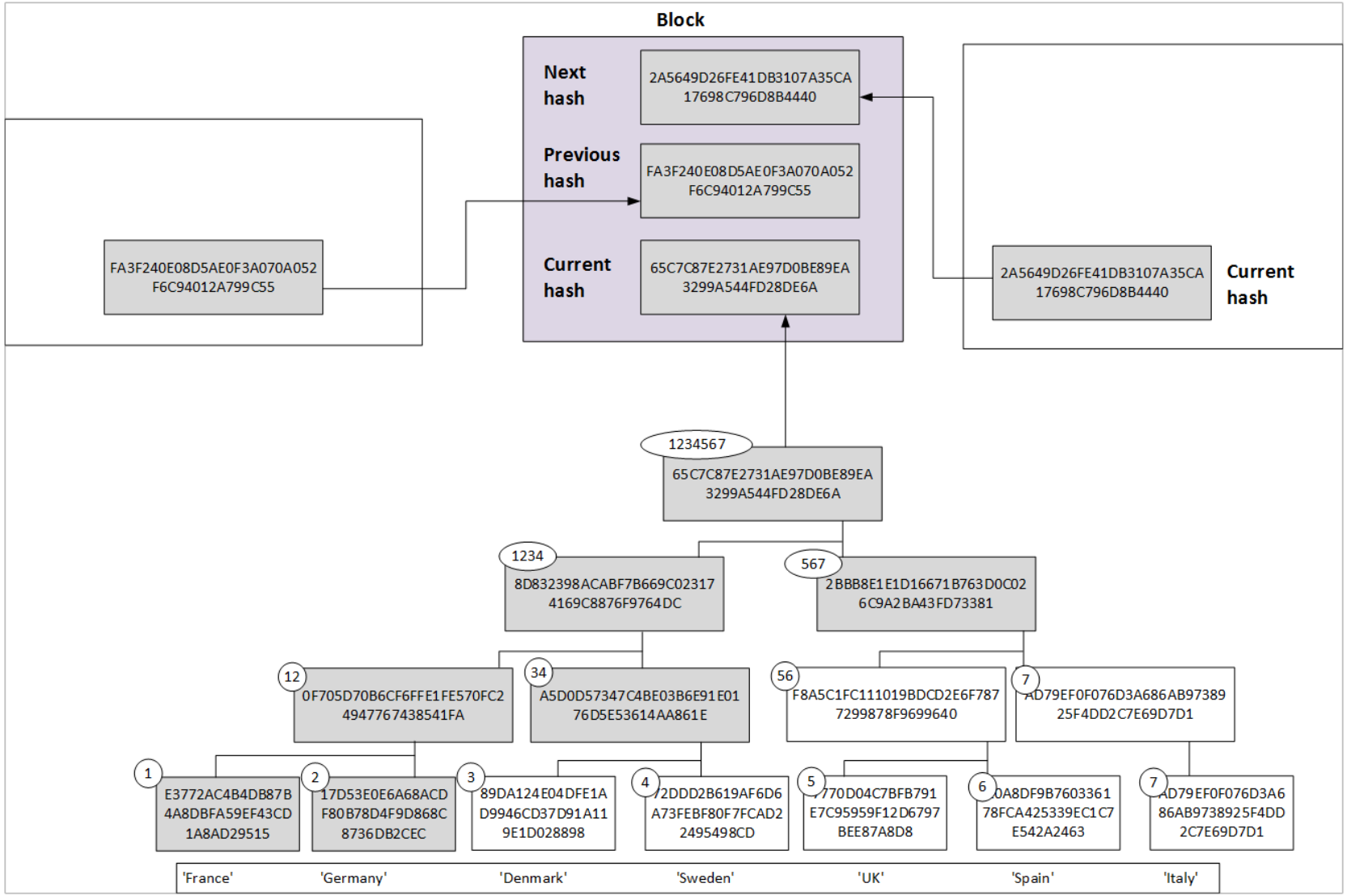
Blockchain and Cryptocurrencies

> Cryptocurrencies
Bitcoin addresses
Blockchain
Mining
Ethereum
Smart Contracts
Blockchain Crypto

Prof Bill Buchanan OBE
http://asecuritysite.com/crypto10
http://asecuritysite.com/encryption

rencies


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

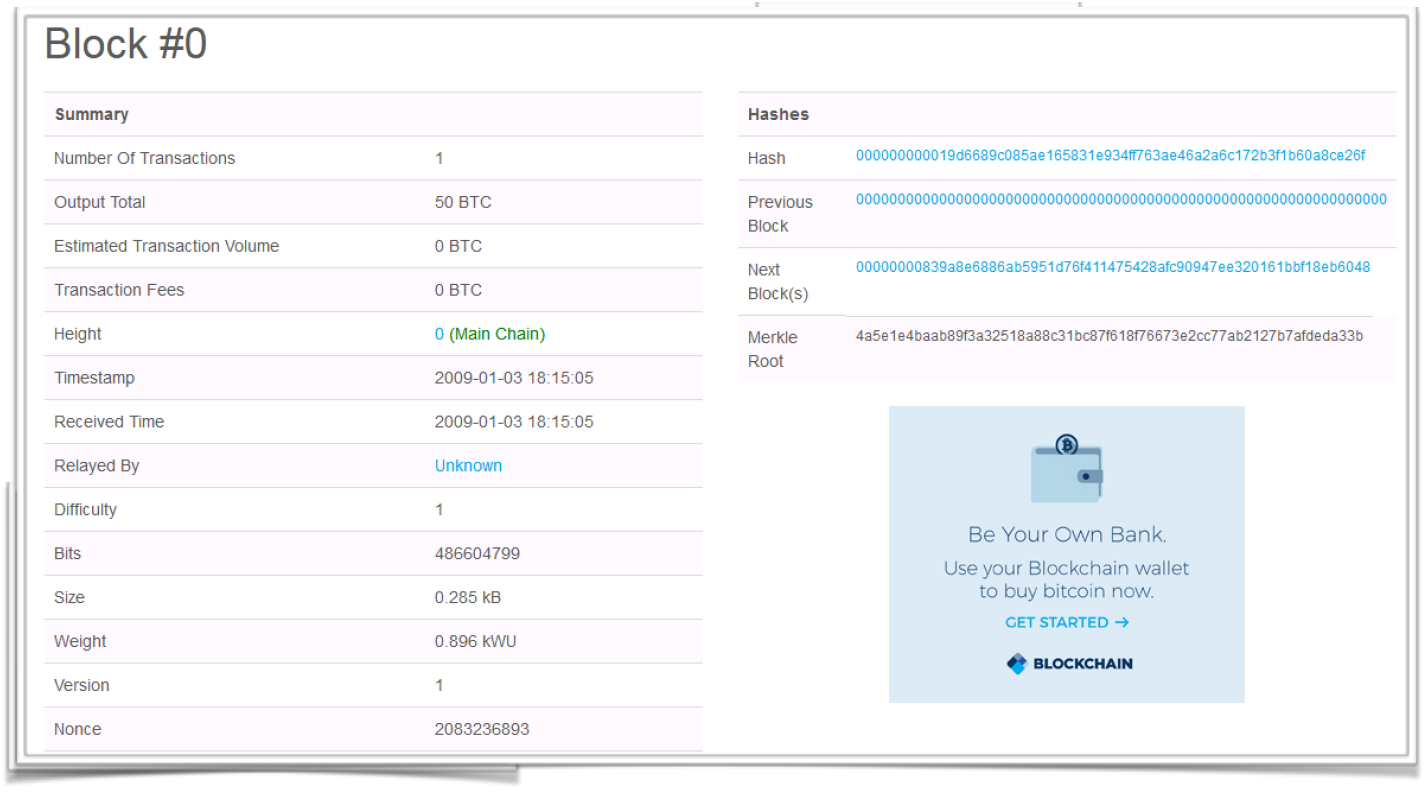
Who is nine years old?

Who is nine years old?

Who is nine years old?

Who is nine years old?

Who is nine years old?

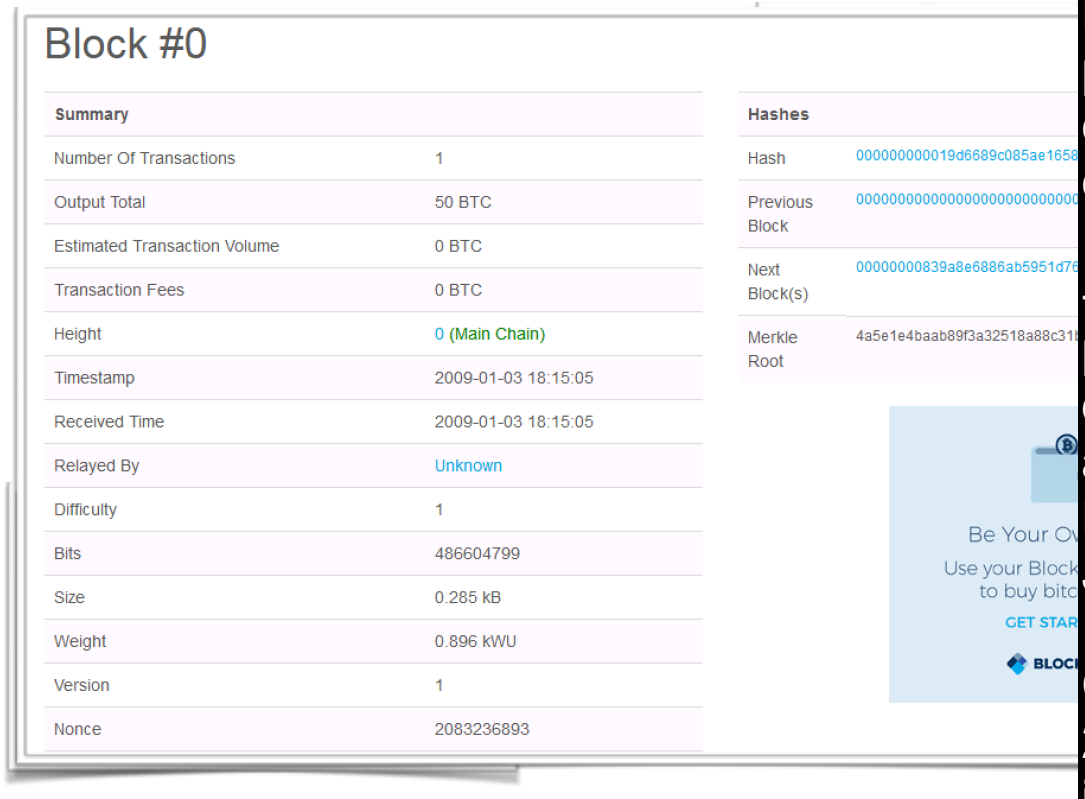


Block #0

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

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

Who is nine 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

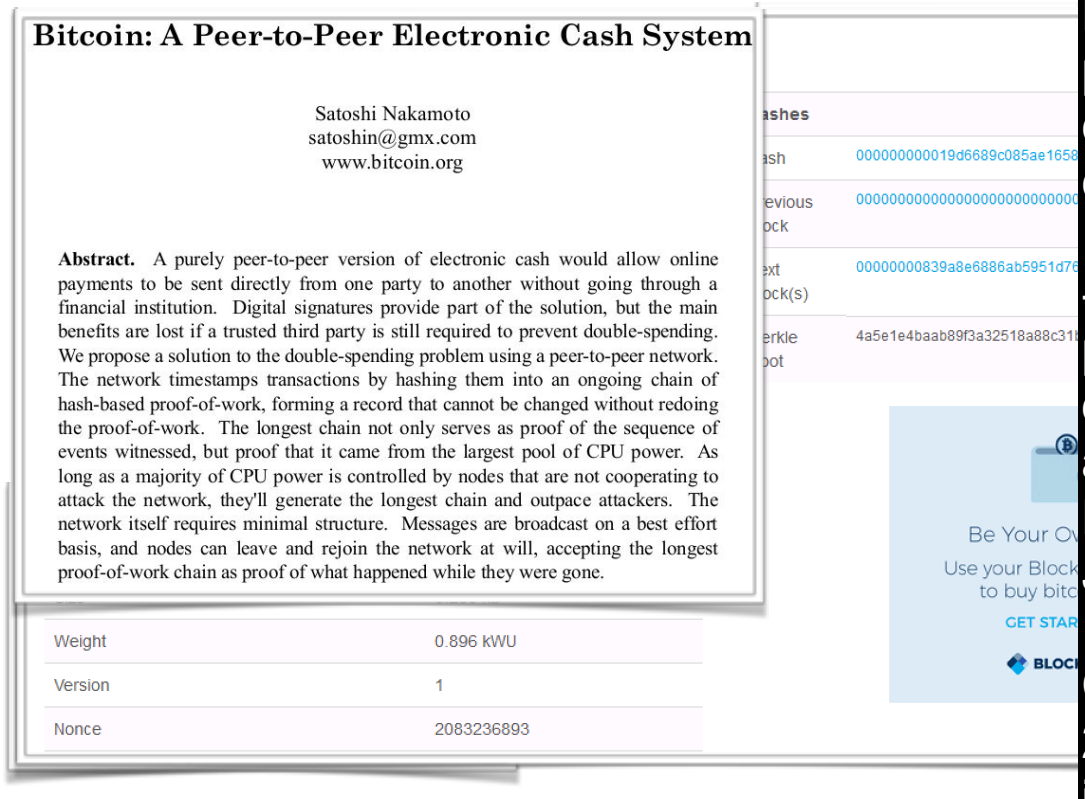
Hashes	
Hash	000000000019d6689c085ae1658
Previous Block	0000000000000000000000000000
Next Block(s)	00000000839a8e6886ab5951d76
Merkle Root	4a5e1e4baab89f3a32518a88c31

Be Your O
Use your Block
to buy bitc
GET STAR
BLOC

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 149GB, and there are 16.5 million

Who is nine 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.

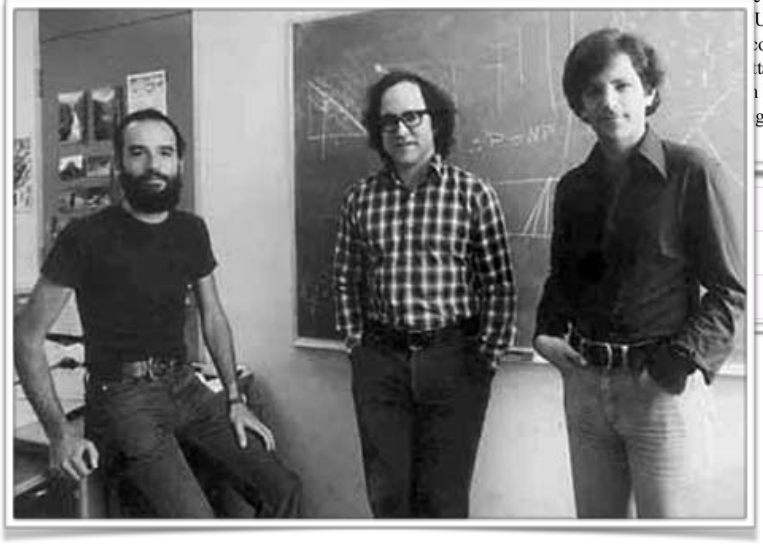
Currently, as of 5 January 2018, the blockchain size is around 149GB, and there are 16.5 million

Who is nine 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 149GB, and there are 16.5 million

Who is nine 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 149GB, and there are 16.5 million

Who is nine 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 149GB, and there are 16.5 million

Who is nine years old?

His work was a hotch-
botch of differing
methods that
rced in the
as public key
the cyber
ent which
the 1990s,
ded by Eric
May and
.

of 5 January
ckchain size
is around 149GB, and
there are 16.5 million

The Most Profitable Crime?

The Most Profitable Crime?

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

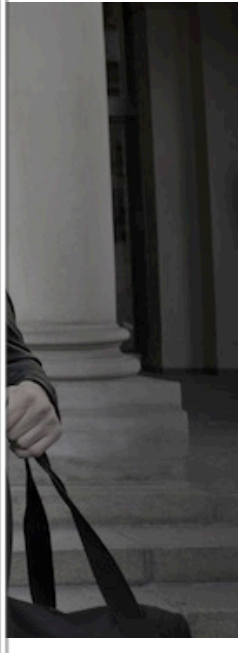
Published on December 21, 2017 Edit article | View stats

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

132 12 6 3

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

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



The Most Profitable Crime?

