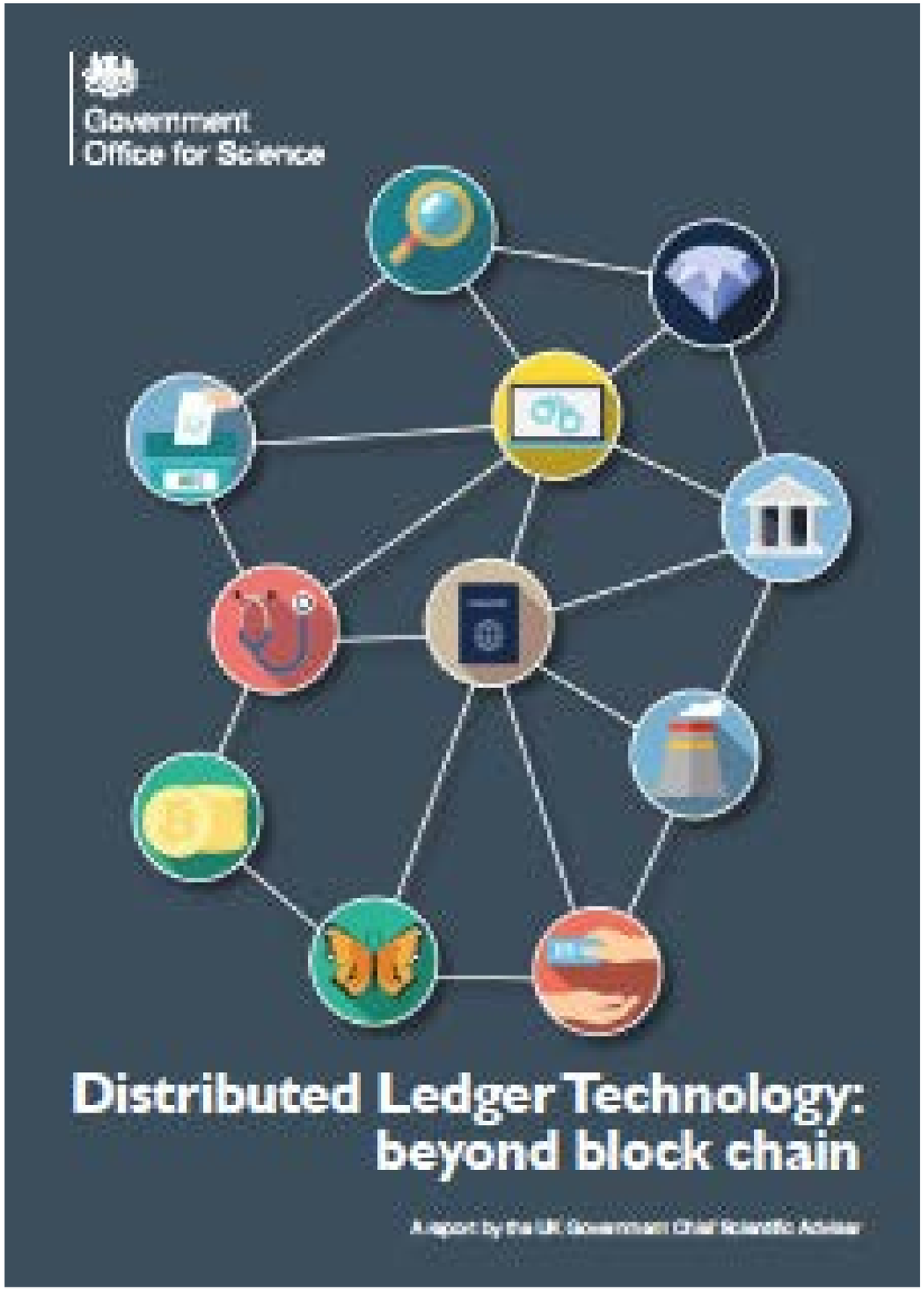
Will Bitcoin and the Block Chain change the way we Live and Work?

