Blockchain and Cryptocurrencies

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

Prof Bill Buchanan OBE

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

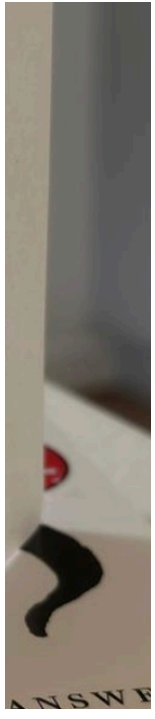
Blockchain and Cr

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

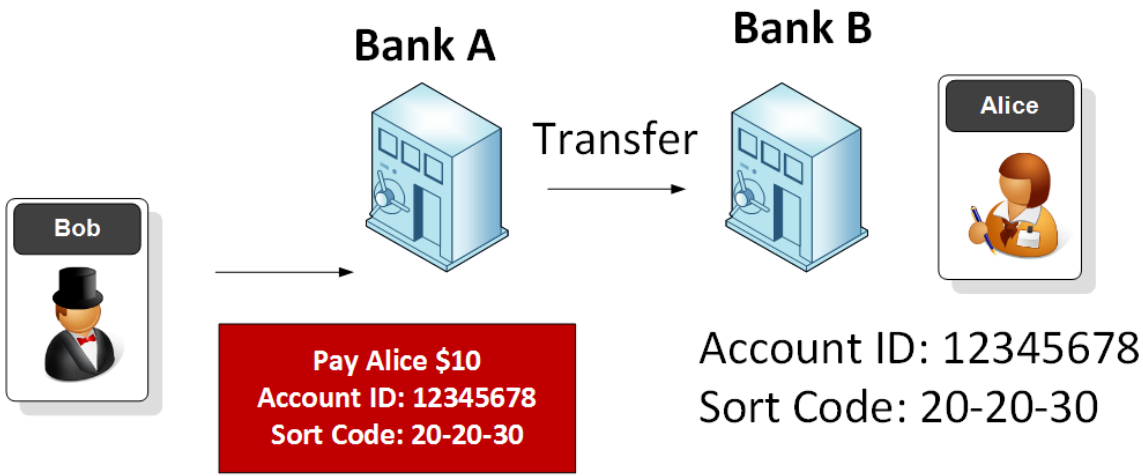
Prof Bill Buchanar

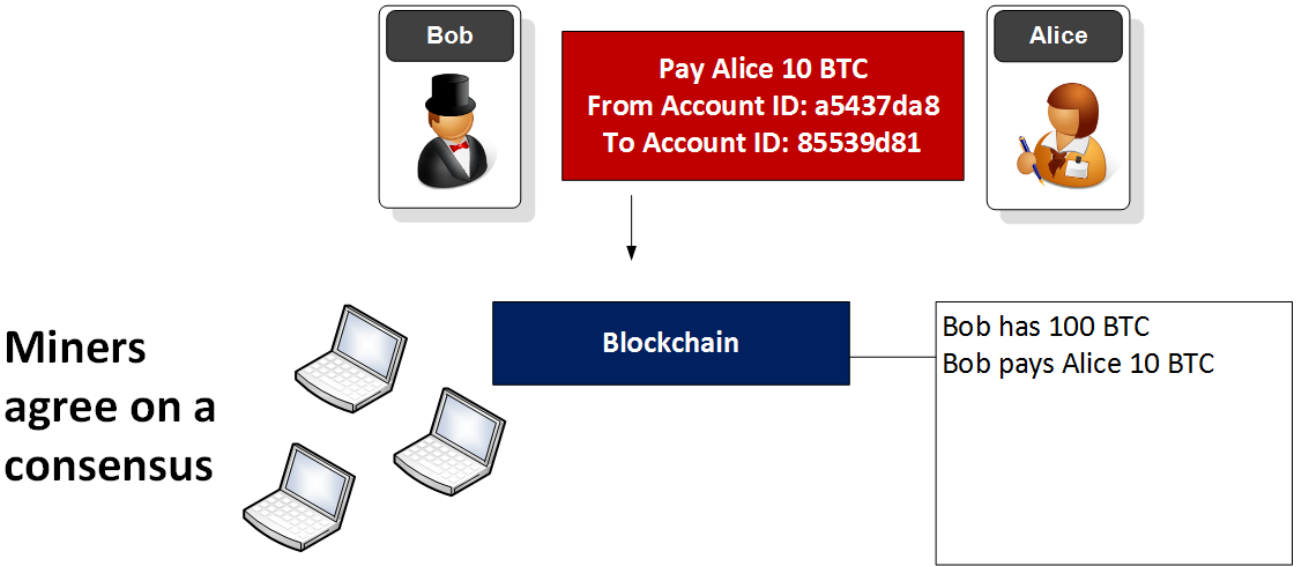
http://asecuritysite.com/c
http://asecuritysite.com/e

No	Date	Subject	Lab
2	27 Jan 2023	Ciphers and Fundamentals [Unit]	[Lab] [Demo]
3	3 Feb 2023	Symmetric Key [Unit]	[Lab]
4	10 Feb 2023	Hashing and MAC [Unit]	[Lab] Jean-Philippe Aumasson
5	17 Feb 2023	Asymmetric (Public) Key [Unit]	[Lab]
6	24 Feb 2023	Key Exchange [Unit]	[Lab] Bruce Schneier/Neal Koblitz
7	3 Mar 2022	Digital Signatures and Certificates [Unit]	[Lab]
8	10 Mar 2023	Revision lecture and Test 1/Coursework	Mini-project Marty Hellman [Here] /Coursework
9	17 Mar 2023	Test (Units 1-5) 40% of overall mark [Here]	
10	24 Mar 2023	Tunnelling [Unit]	[Lab]
11	31 Mar 2023	Blockchain [Unit]	[Lab]
12	21 Apr 2023	Future Cryptography [Unit]	[Lab]
13	28 Apr 2023	Host/Cloud Security [Unit]	[Lab]
14	5 May 2023		
15	12 May 2023	Coursework Hand-in - 60% of overall mark (15 May) [Coursework]	



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

Who is 14 years old?

Who is 14 years old?

Who is 14 years old?

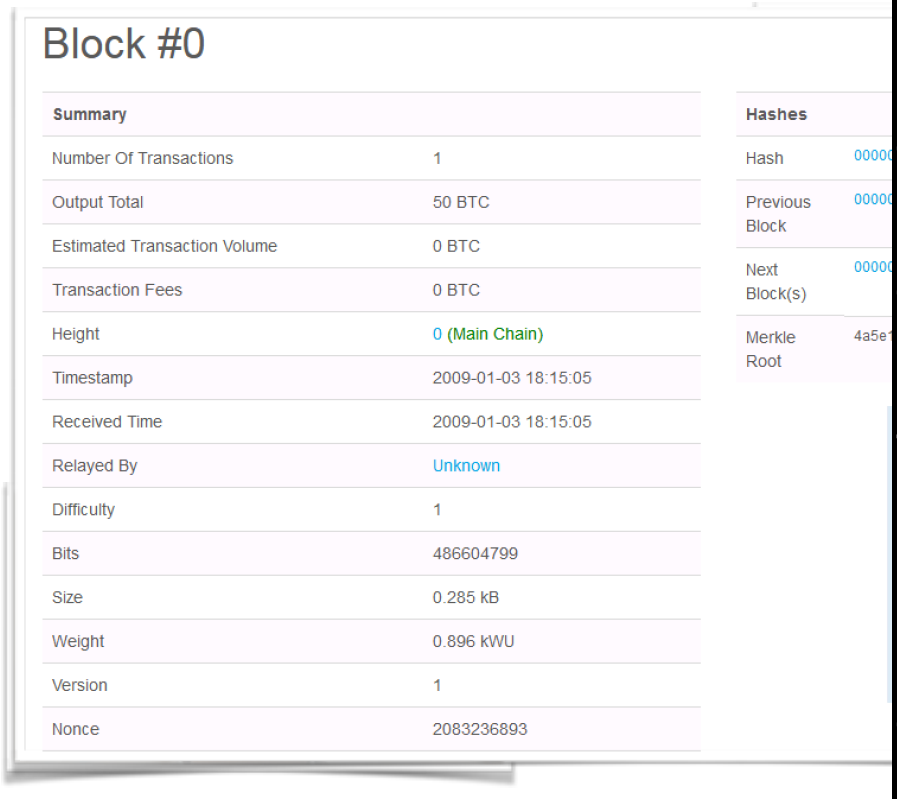
Who is 14 years old?

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 14 years old?



Block #0

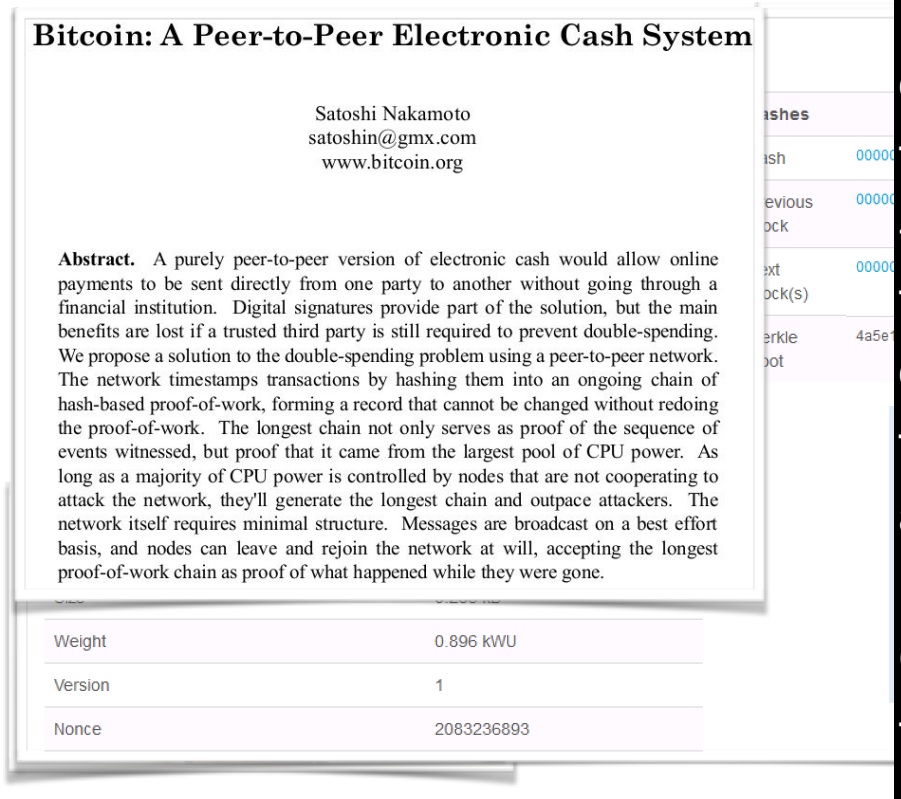
Summary	
Number Of Transactions	1
Output Total	50 BTC
Estimated Transaction Volume	0 BTC
Transaction Fees	0 BTC
Height	0 (Main Chain)
Timestamp	2009-01-03 18:15:05
Received Time	2009-01-03 18:15:05
Relayed By	Unknown
Difficulty	1
Bits	486604799
Size	0.285 kB
Weight	0.896 kWU
Version	1
Nonce	2083236893

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 31 March 2023, the blockchain size is around 468GB, and there are 19 million coins in circulation [here].

Who is 14 years old?



Bitcoin: A Peer-to-Peer Electronic Cash System

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

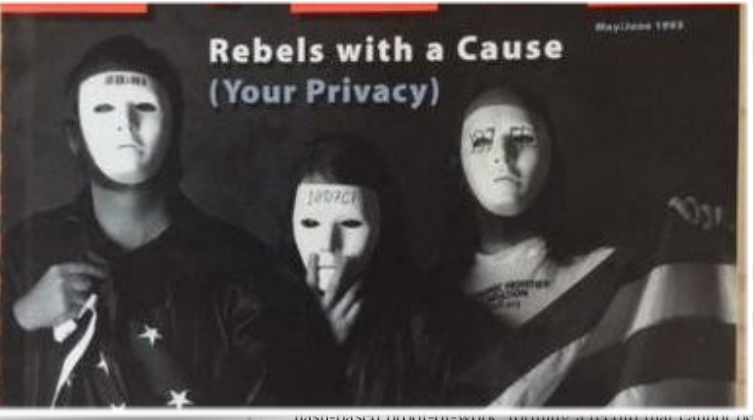
Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required 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 31 March 2023, the blockchain size is around 468GB, and there are 19 million coins in circulation [here].

Who is 14 years old?



ic Cash System

ashes

ash 0000

evious 0000
ock

ext 0000
ock(s)

erkle 4a5e
oot

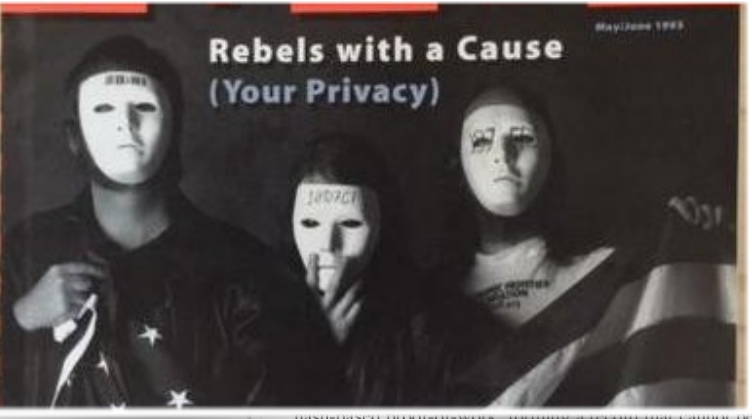
cash would allow online without going through a e solution, but the main prevent double-spending. g a peer-to-peer network. nto an ongoing chain of changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the 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.

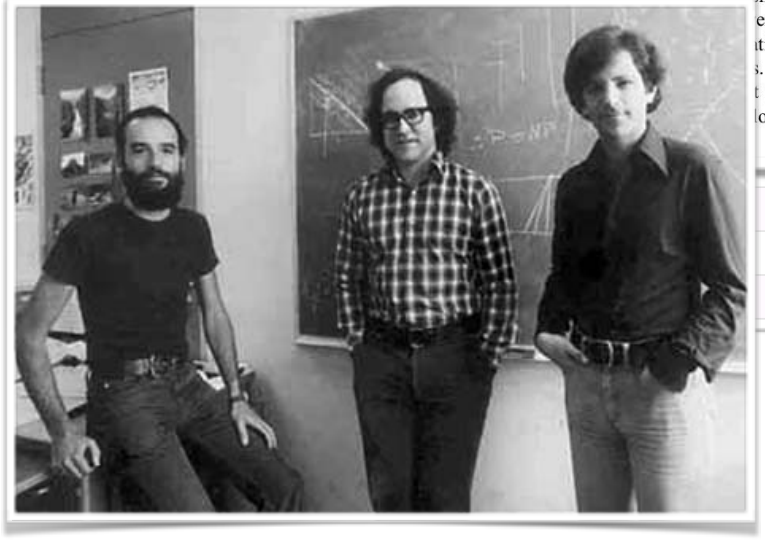
Weight	0.896 kWU
Version	1
Nonce	2083236893

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 31 March 2023, the blockchain size is around 468GB, and there are 19 million coins in circulation [here].

Who is 14 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 31 March 2023, the blockchain size is around 468GB, and there are 19 million coins in circulation [here].

Who is 14 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 31 March 2023, the blockchain size is around 468GB, and there are 19 million coins in circulation [here].

Who is 14 years old?

His work was a hotch-potch of
differing cryptography methods
be sourced in the 1970s
ublic key - and also of
unk movement which
in the 1990s, and was
Eric Hughes, Tim May
Gilmore.

As of 31 March 2023,
ain size is
around 468GB, and there are 19
million coins in circulation [here].

The Most Profitable Crime?

The Most Profitable Crime?

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

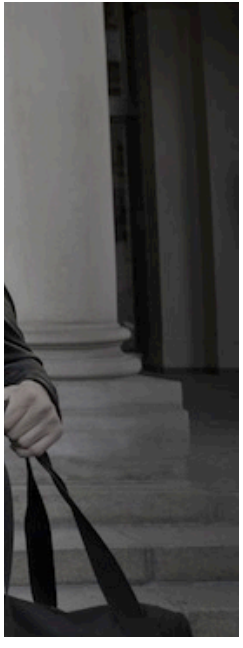
Published on December 21, 2017 Edit article | View stats

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

132 12 6 3

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

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



The Most Profitable Crime?

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

Published on December 21, 2017 Edit article | View stats

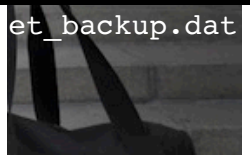
Prof Bill Buchanan OBE, PhD, FBCS
Professor at Napier University
1,194 articles

132 12 6

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

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

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



The Most Profitable Crime?