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

Published on December 21, 2017 Edit article | View stats

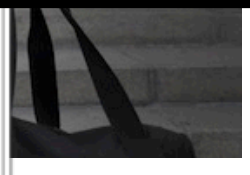
Prof Bill Buchanan OBE, PhD, FBCS
Professor at Napier University
1,194 articles

132 12 6

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

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

```
wallet - Copy.dat

wallet.dat

wallet.dat.1

wallet.dat.zip

wallet.tar

wallet.tar.gz

wallet.zip

wallet_backup.dat

wallet_backup.dat.1

wallet_backup.dat.zip
```



The Most Profitable Crime?

```
wallet - Copy.dat

wallet.dat

wallet.dat.1
```

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?

wallet - Copy.dat

wallet.dat

wallet.dat.1

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

Dimitrios Slamaris
@dim0x69

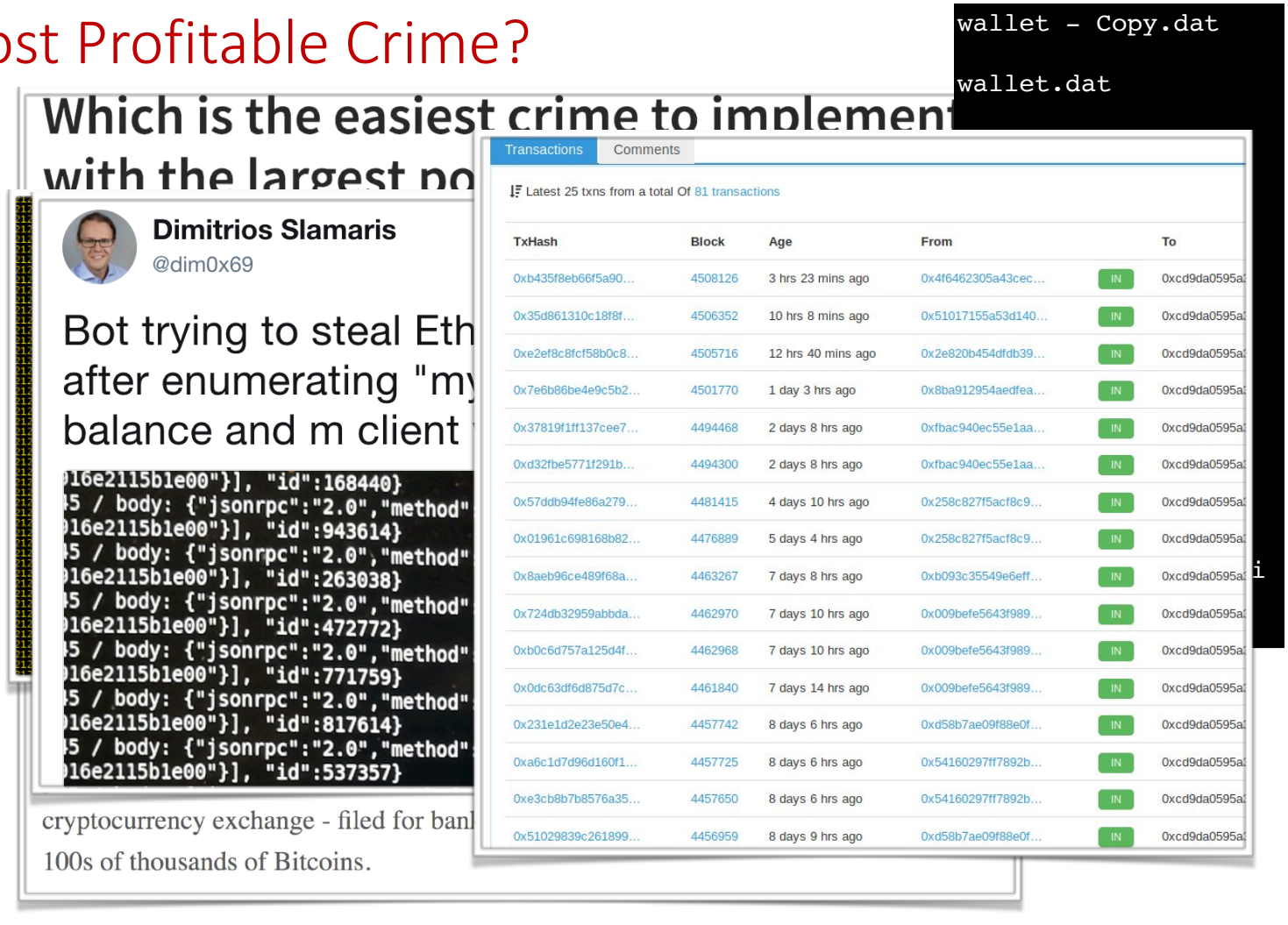
Follow

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}
```

cryptocurrency exchange - filed for bankruptcy after a hacker drained the exchange of 100s of thousands of Bitcoins.

The Most Profitable Crime?



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 is consent?

Who's laws do I comply with?

What are physical borders?

Why does fiat currency exist?

Dear 21st Century …

What is the ownership of something?

What is consent?

What are my rights to privacy?

Who's laws do I comply with?

What are physical borders?

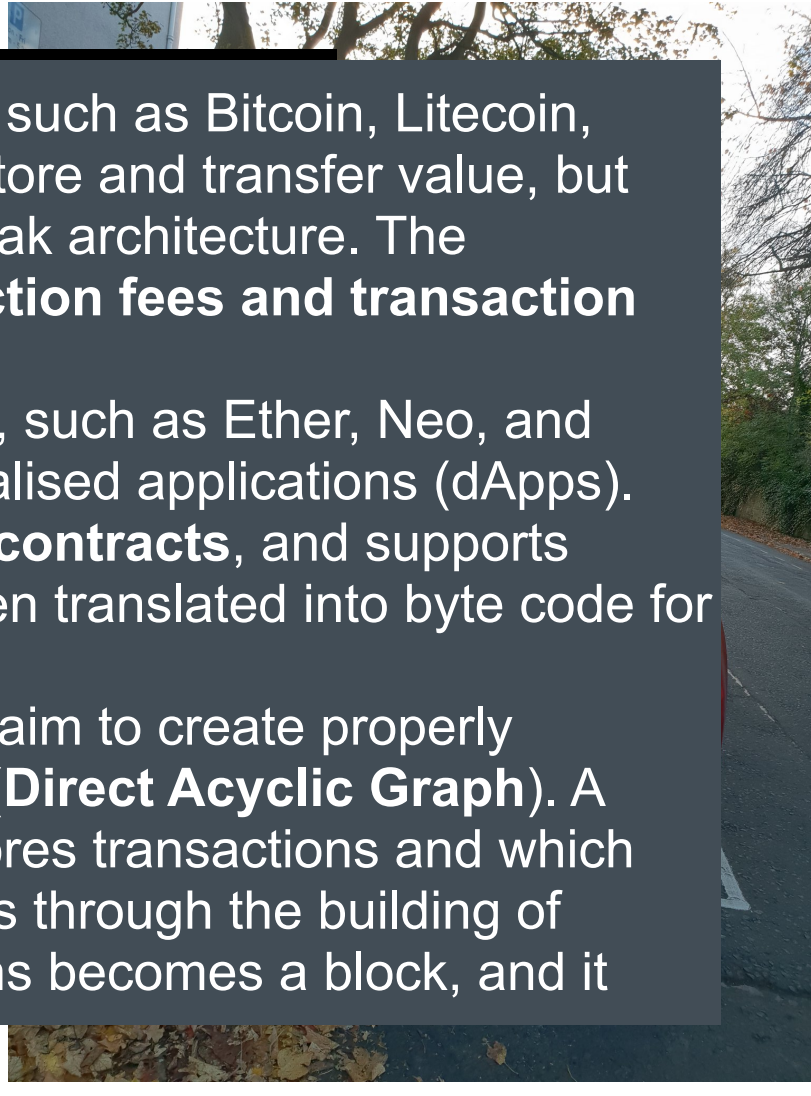
Why does fiat currency exist?

Dear 21st Century

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**.

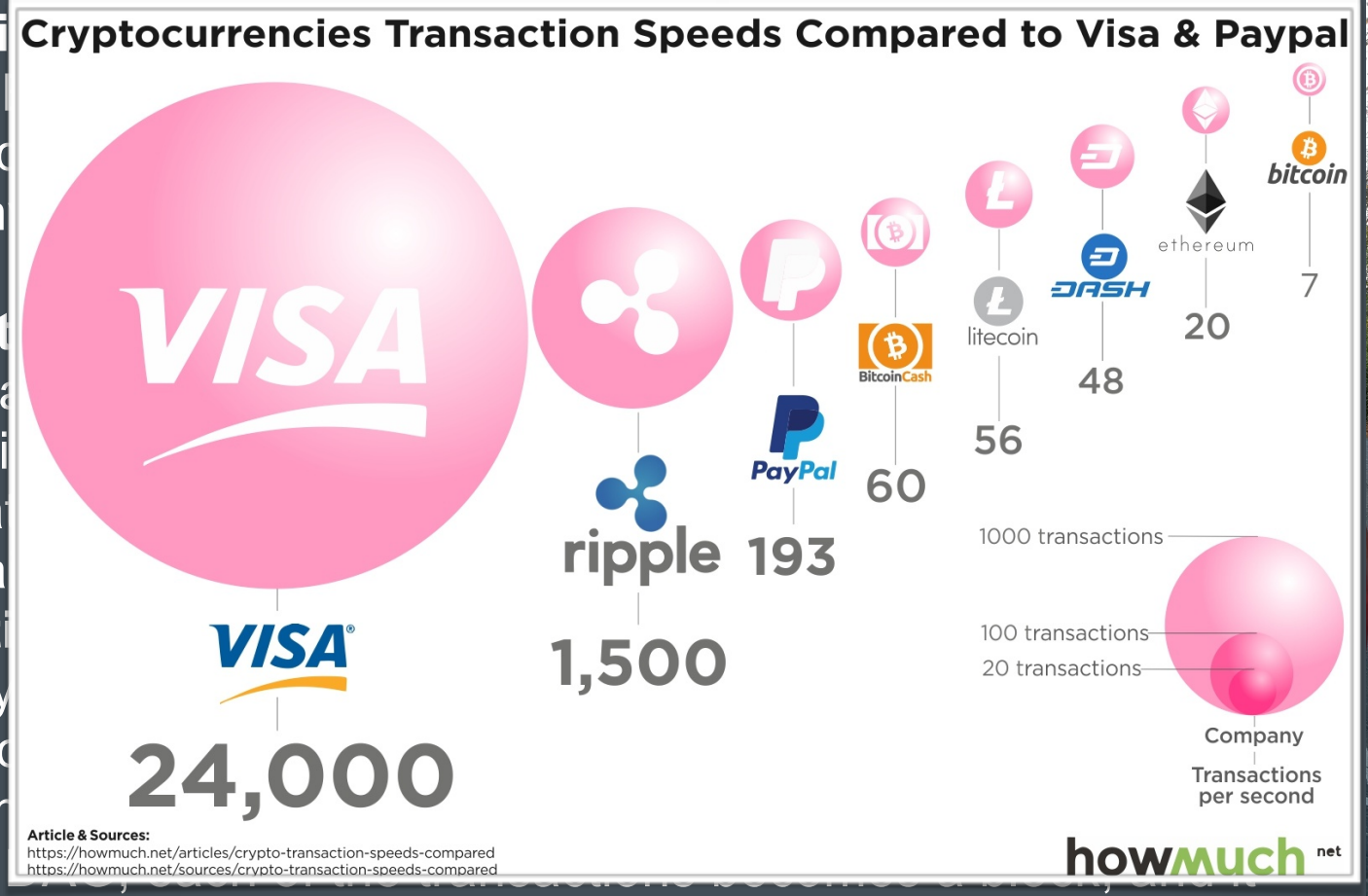
2nd Generation. These cryptocurrencies, such as Ether, Neo, and Lisk, have platforms that support decentralised applications (dApps). This generation adds **coding and smart contracts**, and supports logical operations. A high-level code is then translated into byte code for the Blockchain.

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

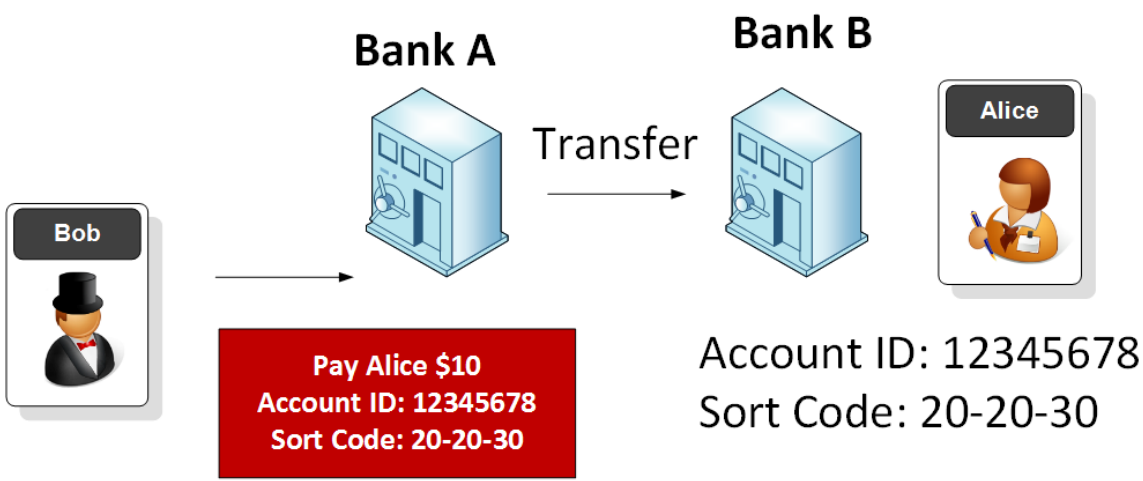


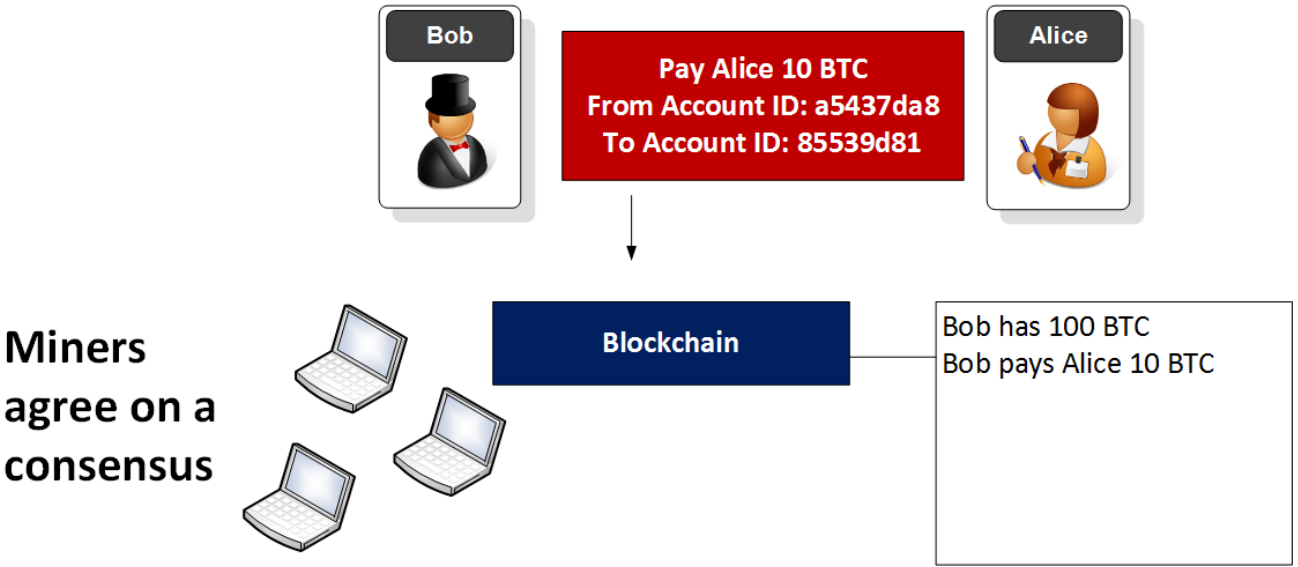
Dear 21st Century

1st Generati
Monero and
have suffered
overheads in
times.
2nd Generat
Lisk, have pla
This generati
logical opera
the Blockcha
