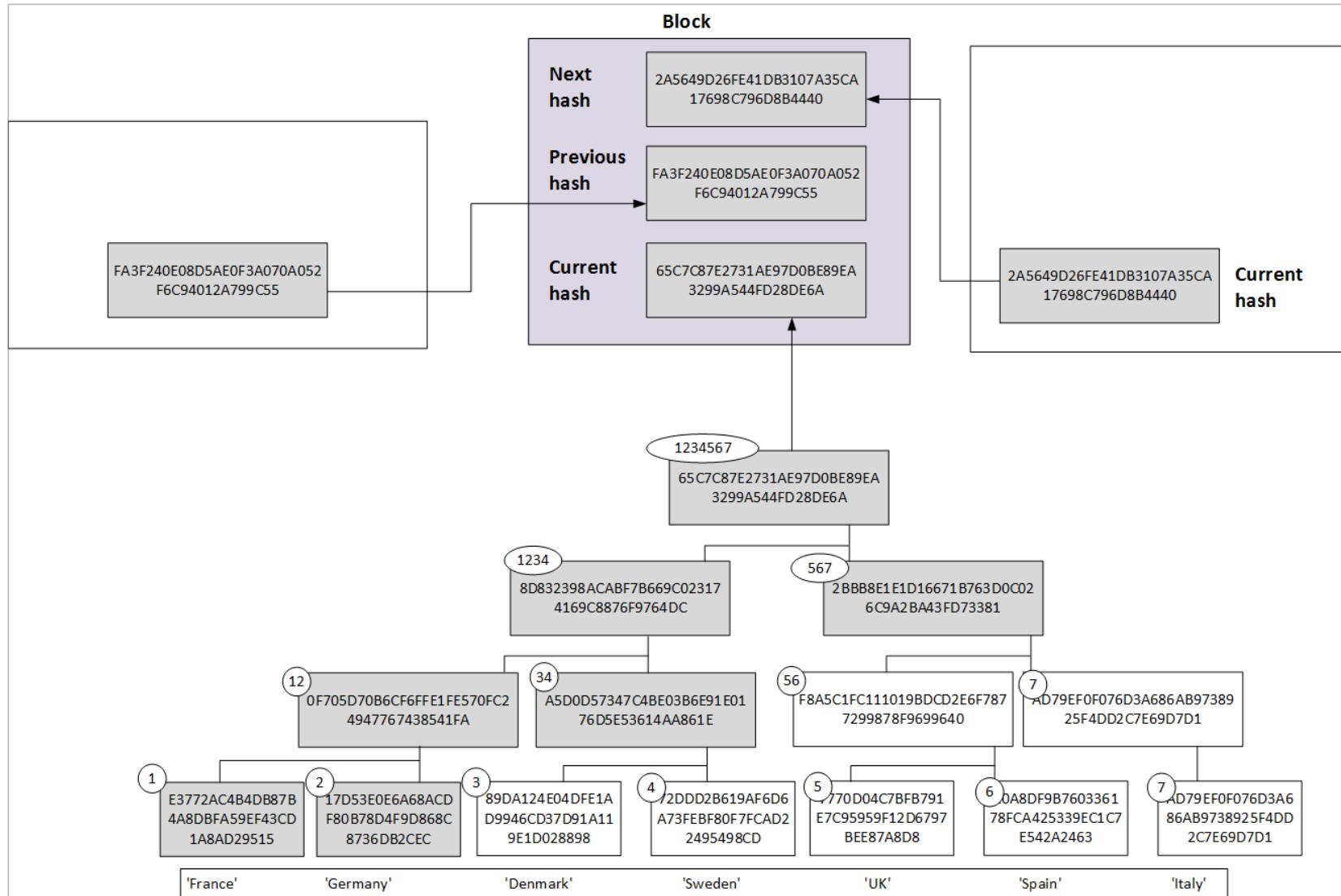


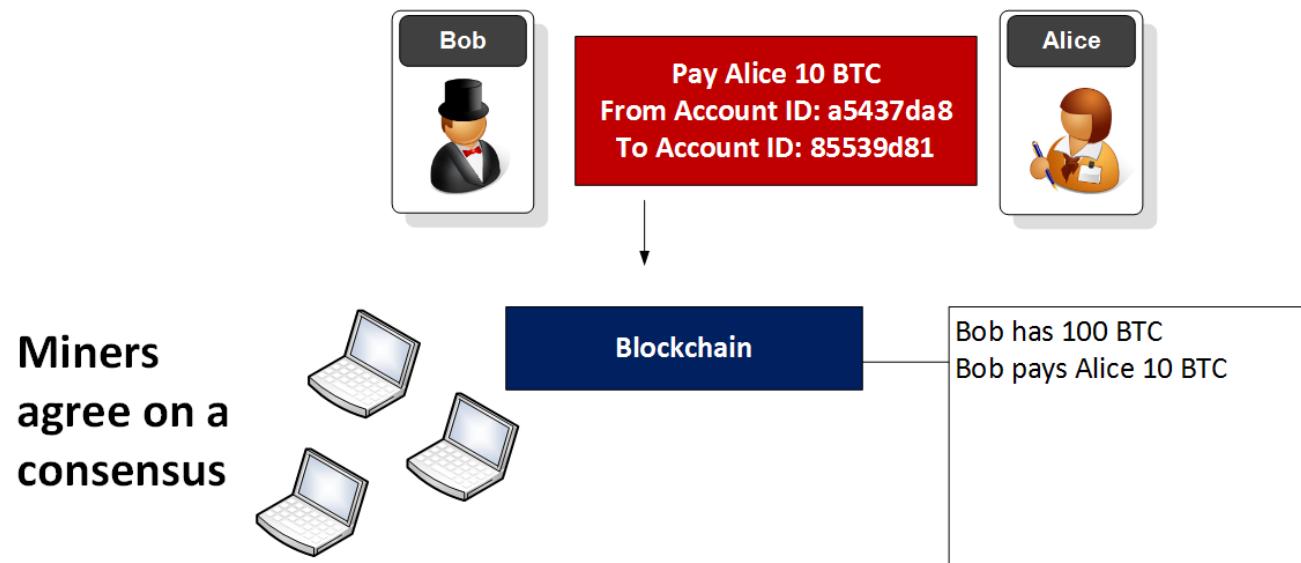
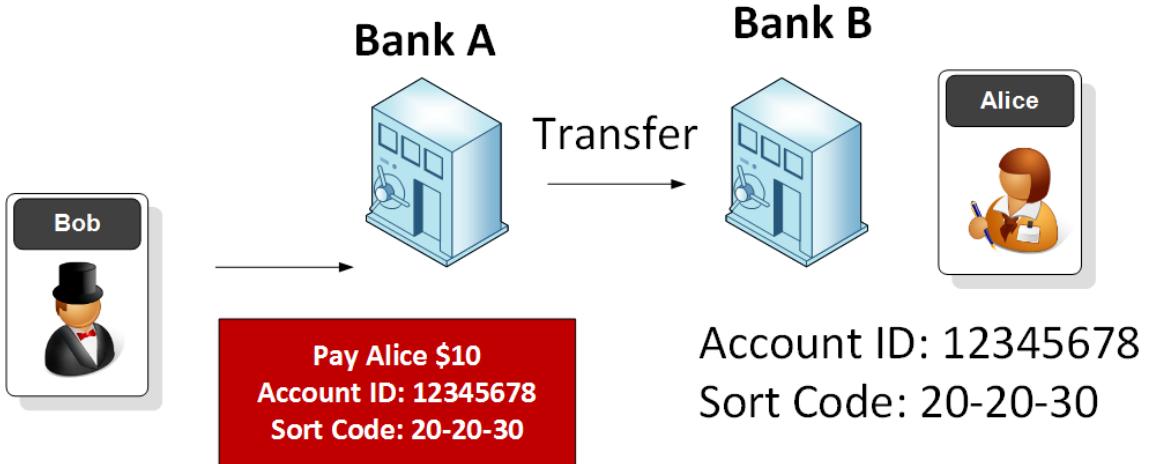
## Blockchain and Cryptocurrencies

Cryptocurrencies  
Bitcoin addresses  
Blockchain  
Mining









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	<a href="#">0 (Main Chain)</a>
Timestamp	2009-01-03 18:15:05
Received Time	2009-01-03 18:15:05
Relayed By	<a href="#">Unknown</a>
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 15 years old?

