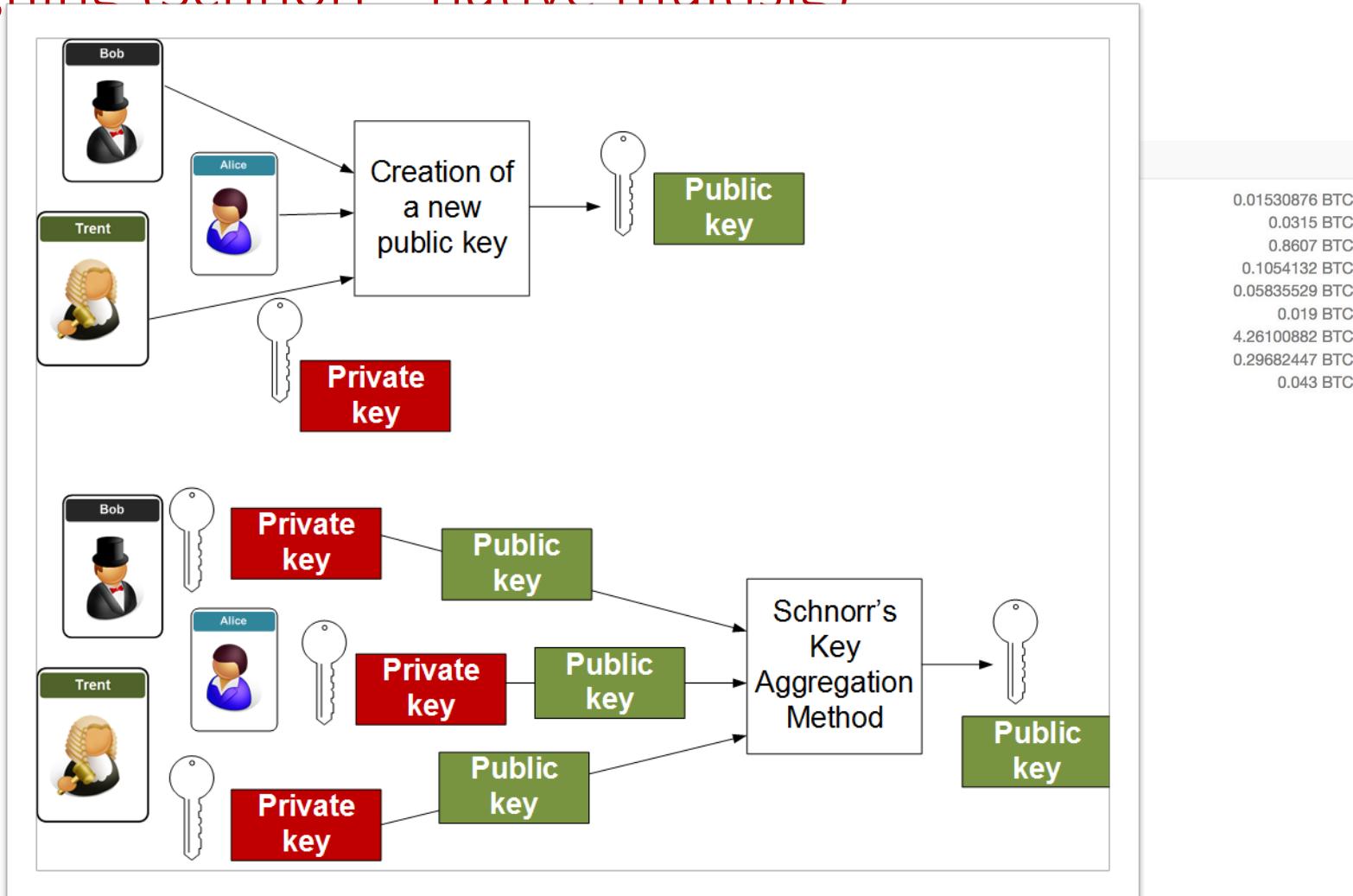
1Gu1fawp7rnHD24HiP1ui9CW2RNxmLSurb
1D5GExtk7K9MDGeNWvyqS5jn83JcPEPFPA
1PZTQGXqpgLWTb2LzuPyetcGtk3HyTSxpe
1MVHnU3Jzz7SEx3BDRnpLNjy7dGkzWxqs
137Vah6Gswbvh1yM8fLVrU3QJDkJWV5g9G
15RxPPh3SYFJTKbJo4AStXakbmLcEhugxd
1FxL1WANoS1VNP53hTaQG8iJxW7f3mEZj
1PuqSmYdRRxcvqvDLDid3FVuZLgzeSD5uo
1JHfqbTomt6nNWwjVKBDAVFU4Gmnu5j8aU
14Qvuut7hs0vM6dEqMGXPZZDmEWQCSPZPR
17Qzie5gtoSUpjQDgQeYy6oDet3QYnSz
1LTqSk6RABTyL3rhF4XeVTKFkuUJa5vEFq
1HHgwc4QXi7ox1ePS2G2QxkQs328mv2eRX
1HyvydVQ4Q3zHnrpC9RJ4BQX2VL7NnL2X9
1oXMPKD6vibCicjXNZCkbfd2aTyfNetAZ
1JniFCBcYnwJfH9UhoRGCWYCLZhDRKnJpE
1BrigDNcmzz8LL84B5hoNEeY75eoZkMSYg
132ixVuHnXy7W9Nu2ZXXKz1ZNMAbMzh9a
143pGz8vQ35WNceEdgcVtPDRxtJnst1eMjy
1PMHRabAPHwxqZXmrCGBSGyNxPtWyJ6ahL
1PJSL49UEF6D93vxhLrYZXVj2dDb9XY3gA
14i1bPWFrFa4D2qdtnFzgUbSPNTgEKDcT
17CxtBMmQ3t1gS4XpvRD8wEA717KGMXhYr
13riMjSfSqb89EsEFaemFXts399YyEZupL
1PiXXGhPu76p1udMzKLX3Twg6Lqiv5TzEw
1Bk7Ndxr7tYHdf6dV8fCMrMbW9hSX1mstA
1HL8nL4Gz4GmEZmsYJwNY7fPHMPecxYkxx
1MV6kHCXmj2Yn5Ze8xW45acTHXfLzfgh8
1J9vf5fxjC8Dwuupp1wu7p2UDL7ZGBCXfE