3rd Generati
distributed sy
traditional Bl
can take som
blocks. With



Payments


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


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

History

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

History

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

Genesis Record

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

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

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

50 BTC

Big accounts

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

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

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

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

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

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

Request Payment

Donation Button

e3a9cbec0c5ec55db3ac02029d8cbaf1370e04e8603d9e5000106091c66c308d 2017-11-14 08:03:03

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

13,083.32386362 BTC

Genesis Record

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

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

Request Payment

Donation Button

Transactions (Oldest First)

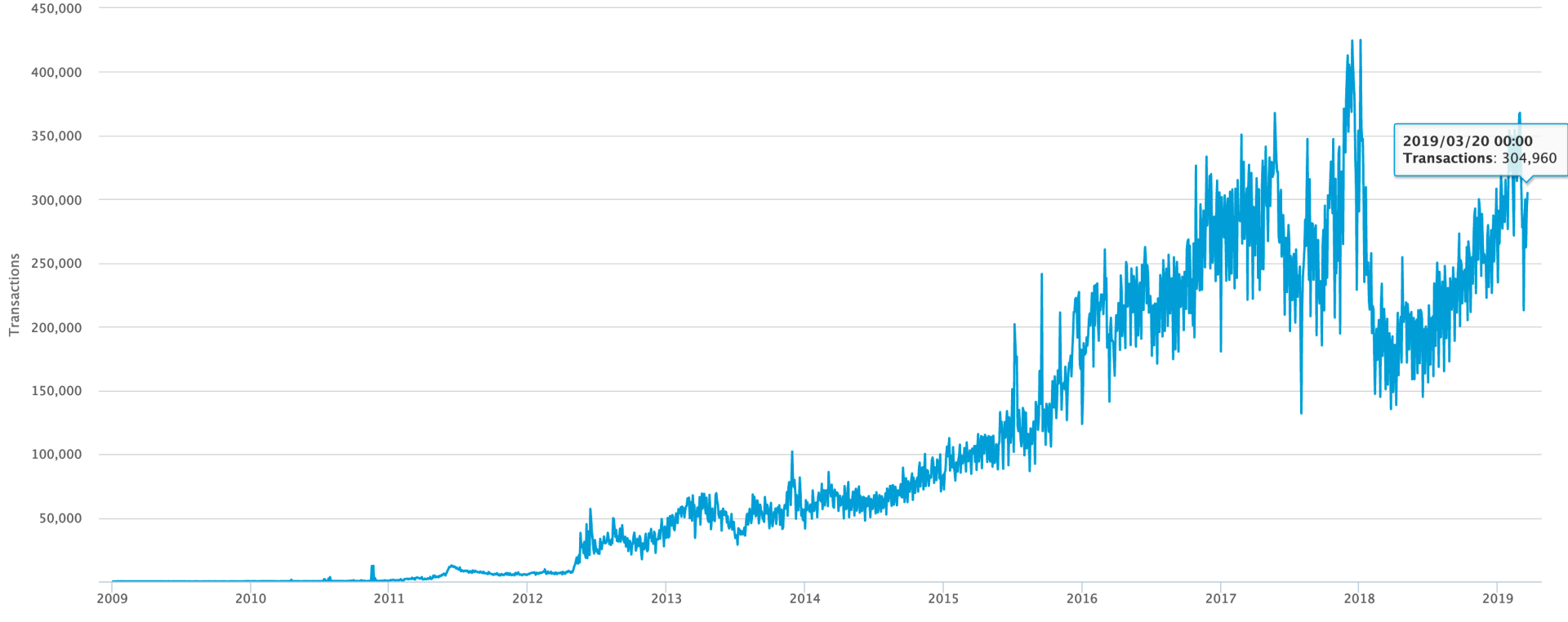
Filter

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

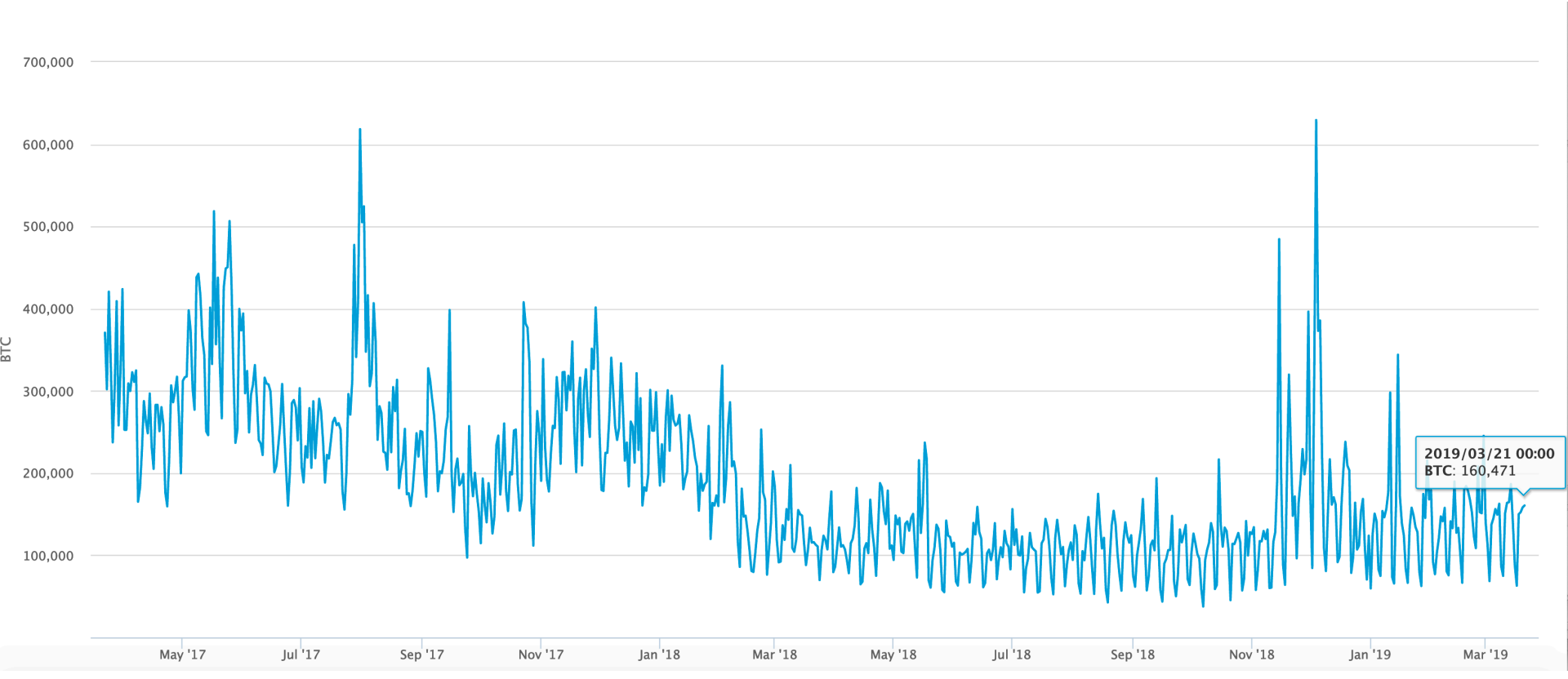
1 Confirmation

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

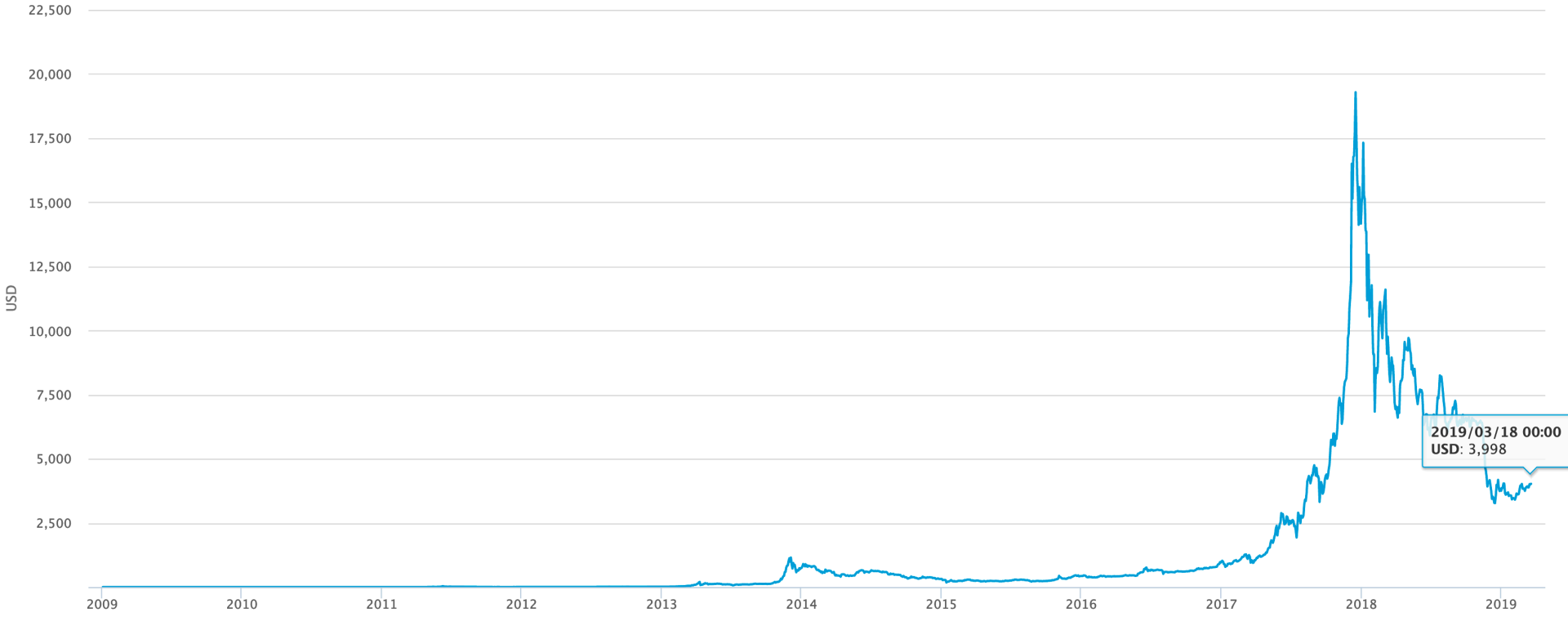
Bitcoin transactions



Transaction value



Bitcoin value



Types

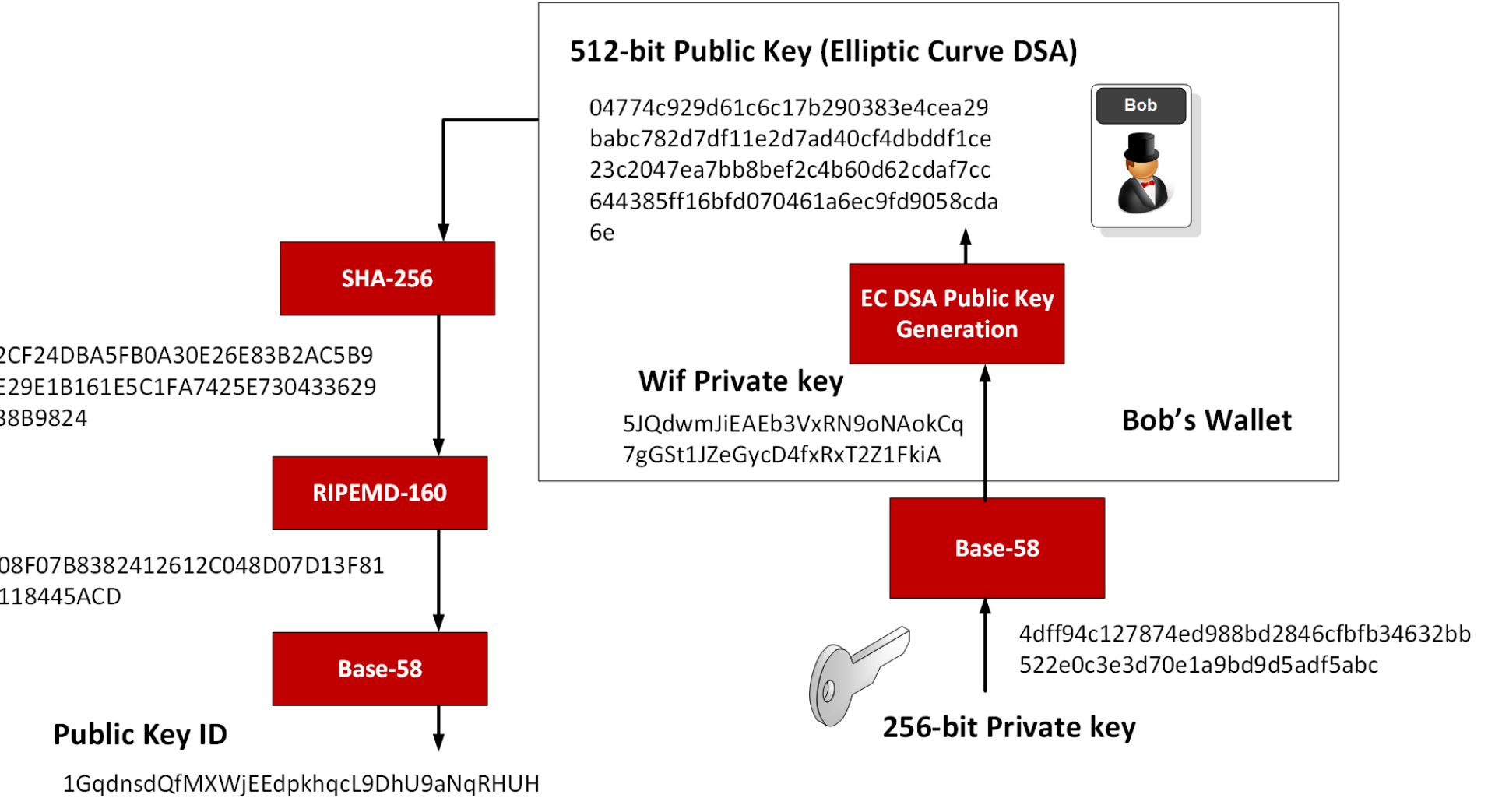
#	Name	Market Cap	Price	Volume (24h)	Circulating Supply	Change (24h)	Price Graph (7d)
1	Bitcoin	$71,088,039,345	$4,038.29	$10,435,962,718	17,603,487 BTC	-1.20%	
2	Ethereum	$14,479,268,416	$137.45	$5,059,103,489	105,341,038 ETH	-1.93%	
3	XRP	$13,030,671,423	$0.312741	$827,506,319	41,666,017,553 XRP *	-1.64%	
4	Litecoin	$3,626,795,540	$59.46	$1,781,003,983	60,993,611 LTC	-1.52%	
5	EOS	$3,312,054,895	$3.65	$1,664,383,267	906,245,118 EOS *	-2.13%	
6	Bitcoin Cash	$2,763,425,545	$156.25	$485,815,357	17,686,200 BCH	-2.48%	