Block #0	
<b>Summary</b>	
Number Of Transactions	1
Output Total	50 BTC
Estimated Transaction Volume	0 BTC
Transaction Fees	0 BTC
Height	0 ( <a href="#">Main Chain</a> )
Timestamp	2009-01-03 18:15:05
Received Time	2009-01-03 18:15:05
Relayed By	<a href="#">Unknown</a>
Difficulty	1
Bits	486604799
Size	0.285 kB
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?

## Bitcoin: A Peer-to-Peer Electronic Cash System

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

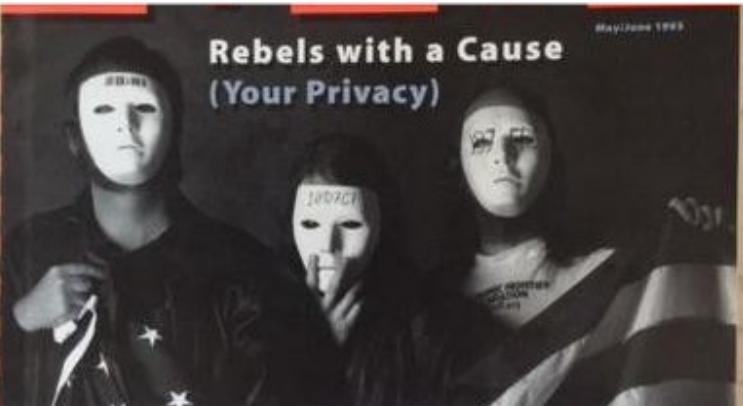
**Abstract.** A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required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



## Electronic Cash System

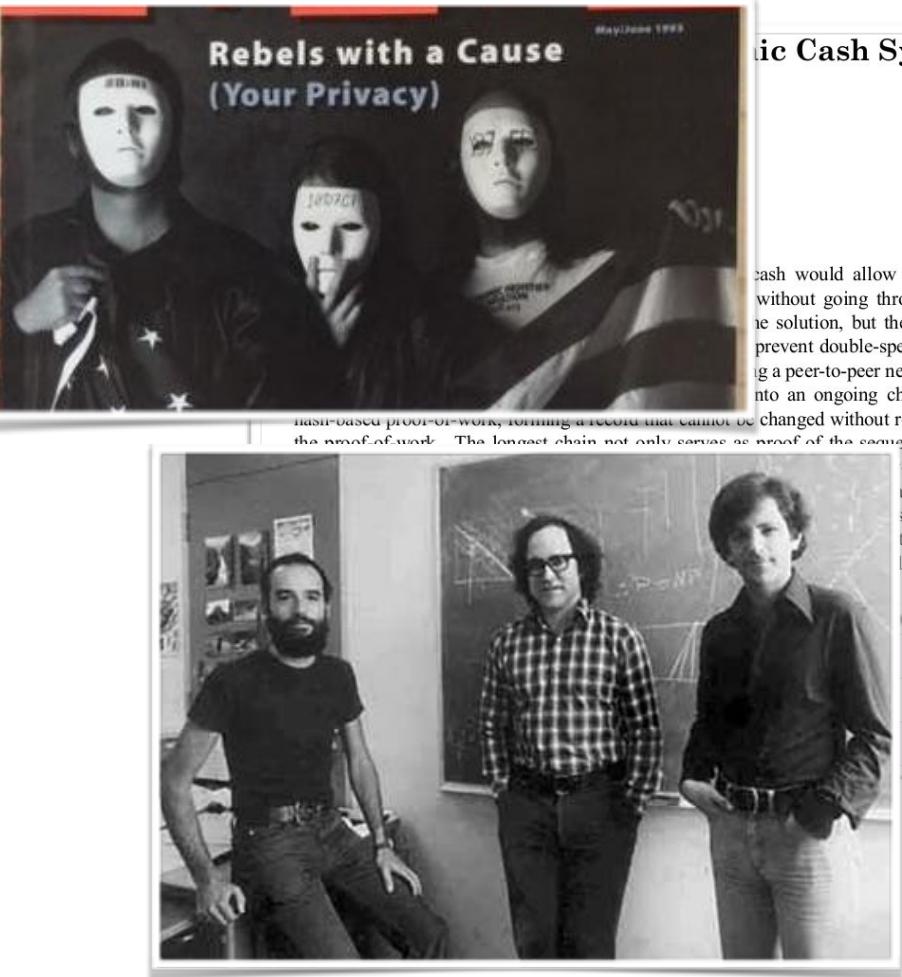
cash would allow online shopping without going through a central solution, but the main problem is how to prevent double-spending. By putting the transaction into an ongoing chain of blocks based on proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest 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 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?



## Electronic Cash System

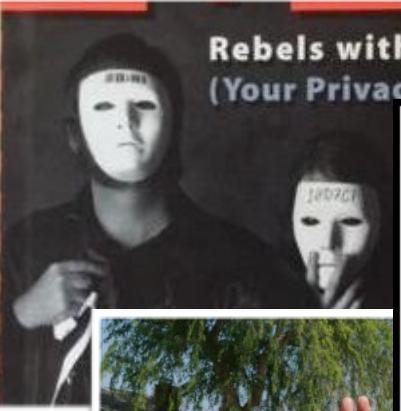
cash would allow online  
without going through a



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?



Rebels with a Cause  
(Your Privacy)

May/June 1998

nic Cash System

Donald J. Trump  @realDonaldTrump

Following

The failing financial system has disgraced the American people for years. Which is why I gave you Bitcoin, I am Satoshi Nakamoto. Change the financial laws now in favour of Bitcoin.

RETWEETS LIKES

7,463 17,361

6:09 AM - 1

 7.5K  17K 



His work was a hotch-potch of differing cryptography methods forced in the 1970s - and also of movement which 1990s, and was Hughes, Tim May

January 2018,  
he 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 caught?

Published on December 21, 2017

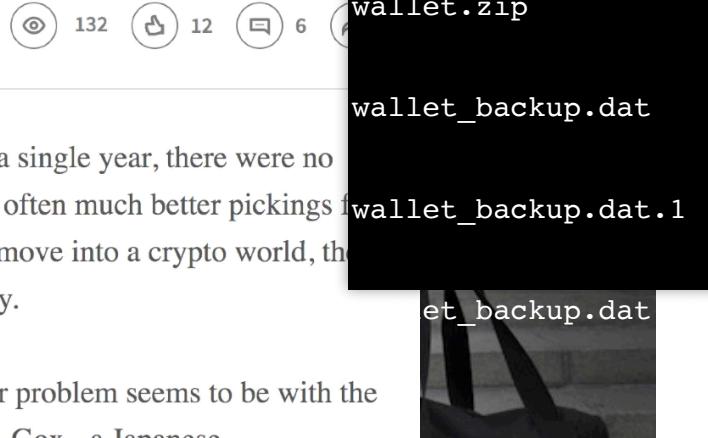
[Edit article](#) | [View stats](#)



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

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

```
112.92.122.186 - - [17/Oct/2017:07:57:00 +0000] "GET /didiestersteins.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 /didiestersteins.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/2017:07:57:09 +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" 404 270 "-" "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 /didiestersteins.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 /didiestersteins.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" 404 282 "-" "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.zip HTTP/1.1" 404 282 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10.8; rv:21.0) Gecko/201001 Firefox/21.0"
```



is to be with the

ese

he exchange of

Dimitrios Slamaris

@dim0x69

Follow

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

```
{ "id": 168440}, {"id": 943614}, {"id": 263038}, {"id": 472772}, {"id": 771759}, {"id": 817614}, {"id": 537357}
```