Martyn Thomas CBE FREng
Livery Company Professor of Information Technology



WORLD ECONOMIC FORUM

COMMITTED TO IMPROVING THE STATE OF THE WORLD

White Paper

Realizing the Potential of Blockchain

A Multistakeholder Approach to the Stewardship of Blockchain and Cryptocurrencies

June 2017

Money

A way of storing and transferring value

Value based on trust

Bitcoin

- They must be secure and unforgeable
- It must be impossible to spend the same bitcoin twice
- It must be possible to send bitcoins across the internet
- The recipient must be able to check that the bitcoin genuinely belongs to the person spending it
- Transactions should be private: there should be no need to identify any real-world person
- Transactions must not be reversible, except by both parties agreeing to a new transaction
- There must be an acceptable way to create new bitcoins that all bitcoin users agree is fair and that cannot undermine the value of the currency

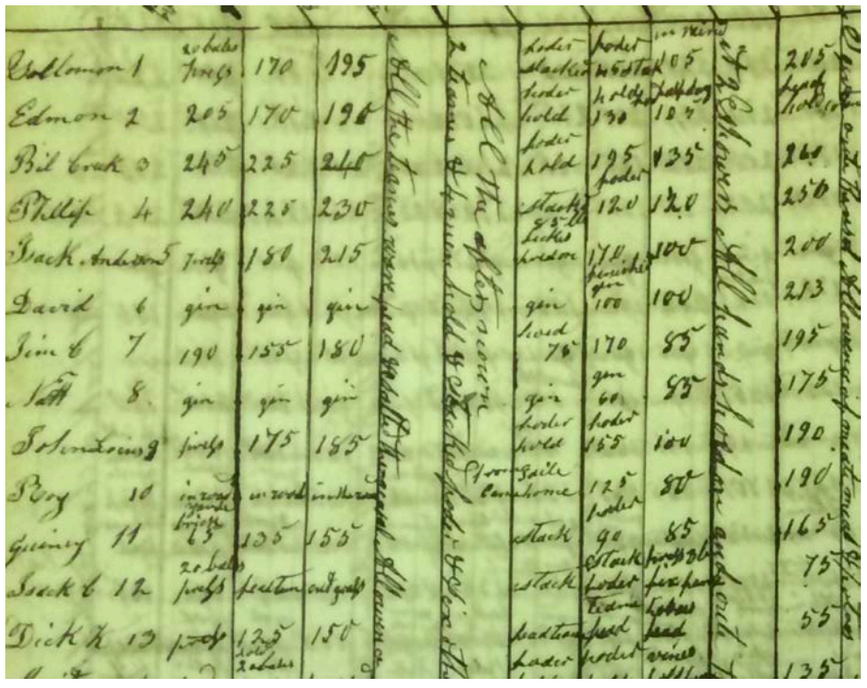
How?

Incredibly, by creating a universally available, unchangeable, unforgeable, indestructible, record of every transaction with every bitcoin from the moment it was created!

This ledger is the *Blockchain*

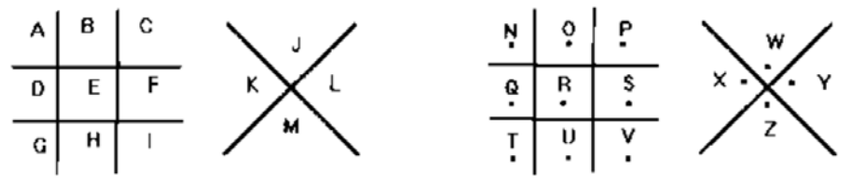
Why are Ledgers so Important?

- A physical record of ownership and transactions
- Necessary for thousands of years
- Almost always with an owner and controller.