7	Binance Coin	$2,136,080,853	$15.13	$157,621,022	141,175,490 BNB *	-0.17%	
8	Stellar	$2,072,632,867	$0.107816	$296,232,212	19,223,806,819 XLM *	-2.92%	
9	Tether	$2,037,521,724	$1.01	$9,493,760,701	2,011,187,463 USDT *	0.17%	
10	TRON	$1,512,247,598	$0.022678	$199,174,791	66,682,072,191 TRX	-1.32%	
11	Cardano	$1,499,118,770	$0.057821	$111,173,464	25,927,070,538 ADA	6.37%	
12	Bitcoin SV	$1,176,686,029	$66.59	$107,924,136	17,670,348 BSV	-1.87%	
13	Monero	$904,586,082	$53.62	$88,525,613	16,869,292 XMR	-3.09%	
14	IOTA	$858,036,178	$0.308698	$40,038,035	2,779,530,283 MIOTA *	3.35%	

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

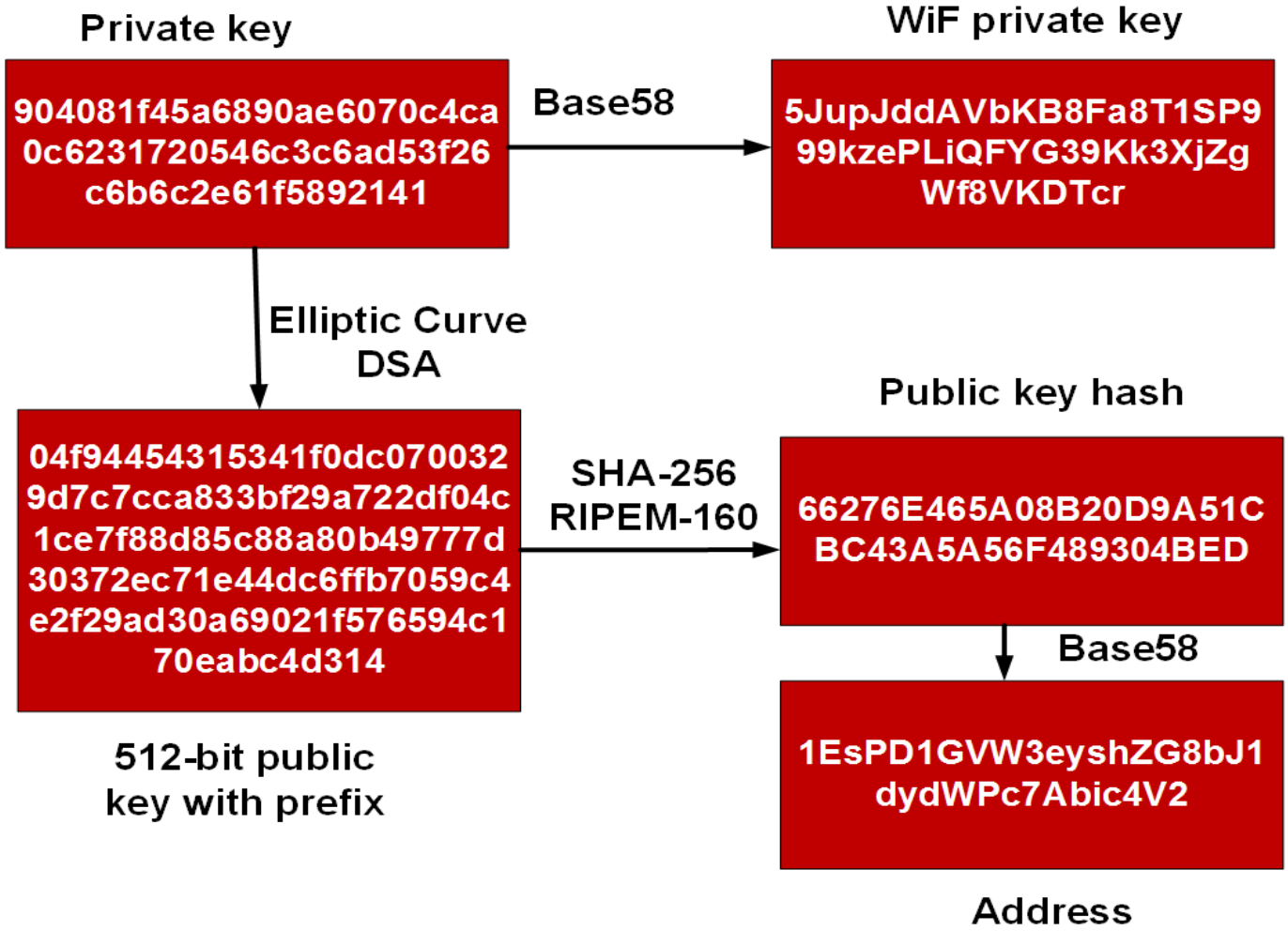
Bitcoin Wallet and Addresses



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

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

Request Payment | Donation Button


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

Private key:
4c0333a50b7724c71b89df148d83f64d49d896e21701007eeb8cada52744aca2

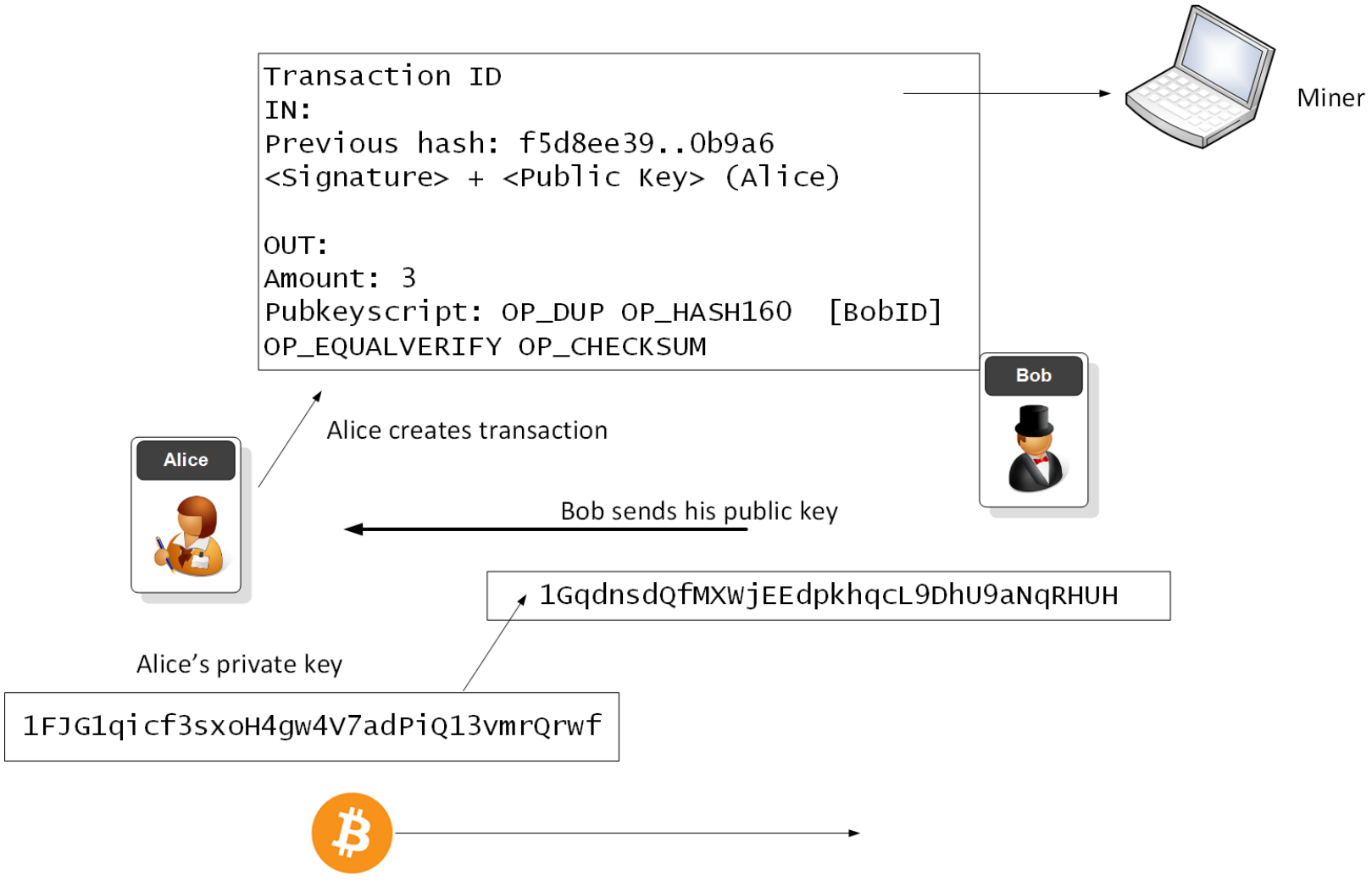
Public key:
0489fc7b8c3f655a10840d35c76ebb5596694045e49e940fb1e7a759da4edf0fafc45bb
bea6f5a56abf14c145c529c8eda9d3ad606f3a0bf4ca01ce991d4987b97

Wif: 5JPmDetQXXvc5aT5efyrg7BxHbH4135owRzq9DD7n2eWQCta5MN

Address: 16RAf9CjnstWCfBJGfrzSSMfTeHJVt8QWw

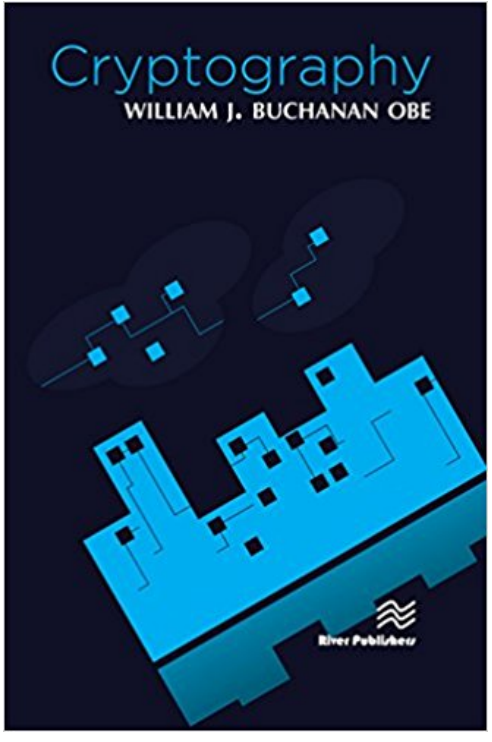
Signed:
4830450220264c4dce5f1cf0dff8d32d21c5d5cf6baed428b12ae6f8594924246a611e9
ee602210096ef8e7054ec7a39f0a35d8de3fd50090b1d125c0e795af8cf3d577b67640
7ca01410489fc7b8c3f655a10840d35c76ebb5596694045e49e940fb1e7a759da4edf0f
afc45bbbea6f5a56abf14c145c529c8eda9d3ad606f3a0bf4ca01ce991d4987b97

Bitcoin transaction



Blockchain and Cryptocurrencies

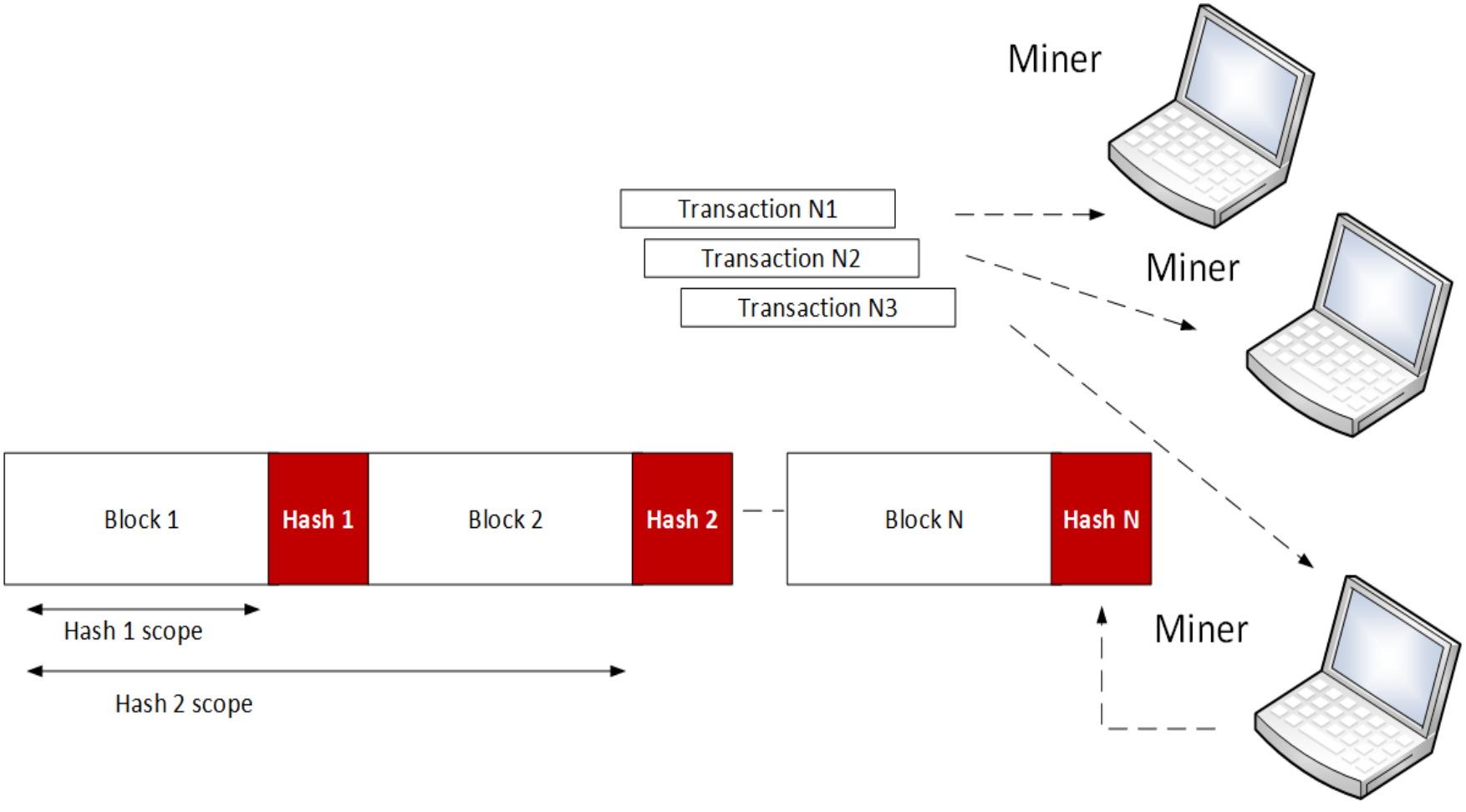
Cryptocurrencies
Bitcoin addresses
> Blockchain
Mining
Ethereum
Smart Contracts
Blockchain Crypto



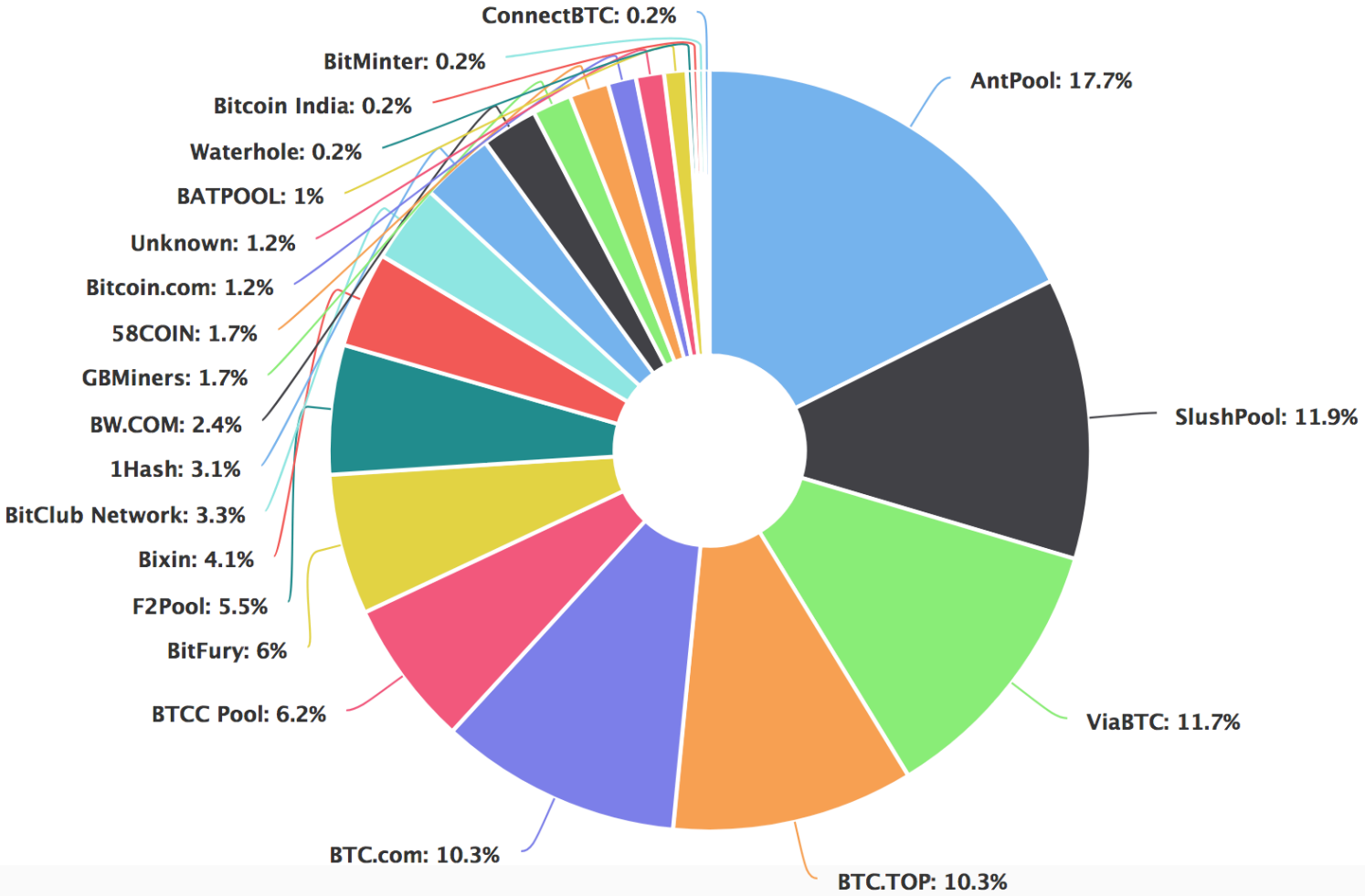
Prof Bill Buchanan OBE

http://asecuritysite.com/crypto10
http://asecuritysite.com/encryption

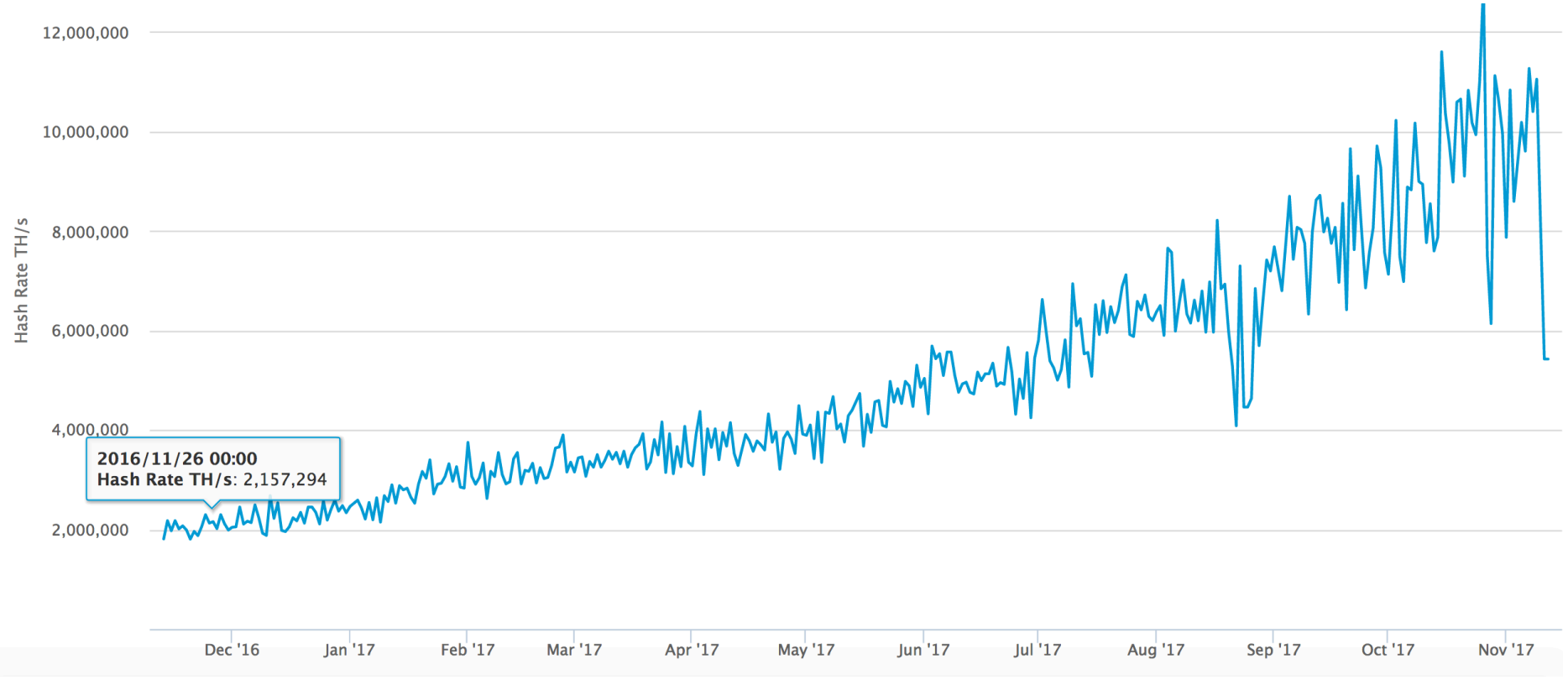
Mining process



Successful miners



Hash Rate TH/s



Mining Processes

- Hash
- 0000000000000000000d98e57b83834a2d1f4387a93d06861bcf3ea5fc498bd55