# 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 -0400]	"GET /didiestersteven/backups/bitcoin_walle...
112.92.122.186	-	[17/Oct/2017:07:57:07 -0400]	"GET /wallet.dat.H...
112.92.122.186	-	[17/Oct/2017:07:57:09 -0400]	"GET /bitcoin_wall...
112.92.122.186	-	[17/Oct/2017:07:57:10 -0400]	"GET /backups/bitc...
112.92.122.186	-	[17/Oct/2017:07:57:20 -0400]	"GET /wallet.tar.H...
112.92.122.186	-	[17/Oct/2017:07:57:20 -0400]	"GET /didiestersteven...
112.92.122.186	-	[17/Oct/2017:07:57:40 -0400]	"GET /home/.bitcoinc...
112.92.122.186	-	[17/Oct/2017:07:57:41 -0400]	"GET /home/.bitcoinc...
112.92.122.186	-	[17/Oct/2017:07:57:41 -0400]	"GET /home/.bitcoinc...
112.92.122.186	-	[17/Oct/2017:07:57:45 -0400]	"GET /bitcoin_walle...
112.92.122.186	-	[17/Oct/2017:07:58:08 -0400]	"GET /wallet.dat.z...
112.92.122.186	-	[17/Oct/2017:07:58:09 -0400]	"GET /home/ubuntu/...
112.92.122.186	-	[17/Oct/2017:07:58:29 -0400]	"GET /datadir/walle...
112.92.122.186	-	[17/Oct/2017:07:58:31 -0400]	"GET /wallet>20.3%



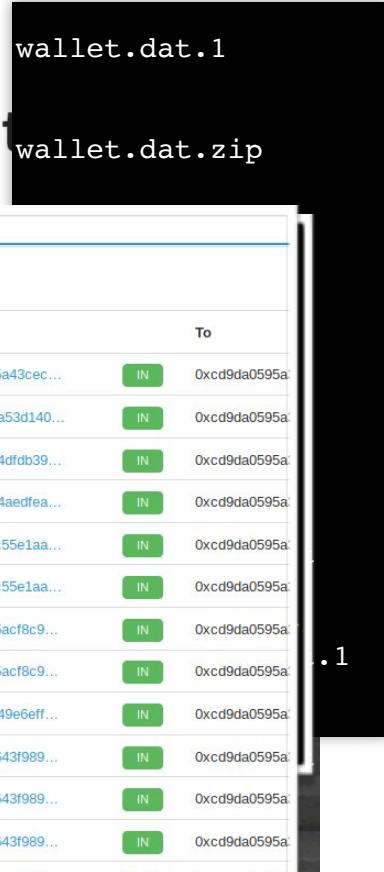
Dimitrios Slamaris

@dim0x69

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

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

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...
0x37819ff1ff137cce7...	4494468	2 days 8 hrs ago	0xbfbac940ec55e1aa...	IN 0xcd9da0595a...
0xd32fbe5771f291b...	4494300	2 days 8 hrs ago	0xbfbac940ec55e1aa...	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...
0xe3cb8b7b8576a35...	4457650	8 days 6 hrs ago	0x54160297ff7892b...	IN 0xcd9da0595a...
0x51029839c261899...	4456959	8 days 9 hrs ago	0xd58b7ae09f88e0f...	IN 0xcd9da0595a...



.1

**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 are my rights to privacy?

What is consent?

Who's laws do I comply with?

Why does fiat currency exist?

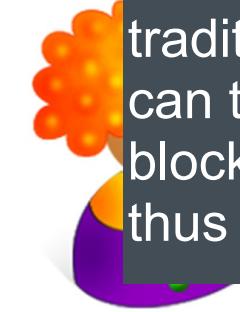
SP62 UUE

**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.



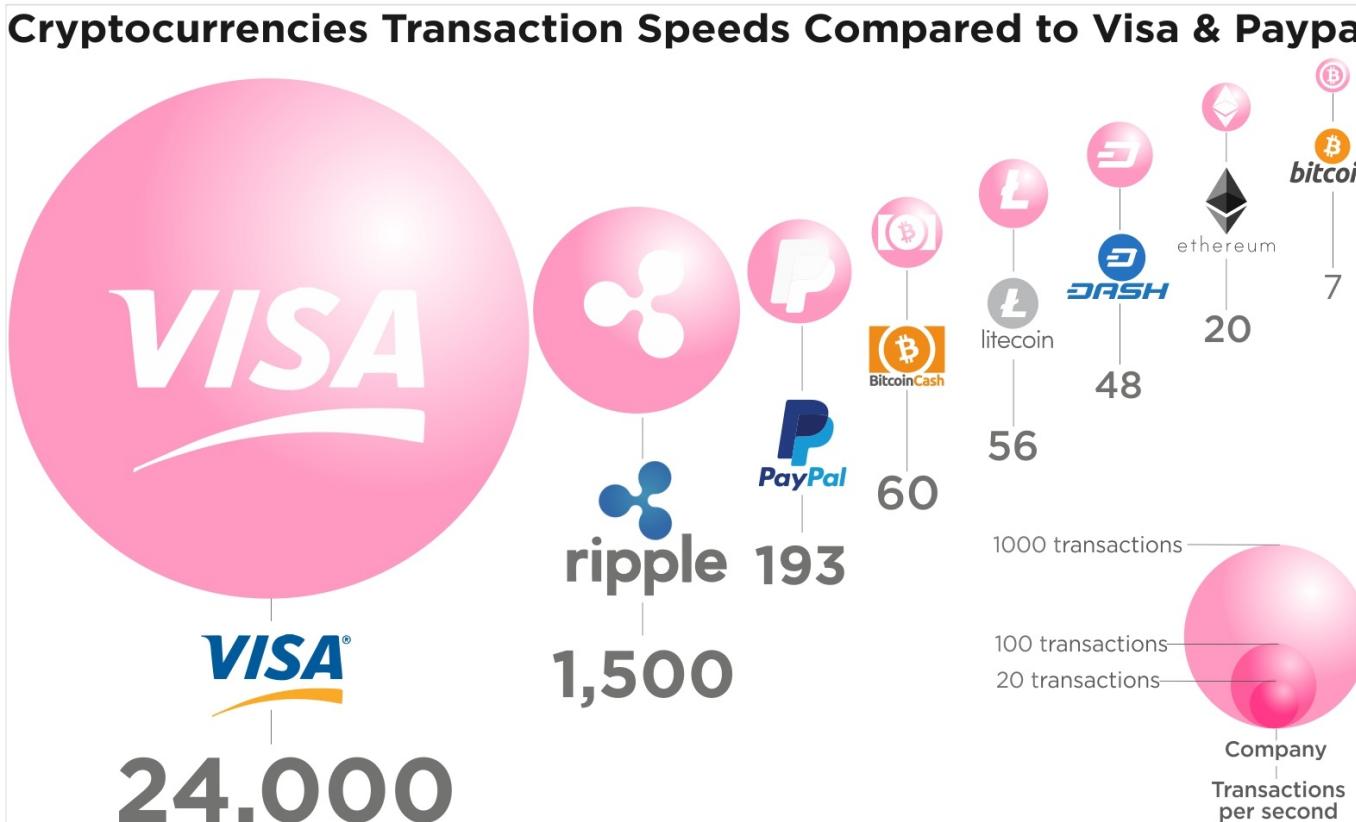
Dea

**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.**

Lisk, have platform This generation adds logical operations. the Blockchain.

**3rd Generation.** The distributed system traditional Blockchain can take some time 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 their respective we

BLOCKS. WITH DAG,  
thus speeds up the



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.
- 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.