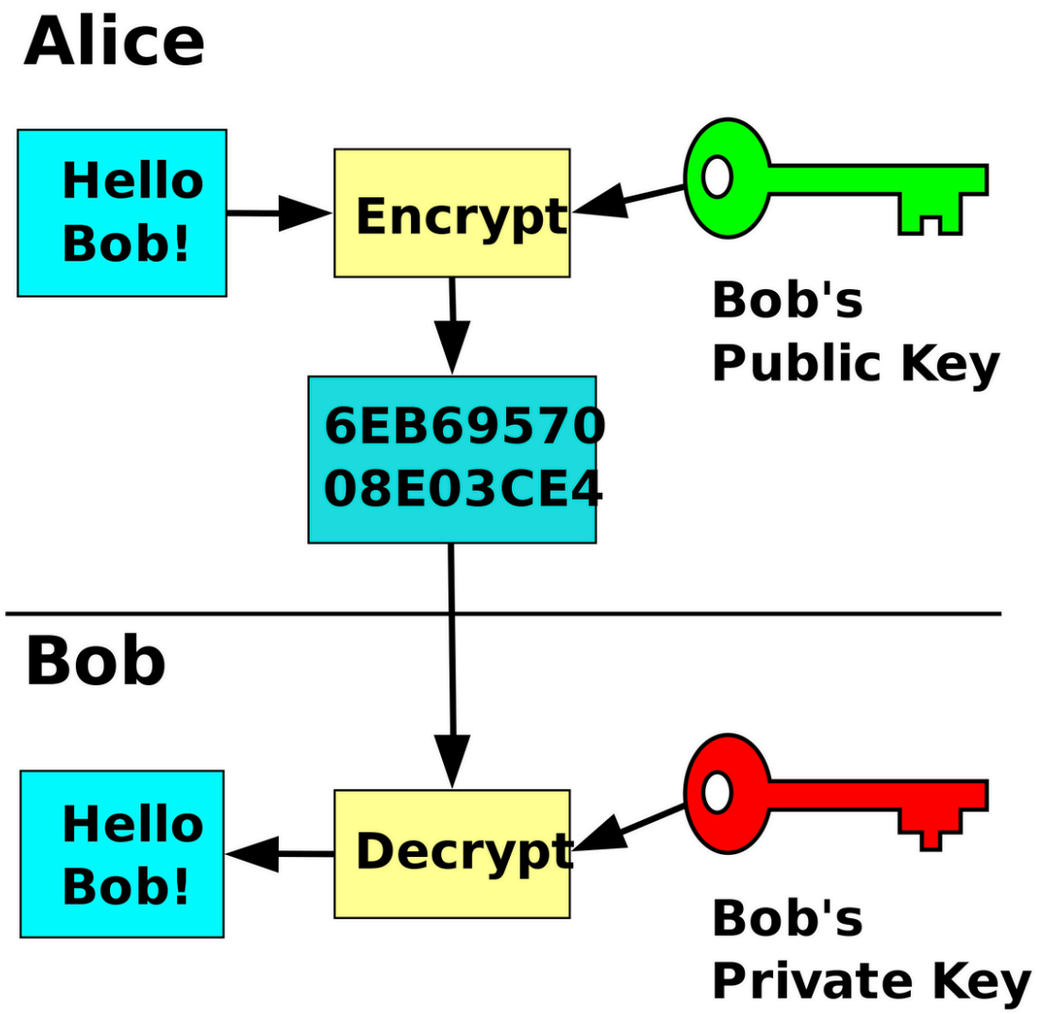


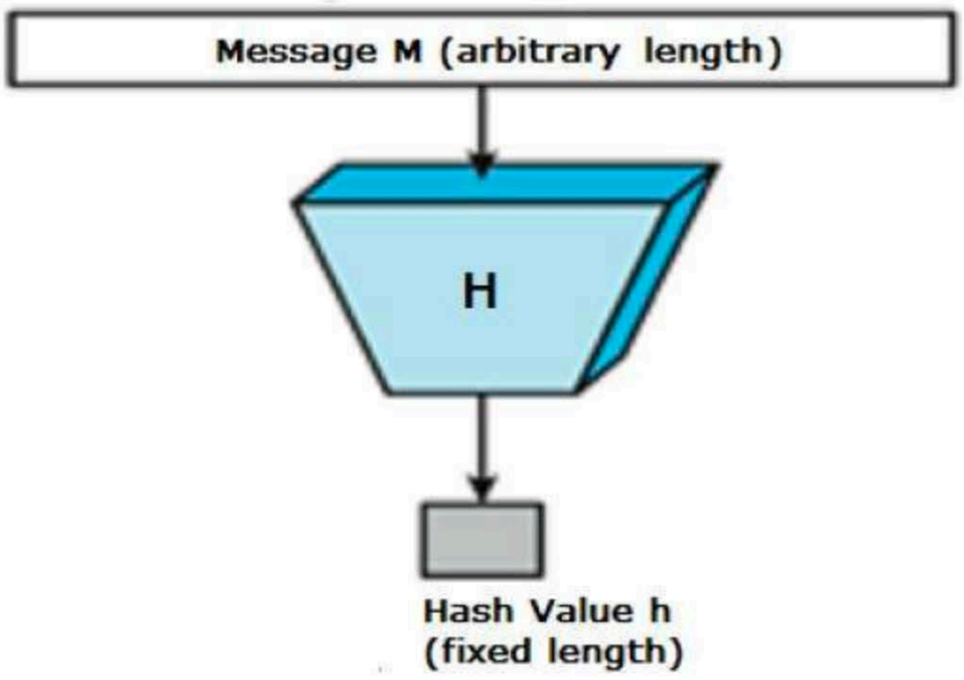
Cryptography

- The world of secret codes
- Turning a readable message (“plaintext”) into an unreadable coded text that the recipient can convert back into the plaintext.
- Centuries old. Thomas Gresham used code in the 16th Century
- But you need a shared “key” …



Public Key cryptography





Hashing

- An operation that converts an arbitrary length input to a fixed length output or “digital fingerprint” (the *hash*)