- Previous Block
- 0000000000000000012138e05f0779765277a9d2ab7e4a2a70882790abf98a0c

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

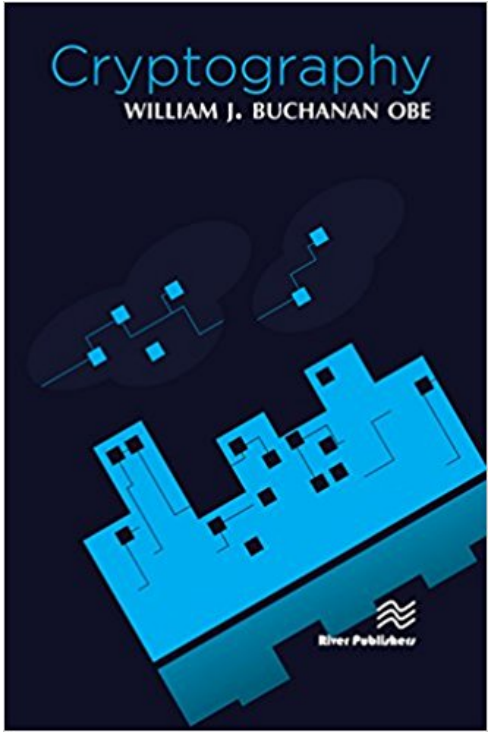
Hashes	
Hash	00000000000000000d98e57b83834a2d1f4387a93d06861bcf3ea5fc498bd55
Previous Block	00000000000000000012138e05f0779765277a9d2ab7e4a2a70882790abf98a0c
Next Block(s)	00000000000000000010e3117695c04d66d31cfa8489b70579dcc2f12c5a2daae
Merkle Root	140d91abab9501d50ace079ba12c80125f48c2b5fe7d9da685ea3ee8ea767e82

Chapter 10: Blockchain and Cryptocurrencies

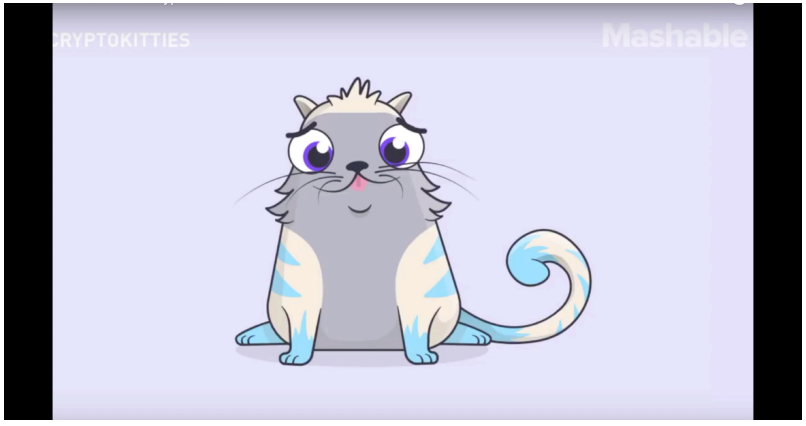
Cryptocurrencies
Bitcoin addresses
Blockchain
Mining
> Ethereum
Smart Contracts
Blockchain Crypto

Prof Bill Buchanan OBE

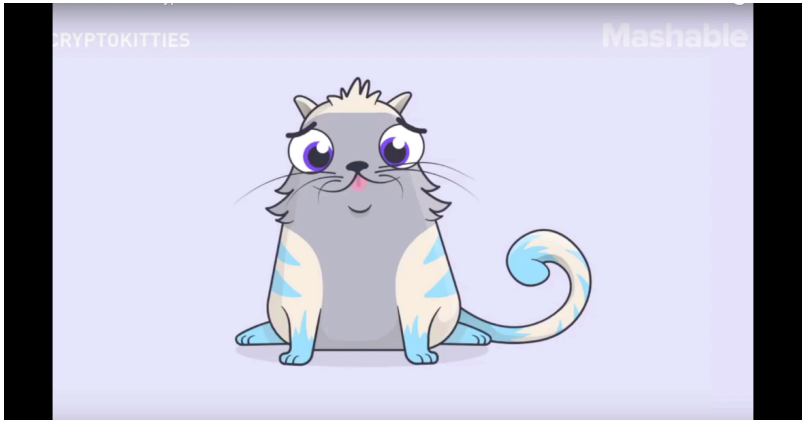
http://asecuritysite.com/crypto10
http://asecuritysite.com/encryption



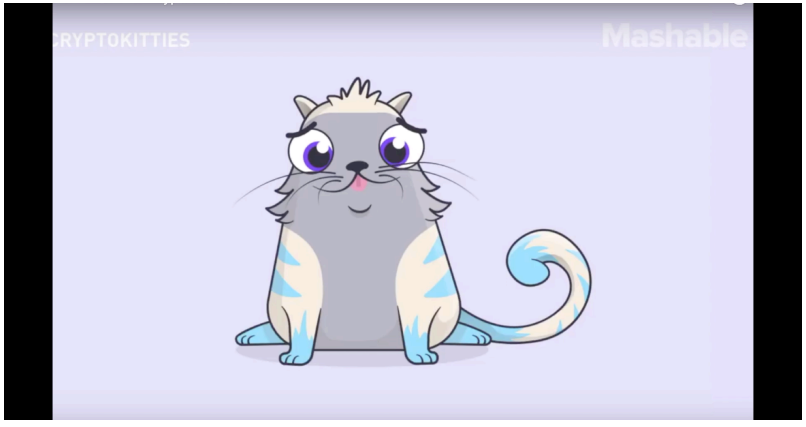
Crypto Kitties

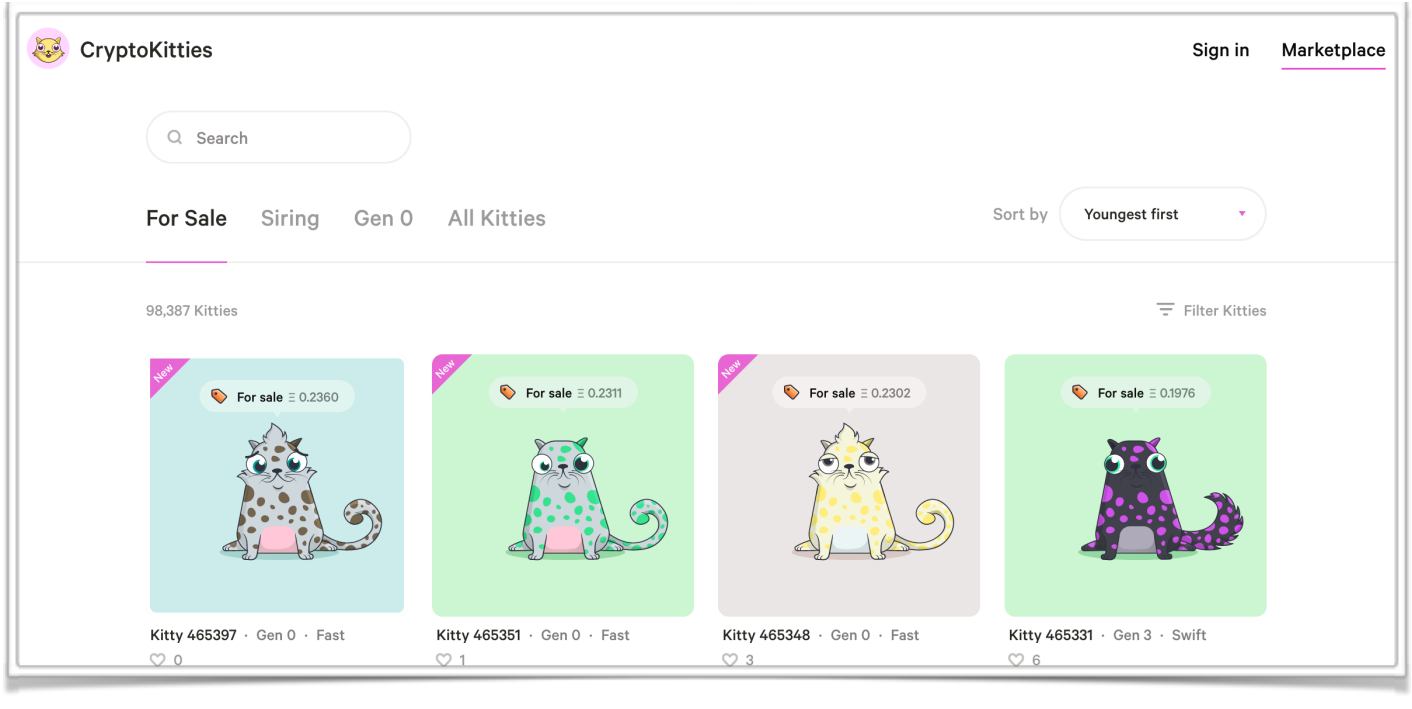


Crypto Kitties

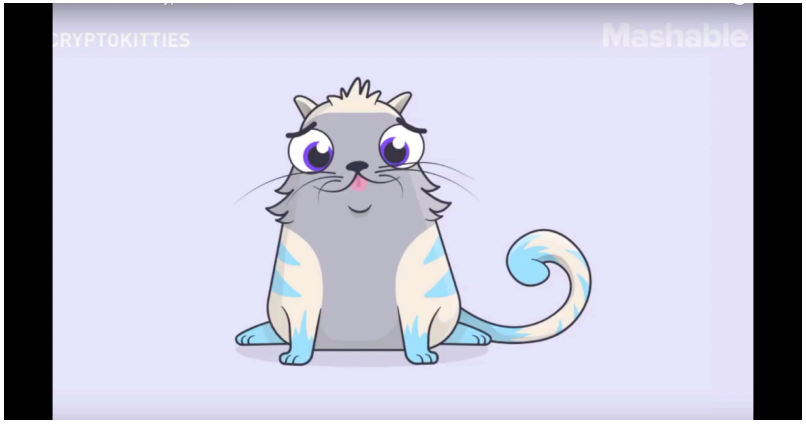


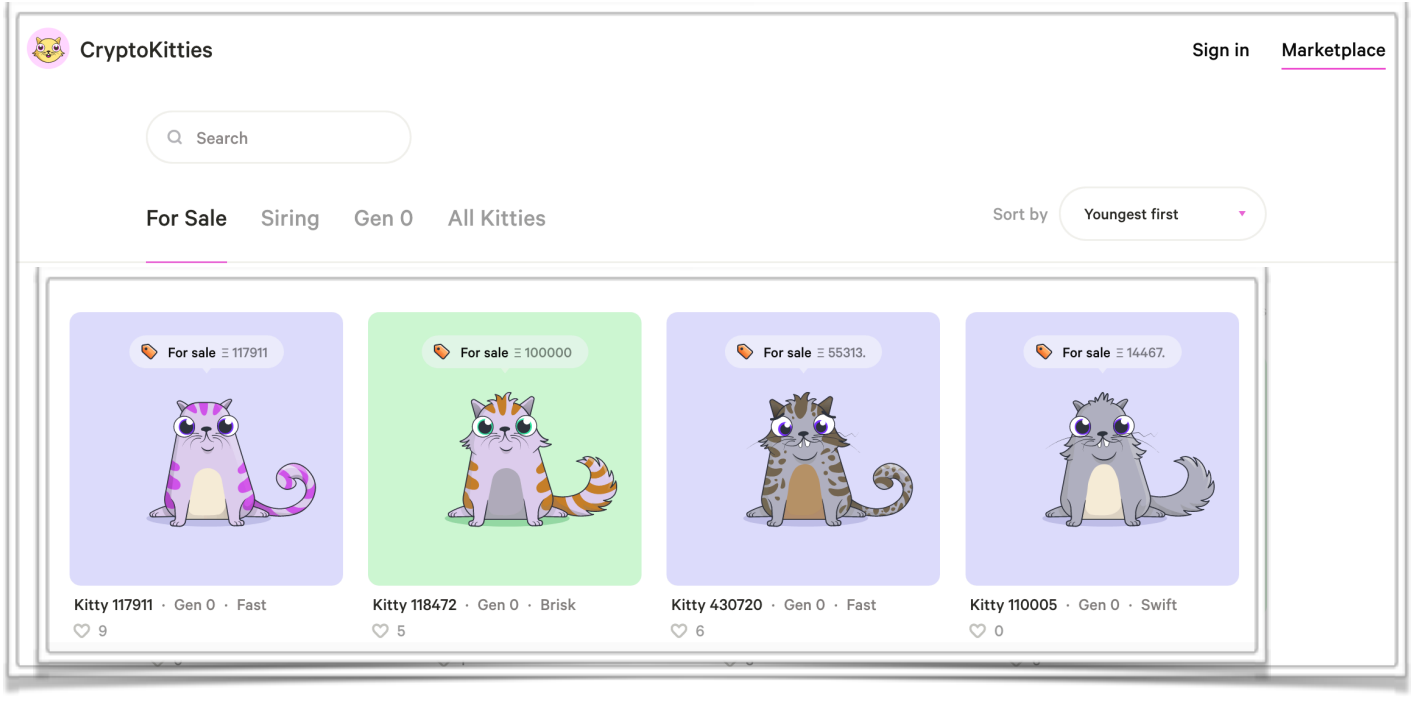
Crypto Kitties



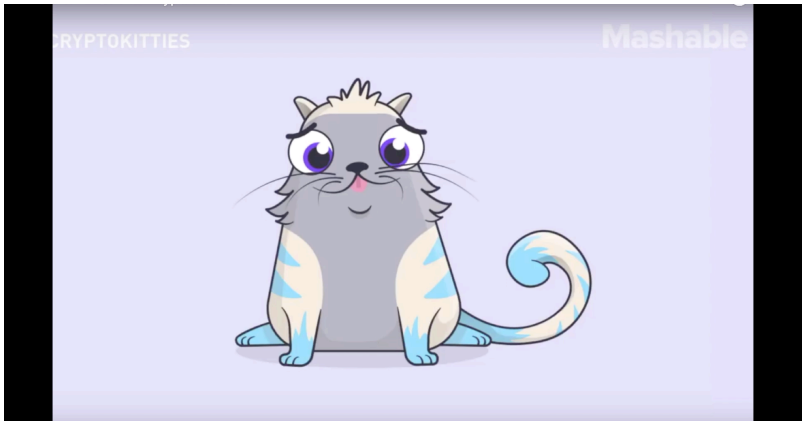


Crypto Kitties



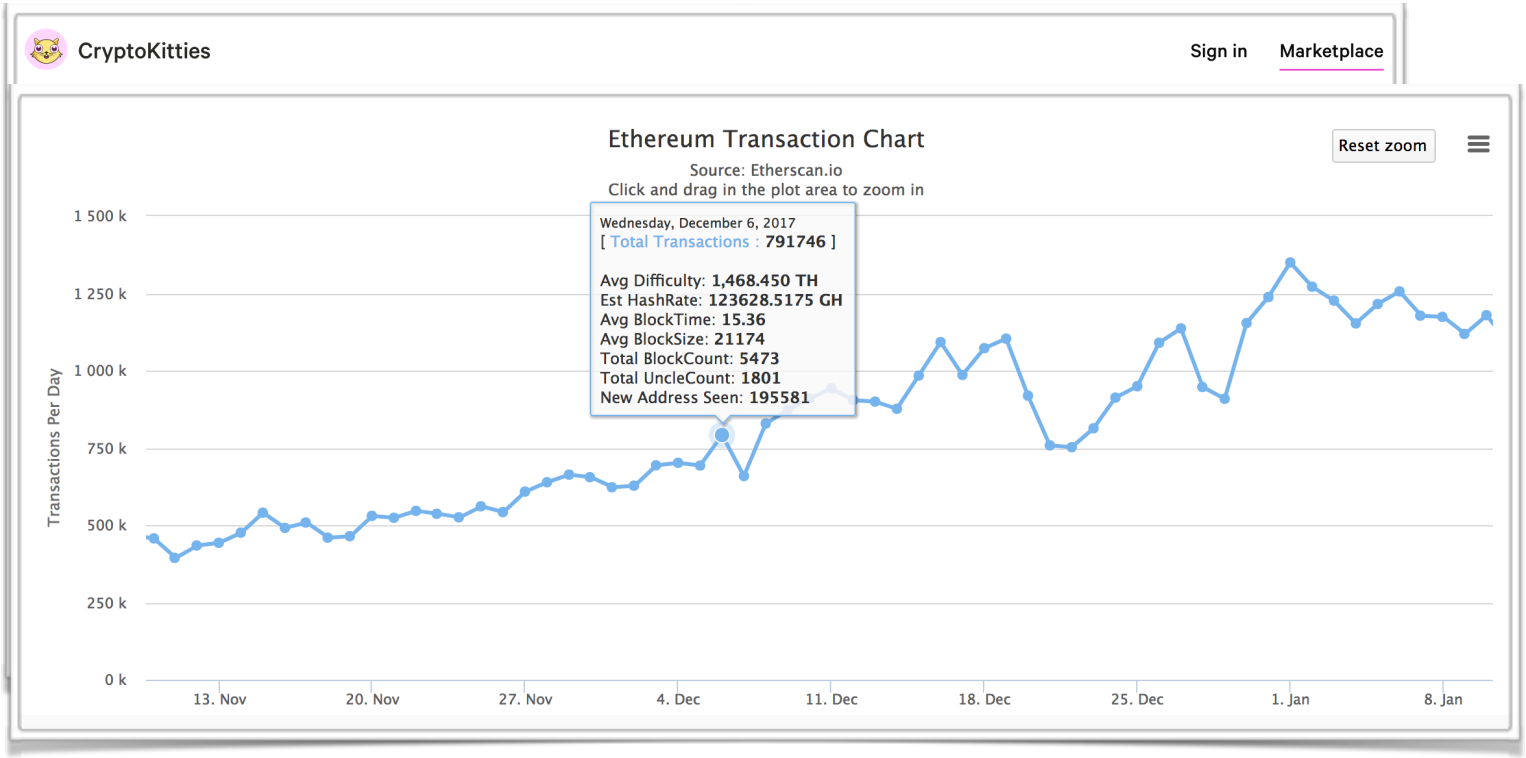


Crypto Kitties



CryptoKitties

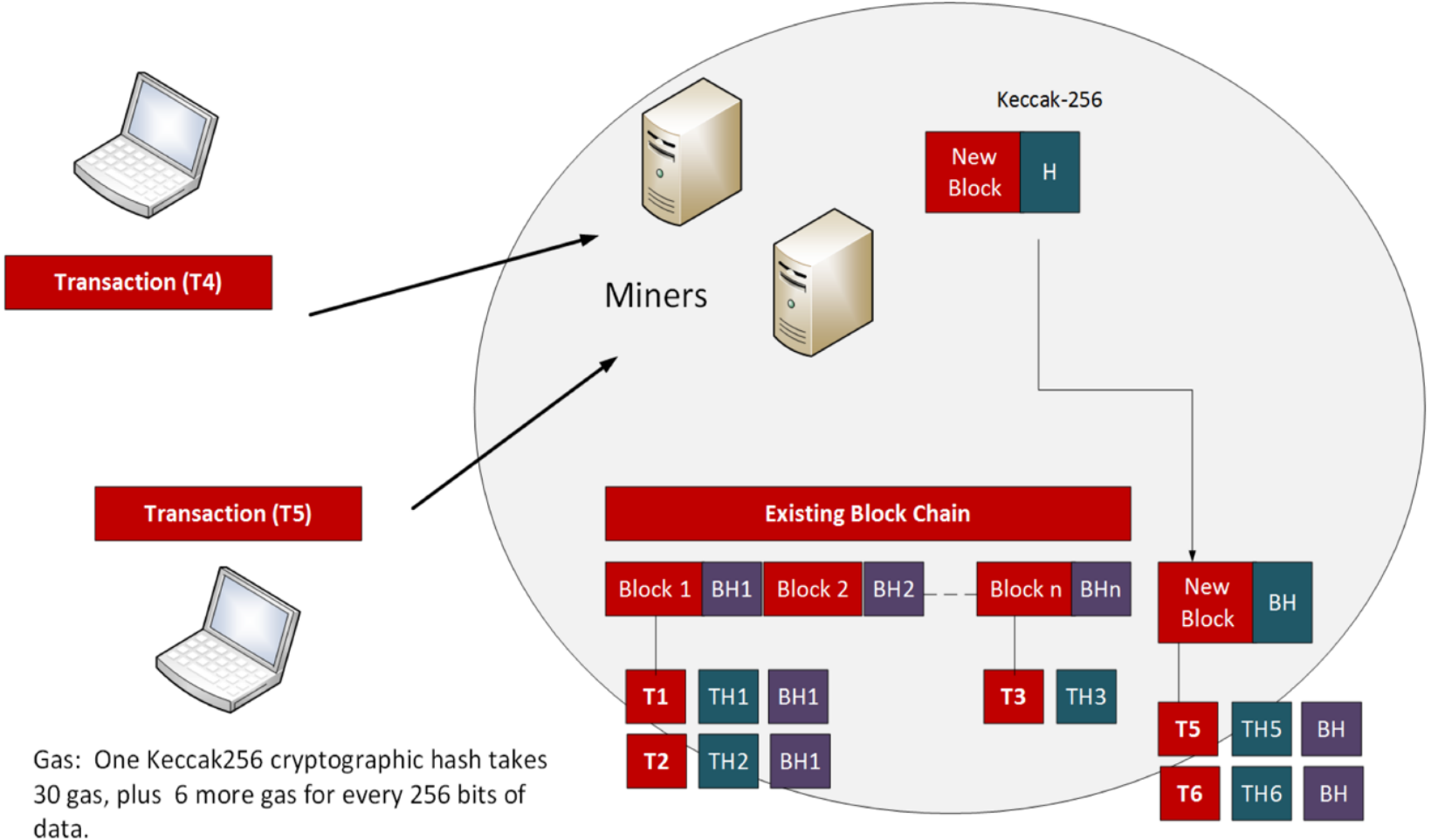
Sign in Marketplace



History

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

Ethereum setup



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

Gas

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

Gas

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

Gas

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

Gas

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

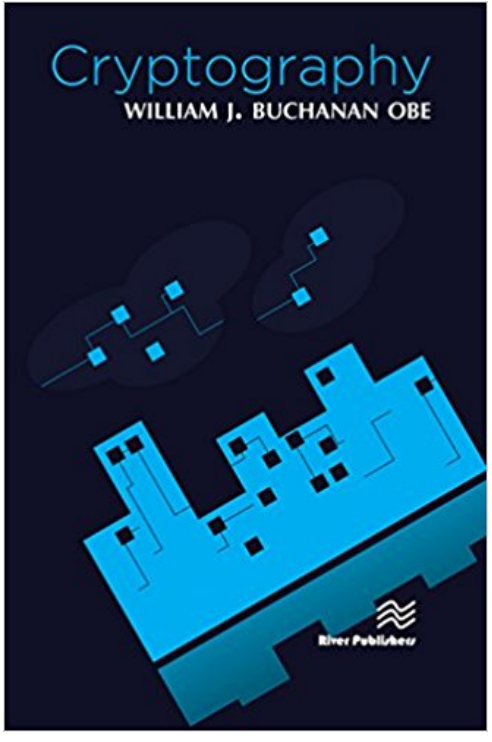
Gas

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

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

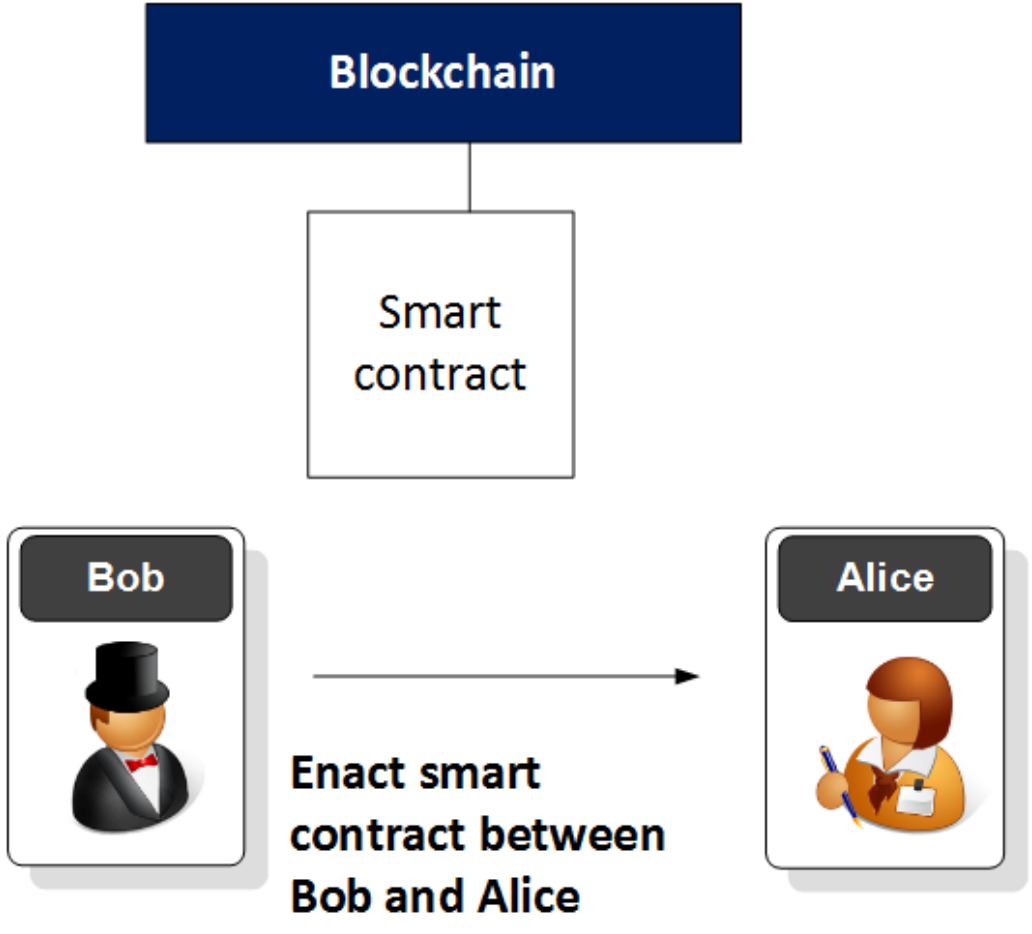
Blockchain and Cryptocurrencies

Cryptocurrencies
Bitcoin addresses
Blockchain
Mining
Ethereum
> Smart Contracts
Blockchain Crypto



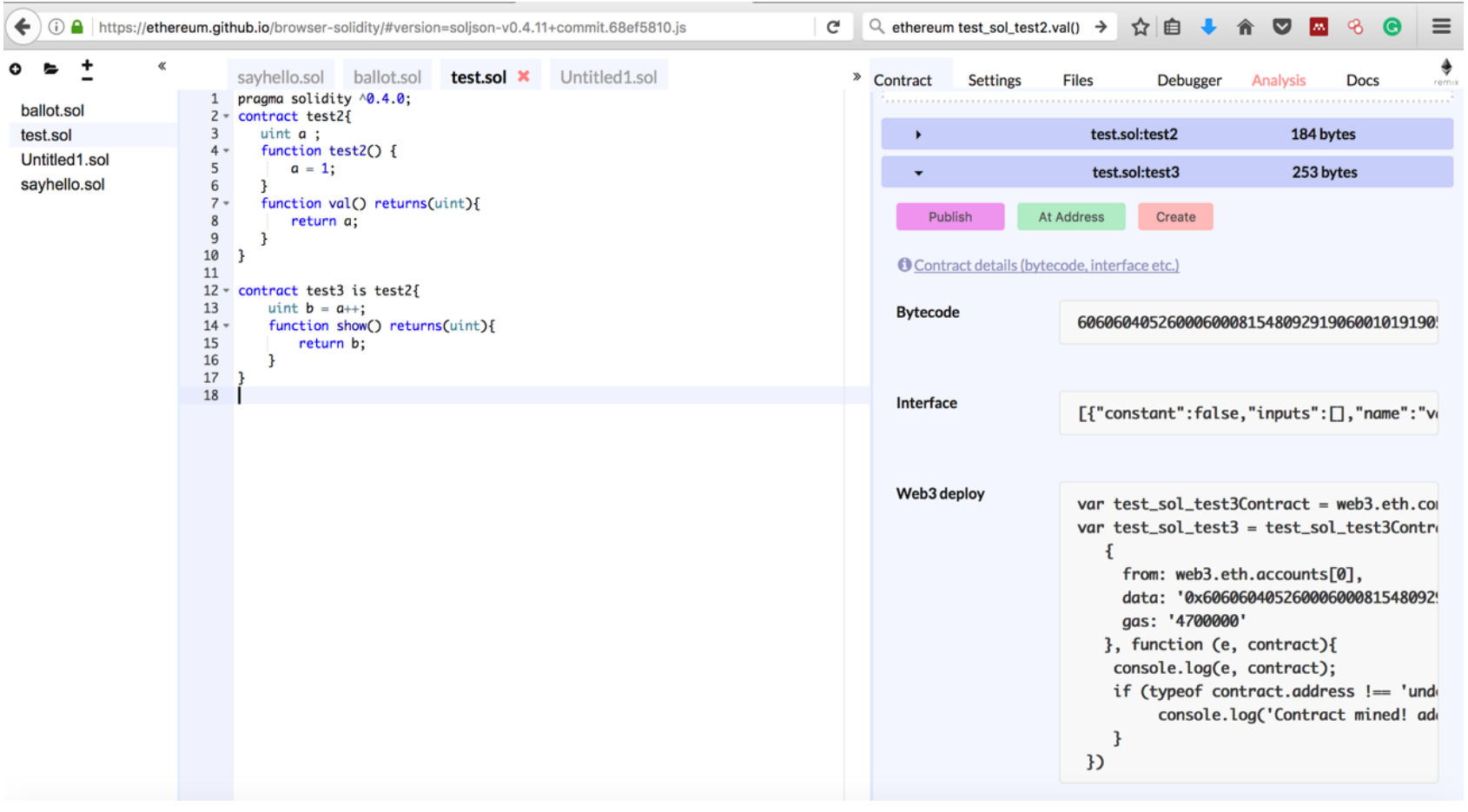
Prof Bill Buchanan OBE
http://asecuritysite.com/crypto10
http://asecuritysite.com/encryption

Smart Contract

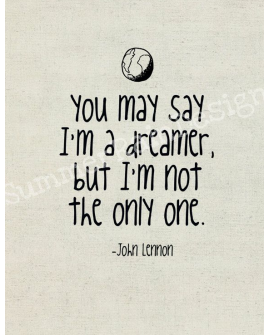