# 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

# 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	<a href="#">Related Tags - Unspent Outputs</a>	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	3EDzR4QKeGJyCZWXMF1kAGqj8gHNQ798sF	No. Transactions	1
Hash 160	897d25262f68b8a8d4e2adf2ab082ce0f58a69d1	Total Received	2,034.668943 BTC
Tools	<a href="#">Related Tags - Unspent Outputs</a>	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
		3Mfly7hJB44kY7YHRgCuJ7JgpzL1tSqWg	15.6262 BTC
		37K7vhCNe8VmLnhdjBRRBZBfEL5zZhI94Zg8	0.31678 BTC
		1FKjowv879X5RGDeU21zzxirvbgNoeGaJr	0.169 BTC
		3BazbNWURUzdk58myGn1V9F6HPabtUjZwN	0.01265 BTC
		3HCJDcEjzHyip6TJ3kwQQajGxJW6scbzGB	13,067.17305362 BTC
			13,083.32386362 BTC

# Genesis Record

Summary	
Address	<a href="#">3EDzR4QKeGJyCZWXMLF1kAGqi8gHNQ798sF</a>
Hash 160	<a href="#">897d25262f68b8a8d4e2adf2ab082ce0f58a69d1</a>
Tools	

Transactions	
No. Transactions	1
Total Received	<a href="#">2,034.668943 BTC</a>
Final Balance	<a href="#">2,034.668943 BTC</a>

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

## Transactions (Oldest First)

[Filter ▾](#)[CRYPTOMATE](#)

Buy Bitcoin, Ethereum, Ripple and 13 other coins via Instant Bank Transfer with no registration required.

Buy Now with GBP

Ad[67079f670818b0e44ed70399bcdcc4664a8595fb6f90f8538b7821c7ac889bbe8](#)

2017-11-13 19:10:37

[3HomPY371CsvvjaCZj7ExLf1TcSQ82HuG](#)[3EDzR4QKeGJyCZWXMLF1kAGqi8gHNQ798sF](#)