- A *one way* process. It is infeasible to turn the hash back into the input
- *Collision resistant* - it is infeasible to find another input that generates the same hash
- A tiny change will lead to a major change in the hash:
  - SHA-224(“the quick brown fox jumps over the lazy dog”) = 730e109bd7a8a32b1cb9d9a09aa2325d2430587ddbc0c38bad911525
  - SHA-224(“the quick brown fox jumps over the lazy dog.”) =

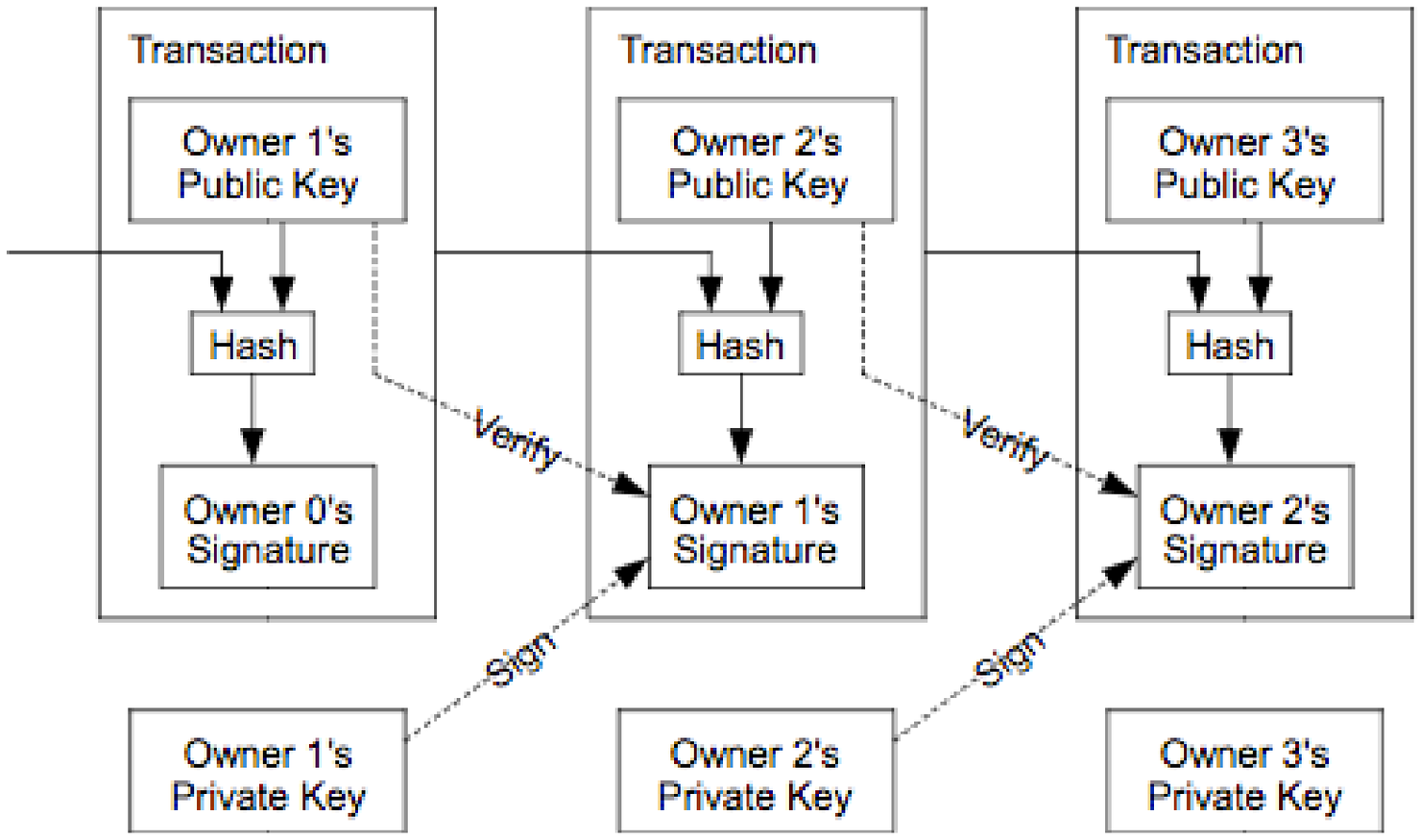
Digital Signatures
Hashing + Public key cryptography