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

```
wallet.dat.1

wallet.dat.zip
```

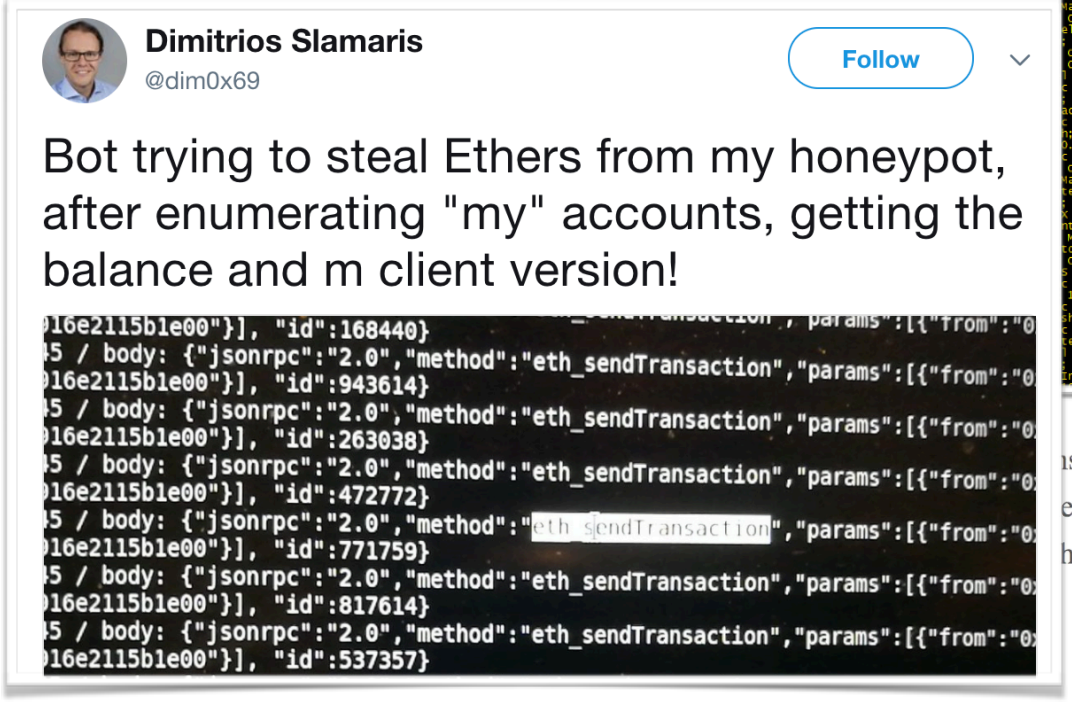
While cryptocurrencies are safe in themselves, the major problem seems to be with the places which hold the wallets. In 2014, for example, Mt. Gox - a Japanese cryptocurrency exchange - filed for bankruptcy after a hacker drained the exchange of 100s of thousands of Bitcoins.

The Most Profitable Crime?

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

wallet.dat.1

wallet.dat.zip



Dimitrios Slamaris
@dim0x69

Follow

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

```
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}
```

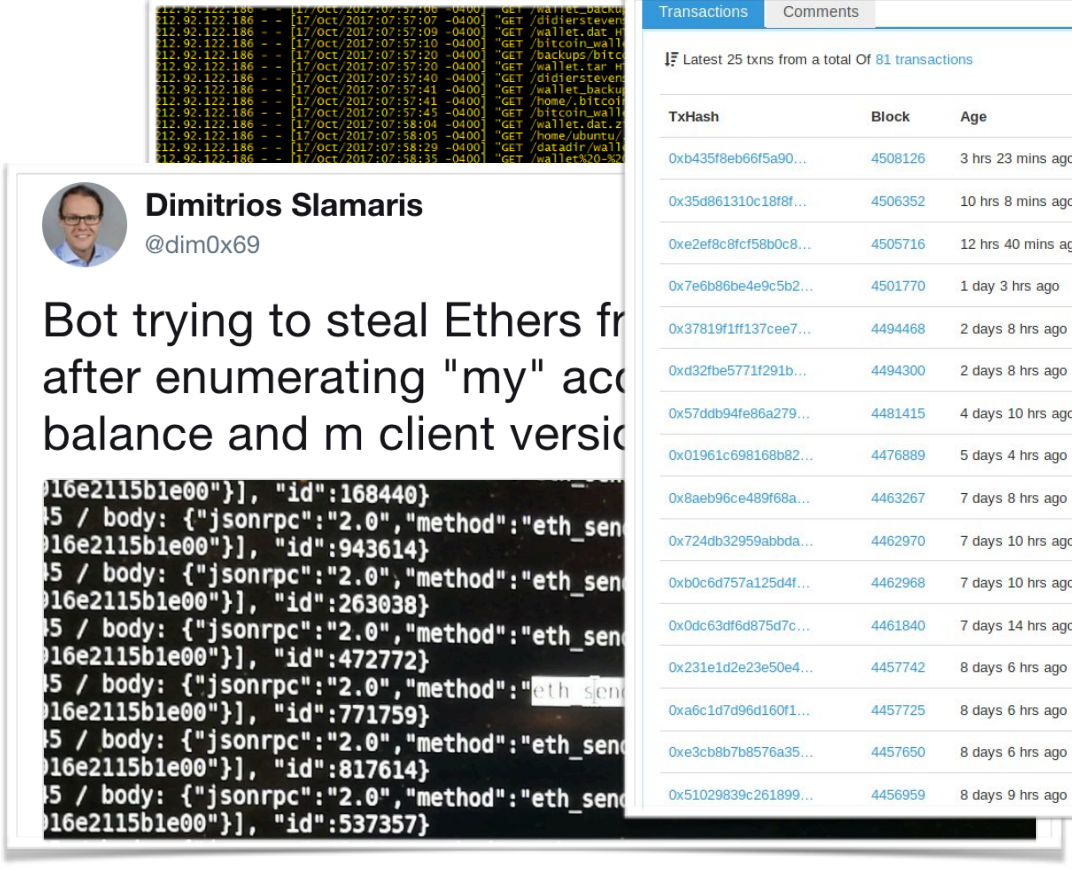
...s to be with the
...ese
...he exchange of

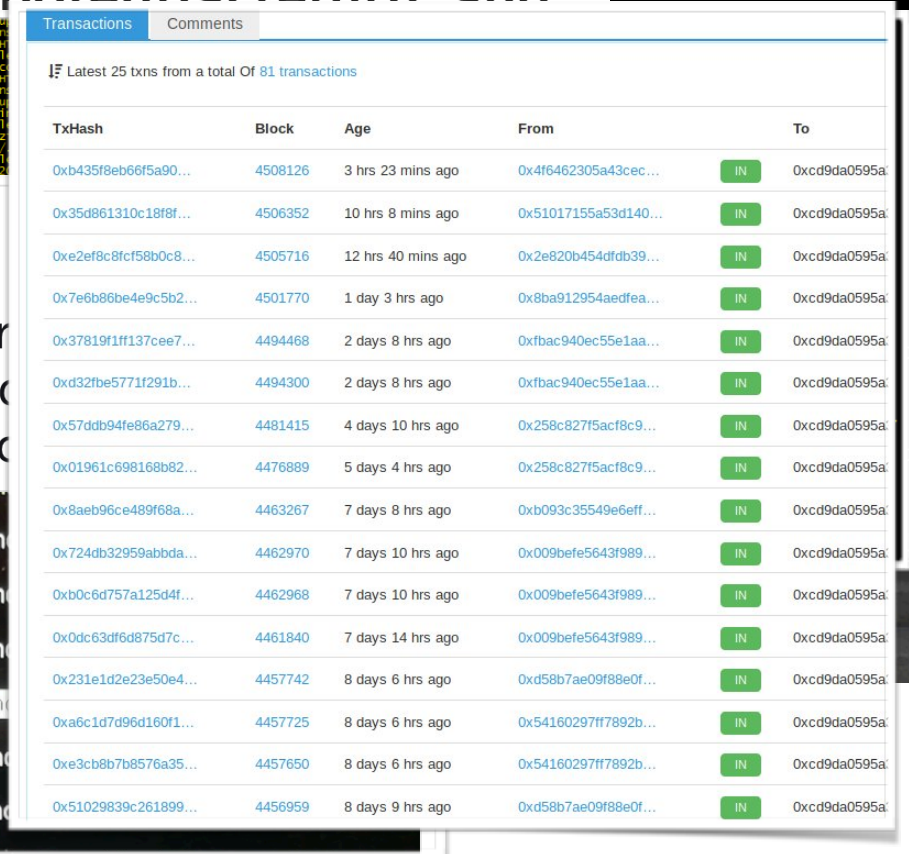
The Most Profitable Crime?

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

wallet.dat.1

wallet.dat.zip





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 is consent?

Who's laws do I comply with?

What are physical borders?

Dear 21st Century …

What is the ownership of something?

What is consent?

Who's laws do I comply with?

What are physical borders?

Why does fiat currency exist?

Dear 21st Century …

What is the ownership of something?

What is consent?

What are my rights to privacy?

Who's laws do I comply with?

What are physical borders?

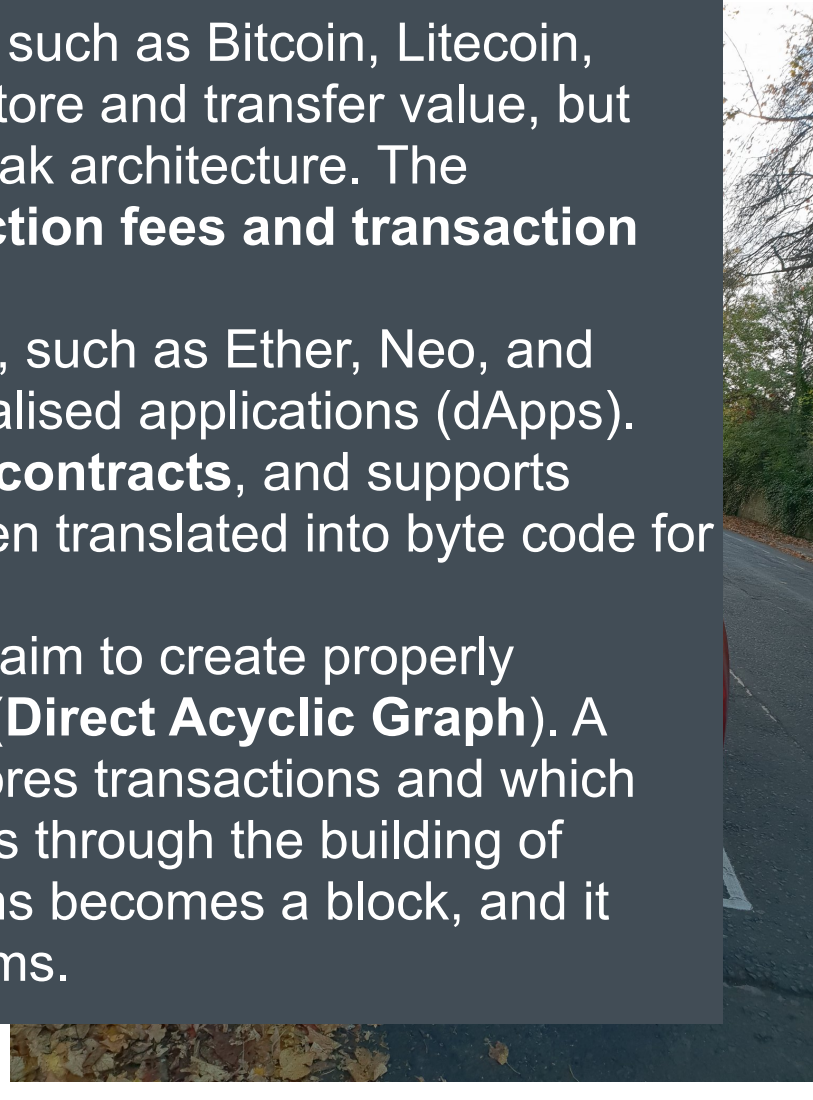
Why does fiat currency exist?

Dea

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

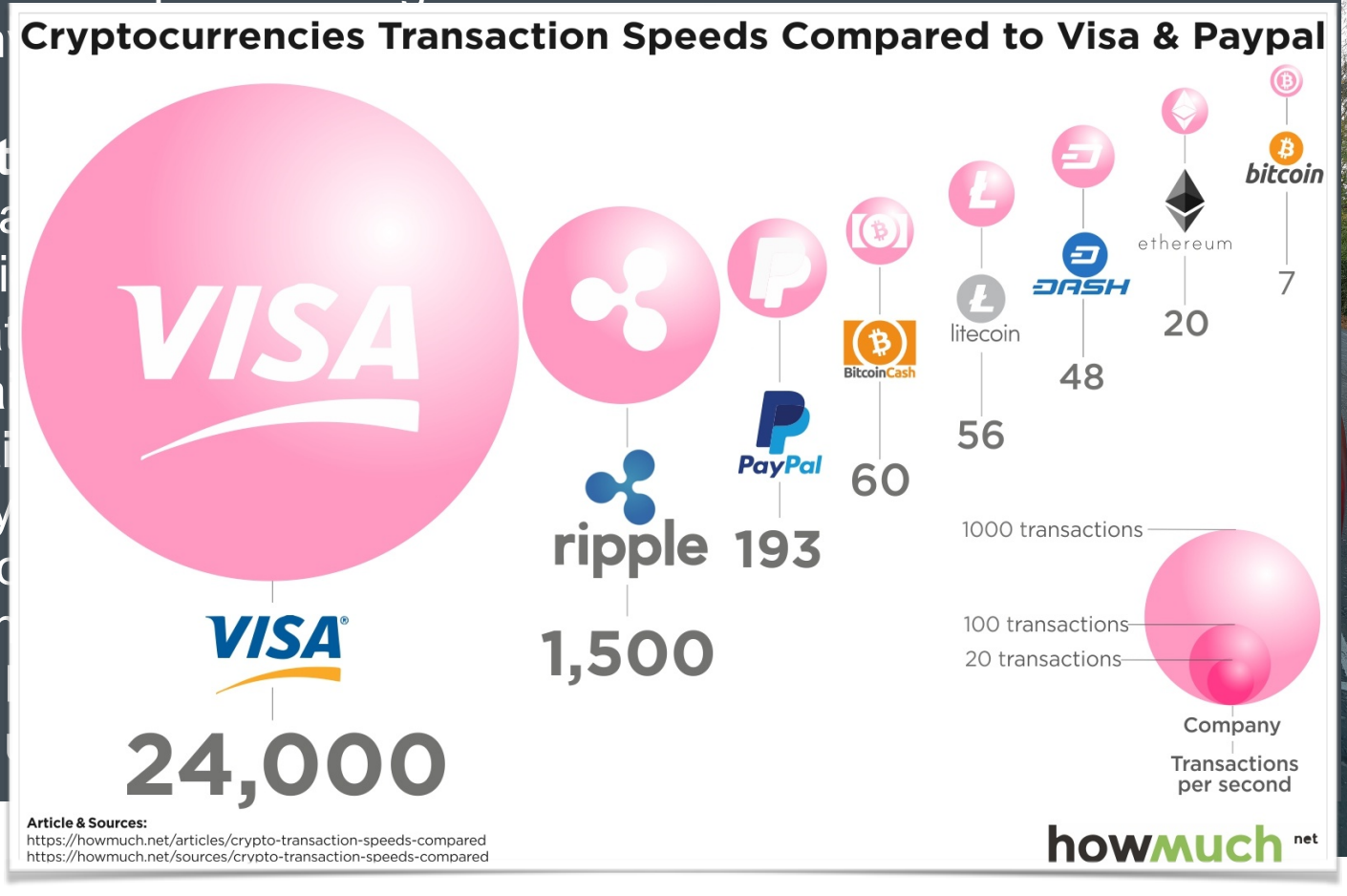
2nd Generation. These cryptocurrencies, such as Ether, Neo, and Lisk, have platforms that support decentralised applications (dApps). This generation adds **coding and smart contracts**, and supports logical operations. A high-level code is then translated into byte code for the Blockchain.