31r32c4hHUjwkcLCbXU5XebPQkEBkXkJew
1oXGCyr2Wup5dahXrwC5autn5b6j2GNj7
1Dj6q6oRsGSGtYdVMNTn1BroBDfi8QgKrS
1KtiphoFU576nRC1tkKRZvS2iVcfJWXdzW
15QcmiZxe7F2SHmrnsvZAcuKvgNEuJu14c
3DsXnWVo5He88VERXwaBHtgDgz3DR4QaHP
14sLwu4J18PTsB6GqFvLAveFWoyZRd38w
1GqhD8SNxw83C5HZ1WwZYWmtd4MVUTPwLi
19UyVvtaWpnVQmCVDewnNqNiaq4h7qvxi

0.01530876 BTC
0.0315 BTC
0.8607 BTC
0.1054132 BTC
0.05835529 BTC
0.019 BTC
4.26100882 BTC
0.29682447 BTC
0.043 BTC

Signing (Schnorr - native multisig)



Signing (Schnorr - native multisig)

Block #477120

Summary	
Number Of Transactions	129
Output Total	1,851.11145606 BTC
Estimated Transaction Volume	30.69594178 BTC
Transaction Fees	0.05159445 BTC
Height	477120 (Main Chain)
Timestamp	2017-07-23 04:46:31
Received Time	2017-07-23 04:46:31
Relayed By	BATPOOL
Difficulty	804,525,194,568.13
Bits	402742748
Size	45.275 kB
Weight	180.856 kWU
Version	0x20000012
Nonce	1832786046
Block Reward	12.5 BTC

Signing (Schnorr - native multisig)