- To *sign* a message:
  - Hash the message
  - Encrypt the hash with your **private** key
  - Send the message and hash together to the recipient

- To *verify* a message:
  - Hash the message (only)
  - Decrypt the hash with the sender's **public** key
  - Compare the decrypted hash with the one you have generated
  - **If the two hashes match then the message is unchanged and must have come from the sender**

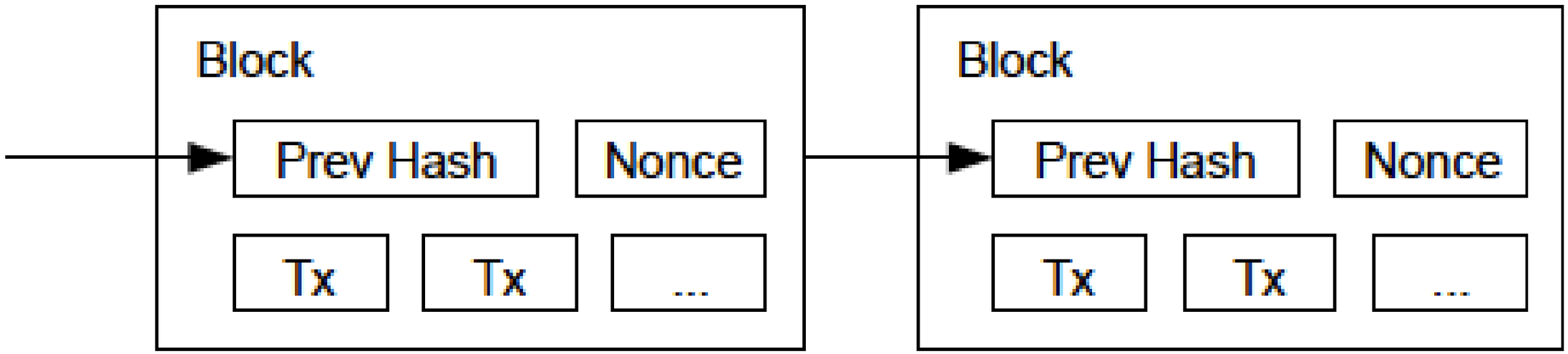
Bitcoin and Bitcoin transactions

We define an electronic coin as a chain of digital signatures. Each owner transfers the coin to the next by digitally signing a hash of the previous transaction and the public key of the next owner and adding these to the end of the coin. A payee can verify the signatures to verify the chain of ownership.