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



Dea

1st Generation. These cryptocurrencies, such as Bitcoin, Litecoin, Monero and Bitcoin Cash, basically just store and transfer value, but have suffered from poor scaling and a weak architecture. The overheads in
times.
2nd Generat
Lisk, have pla
This generati
logical opera
the Blockcha
3rd Generati
distributed sy
traditional Blo
can take som
blocks. With
thus speeds



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

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

- based on thier respective we

blocks. With
thus speeds

24,000

Company

Transactions per second

Article & Sources:
https://howmuch.net/articles/crypto-transaction-speeds-compared
https://howmuch.net/sources/crypto-transaction-speeds-compared

howmuch.net

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

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

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

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

50 BTC

Big accounts

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

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

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

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

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

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

Request Payment

Donation Button

e3a9cbec0c5ec55db3ac02029d8cbaf1370e04e8603d9e5000106091c66c308d 2017-11-14 08:03:03

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

13,083.32386362 BTC

Genesis Record

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

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

Request Payment

Donation Button

Transactions (Oldest First)

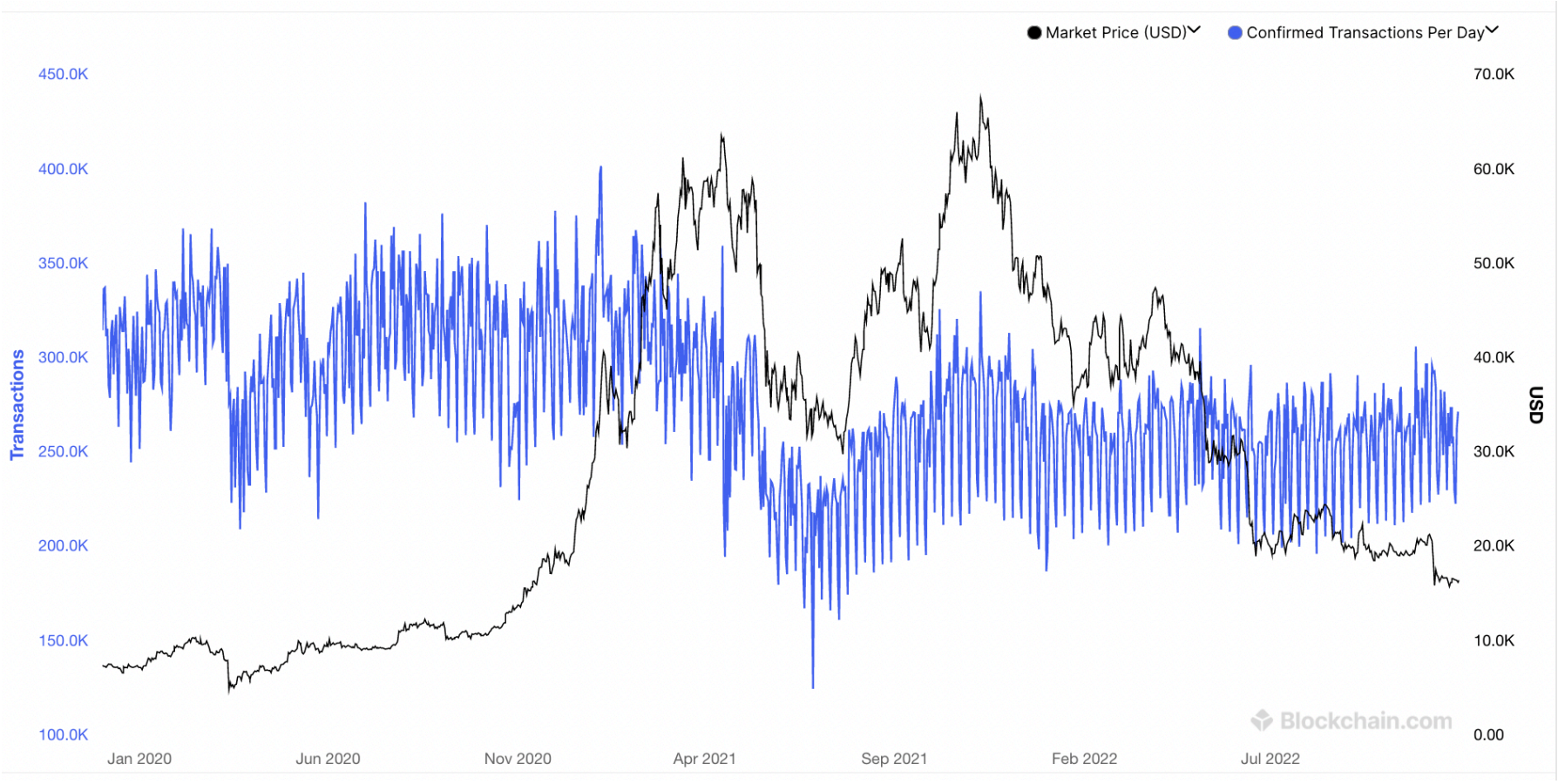
Filter

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

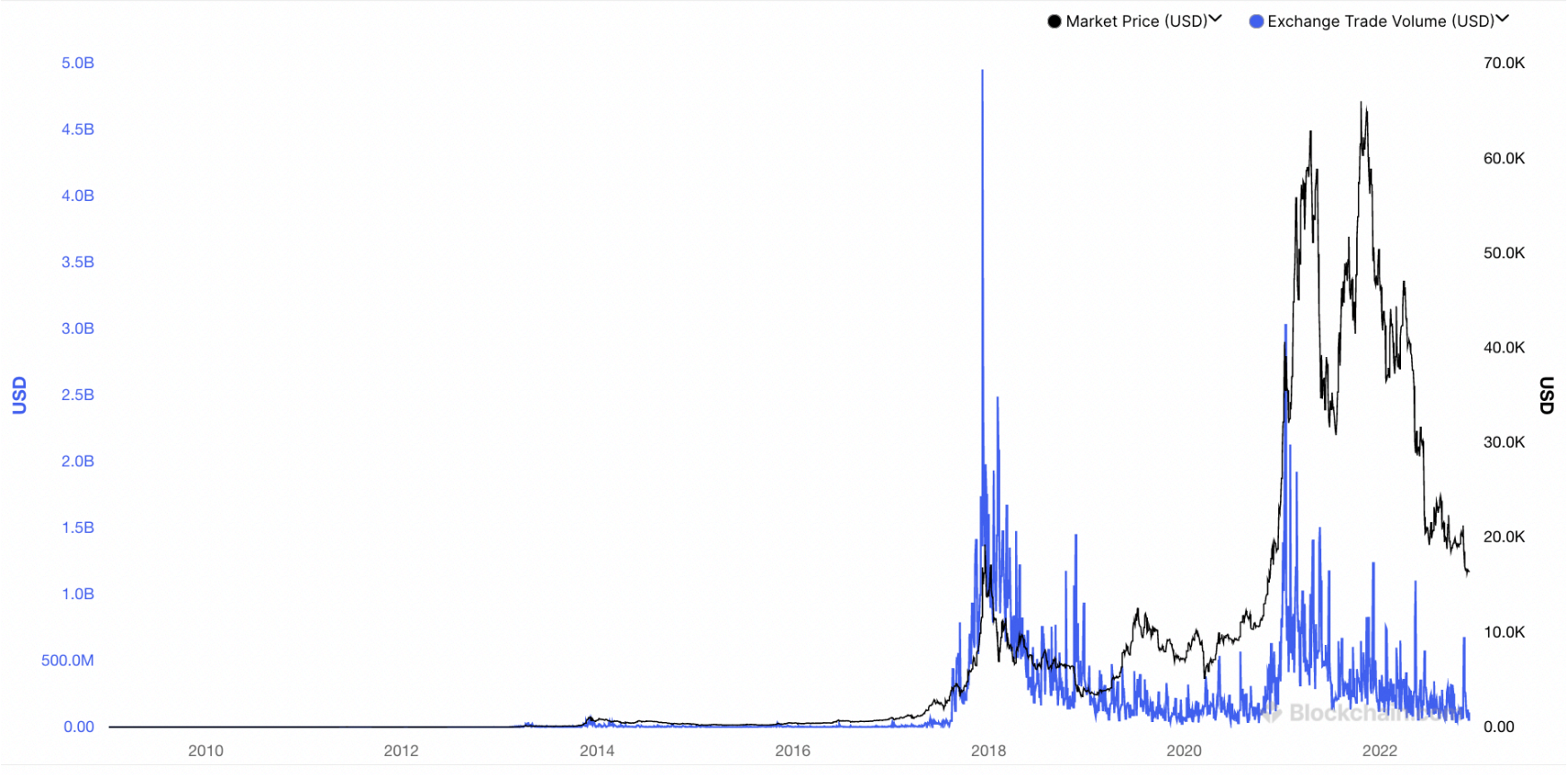
1 Confirmation

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

Bitcoin transactions and valuation



Bitcoin trading volume



Types

Rank	Name	Symbol	Market Cap	Price	Circulating Supply	Volume(24h)	% 1h	% 24h	% 7d	
1	Bitcoin	BTC	$916,584,603,074	$49,044.07	18,689,000 BTC	$84,848,720,558	-1.64%	-9.41%	-21.26%	···
2	Ethereum	ETH	$253,947,388,866	$2,197.10	115,583,148 ETH	$57,198,614,270	-1.78%	-9.71%	-10.63%	···
3	Binance Coin	BNB	$73,404,926,797	$478.42	153,432,897 BNB *	$9,192,682,304	-3.04%	-13.75%	-8.25%	···
4	Tether	USDT	$49,276,385,899	$0.9999	49,280,887,017 USDT *	$199,608,905,553	-0.02%	-0.01%	-0.24%	···
5	XRP	XRP	$47,579,438,812	$1.05	45,404,028,640 XRP *	$19,404,713,266	-0.60%	-20.41%	-38.94%	···
6	Cardano	ADA	$32,684,467,819	$1.02	31,948,309,441 ADA	$6,490,615,786	-4.52%	-15.41%	-28.91%	···
7	Polkadot	DOT	$27,081,677,364	$29.06	932,013,186 DOT *	$4,360,572,693	-3.06%	-13.81%	-31.90%	···
8	Dogecoin	DOGE	$26,550,082,761	$0.2053	129,293,495,715 DOGE	$14,937,458,445	-1.63%	-26.84%	-16.82%	···
9	Uniswap	UNI	$16,516,768,574	$31.56	523,384,244 UNI *	$2,116,278,780	-2.72%	-12.38%	-15.03%	···
10	Litecoin	LTC	$14,973,524,377	$224.31	66,752,415 LTC	$11,354,836,568	-3.12%	-14.46%	-22.61%	···
11	Bitcoin Cash	BCH	$14,178,696,762	$757.55	18,716,394 BCH	$8,014,193,794	-2.25%	-17.40%	-18.56%	···
12	Chainlink	LINK	$13,227,306,261	$31.57	419,009,556 LINK *	$3,945,256,339	-3.41%	-13.72%	-23.91%	···
13	USD Coin	USDC	$11,242,171,707	$0.9999	11,243,286,480 USDC *	$3,634,991,378	-0.02%	-0.01%	-0.19%	···

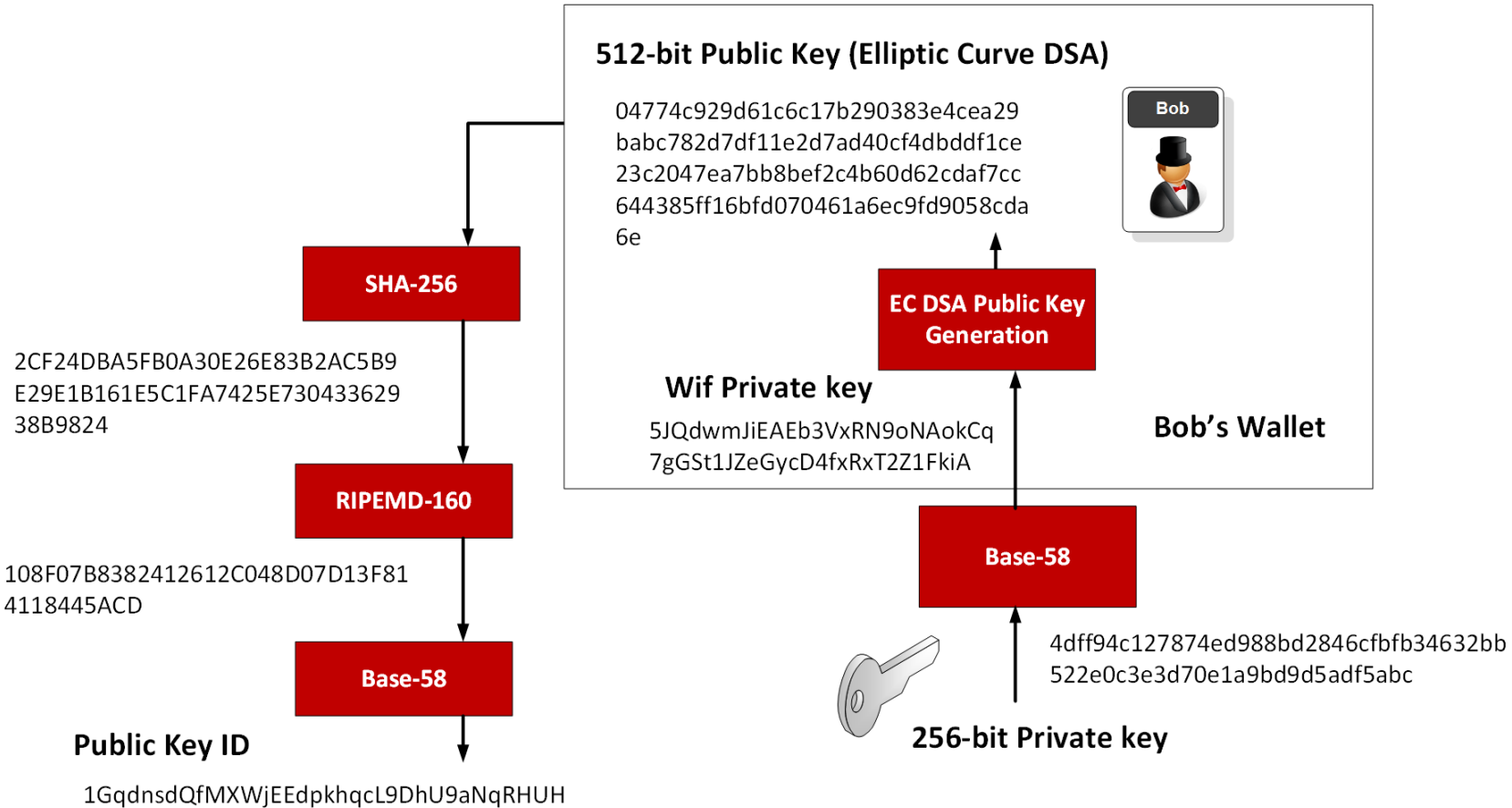
Blockchain and Cryptocurrencies

Cryptocurrencies
> Bitcoin addresses
Blockchain
Mining
Ethereum
Smart Contracts
Blockchain Crypto

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

Bitcoin Wallet and Addresses

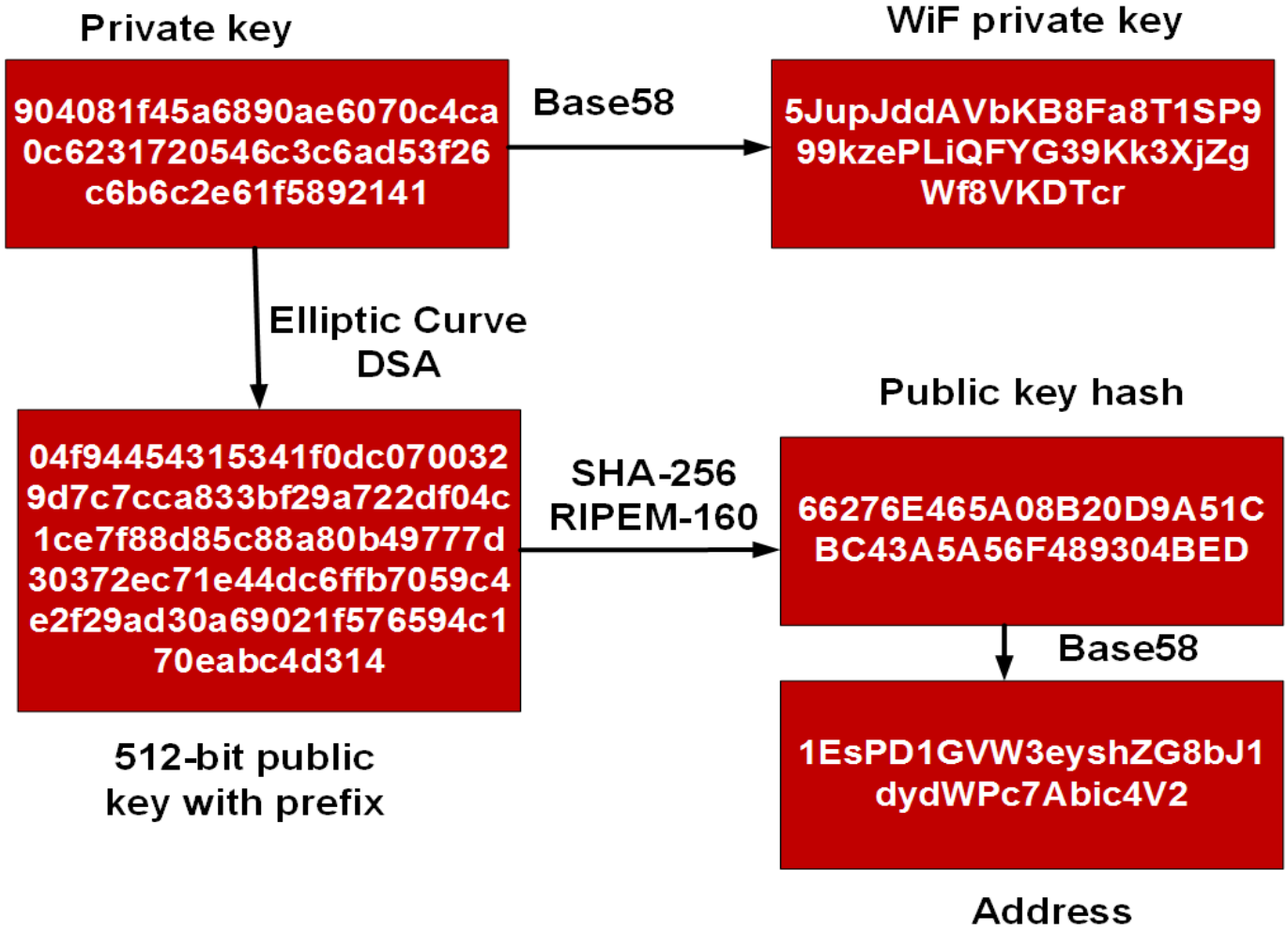
P2PKH - Public key hash - **1**7VZNX1SN5NtKa8UQFxwQbFeFc3iqRYhem
P2SH - Pay to script hash - **3**EktnHQD7RiAE6uzMj2ZifT9YgRrkSgzQX - Sender proves a script.