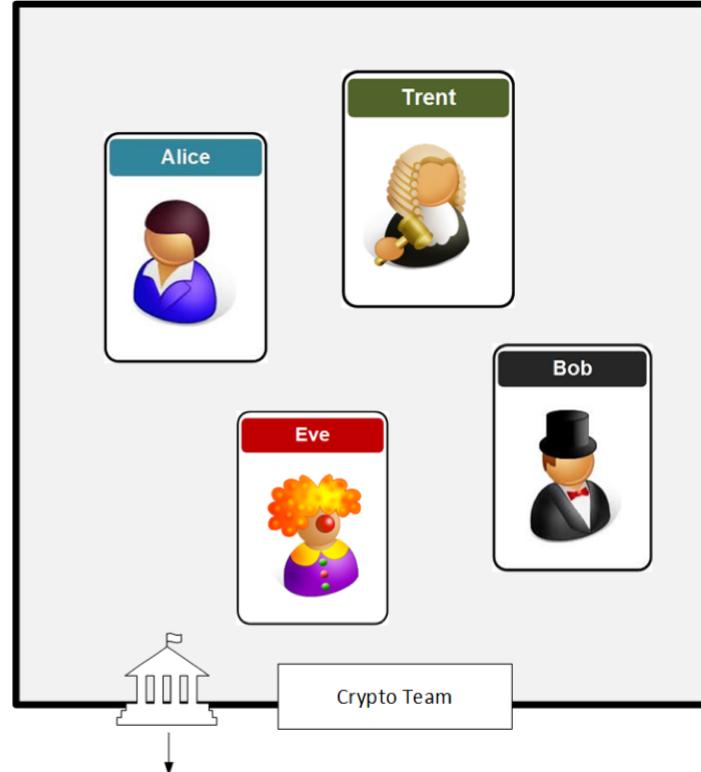
Block #477120

Summary	
Number Of Transactions	129
Output Total	1,851.11145606 BTC
Estimated Transaction Volume	30.69594178 BTC
Transaction Fees	0.05159445 BTC
Height	477120 (Main Chain)
Timestamp	2017-07-23 04:46:31
Received Time	2017-07-23 04:46:31
Relayed By	BATPOOL
Difficulty	804,525,194,568.13
Bits	402742748
Size	45.275 kB
Weight	180.856 kWU
Version	0x20000012
Nonce	1832786046
Block Reward	12.5 BTC

Hashes	
Hash	000000000000000015411ca4b35f7b48ecab015b14de5627b647e262ba0ec40
Previous Block	000000000000000022552c92fdc5ac6c31a95f54d9ed9fcdf0fe0ff134773
Next Block(s)	0000000000000000278fb704dfa2e6e517765144461f2fc5981da12a6b7b4
Merkle Root	8a13a3f9326b1073faa078007fadda8d1e9d46a50f4948055b7087c2ca8ee88d

Ring Signatures

I know one of you leaked the information.
But which of you was it?



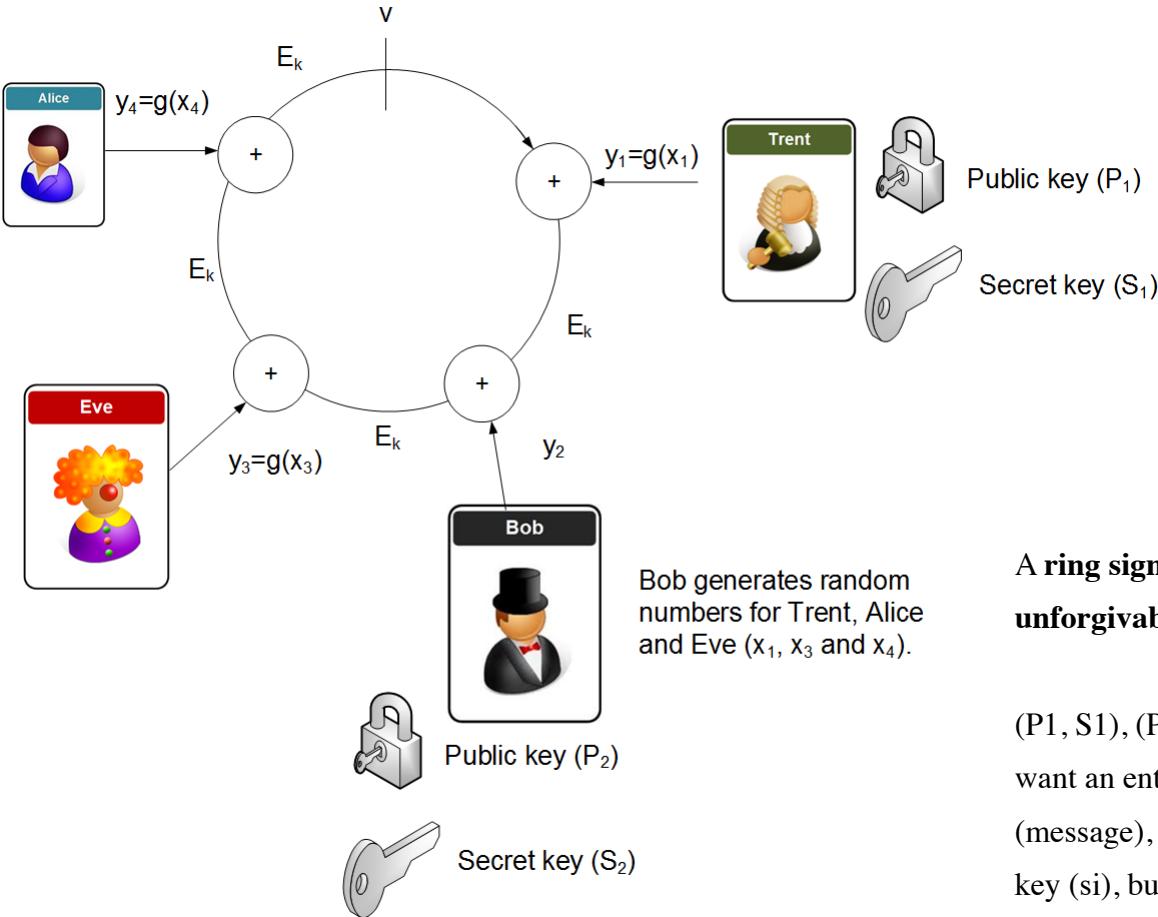
We have a secret.