From *Bitcoin: A Peer-to-Peer Electronic Cash System* by Satoshi Nakamoto

Verifying transactions
and building the Blockchain



From *Bitcoin: A Peer-to-Peer Electronic Cash System*
by Satoshi Nakamoto

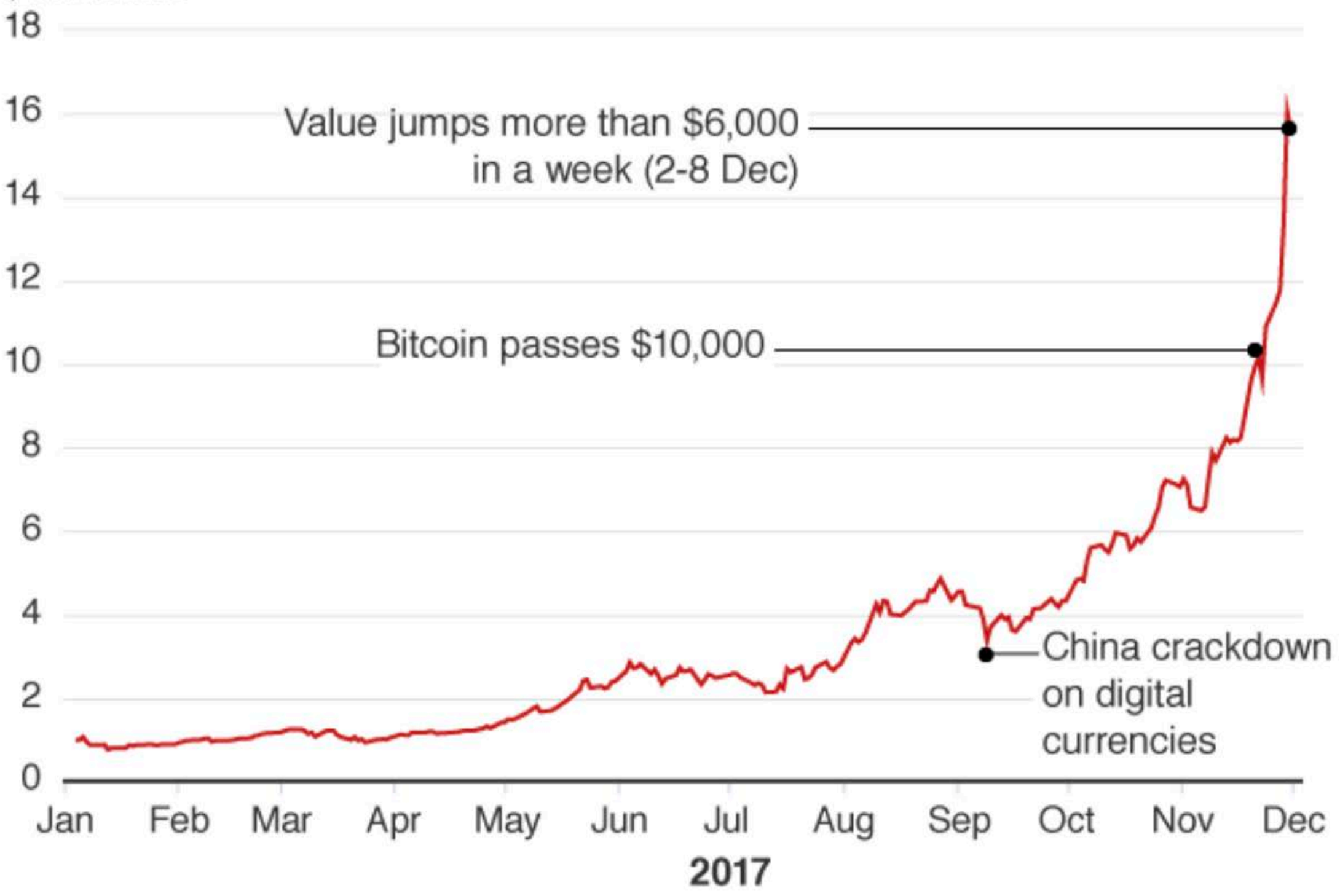
Table 1: Top 10 Cryptocurrencies, as of 17 June 2017