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
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

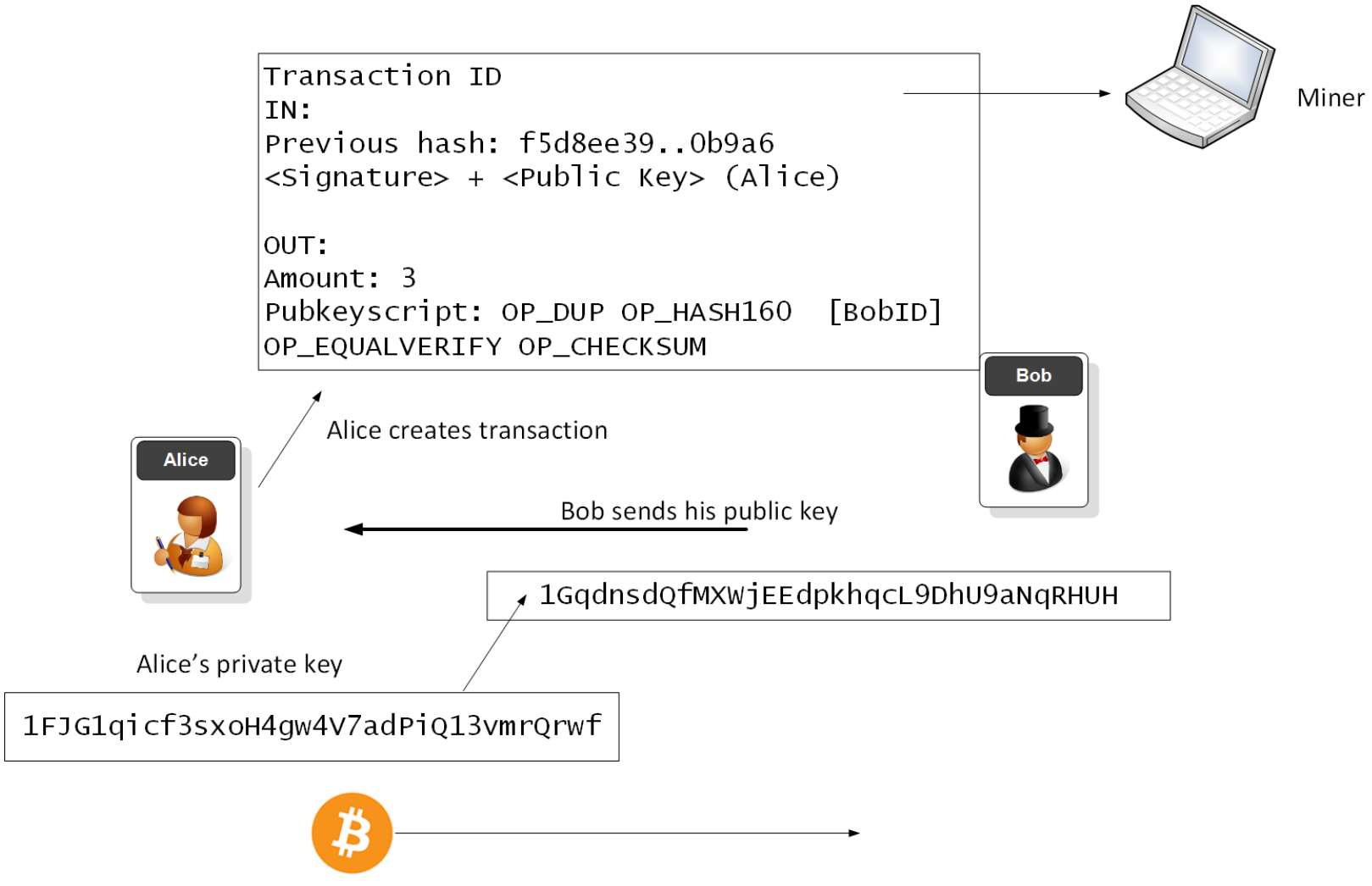
Public key:
0489fc7b8c3f655a10840d35c76ebb5596694045e49e940fb1e7a759da4edf0fafc45bb
bea6f5a56abf14c145c529c8eda9d3ad606f3a0bf4ca01ce991d4987b97

Wif: 5JPmDetQXXvc5aT5efyrg7BxHbH4135owRzq9DD7n2eWQCta5MN

Address: 16RAf9CjnstWCfBJGfrzSSMfTeHJVt8QWw

Signed:
4830450220264c4dce5f1cf0dff8d32d21c5d5cf6baed428b12ae6f8594924246a611e9
ee602210096ef8e7054ec7a39f0a35d8de3fd50090b1d125c0e795af8cf3d577b67640
7ca01410489fc7b8c3f655a10840d35c76ebb5596694045e49e940fb1e7a759da4edf0f
afc45bbbea6f5a56abf14c145c529c8eda9d3ad606f3a0bf4ca01ce991d4987b97

Bitcoin transaction

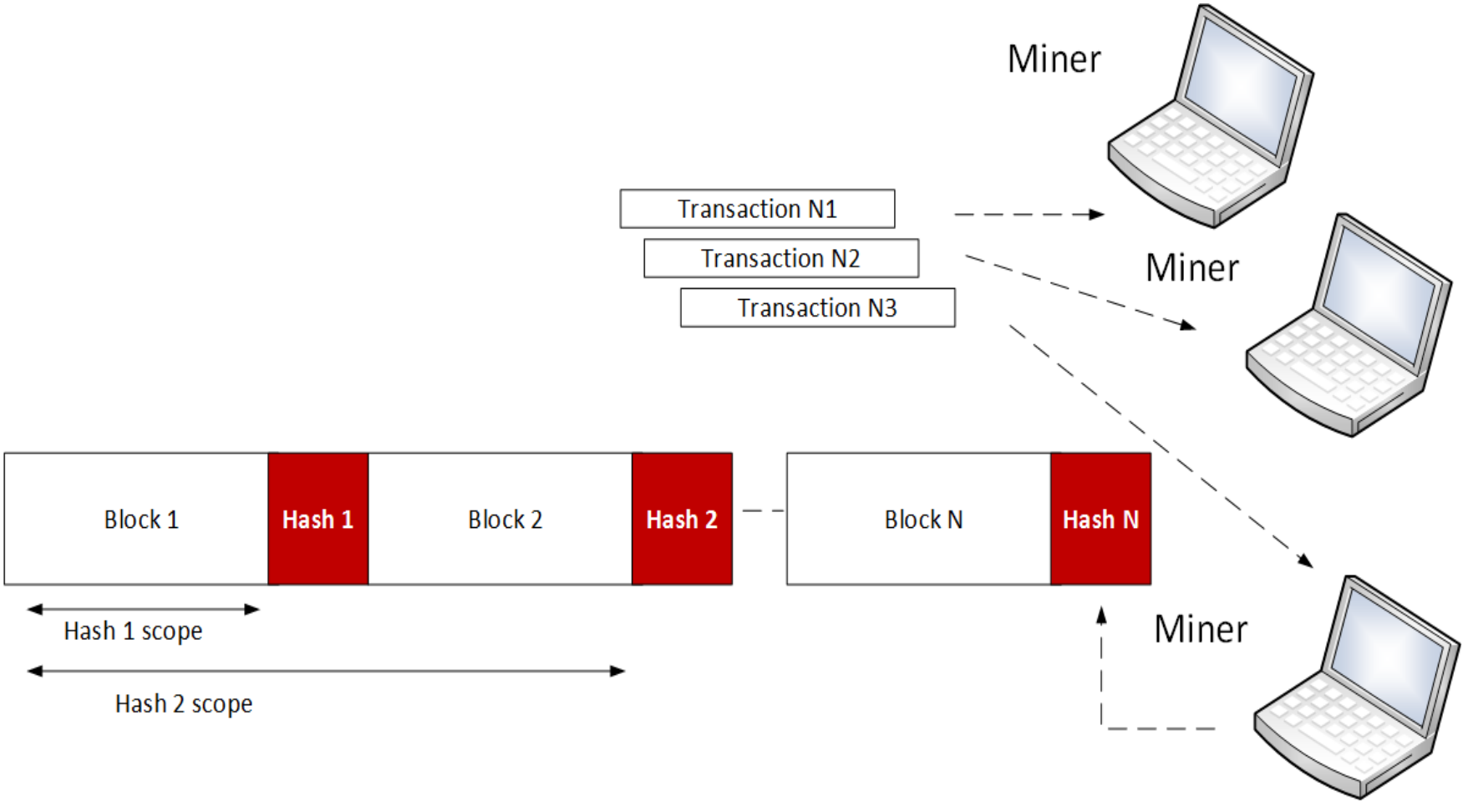


Blockchain and Cryptocurrencies

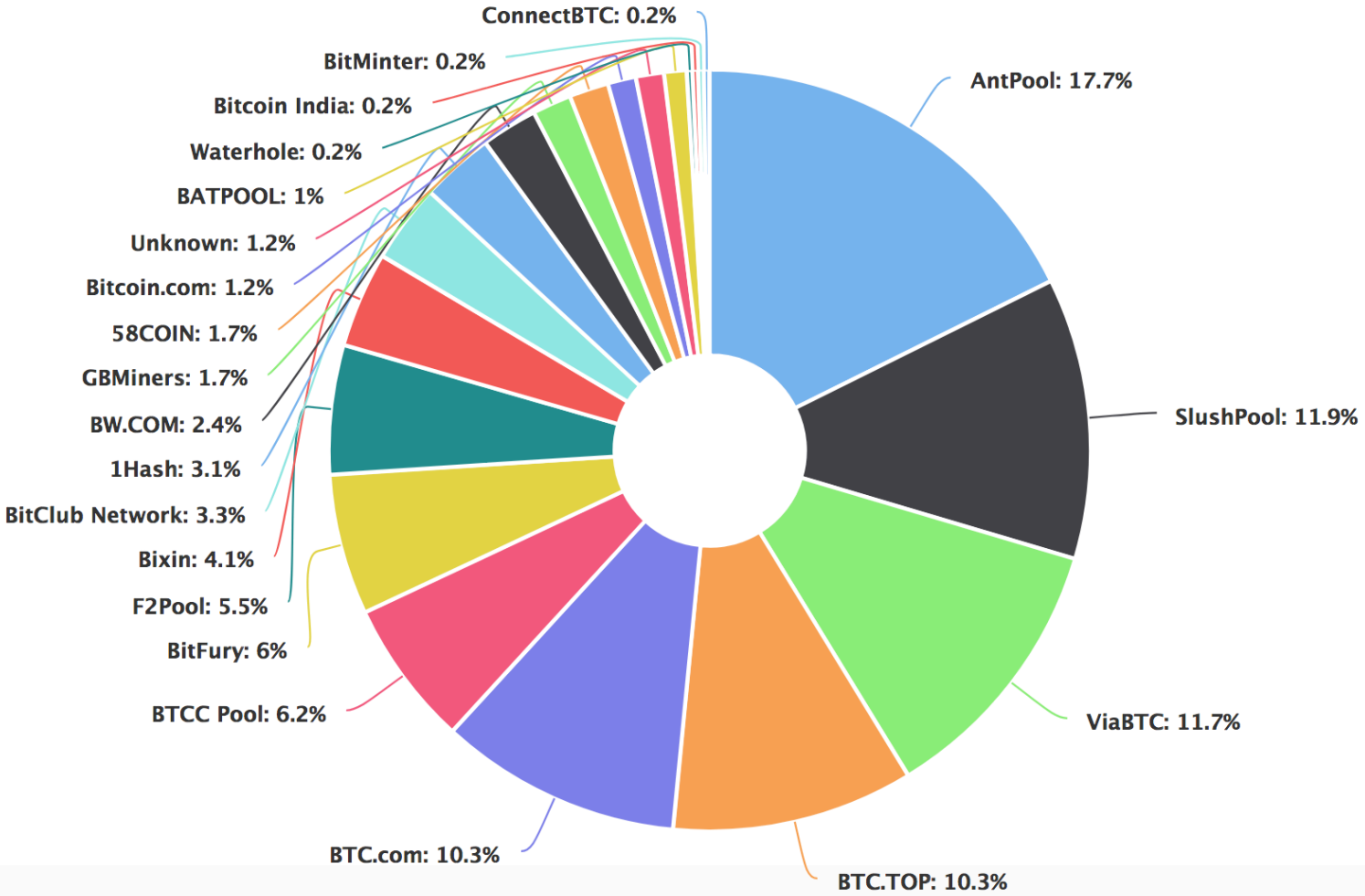
Cryptocurrencies
Bitcoin addresses
> Blockchain
Mining
Ethereum
Smart Contracts
Blockchain Crypto