Signed,
A member of the crypto team

ring signature, and
which provides
anonymity,
unforgivably and
collusion resistance.



Ring Signatures

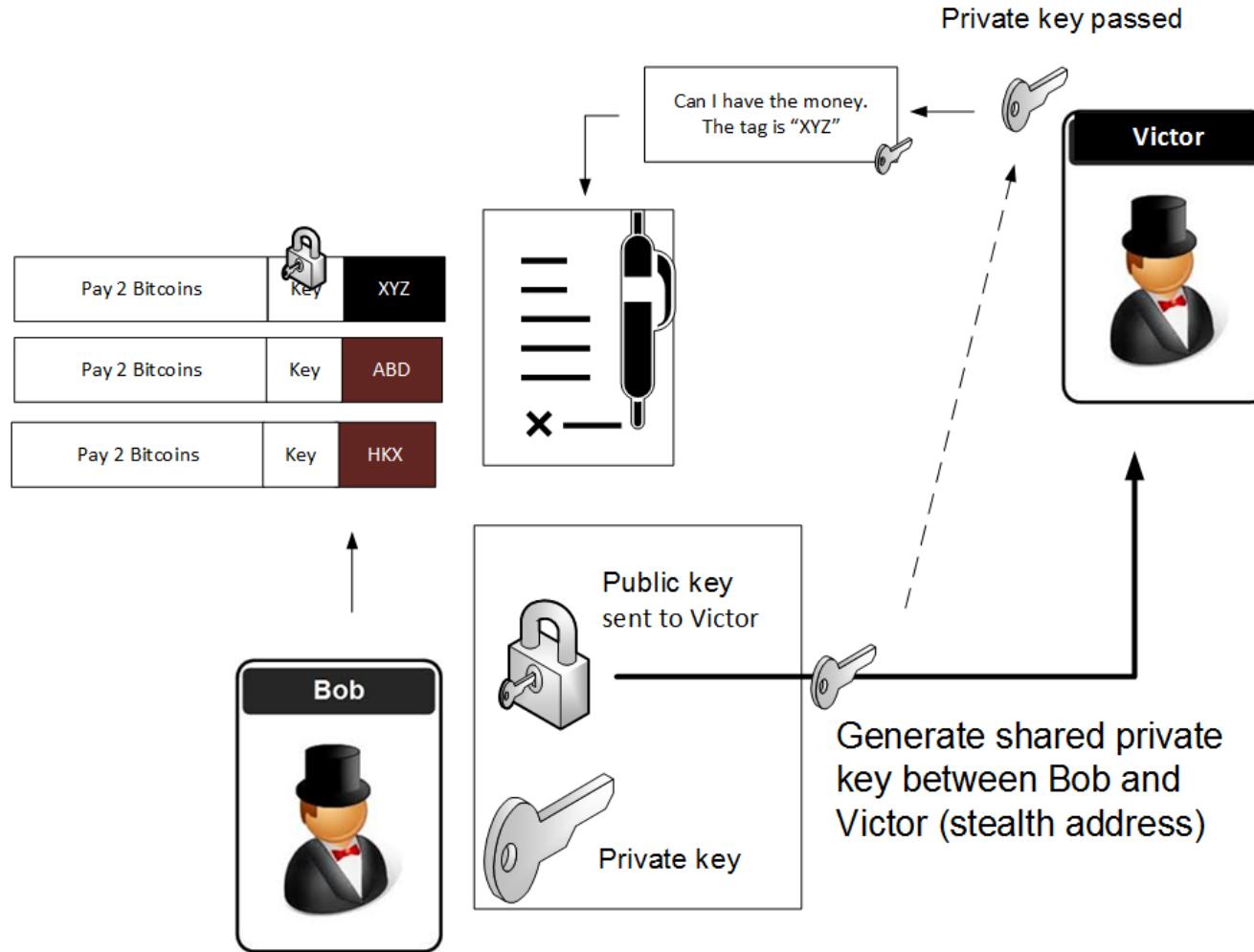


A **ring signature** provides **anonymity**, **unforgivably** and **collusion resistance**.