Rank	Name	US$ Market Cap	US$ Price	Circulating Supply
1	Bitcoin	43,630,891,619	2660.98	16,396,550 BTC
2	Ethereum	34,736,739,597	375.25	92,569,593 ETH
3	Ripple	10,215,346,626	0.266787	38,290,271,363 XRP
4	Litecoin	2,428,105,598	47.06	51,592,007 LTC
5	Ethereum Classic	1,950,098,114	21.04	92,694,964 ETC
6	NEM	1,848,834,000	0.205426	8,999,999,999 XEM
7	Dash	1,295,180,283	175.78	7,368,399 DASH
8	IOTA	1,177,470,178	0.423622	2,779,530,283 MIOTA
9	BitShares	888,444,894	0.342215	2,596,160,000 BTS
10	Stratis	766,295,675	7.79	98,428,282 STRAT

Source: CryptoCurrency Market Capitalizations, https://coinmarketcap.com/currencies, accessed 17 June 2017

2017: Bitcoin's unstoppable run

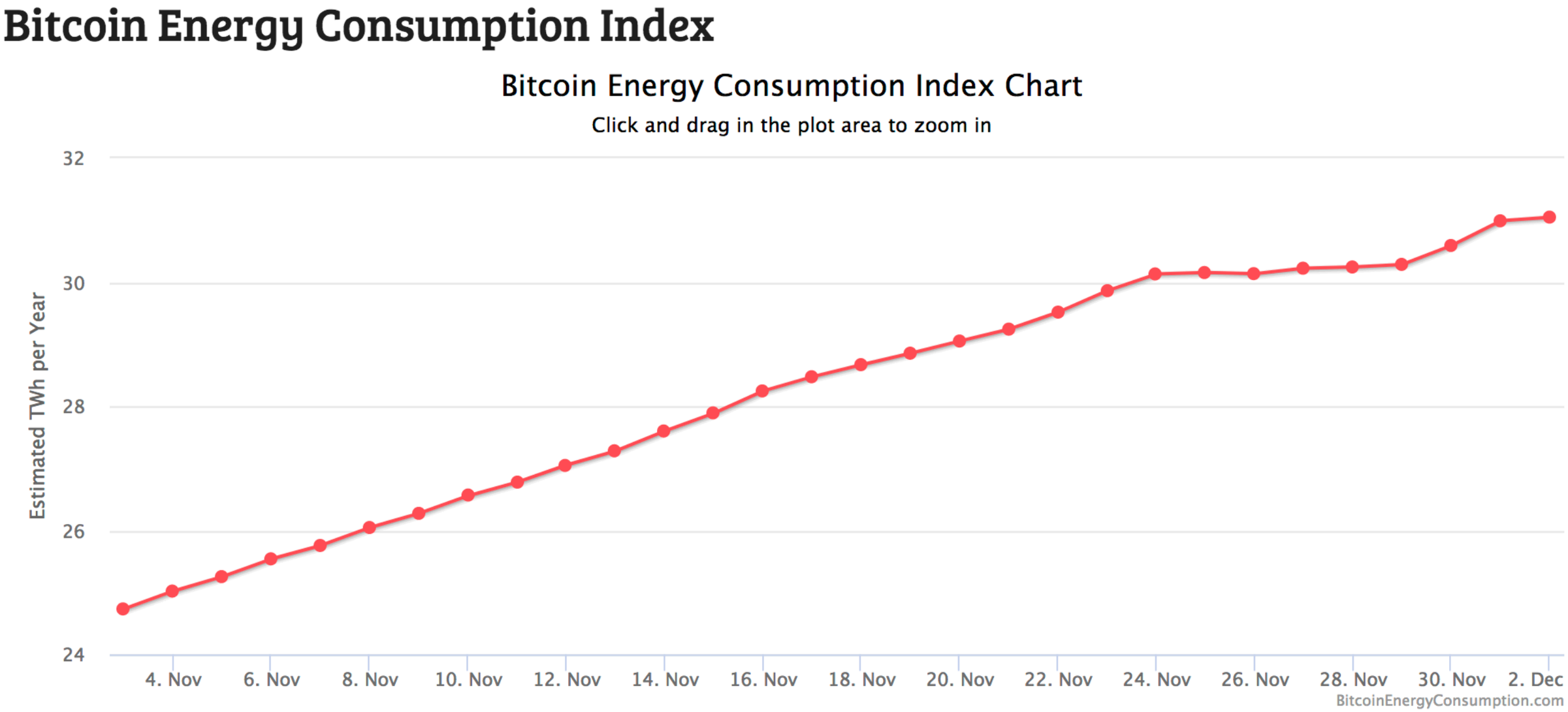
Bitcoin exchange rate with US dollar



Source: Bloomberg. Data to 8 December, 10:15 GMT

BBC

Bitcoin energy usage in November 2017 rose from 25 to 31 TWh per year



Private Blockchains can be much quicker and cheaper

- If you are willing to sacrifice some of Bitcoin's properties, you can build blockchains that are much cheaper and quicker to run than the Bitcoin system.

- For example, use one or more "trusted verifiers" instead of miners, and accept the loss of independence, while keeping the security, certainty and prevention of forgeries.

- Blockchain allows parties to maintain accurate shared records with their counterparties and to do so efficiently. This is a common requirement in financial markets and elsewhere.

Blockchain or Database?

- A single database must be owned and controlled by someone

- A distributed database is shared across different network nodes but relies on the nodes trusting each other

- Blockchain technology allows nodes to share data, safely and securely across a network and to agree on the validity of the data, even if the different parties do not fully trust each other.

"The practical consequence is for the first time a way for one Internet user to transfer a unique piece of digital property to another Internet user, such that the transfer is guaranteed to be safe and secure, everyone knows that the transfer has taken place, and nobody can challenge the legitimacy of the transfer. The consequences of this breakthrough are hard to overstate."