```
pragma solidity ^0.4.0;
contract test2{
   uint a ;
   function test2() {
      a = 1;
   }
   function val() returns(uint){
      return a;
   }
}

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

Compile with Solidity



A Future World?



Attestation A

Claim: Robert has Type 2 Diabetes
Date: 1 Jan 2017
Valid: 10 Sept 2018

Signed: GP Burns

Attestation B

Claim: Rab is over 60 years old
Date: 1 Sept 2017
Valid: 10 Sept 2028

Signed: Young Scot

Bob

Bob Smith

aka Robert Smith
aka Rab Smith
aka Bobby Smith

One-time claim

Council Contract

Description: Free Edin Bus Travel
Requirement: Over 60
Claims: Attestation B

Signed: Edin Busses

NHS Contract

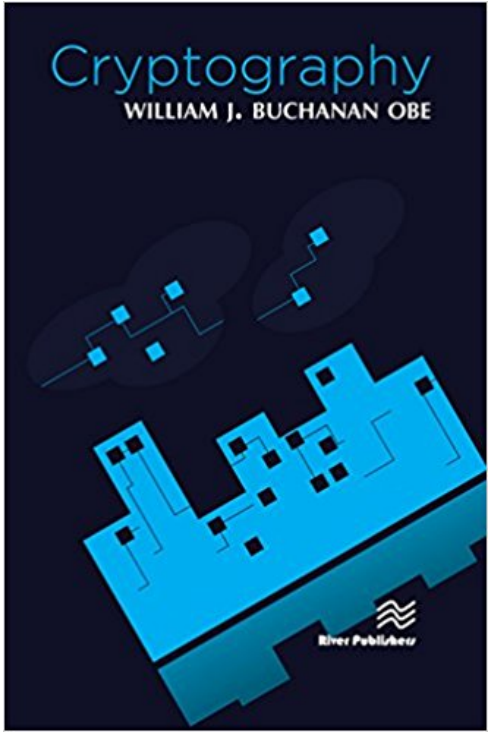
Description: Diabetes Support
Requirement: Has diabetes
Claims: Attestation A
Results: Discount from Boots on medicine

Signed: NHS Lothian

Blockchain

Blockchain and Cryptocurrencies

Cryptocurrencies
Bitcoin addresses
Blockchain
Mining
Ethereum
Smart Contracts
> Blockchain Crypto

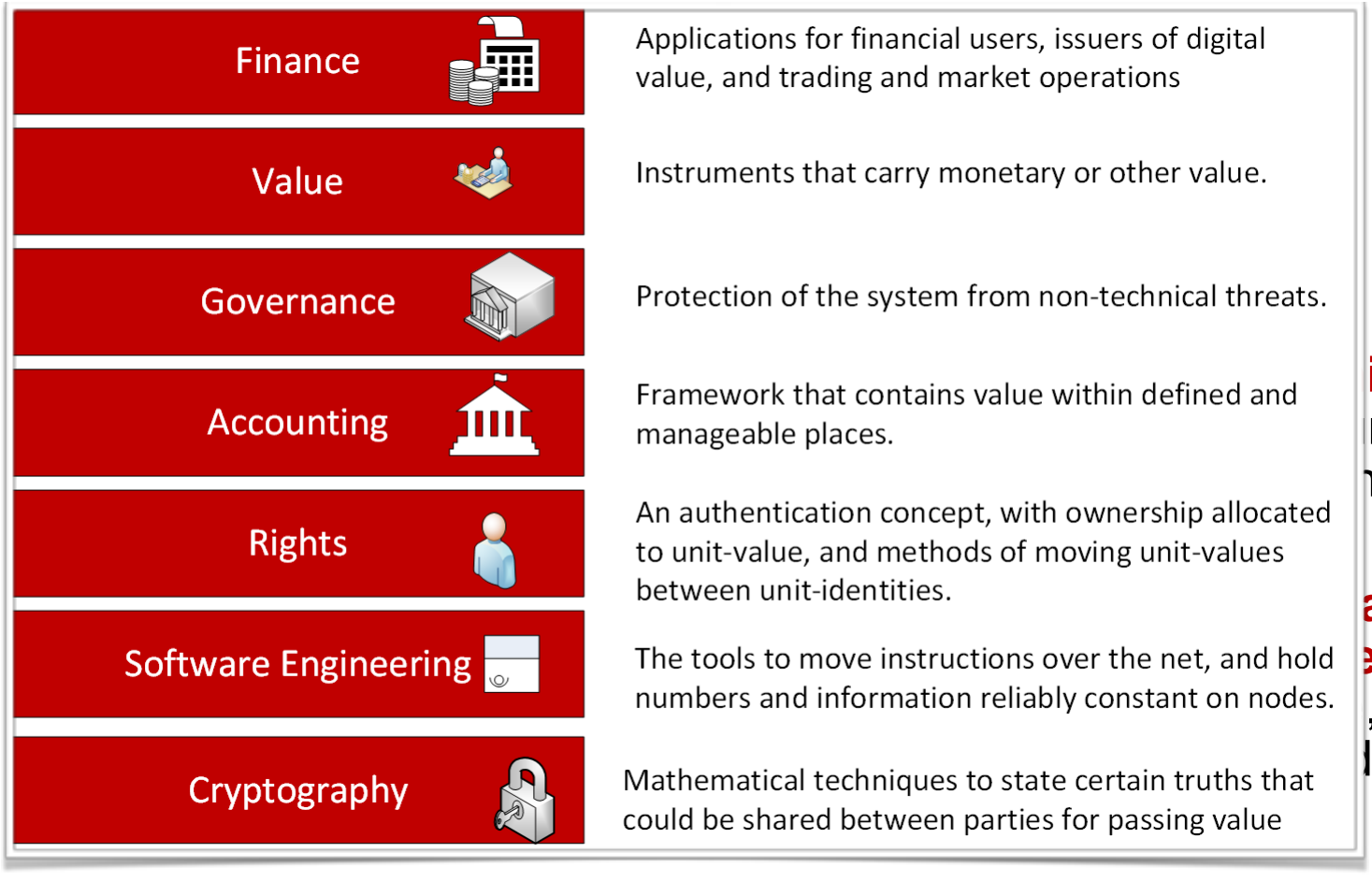


Prof Bill Buchanan OBE
http://asecuritysite.com/crypto10
http://asecuritysite.com/encryption

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.

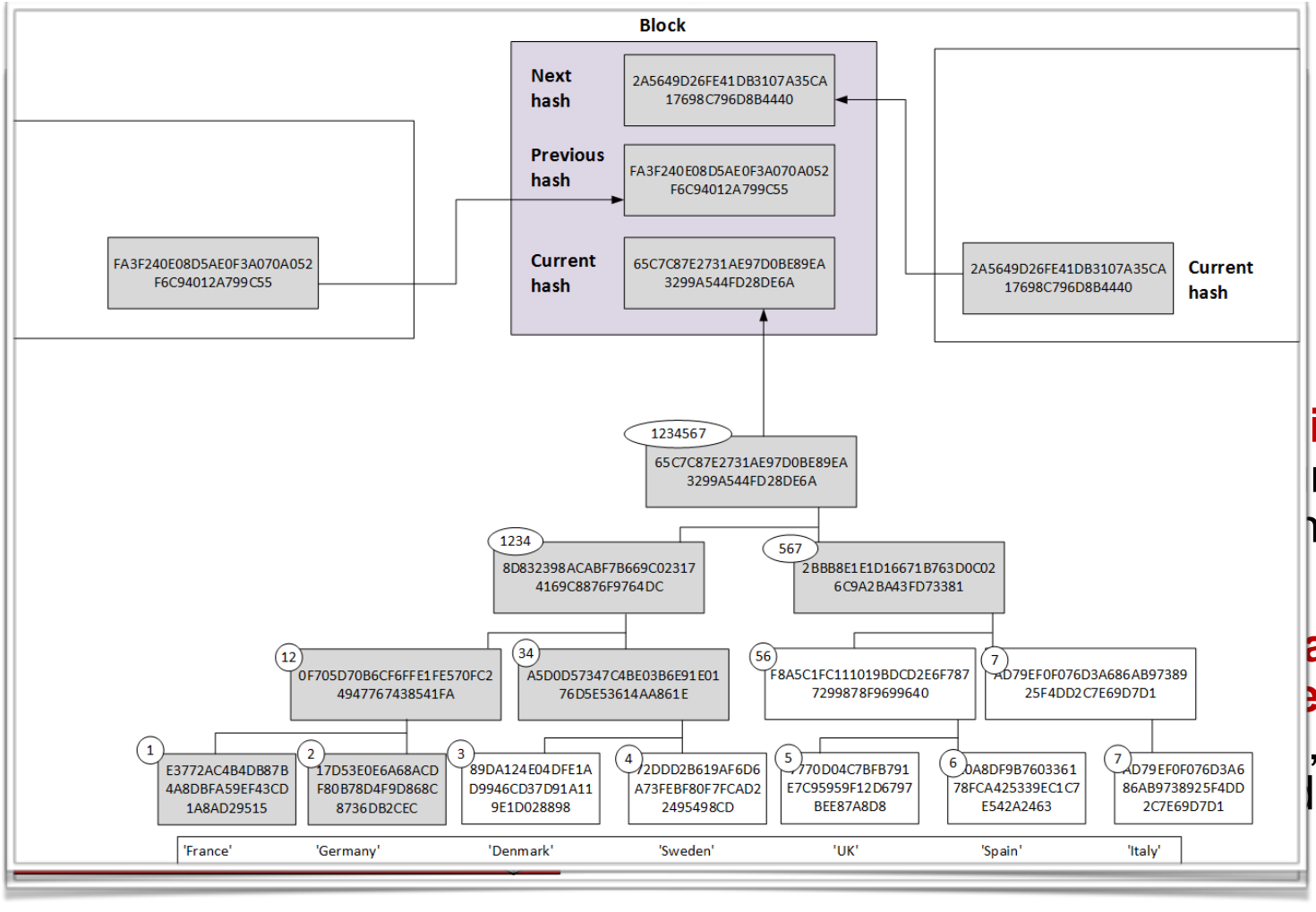
Merkle Trees



ing: Zero-
res, bullet
nding

and
e
,
l so on.