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

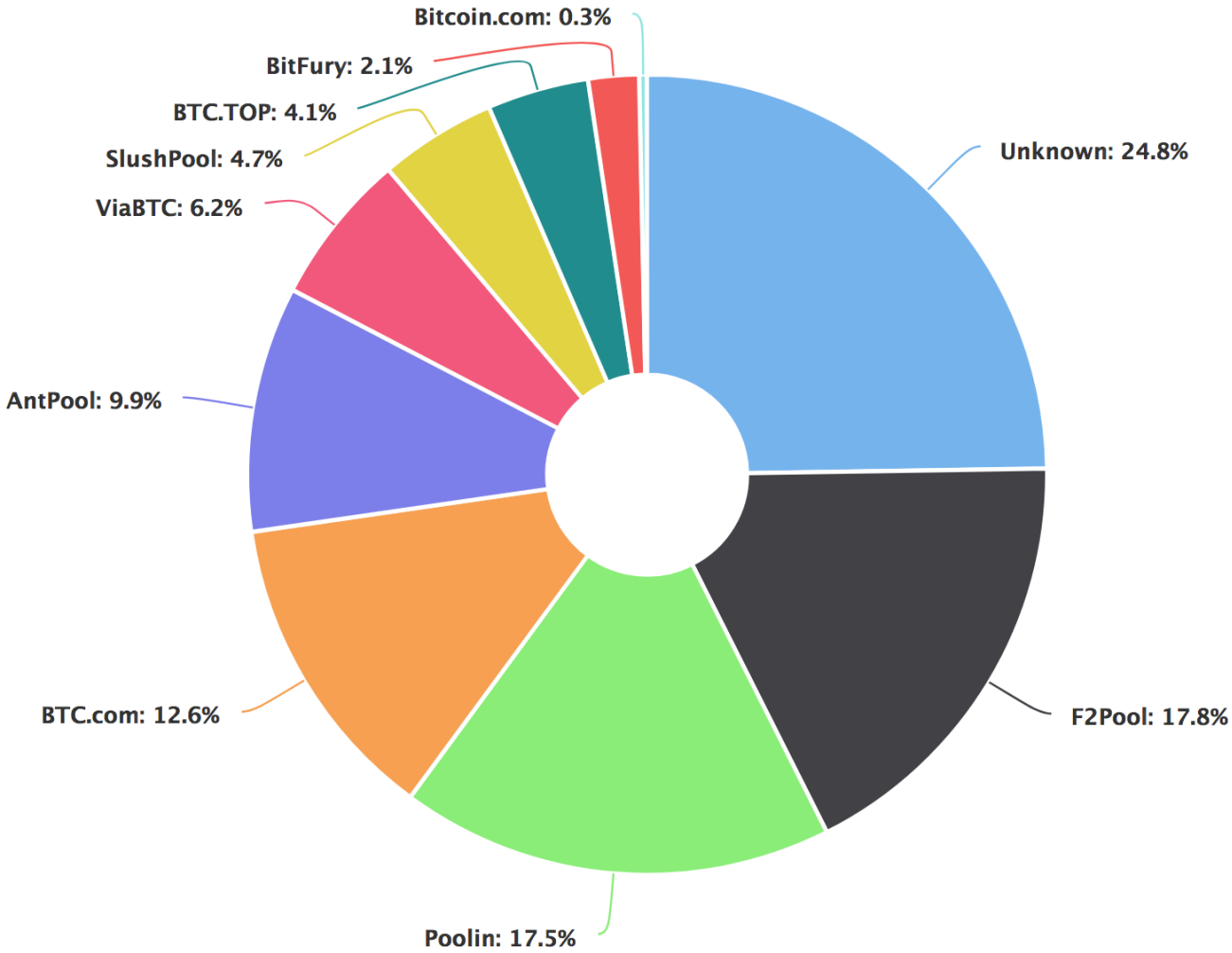
Mining process



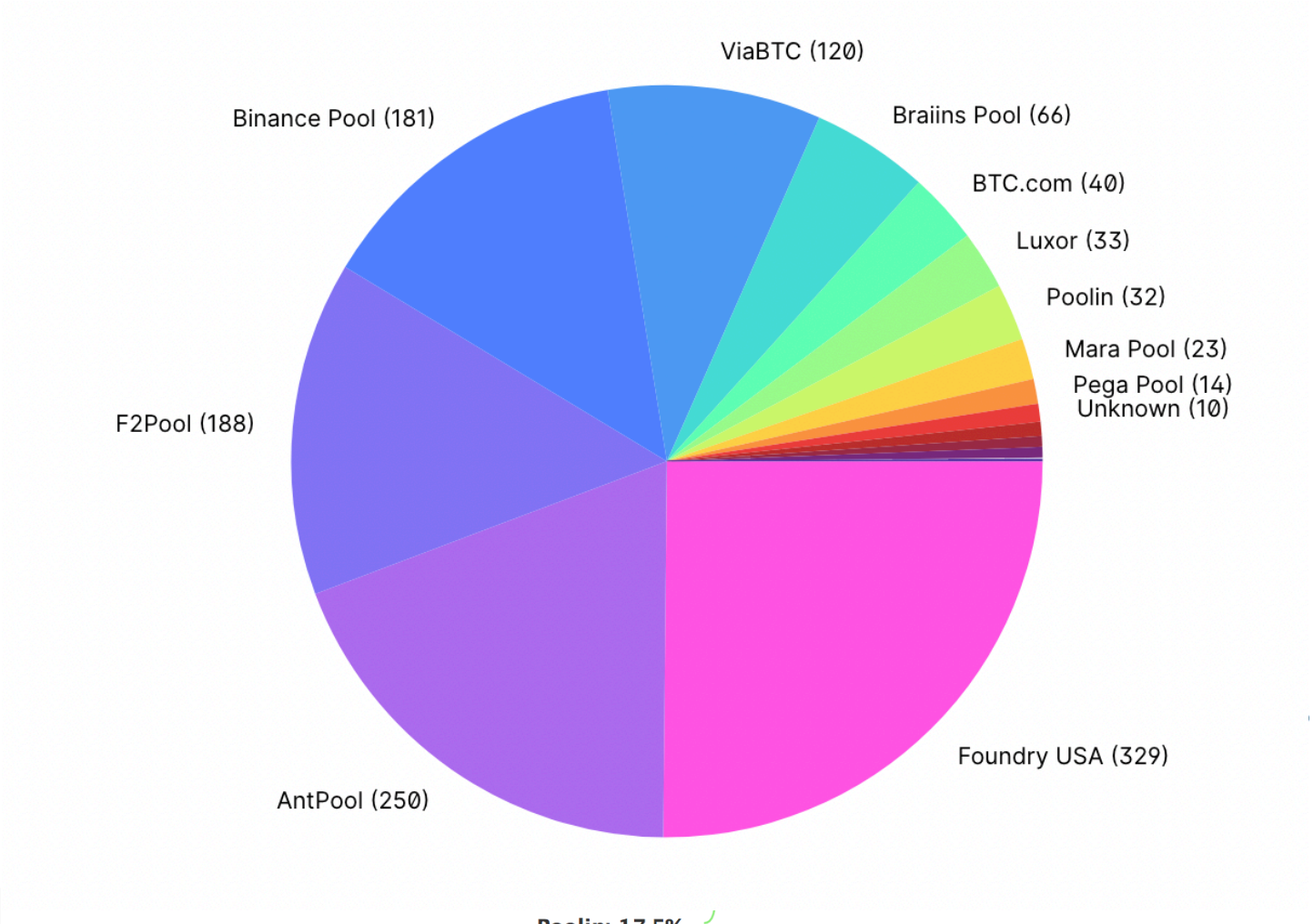
Successful miners (2018 and 2019)



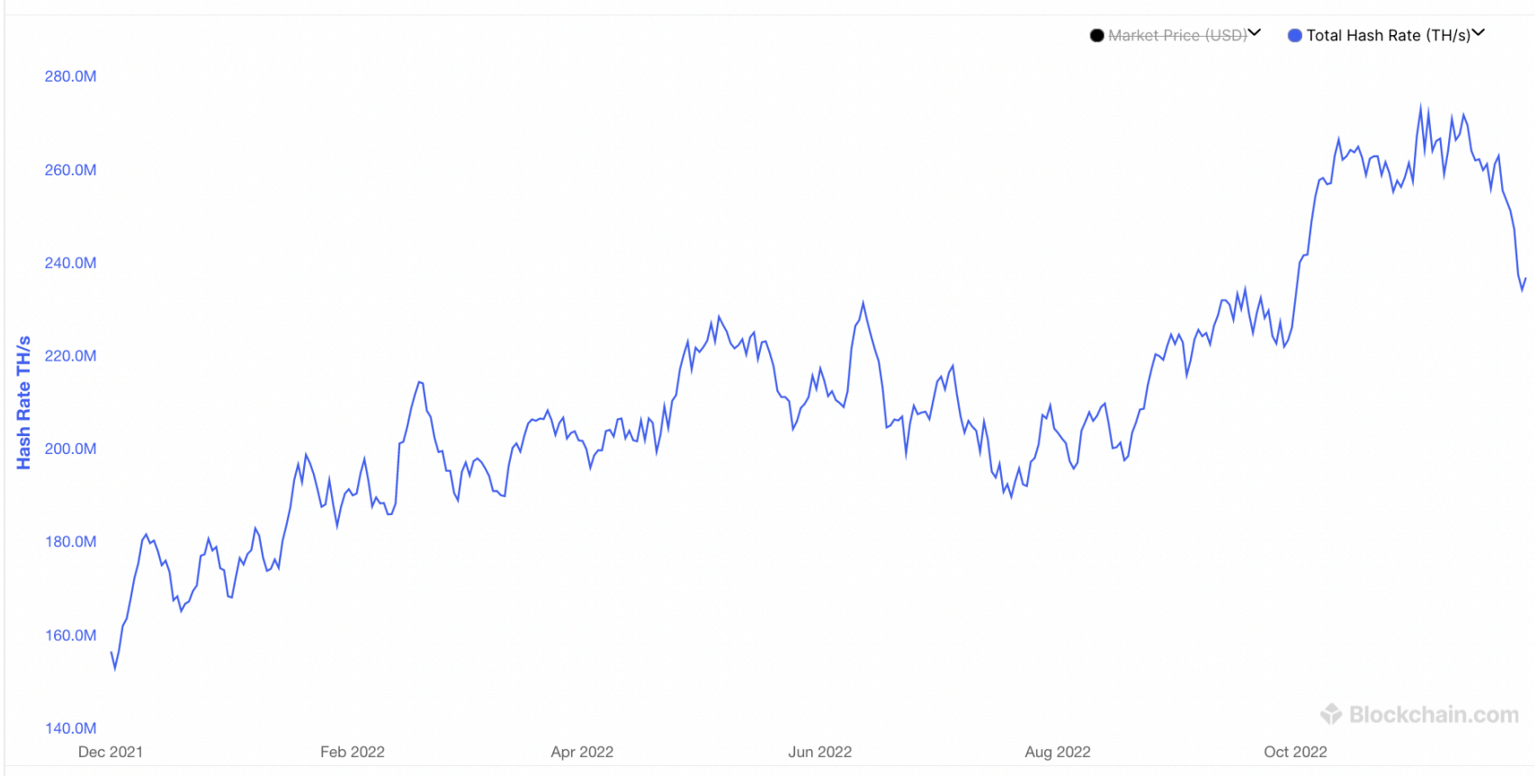
Successful miners (2018 and 2019)



Successful miners (2018 and 2019)



Hash Rate TH/s



Mining Processes

- Hash
- 0000000000000000d98e57b83834a2d1f4387a93d06861bcf3ea5fc498bd55
- Previous Block
- 0000000000000000012138e05f0779765277a9d2ab7e4a2a70882790abf98a0c

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	00000000000000000000385b3a5aa6ba0c4e9d2bf80a54bda9251b96d5f50b2a3
Confirmations	1
Timestamp	2022-11-30 20:25
Height	765355
Miner	F2Pool
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

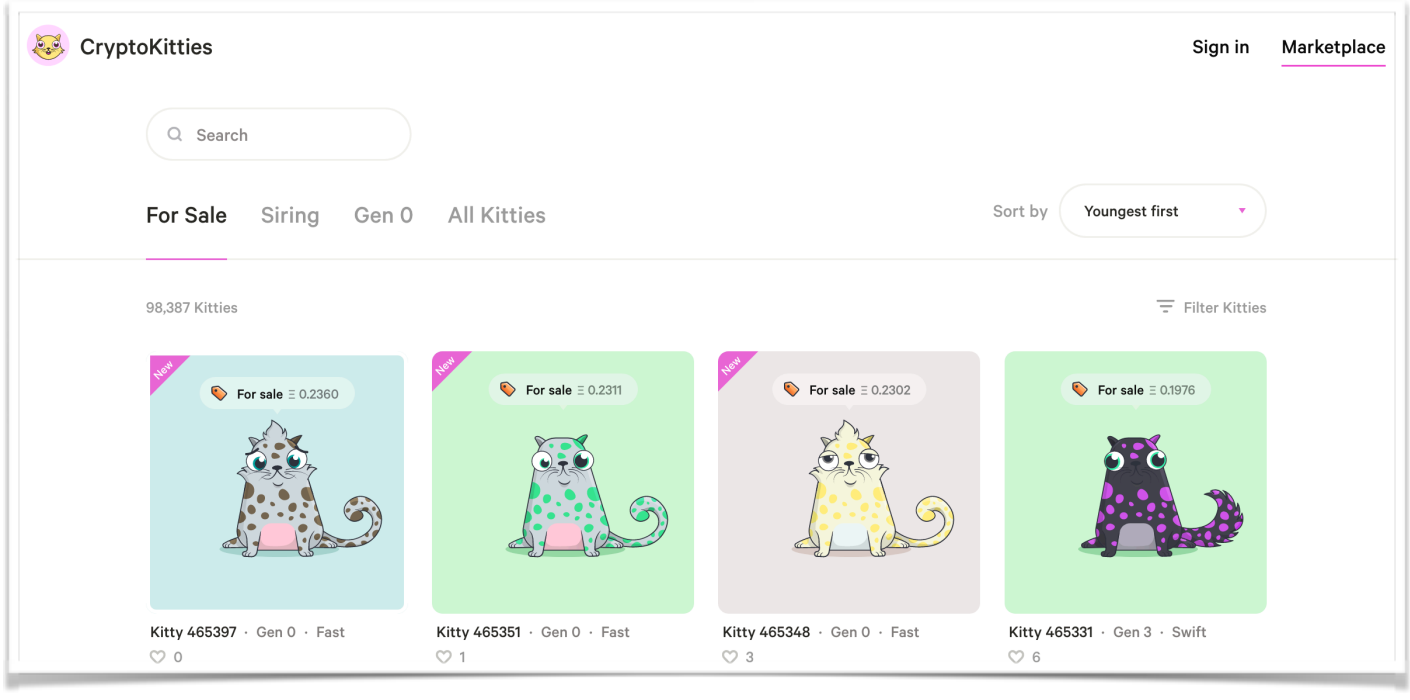
Chapter 10: Blockchain and Cryptocurrencies

Cryptocurrencies
Bitcoin addresses
Blockchain
Mining
> Ethereum
Smart Contracts
Blockchain Crypto

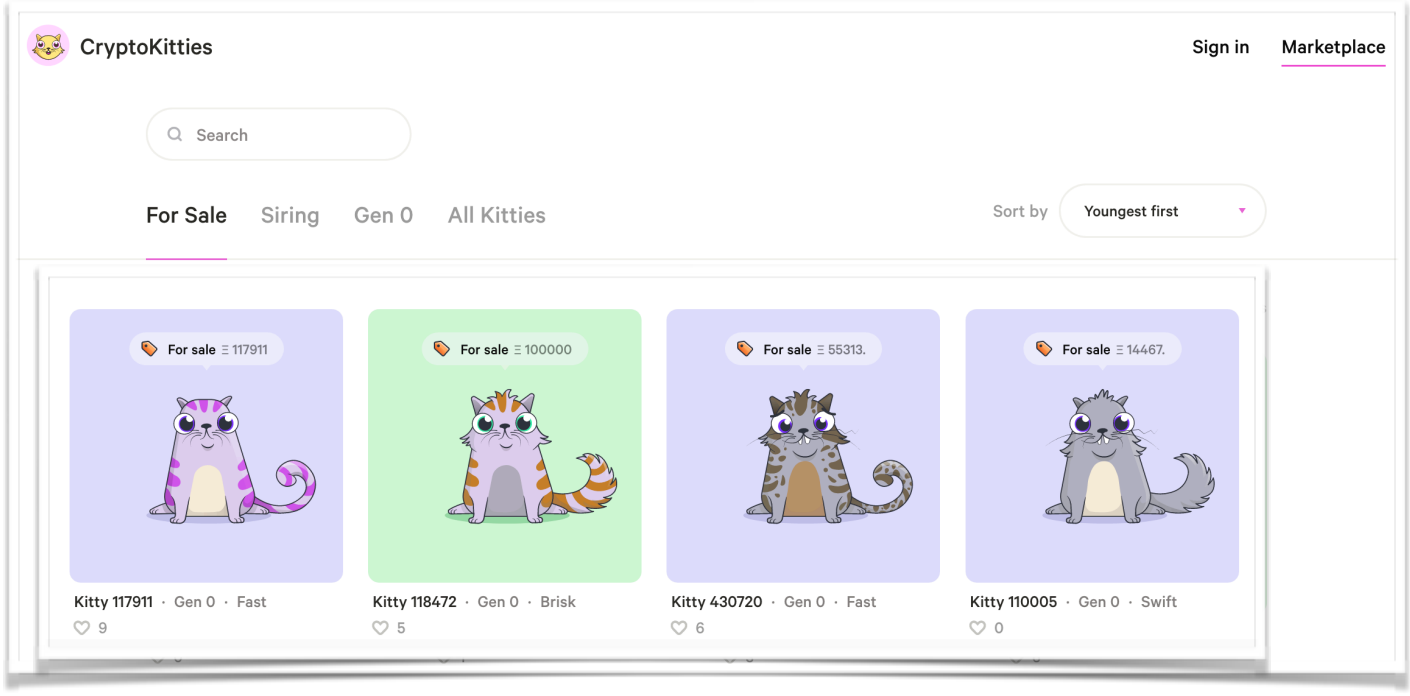
Prof Bill Buchanan OBE
https://asecuritysite.com/blockchain/