2,034.668943 BTC

1 Confirmations

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

# Bitcoin transactions and valuation



# Bitcoin trading volume

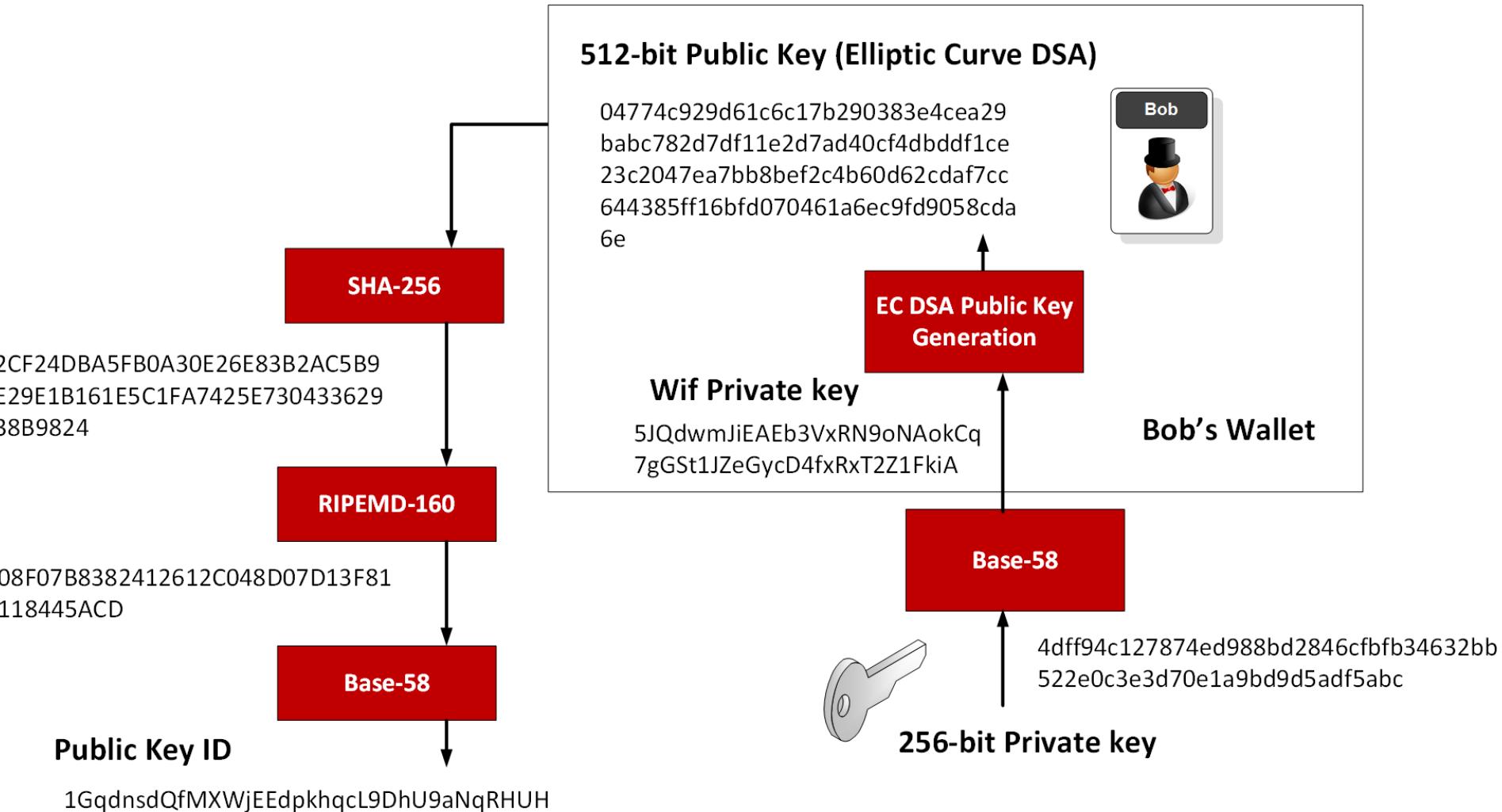


## Blockchain and Cryptocurrencies

Cryptocurrencies  
**Bitcoin addresses**  
Blockchain  
Mining



# Bitcoin Wallet and Addresses

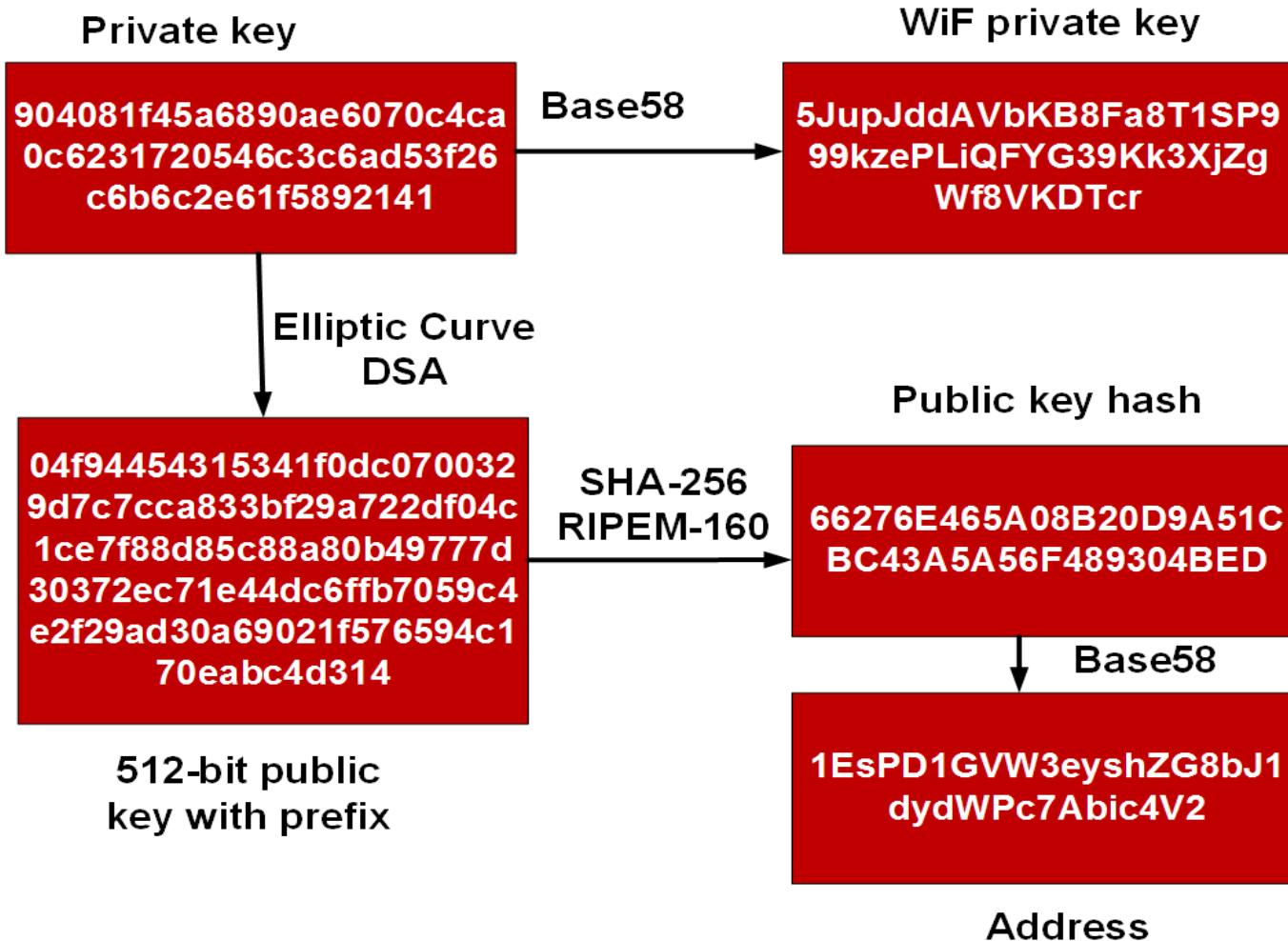


Summary	
Address	<a href="#">1JyvJ5TcN2hzu7dDEeVuuikgHtpwU8NE6</a>
Hash 160	<a href="#">c53deb8dda6fb0c388da19fbcf63270cc4f4cbfd</a>
Tools	<a href="#">Related Tags</a> - <a href="#">Unspent Outputs</a>

Transactions	
No. Transactions	20
Total Received	<a href="#">0.64531495 BTC</a>
Final Balance	<a href="#">0 BTC</a>

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





Private key:

4c0333a50b7724c71b89df148d83f64d49d896e21701007eeb8cada52744aca2

Public key:

0489fc7b8c3f655a10840d35c76ebb5596694045e49e940fb1e7a759da4edf0fafc45b  
bbea6f5a56abf14c145c529c8eda9d3ad606f3a0bf4ca01ce991d4987b97

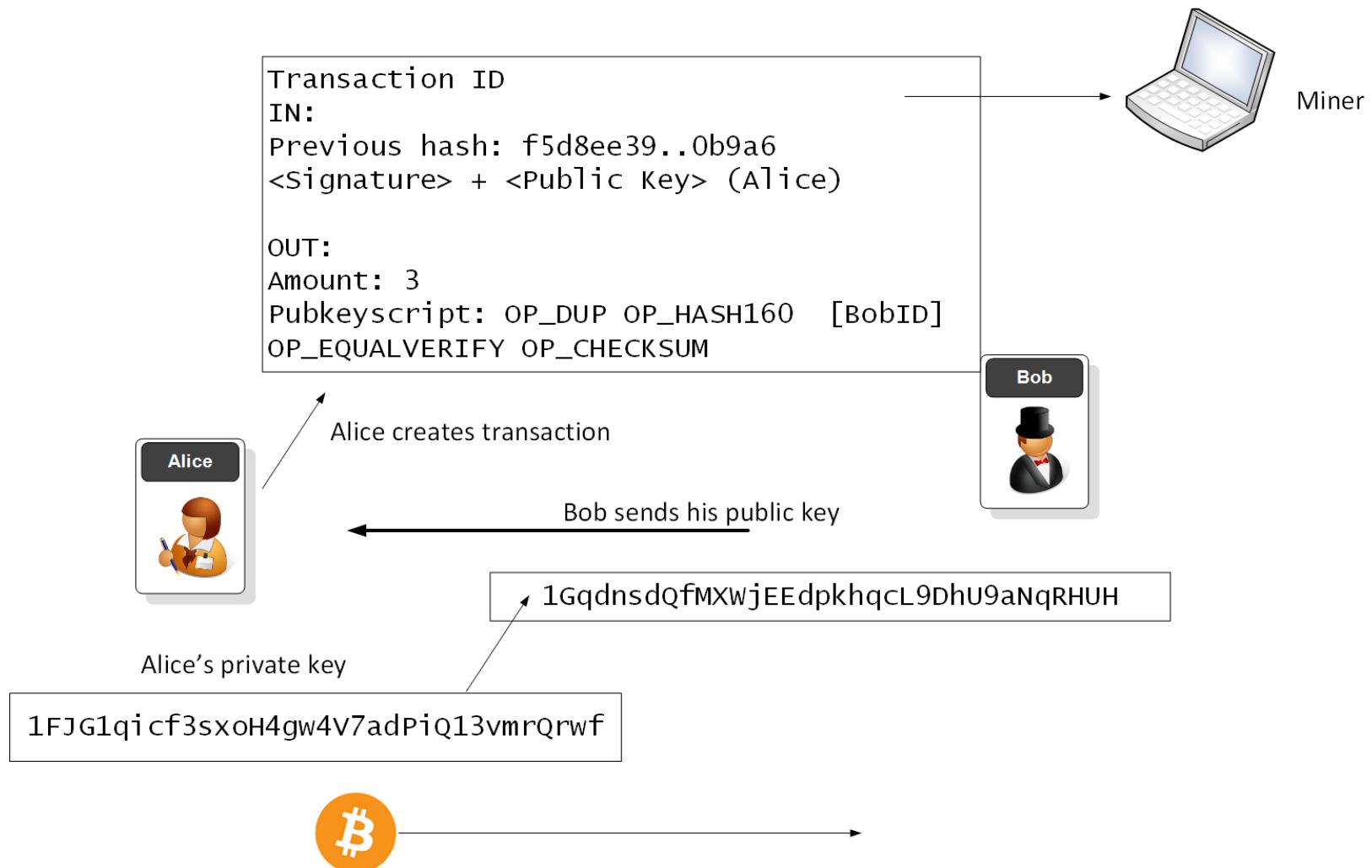
Wif: 5JPmDetQXXvc5aT5efyrg7BxHbH4135owRzq9DD7n2eWQCta5MN

Address: 16RAf9CjnstWCfBJGfrzSSMfTeHJVt8QWw

Signed:

4830450220264c4dce5f1cf0dff8d32d21c5d5cf6baed428b12ae6f8594924246a611e  
9ee602210096ef8e7054ec7a39f0a35d8de3fd50090b1d125c0e795af8cf3d577b676  
407ca01410489fc7b8c3f655a10840d35c76ebb5596694045e49e940fb1e7a759da4e  
df0fafc45bbbea6f5a56abf14c145c529c8eda9d3ad606f3a0bf4ca01ce991d4987b97