Merkle Trees

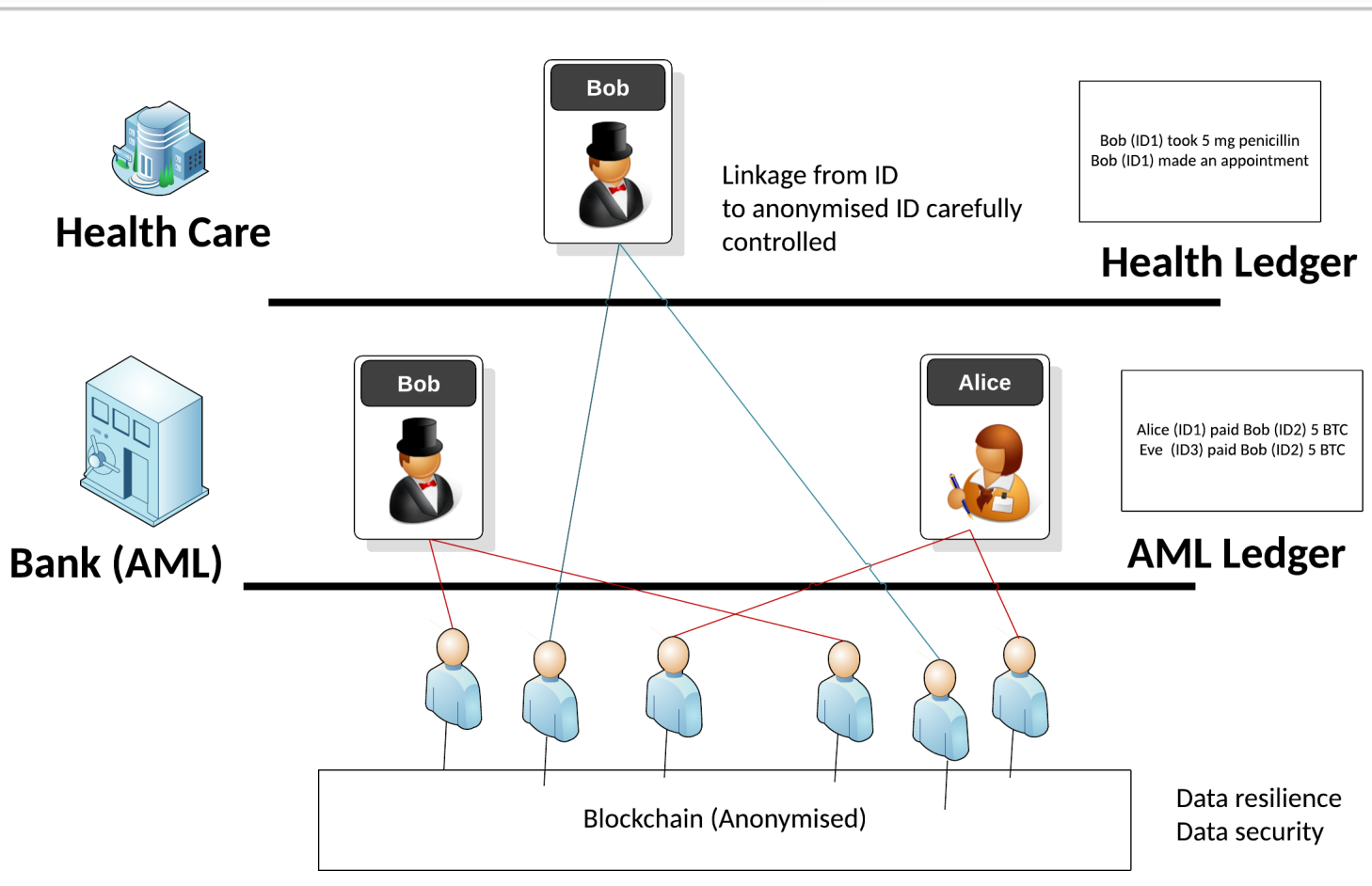


ing: Zero-
res, bullet
nding

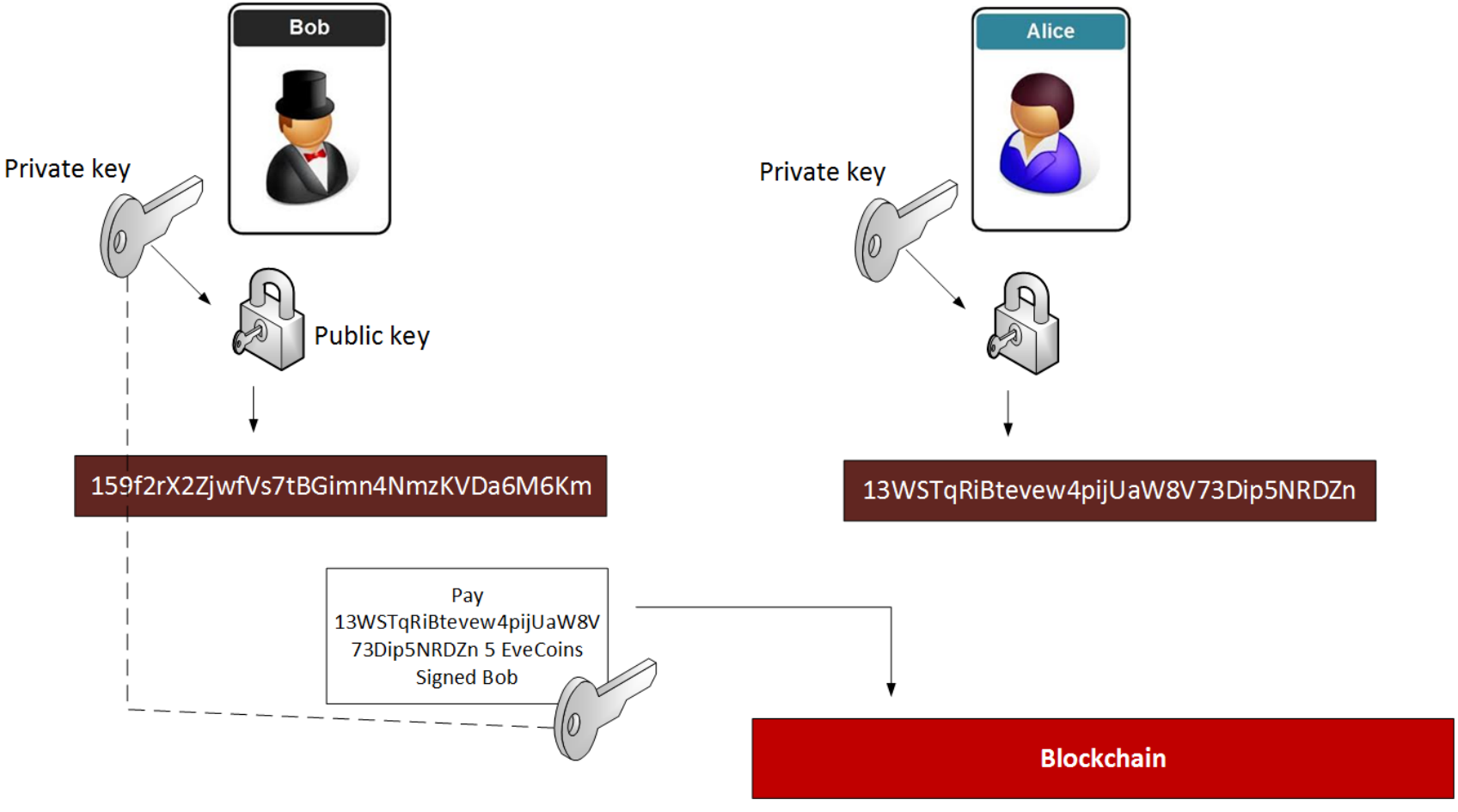
and
e

,
l so on.

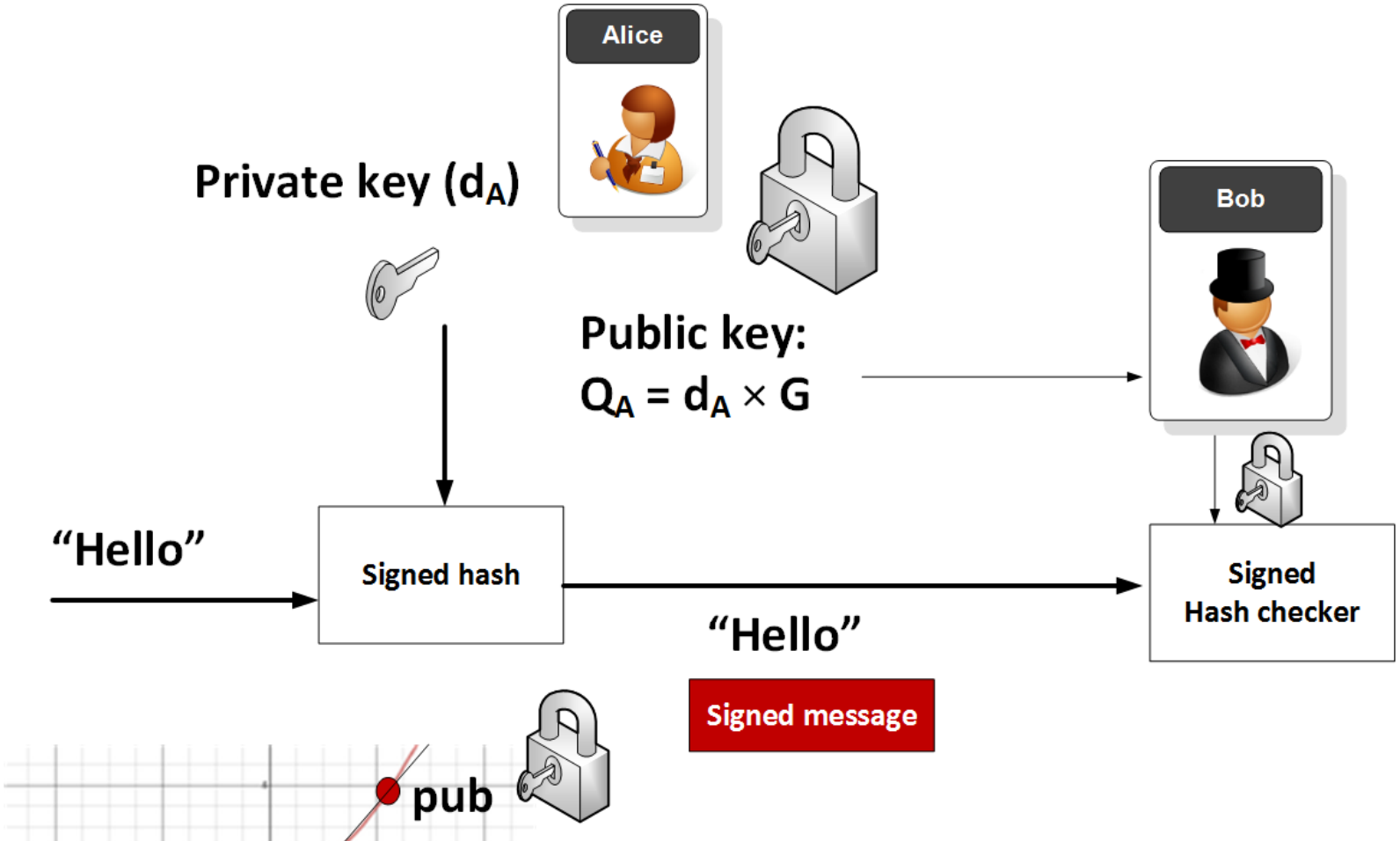
Merkle Trees



Signing


Bob
Private key
Public key
159f2rX2ZjwfVs7tBGimn4NmzKVDa6M6Km
Alice
Private key
13WSTqRiBtevew4pijUaW8V73Dip5NRDZn
Pay
13WSTqRiBtevew4pijUaW8V
73Dip5NRDZn 5 EveCoins
Signed Bob
Blockchain

Signing (ECDSA)



Signing (ECDSA)

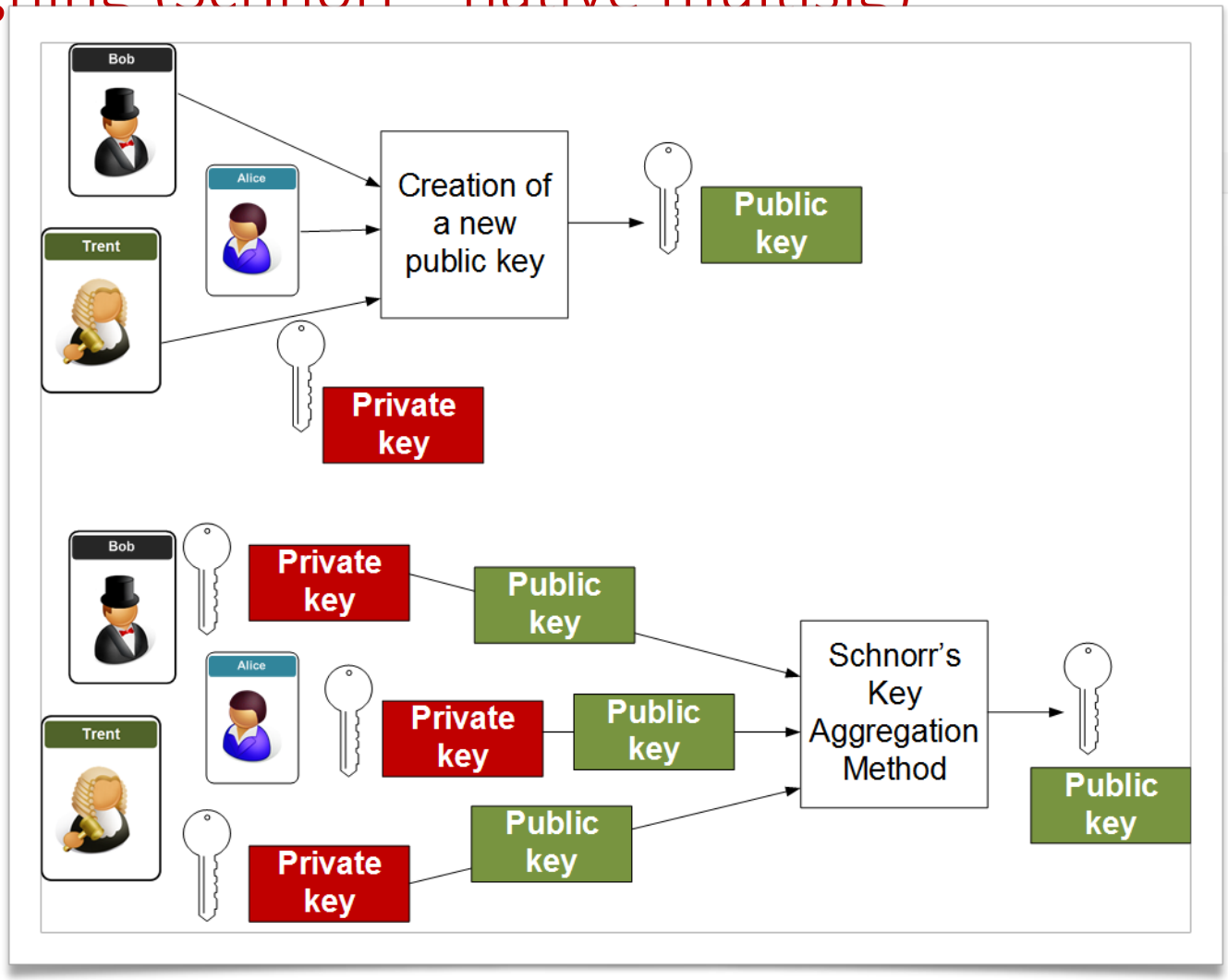
```
Message:        Hello
Hash (SHA-256): 185f8db32271fe25f561a6fc938b2e264306ec304eda518007d1764826381969

========Elliptic Curve details =============
N:      115792089237316195423570985008687907852837564279074904382605163141518161494337
G:      (55066263022277343669578718895168534326250603453777594175500187360389116729240L,
32670510020758816978083085130507043184471273380659243275938904335757337482424L)

========Create key pair =============
Private key:    54260937083493926038981685815910187164039687608704947340586607702205641918578
Public key:     (51462476226125324693025684915790979951700251074620825319023668376690501350840L,
80137489009097522664481006712918181535677174259818547781755223887788639948939L)

=======Signature generation (r,s) ==============
r= 636704063728040746068438717766447370792709280767385942762680911038141288992 90
s= 135037138853685559592866453073709672610739933868095822034745750432386472116 21

=======Signature verification (v==r) ==============
V= 636704063728040746068438717766447370792709280767385942762680911038141288992 90
Verified:       True
```