Crypto Kitties

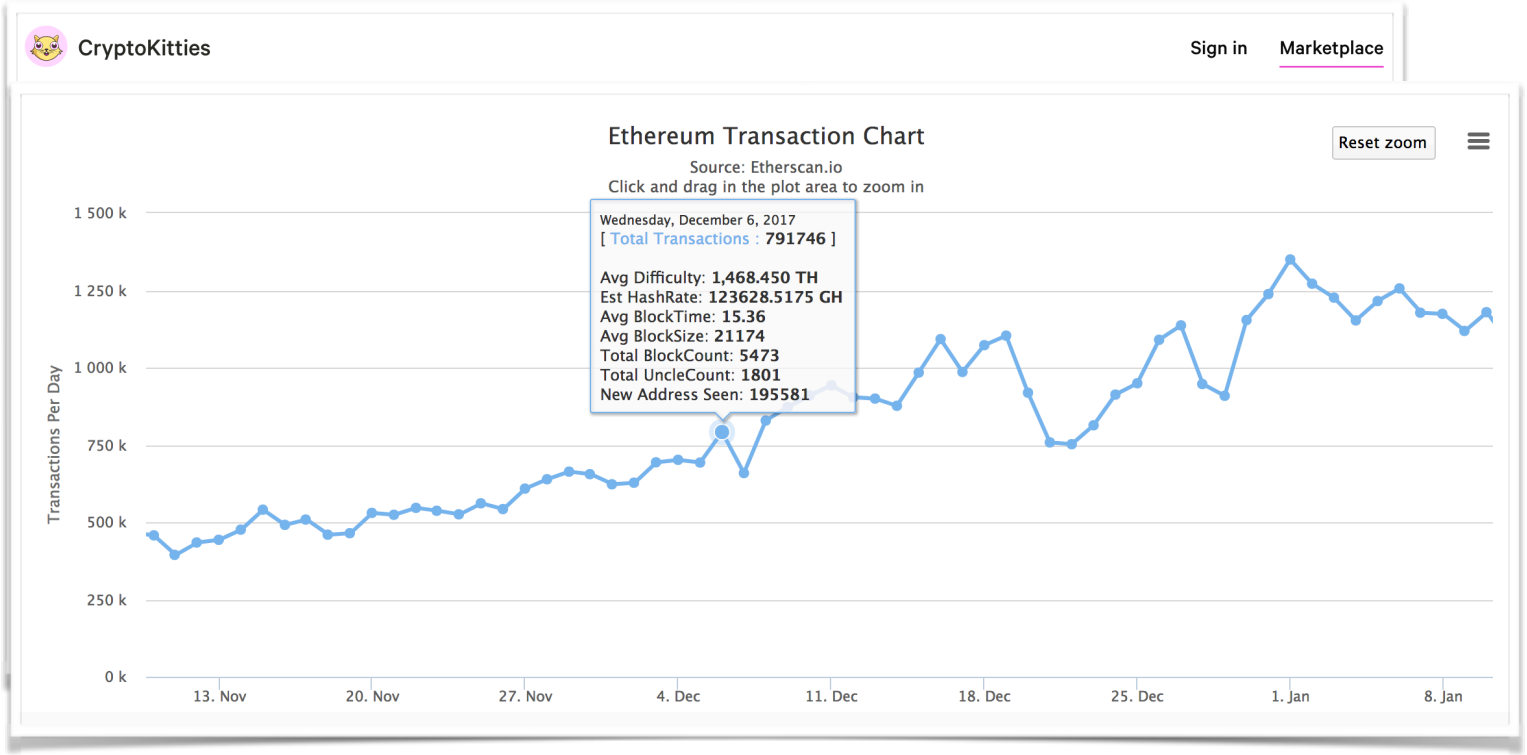
Crypto Kitties



Crypto Kitties



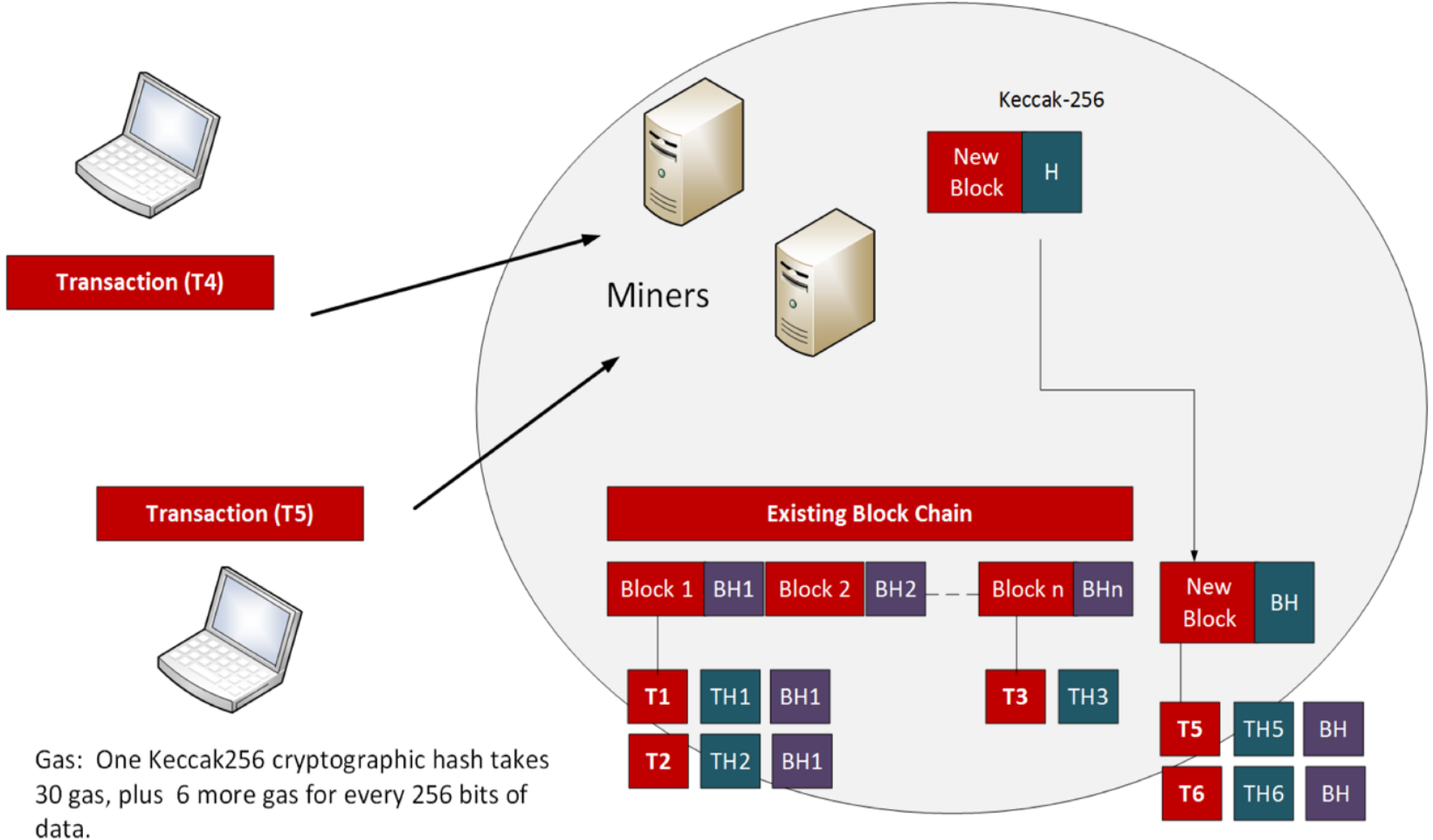
Crypto Kitties



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: 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.

Gas

Hash	0×5a0b54d5dc17e0aadc383d2db43b0a0d3e029...
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

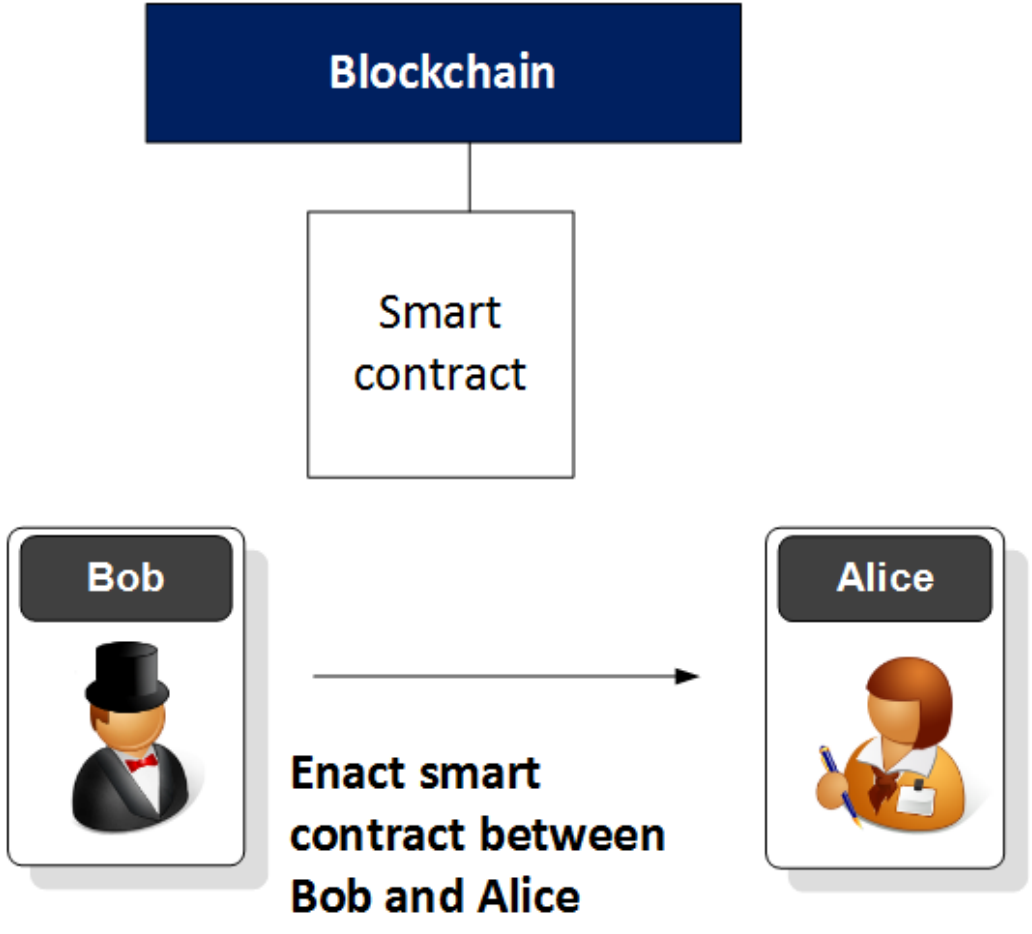
Hash	0×3bcab6d3db3e64147ac881aa9928e1bdc...		2020-03-20 07:00
	0×5a0b54d5dc17e0aadc383d2db43b0a0d...	→	0×8fd00f170fdf3772c5ebdcd90bf257316c691
Fee	0.00012600 ETH (21000 GAS - 6000000000 WEI)		-98.512346513586285551 ETH

Blockchain and Cryptocurrencies

Cryptocurrencies
Bitcoin addresses
Blockchain
Mining
Ethereum
> Smart Contracts
Blockchain Crypto

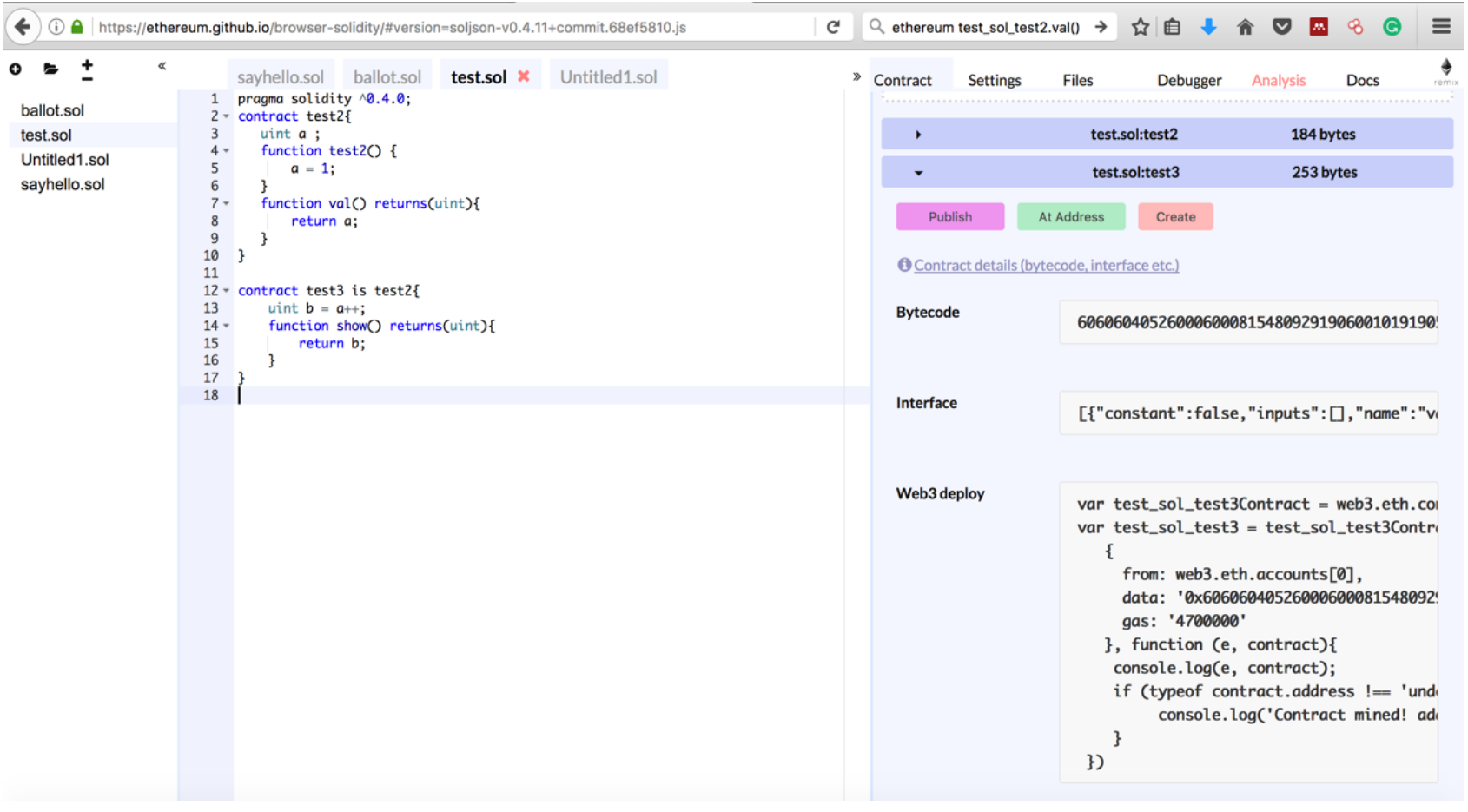
Prof Bill Buchanan OBE
https://asecuritysite.com/blockchain/

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



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.

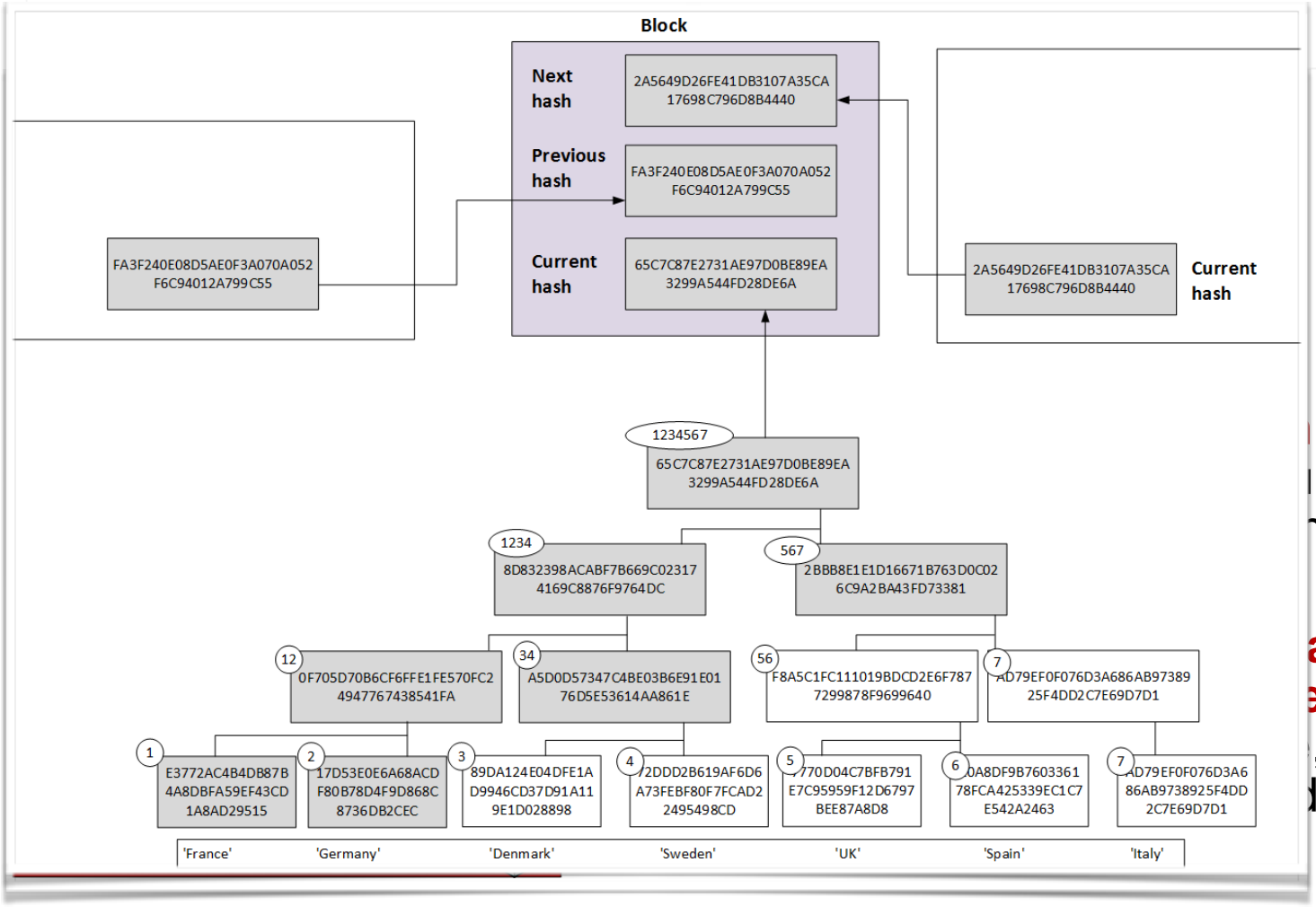
Merkle Trees

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-
res, bullet
nding

and
e
,
d so on.