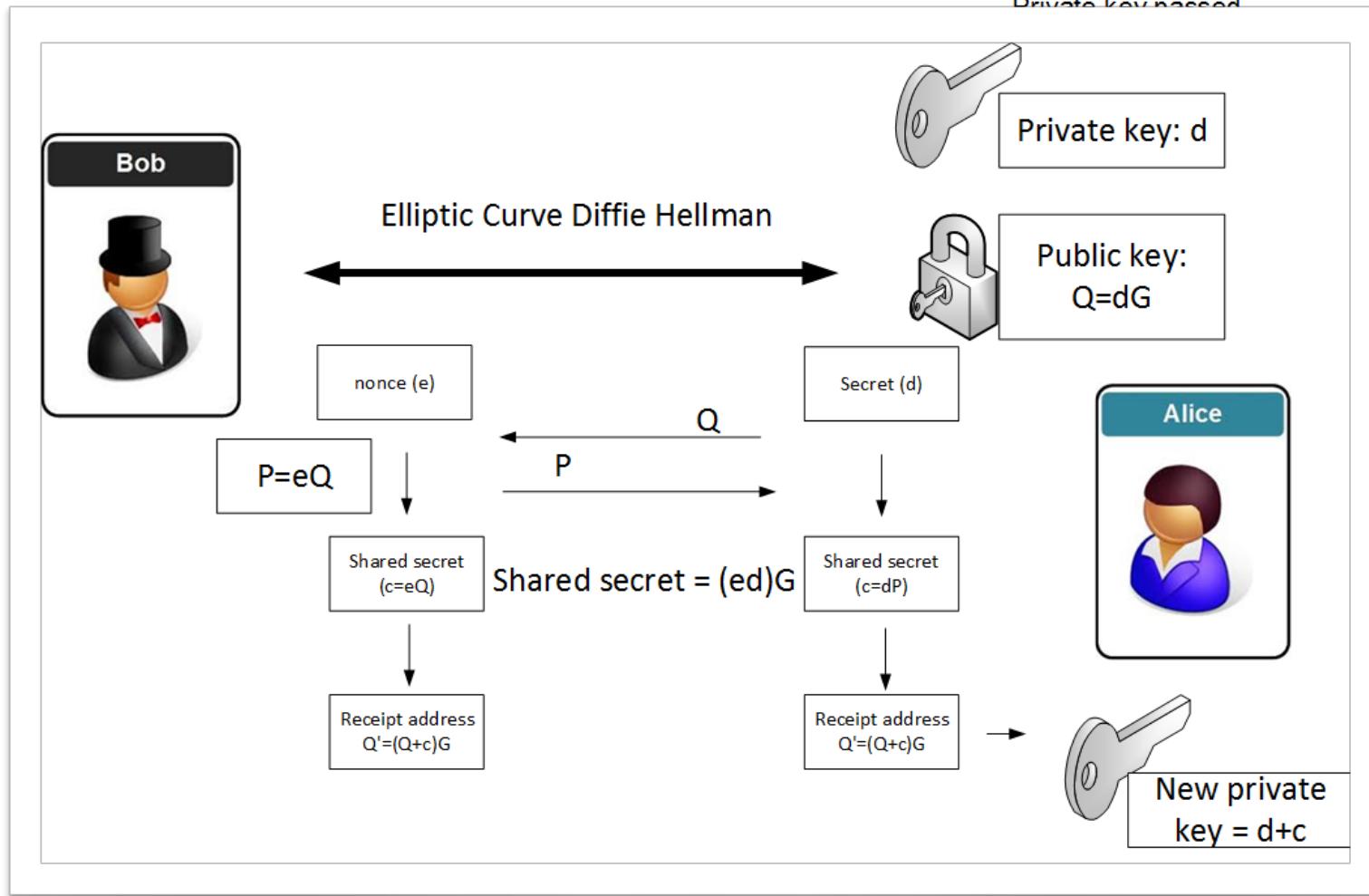
$(P_1, S_1), (P_2, S_2), \dots, (P_n, S_n)$. If we want an entity i to sign a message (message), they use their own secret key (s_i), but the public keys of the others in the group ($m, s_i, P_1 \dots P_n$)