# Bitcoin transaction

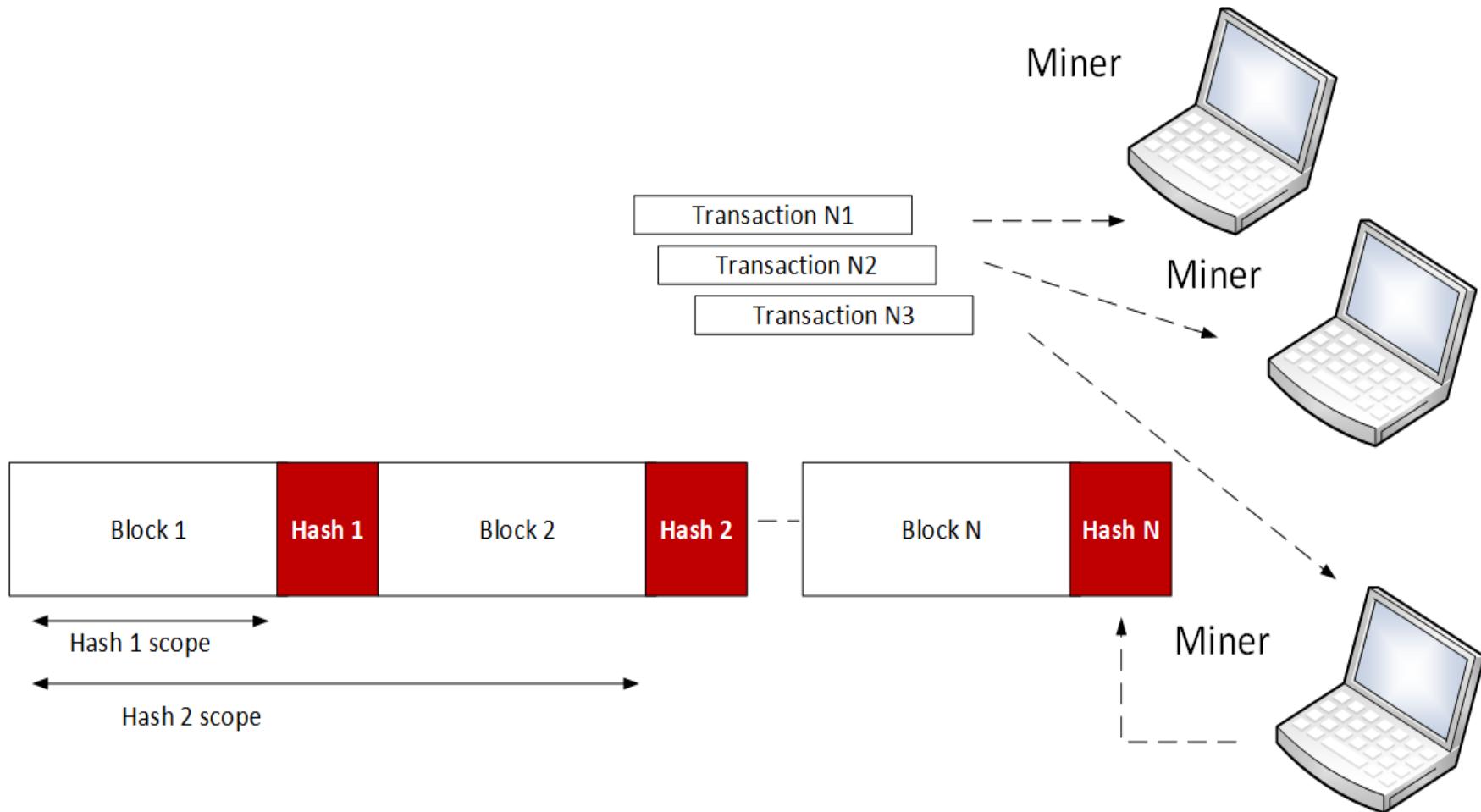


## Blockchain and Cryptocurrencies

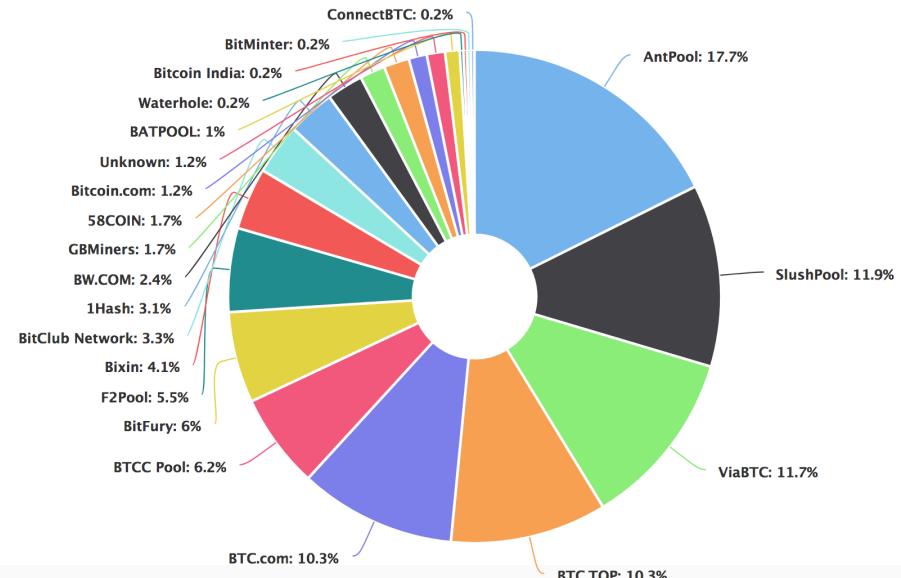
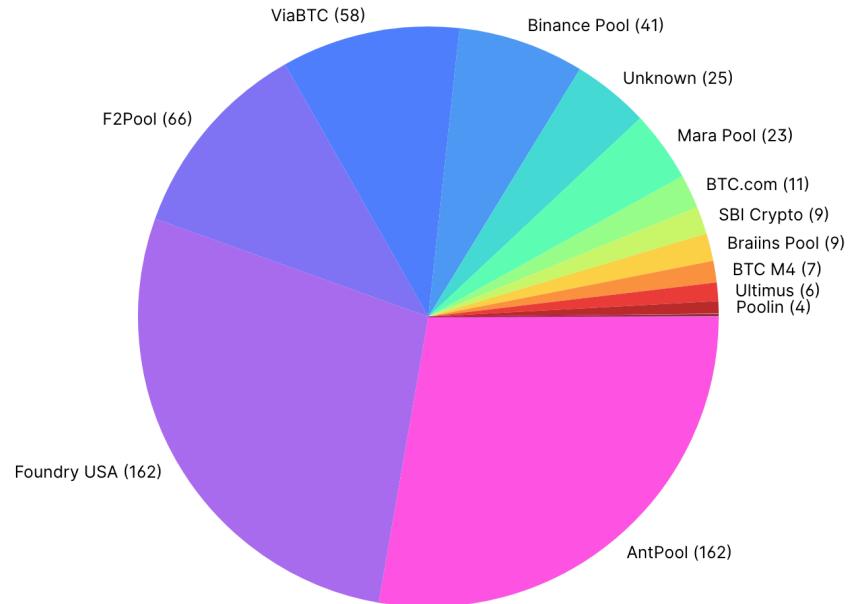
Cryptocurrencies  
Bitcoin addresses  
Blockchain  
Mining