Merkle Trees

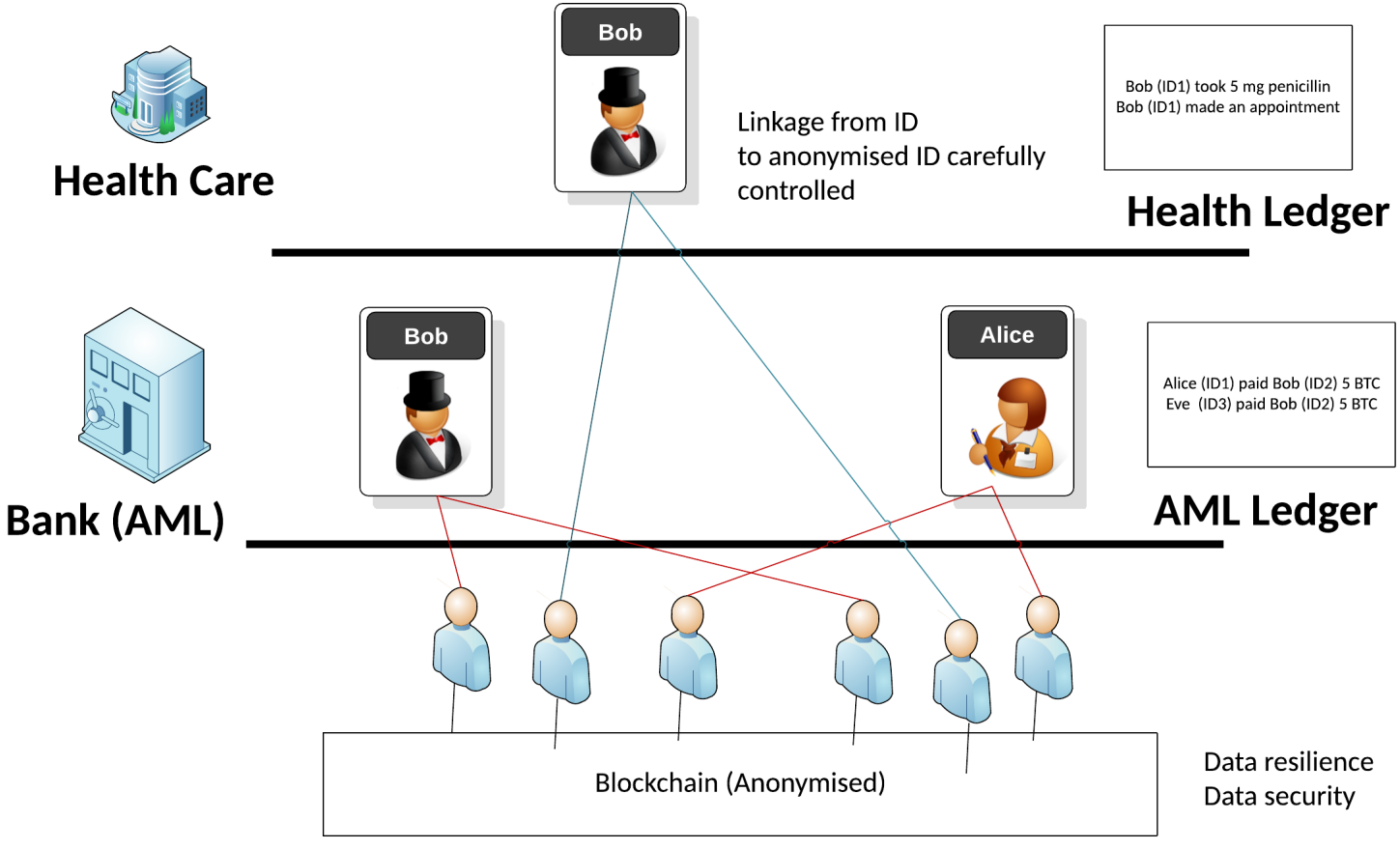


ing: Zero-
res, bullet
nding

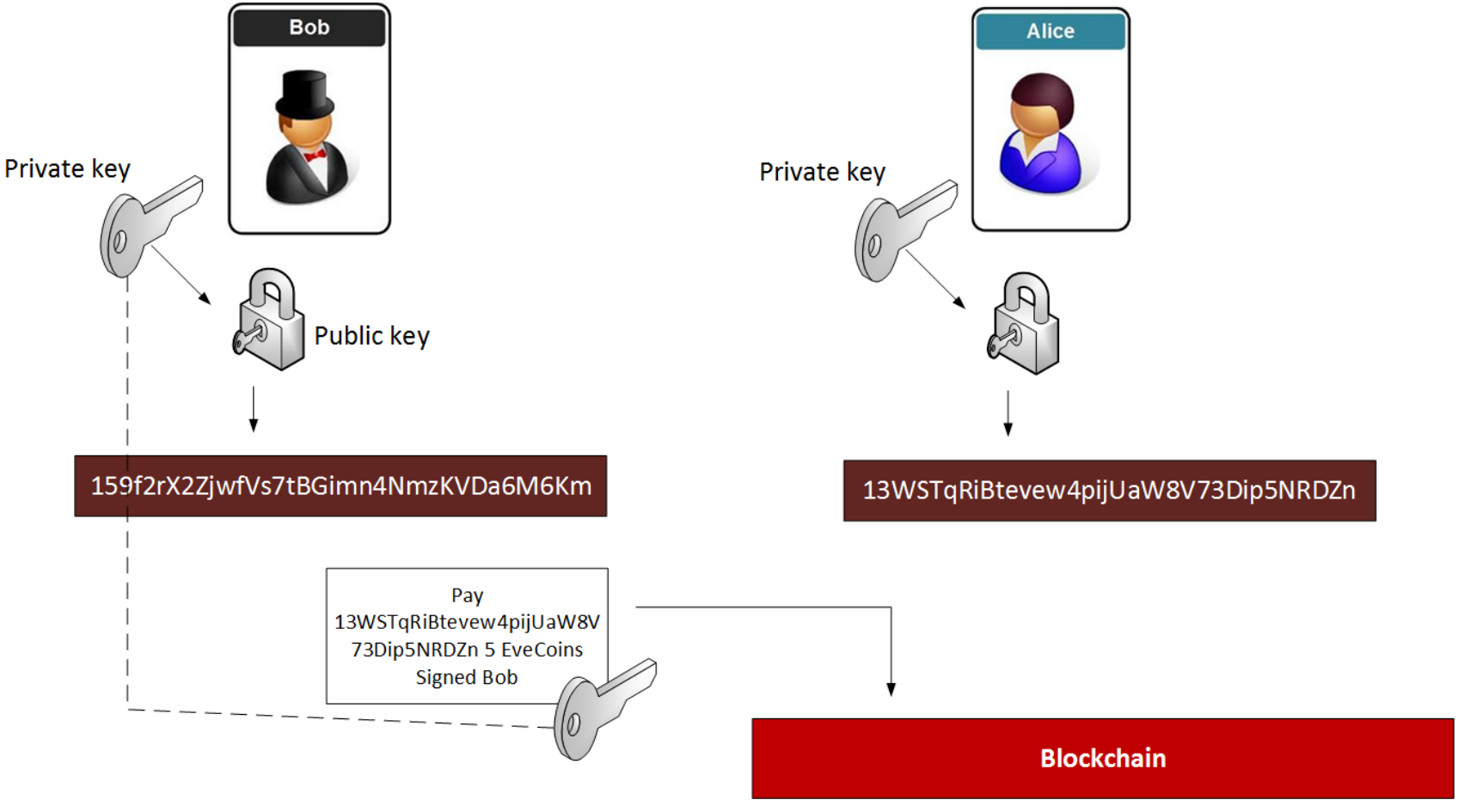
and
e

,
d so on.

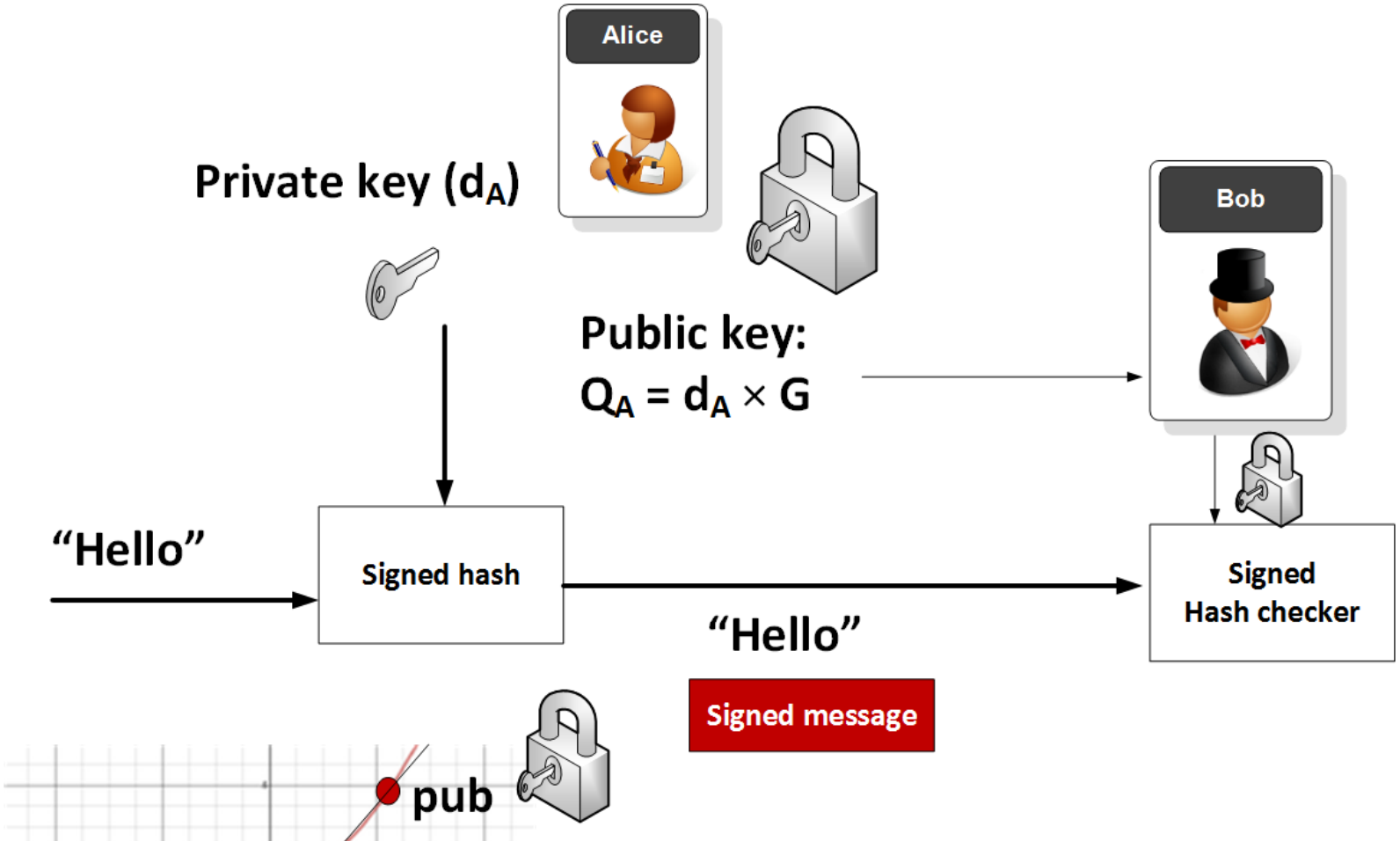
Merkle Trees



Signing


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

Signing (ECDSA)



Signing (ECDSA)