Signing (Schnorr - native multisig)

f0dfd34db8d5ed88fd63b9158e3c607fb43b018cb83d9eb3286b37895e90f21c

1Gu1fawp7rnHD24HiP1ui9CW2RNxmLSurb	31r32c4hHUjwkcLCbXU5XebPQkEBkXkJew	0.01530876 BTC
1D5GExtk7K9MDGeNWvyqS5jn83JcPEPFPA	1oXGCyr2Wup5dahXrwC5autn5b6j2GNj7	0.0315 BTC
1PZTQGXqpgLWTb2LzuPyetcGtk3HyTSxpe	1Dj6q6oRsGSGtYdVMNTn1BroBDfi8QgKrS	0.8607 BTC
1MVHnU3Jzz7SEx3BDRnpLNJyt7dGkzWxqs	1KtiphoFU576nRCtkRRZvS2ivVcFjWXdzW	0.1054132 BTC
137Vah6Gswbvhy1M8fLVrU3QJDKjWV5g9G	15QcmiZXe7F2SHmrnsvZAcuKvgNEuJU14c	0.05835529 BTC
15RxPPh3SYFJTKbJo4AStXakbMLcEhugxd	3DsXnWVo5He88VErXwaBHtgDgz3DR4QaHP	0.019 BTC
1FxL1WANoS1VNP53hTaQG8iJXrW7f3mEZj	14sLwu4J18PTsB6GqFvLAv4eFWoyZRd38w	4.26100882 BTC
1PuqSrmYdRRxcvqDLDid3FVuZLgzeSD5uo	1GqHd8SNxw83C5HZ1WwZYWmtd4MVUTPwLi	0.29682447 BTC
1JHfqbTomt6nNWwjVKBDaVFU4Gmnu5j8aU	19UyVvytaWpnVQmCVDewnNqNiaq4h7qvxj	0.043 BTC
14QvuuT7hsoVM6dEqMGXPZZDmEWQCSPZPR		
17Qzie5gtoSZupjQDgQeYy6oDet3QYnSzs		
1LTqSk6RABTyL3rhF4XeVTKFkuUJa5vEFq		
1HHgwc4QXi7ox1ePS2G2QxkQs328mv2eRX		
1HyvydVQ4Q3zHnrpC9RJ4BQX2VL7NnL2X9		
1oXMPKD6vibCicjXNZCkbfd2aTyfNetAZ		
1JniFCBcYnwJfH9UhoRGCWYCLZHdRKnJpE		
1BrigDNcmzz8LL84B5hoNEeY75eoZkMSYg		
132ixVUhHnXy7W9Nu2ZXXKz1ZNMABmzh9a		
143pGz8vQ35WNcEDgcVtPDRxtJnst1eMjy		
1PMHRabAPHxwqZXmrCGBSGyNxPtWyJ6ahL		
1PJSL49UEF6D93vxhLrYZXVj2dDb9XY3gA		
14i1bPWrFrFa4D2qdtnFzgUbSPNTgEKDcT		
17CxtBMmQ3t1gS4XpvRD8wEA717KGMXhYr		
13riMjSfSqb89EsEFaemFXts399YyEZupL		
1PiXXGhPu76p1udMzKLX3Twg6Lqiv5TzEw		
1Bk7Ndxr7tYHdf6dV8fCMrMbW9hSX1mstA		
1HL8nL4Gz4GmEZmsYJwNY7fPHMPecxYkxx		
1MV6kHCXmj2YnSZe8xW45acTHXfLzfgzh8		
1J9vf5fxjC8Dwuupp1wu7p2UDL7ZGBCXfE		

Signing (Schnorr - native multisig)



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)

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	00000000000000000015411ca4b35f7b48ecab015b14de5627b647e262ba0ec40
Previous Block	00000000000000000022552c92fdc5ac6c31a95f54d9ed9fcdf0fe00ff134773
Next Block(s)	00000000000000000278fb704dfaf2e6e517765144461f2fc5981da12a6b7b4
Merkle Root	8a13a3f9326b1073faa078007fadda8d1e9d46a50f4948055b7087c2ca8ee88d

Signing (Schnorr - native multisig)

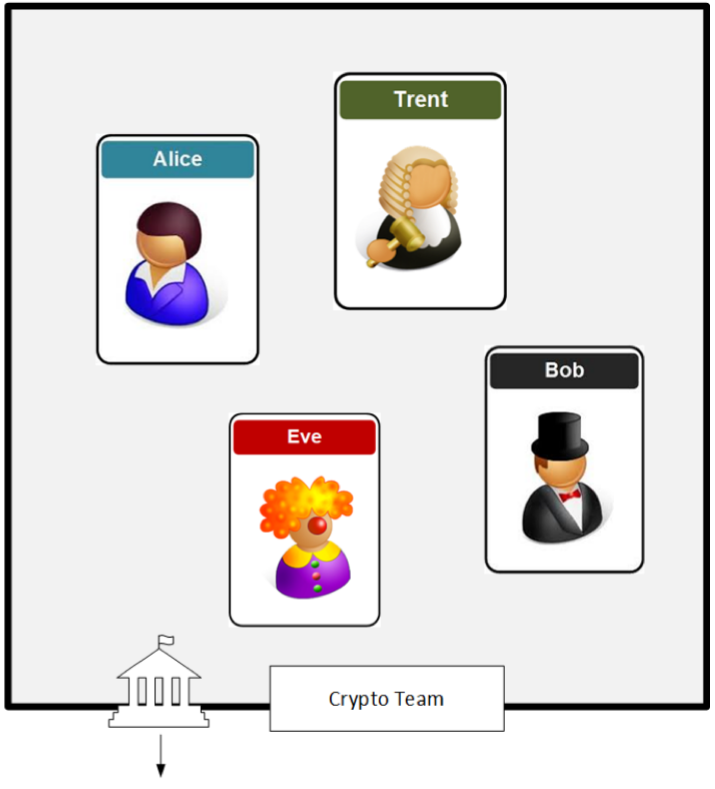
Block #477120

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	00000000000000000015411ca4b35f7b48ecab015b14de5627b647e262ba0ec40
Previous Block	00000000000000000022552c92fdc5ac6c31a95f54d9ed9fcdf0fe00ff134773
Next Block(s)	00000000000000000278fb704dfaf2e6e517765144461f2fc5981da12a6b7b4
Merkle Root	8a13a3f9326b1073faa078007fadda8d1e9d46a50f4948055b7087c2ca8ee88d

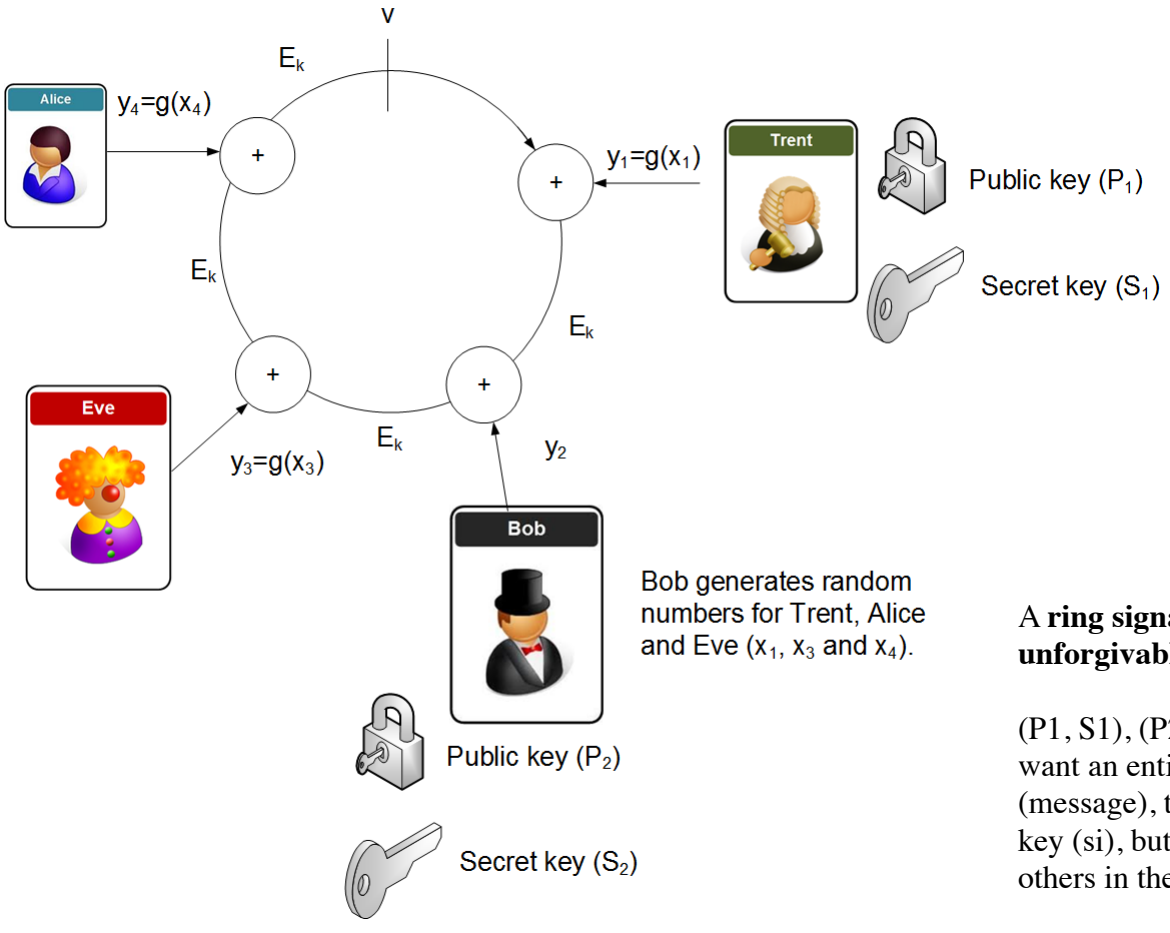
Ring Signatures

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



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

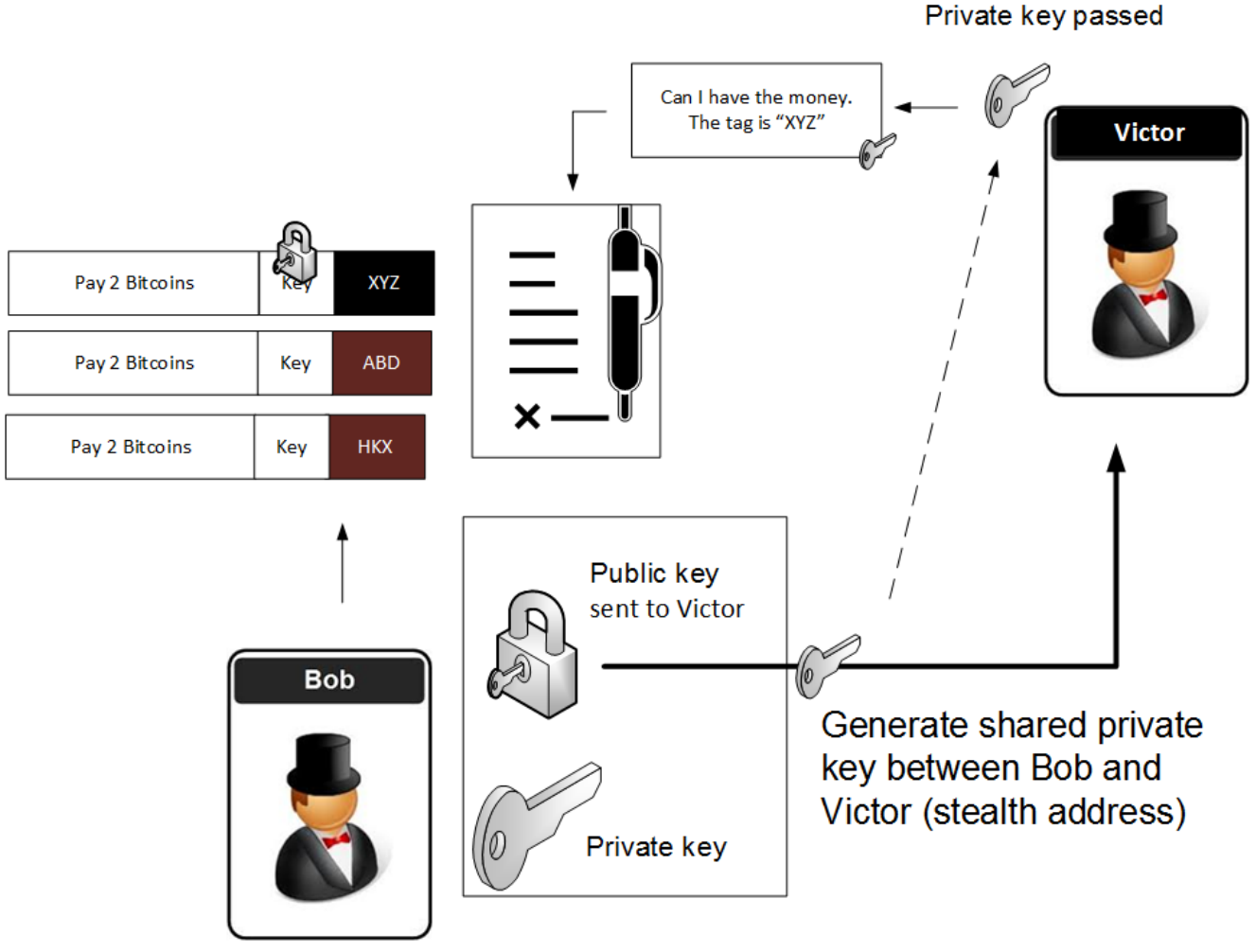
Ring Signatures



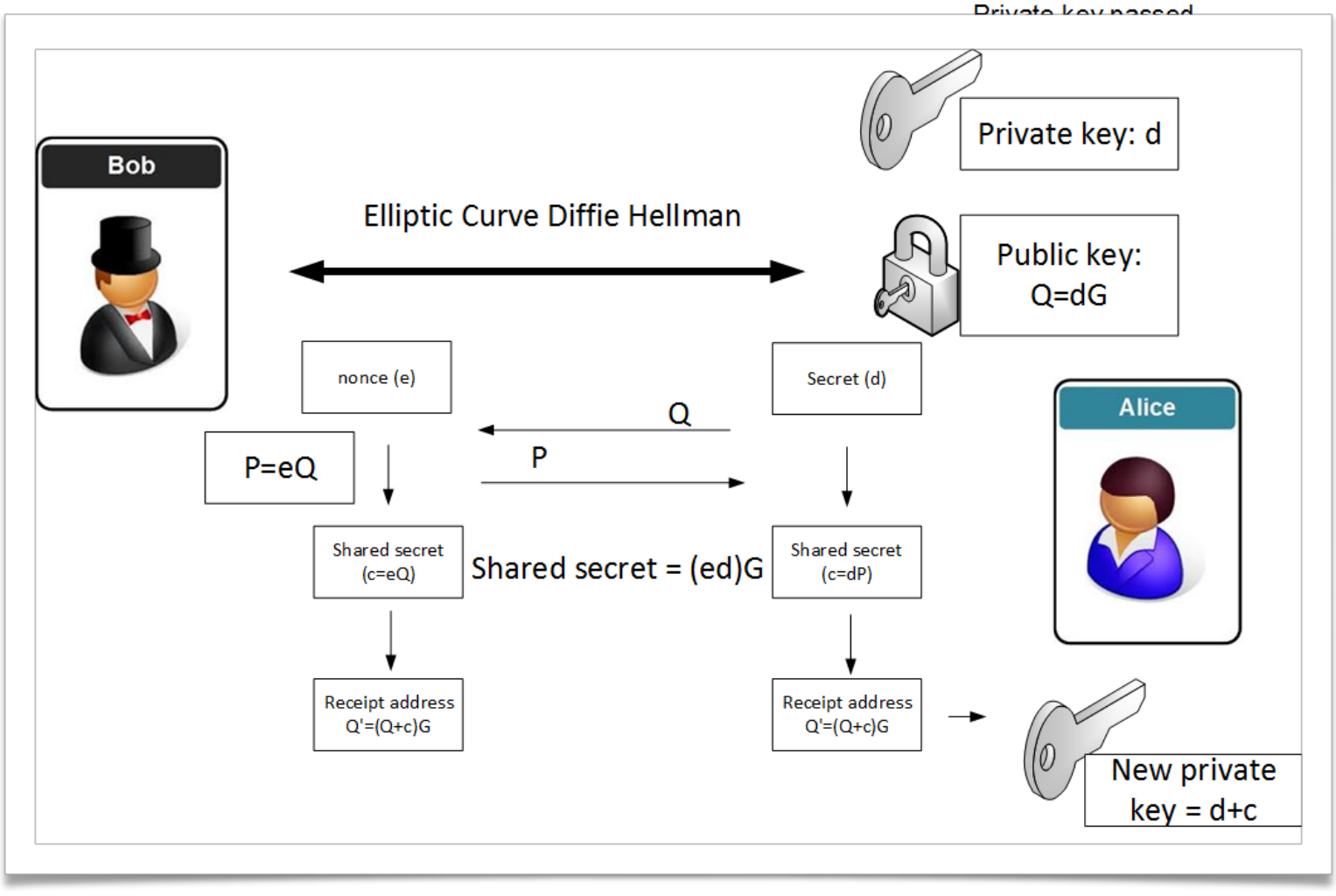
A **ring signature** provides **anonymity**, **unforgivably** and **collusion resistance.**

(P1, S1), (P2, S2), …, (Pn, Sn). If we want an entity i to sign a message (message), they use their own secret key (si), but the public keys of the others in the group (m,si,P1…Pn)

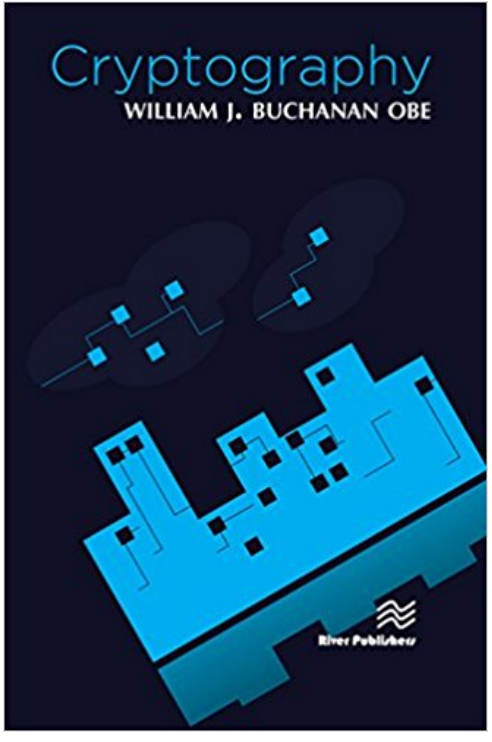
Stealth Address



Stealth Address



Chapter 10: Blockchain and Cryptocurrencies



Cryptocurrencies
Bitcoin addresses
Blockchain
Mining
Ethereum
Smart Contracts

Prof Bill Buchanan OBE
http://asecuritysite.com/crypto10
http://asecuritysite.com/encryption

LiveSlides web content

To view

Download the add-in.

liveslides.com/download

Start the presentation.