Stealth Address



Stealth Address



Blockchain and Cryptocurrencies

Cryptocurrencies

Bitcoin addresses

Blockchain

Mining

Ethereum

Smart Contracts

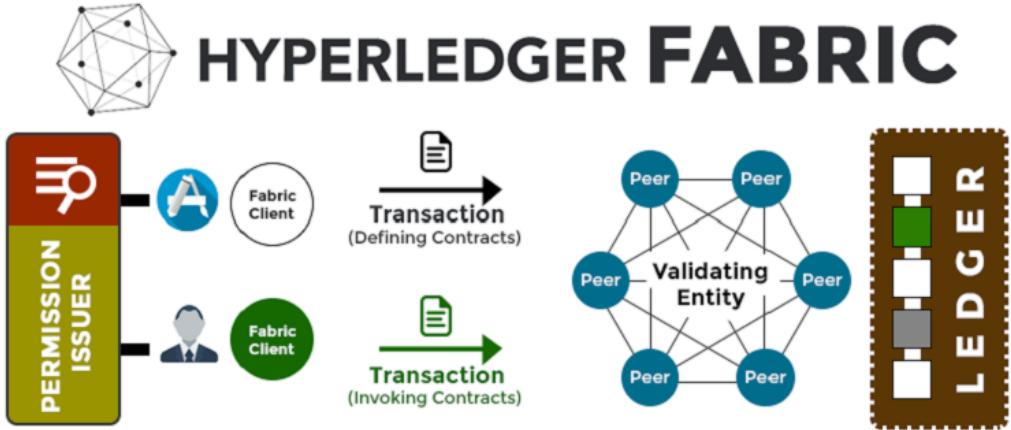
Hyperledger

Prof Bill Buchanan OBE

<https://asecuritysite.com/blockchain/>



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.

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

VS

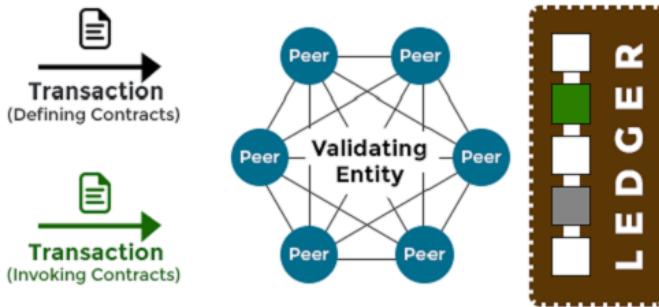
ETHEREUM

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.

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.

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.



HYPERLEDGER

Distributed Ledgers



Java-based Ethereum client



Permissionable smart contract machine (EVM)



Enterprise-grade DLT with privacy support



Decentralized identity



Mobile application focus



Permissioned & permissionless support; EVM transaction family

Libraries



Tools



Domain-Specific



Assets have key pairs (similar to SSL).

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

Blockchain and Cryptocurrencies

Cryptocurrencies

Bitcoin addresses

Blockchain

Mining

Ethereum

Smart Contracts

Hyperledger

Prof Bill Buchanan OBE

<https://asecuritysite.com/blockchain/>