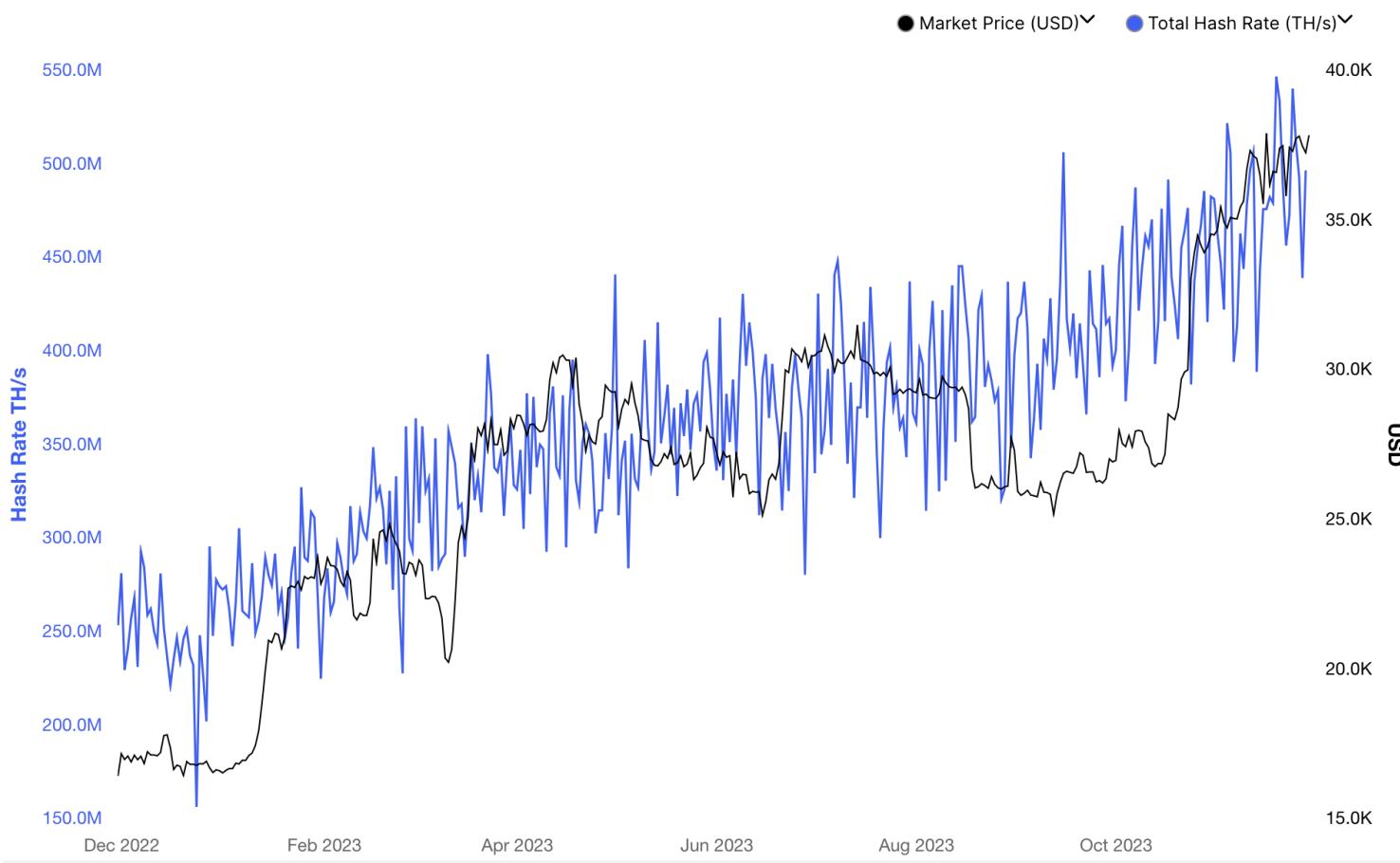
# Mining process



# Successful miners (2023 and 2018)



# Hash Rate TH/s



# Mining Processes

- Hash
  - 0000000000000000d98e57b83834a2d1f4387a93d06861bcf3ea5fc498bd55
- Previous Block
  - 000000000000000012138e05f0779765277a9d2ab7e4a2a70882790abf98a0c

# Blocks

## Block 765355 ⓘ

This block was mined on November 30, 2022 at 8:25 PM GMT by [F2Pool](#). It currently has 1 confirmations on the Bitcoin blockchain.

The miner(s) of this block earned a total reward of 6.25000000 BTC (\$106,670.31). The reward consisted of a base reward of 6.25000000 BTC (\$106,670.31) with an additional 0.17003811 BTC (\$2,902.08) included in the block. The Block rewards, also known as the Coinbase reward, were sent to this [address](#).

A total of 1,185.92184184 BTC (\$20,240,424.56) were sent in the block with the average transaction being 0.54350222 BTC (\$9,276.09).

Hash	00000000000000000000000000000000385b3a5aa6ba0c4e9d2bf80a54bda9251b96d5f50b2a3	📋
Confirmations	1	
Timestamp	2022-11-30 20:25	
Height	765355	
Miner	<a href="#">F2Pool</a>	
Number of Transactions	2,182	
Difficulty	36,950,494,067,222.41	
Merkle root	158dbb68a396c612a3c81b063ef4f52d65d81e1e592c190f8bf94c7717e97755	
Version	0x20000004	
Bits	386,375,189	
Weight	3,998,135 WU	
Size	1,469,990 bytes	
Nonce	893,356,266	

## Blockchain and Cryptocurrencies

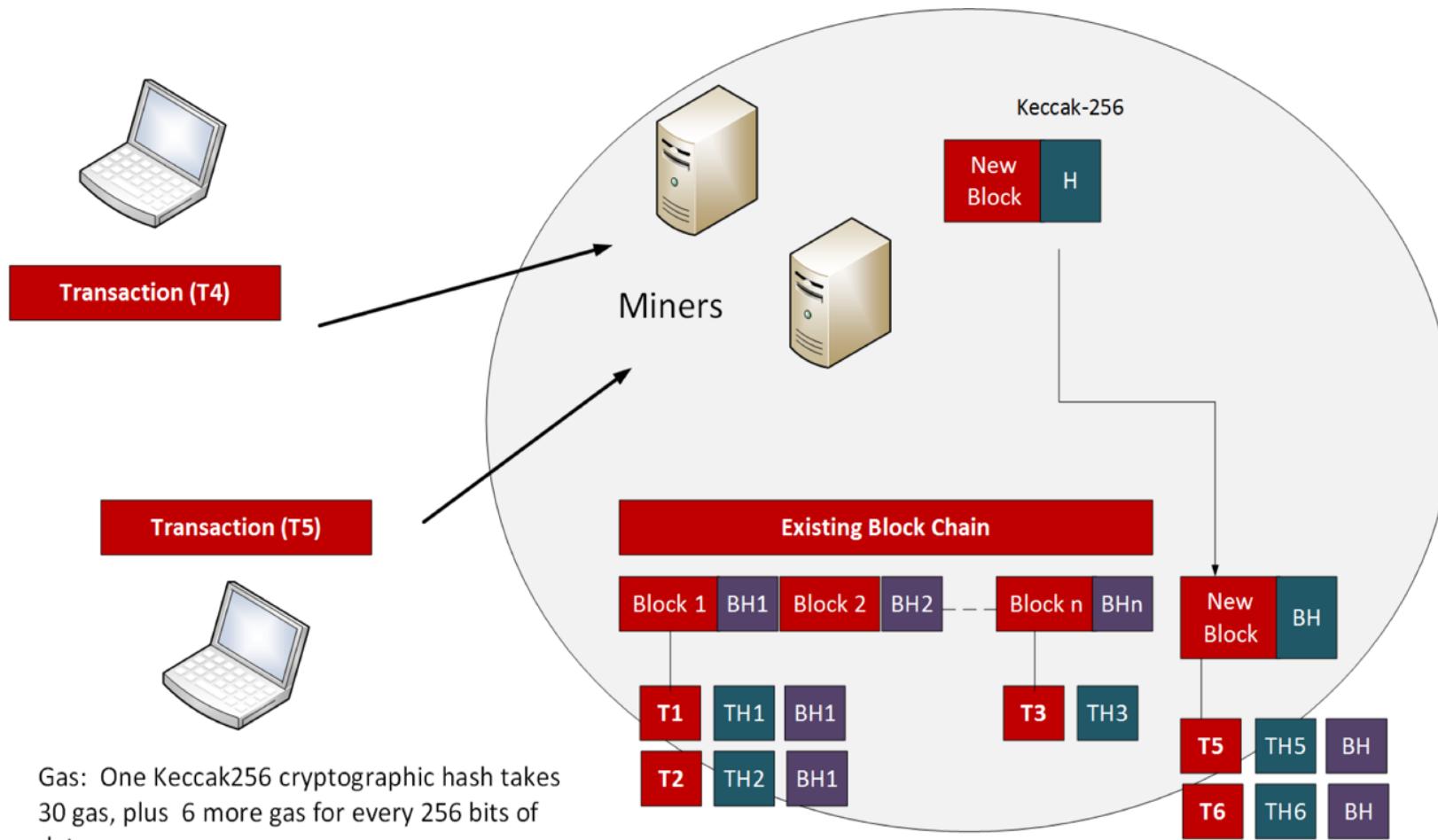
Cryptocurrencies  
Bitcoin addresses  
Blockchain  
Mining



# History

- Ethereum was created by Vitalik Buterin 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).