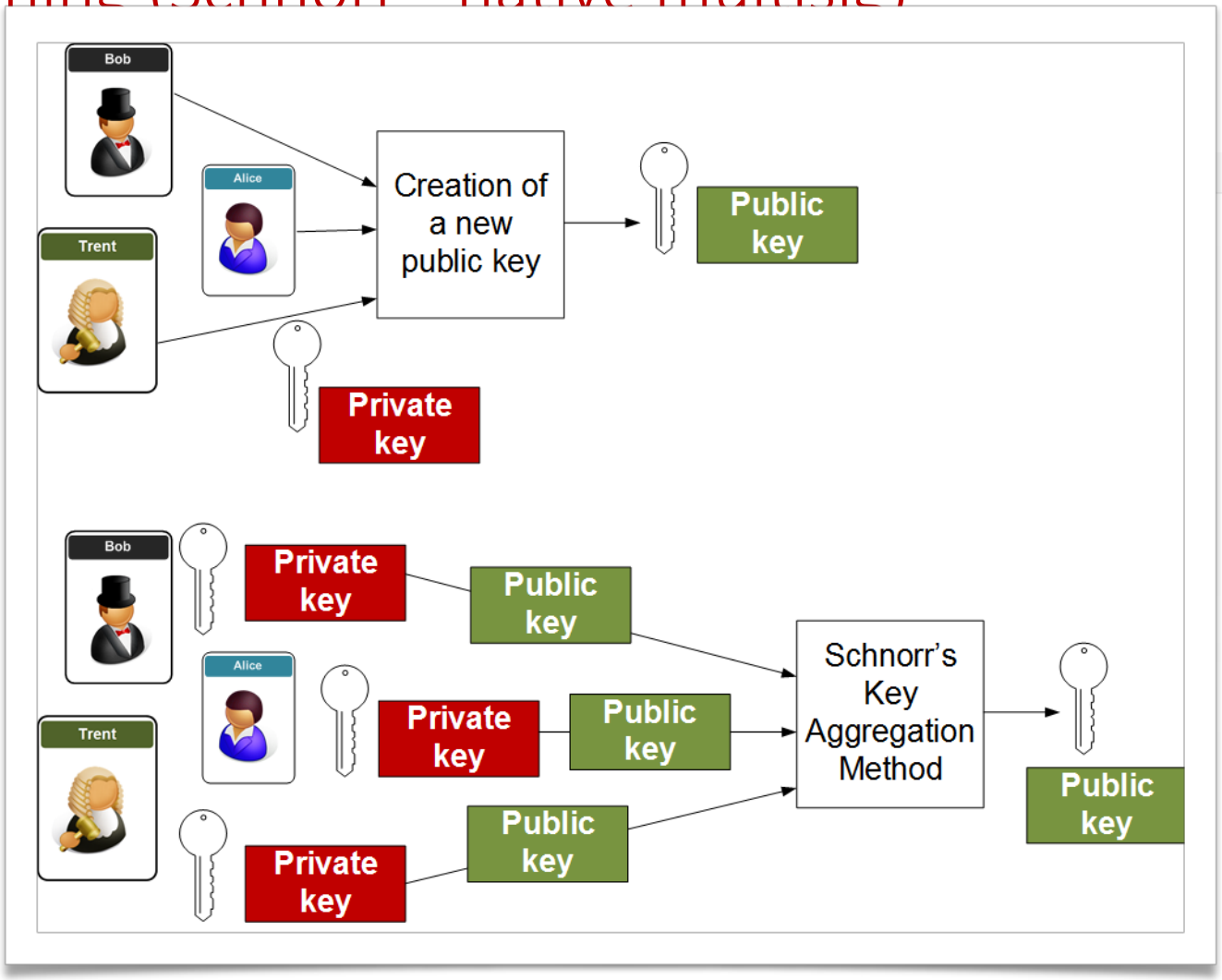
```
Message:        Hello
Hash (SHA-256): 185f8db32271fe25f561a6fc938b2e264306ec304eda518007d1764826381969

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

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

=======Signature generation (r,s) ==============
r= 6367040637280407460684387177664473707927092807673859427626809110381412889929O
s= 13503713885368555959286645307370967261073993386809582203474575043238647211621

=======Signature verification (v==r) ==============
V= 6367040637280407460684387177664473707927092807673859427626809110381412889929O
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)

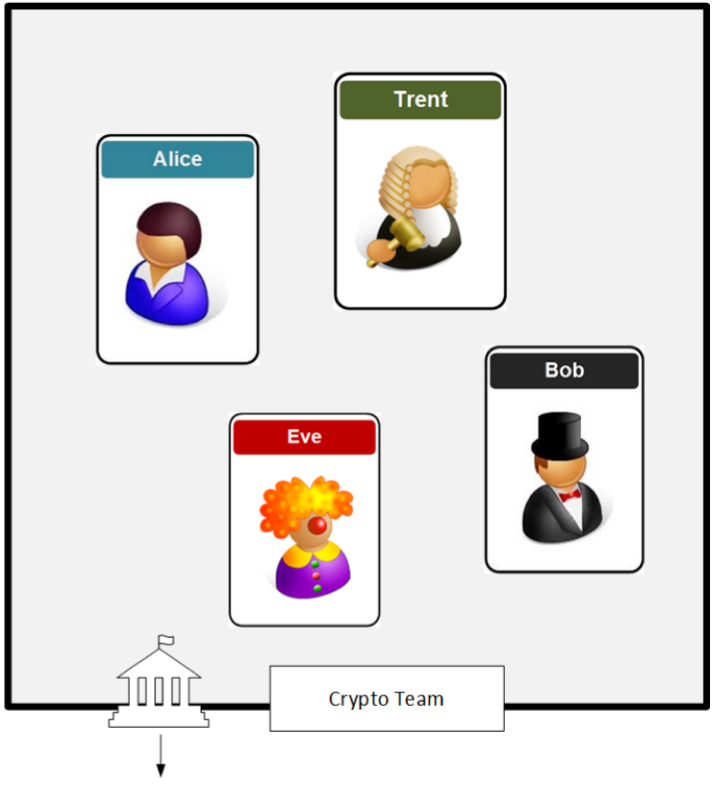
Block #477120

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?

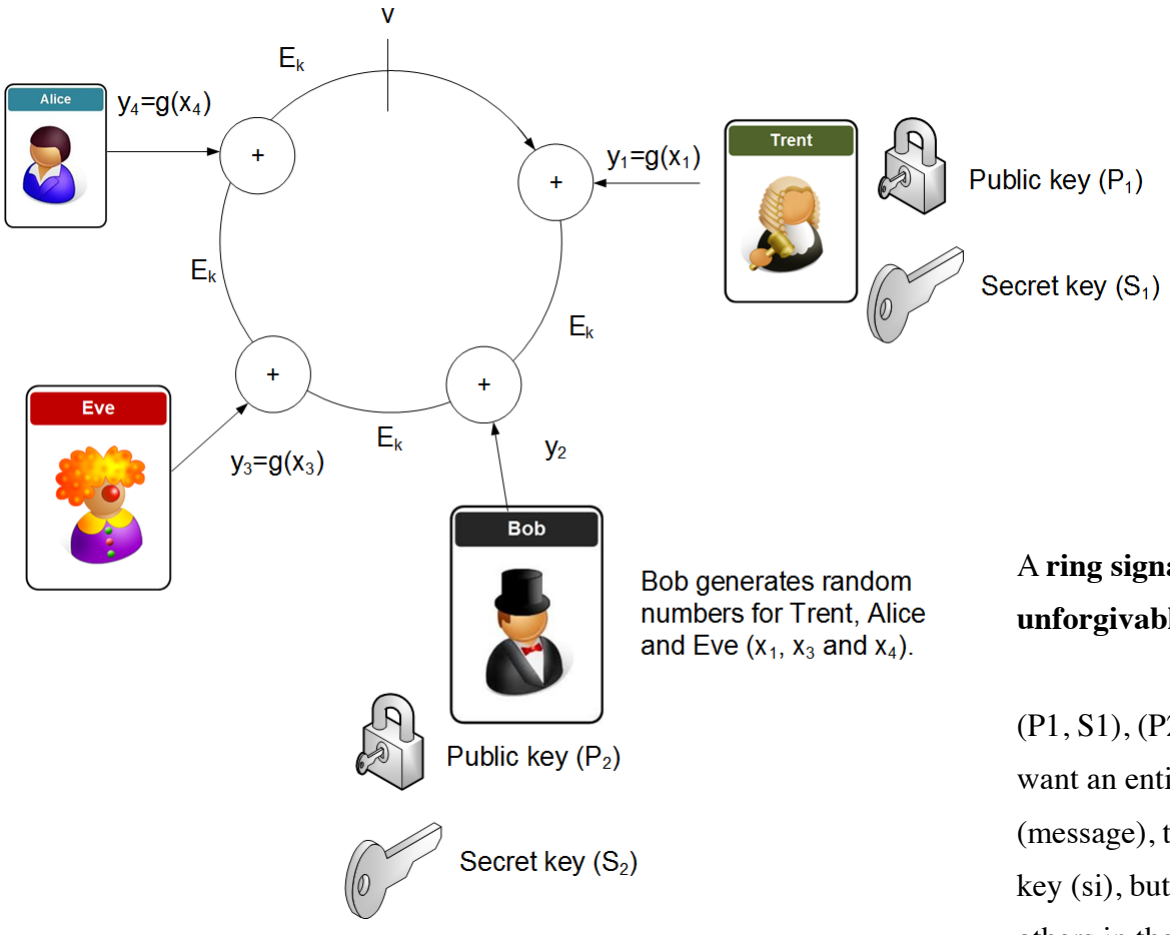


We have a secret.

Signed,
A member of the crypto team

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

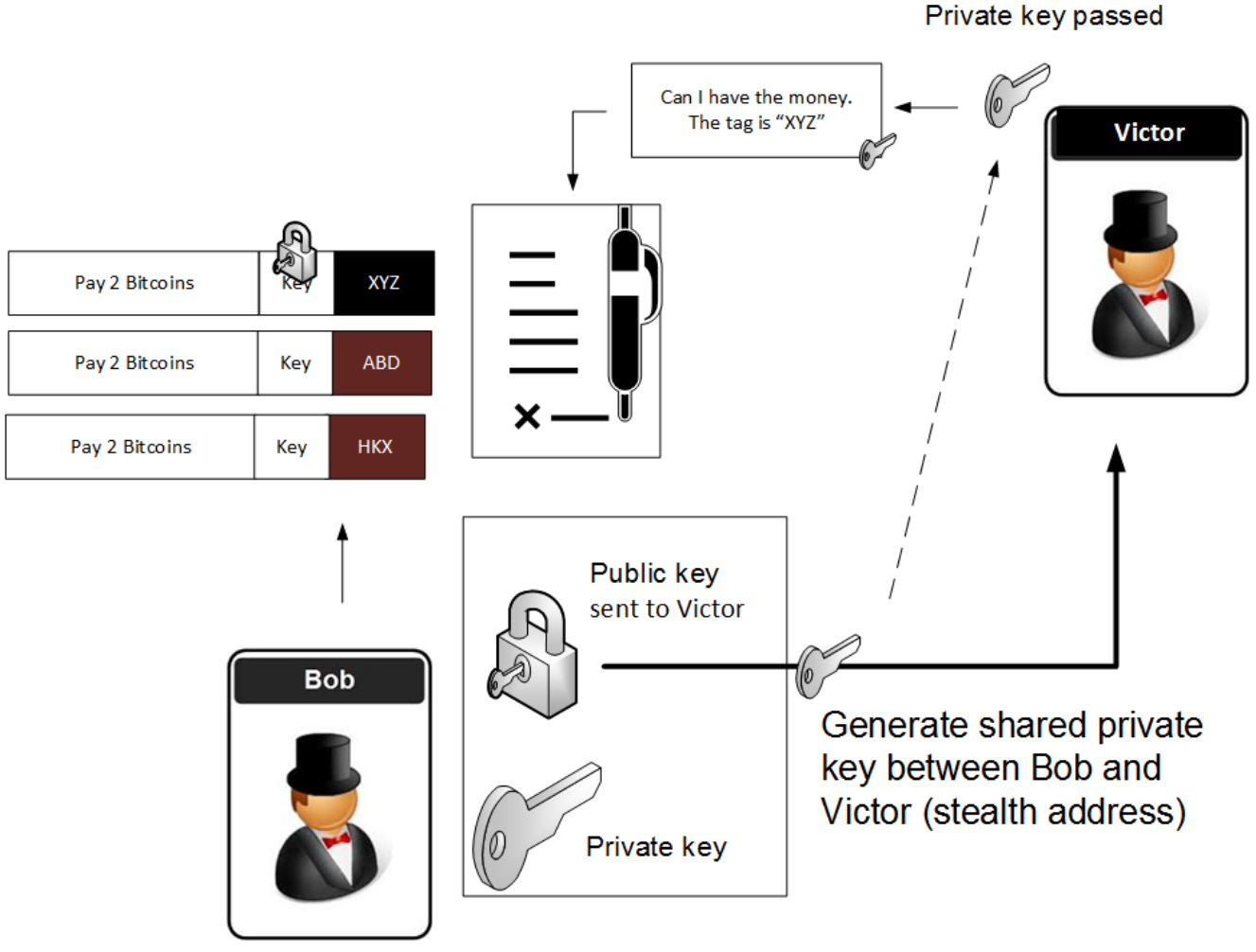
Ring Signatures



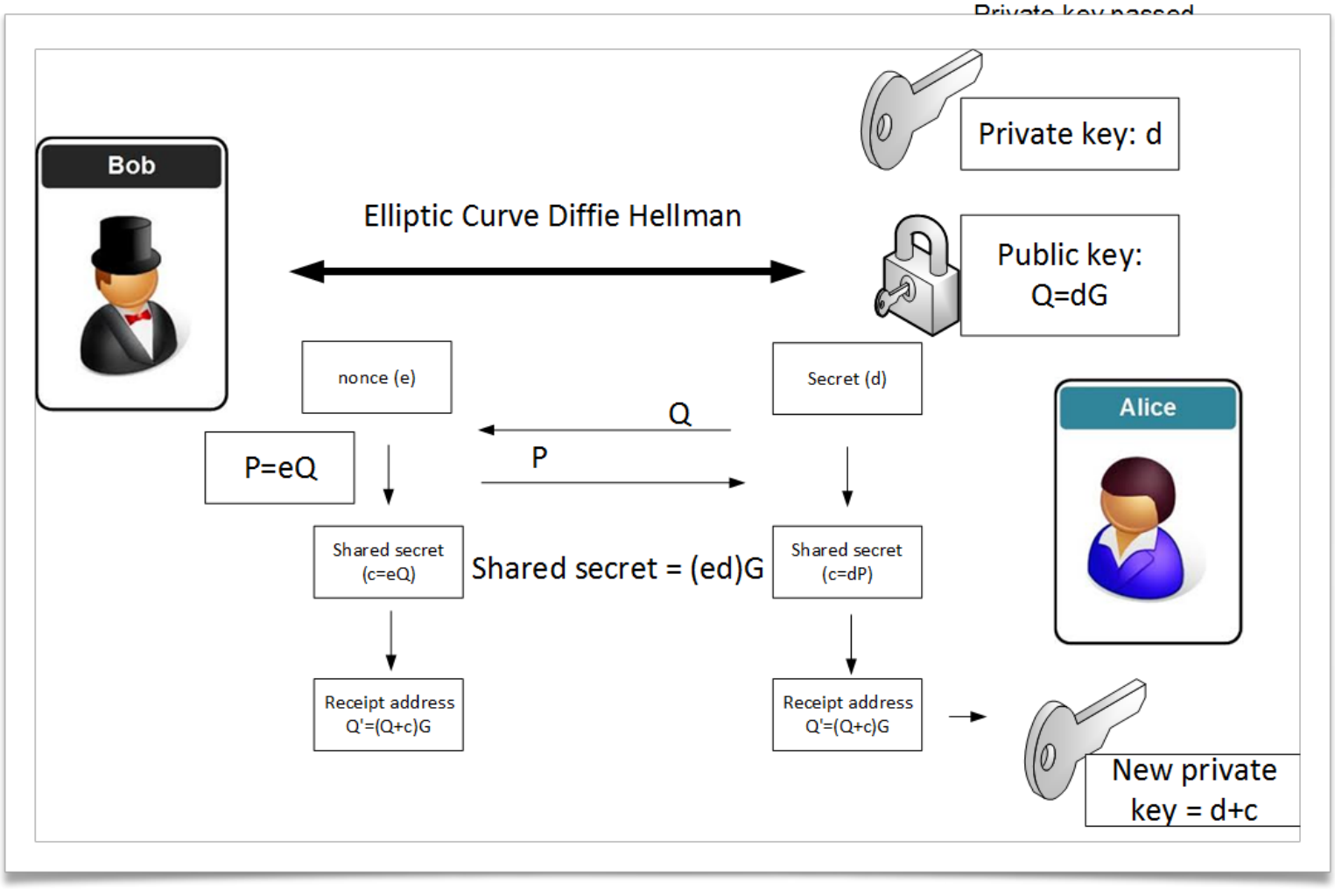
A **ring signature** provides **anonymity**, **unforgivably** and **collusion resistance.**

(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

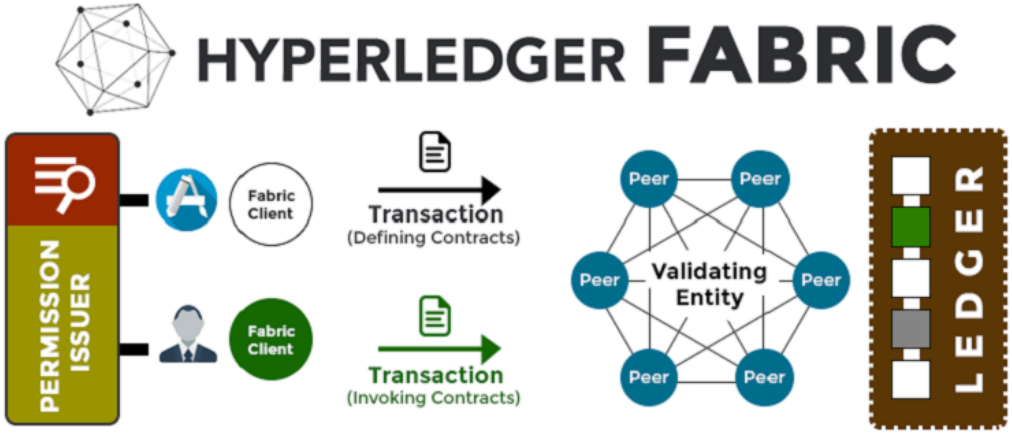


Chapter 10: Blockchain and Cryptocurrencies

Cryptocurrencies
Bitcoin addresses
Blockchain
Mining
Ethereum
Smart Contracts
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.

101 Blockchains | HYPERLEDGER VS ETHEREUM

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

HYPERLEDGER

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

VS

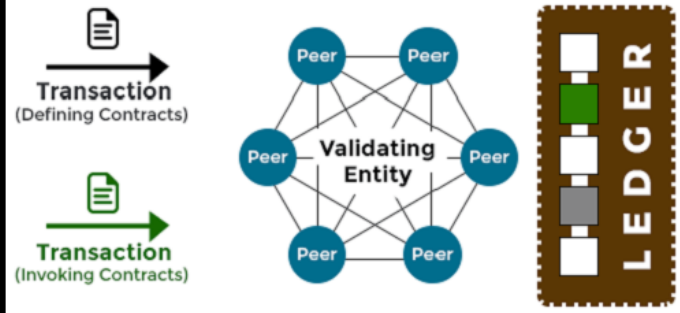
ETHEREUM

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

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

CREATED BY 101BLOCKCHAINS.COM

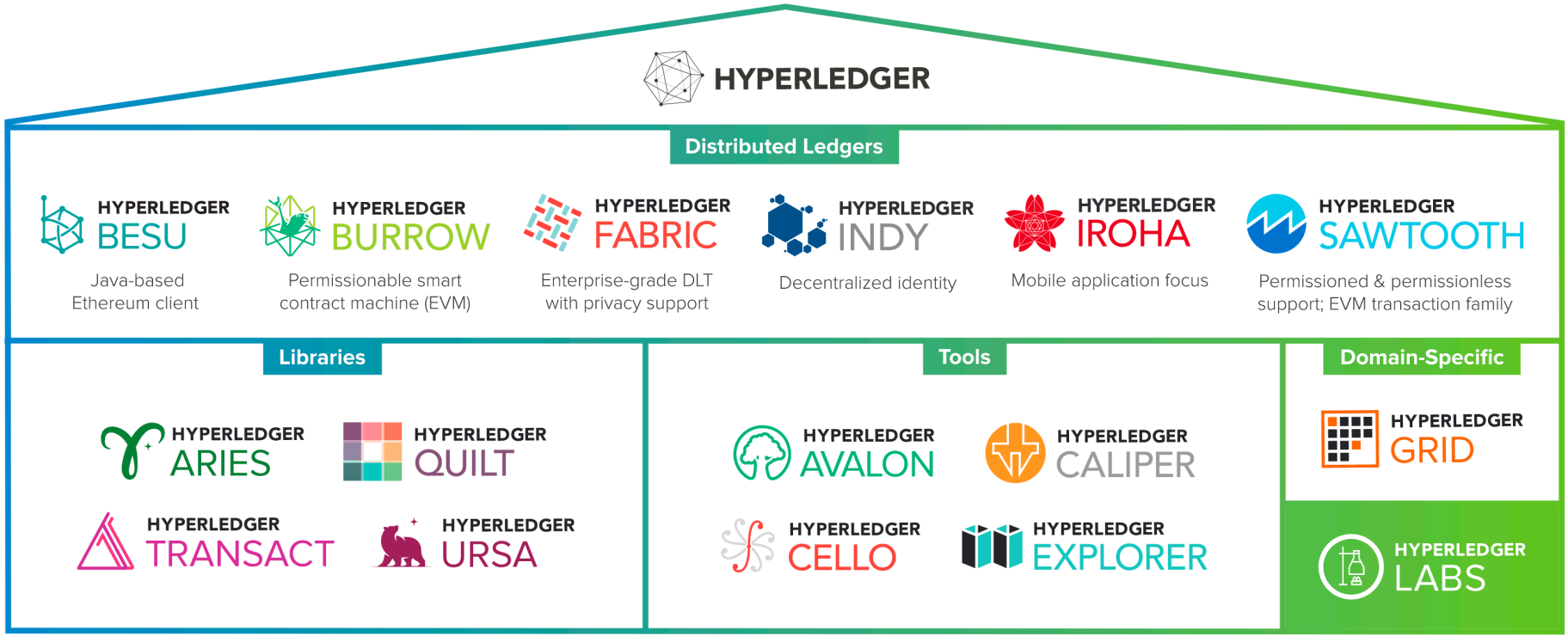
ERLEDGER FABRIC



Key features:

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

101 Blockchains | HYPERLEDGER VS ETHEREUM



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

Chapter 10: Blockchain and Cryptocurrencies

Cryptocurrencies
Bitcoin addresses
Blockchain
Mining
Ethereum
Smart Contracts
Hyperledger

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