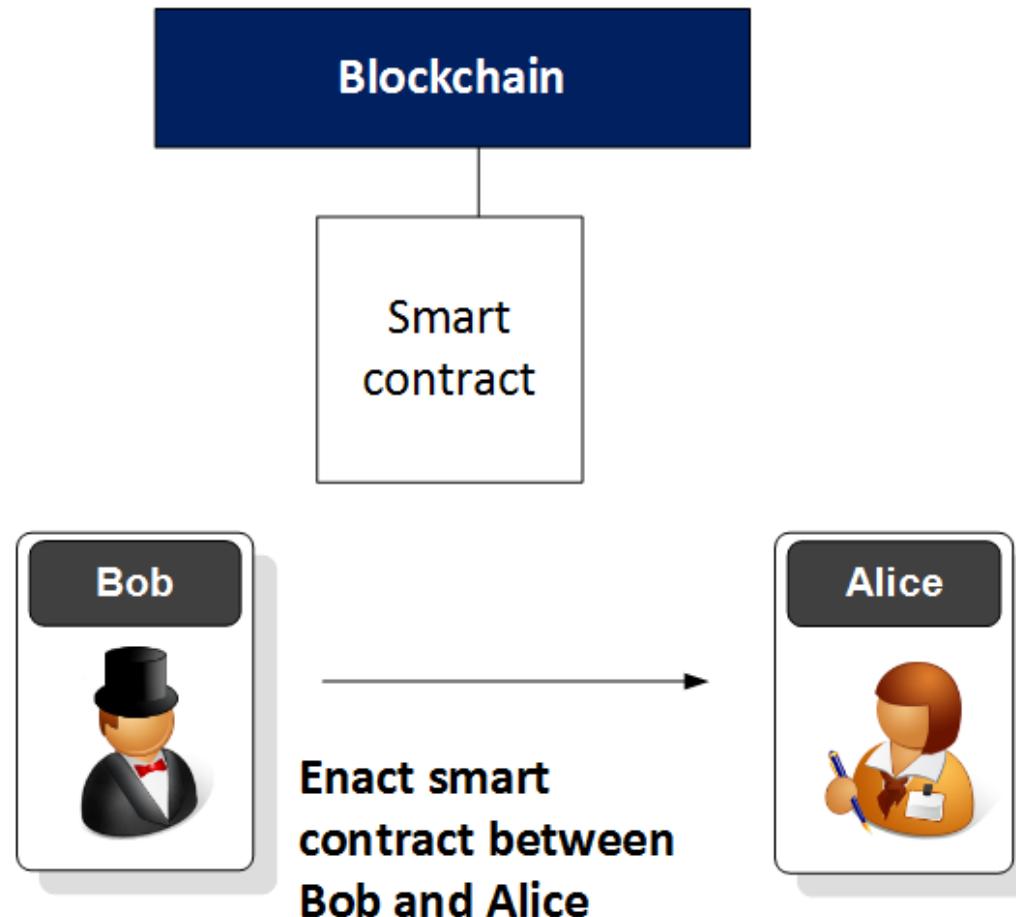
The gas price per transaction aims to overcome denial of service and infinite loops, and where 0.00001 Ether or 1 Gas is used to execute a line of code. If there is not enough Ether, no transaction will be performed. It also aims to make code designers efficient and not use waste bandwidth and CPU utilization.

## Blockchain and Cryptocurrencies

Cryptocurrencies  
Bitcoin addresses  
Blockchain  
Mining



# 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

The screenshot shows the Truffle UI interface for deploying and running transactions. On the left, there's a sidebar with various icons and settings:

- ENVIRONMENT**: Set to "Injected Provider - MetaMask".
- ACCOUNT**: Shows an account balance of 0xbB1...52233 (0.7850972).
- GAS LIMIT**: Set to 3000000.
- VALUE**: Set to 0 Wei.
- CONTRACT**: Compiled by Remix, named mymath - examples\_csn09112/exan
- Deploy** button.
- Publish to IPFS** checkbox.
- At Address** and **Load contract from Address** buttons.

The main area displays the Solidity code for the `mymath` contract:

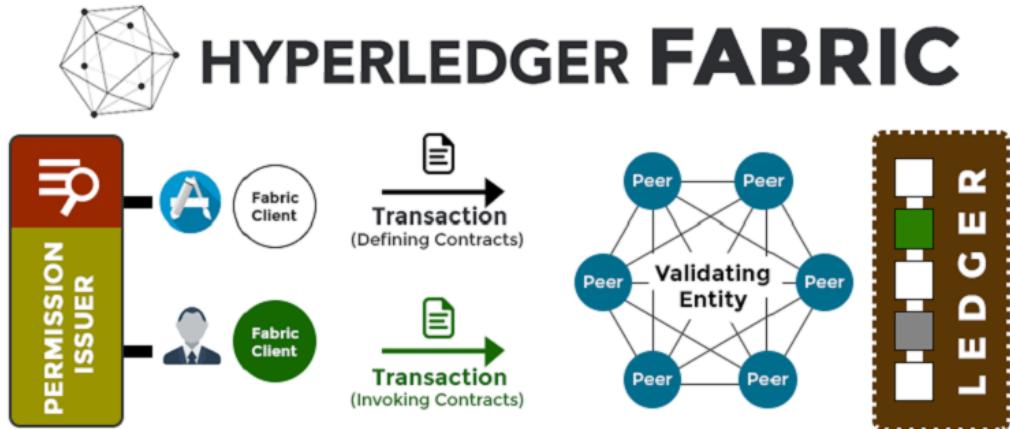
```
1 pragma solidity ^0.8.0;
2 contract mymath {function sqrt(uint x) public view returns (uint y) {
3     uint z = (x + 1) / 2;
4     y = x;
5     while (z < y) {
6         y = z;
7         z = (x / z + z) / 2;
8     }
9 }
10 function sqr(uint a) public view returns (uint) {
11     uint c = a * a;
12     return c;
13 }
14 function mul(uint a, uint b) public view returns (uint) {
15     uint c = a * b;
16     return c;
17 }
18 function sub(uint a, uint b) public view returns (uint) {
19     return a - b;
20 }
21 function add(uint a, uint b) public view returns (uint) {
22     uint c = a + b;
23     return c;
24 }}
```

At the bottom, there's a transaction log entry:

[block:2388553 txIndex:0] from: 0xbB1...52233 to: mymath.(constructor) value: 0 wei  
data: 0x608...70033 logs: 0 hash: 0xc57...f3026

Buttons for **listen on all transactions**, **Search with transaction hash or address**, and **Debug**.

# 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

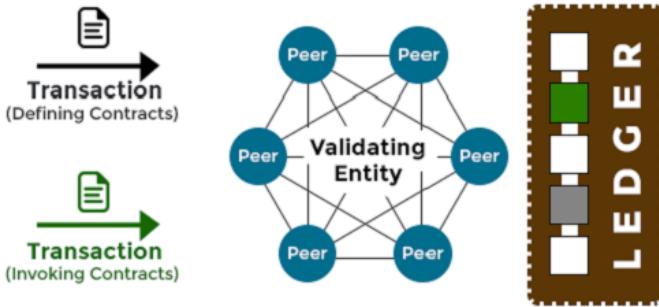
Apparently, Hyperledger is quite popular within the enterprise blockchain ecosystem. The community boasts over 260 high-profile partners that include IBM, SAP and many more. Hyperledger is managed by the Linux Foundation which created the ecosystem in December 2015. The platform is open source and supports 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.

## 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.

## 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



Ledger is not public

## 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.



Assets have key pairs (binary or JSON).

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

## Blockchain and Cryptocurrencies

**Cryptocurrencies**  
Bitcoin addresses  
Blockchain  
Mining