Marc Andreesen, US software engineer and venture capitalist

World Economic Forum

"Distributed ledger technology promises to have far-reaching economic and social implications. … blockchain appears likely to transform a number of important industries that provide or rely upon third-party assurance.

It could prove to be a broader force for transparency and integrity in society, including in the fight against bribery and corruption.

It could also lead to extensive changes in supply chains and governmental functions, such as central banking."

Smart Contracts

This [affects] much more than the financial services industry. *Innovators are programming this new digital ledger to record anything of value to humankind – birth and death certificates, marriage licenses, deeds and titles of ownership, rights to intellectual property, educational degrees, financial accounts, medical history, insurance claims, citizenship and voting privileges, location of portable assets, provenance of food and diamonds, job recommendations and performance ratings, charitable donations tied to specific outcomes, employment contracts, managerial decision rights* ***and anything else that we can express in [computer] code.***

World Economic Forum Report

e software — *Etherium* was designed specifically to allow any

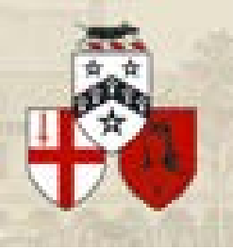
"The business community has been quick to appreciate the possibilities. Distributed ledgers can provide new ways of assuring ownership and provenance for goods and intellectual property. For example, Everledger provides a distributed ledger that assures the identity of diamonds, from being mined and cut to being sold and insured. In a market with a relatively high level of paper forgery, it makes attribution more efficient, and has the potential to reduce fraud and prevent 'blood diamonds' from entering the market."

https://www.gov.uk/government/news/distributed-ledger

UK Government Office for Science *use cases* for **Blockchain**

1. protecting critical infrastructure against cyberattacks
2. reducing operational costs and tracking eligibility for welfare support, while offering greater financial inclusion
3. transparency and traceability of how aid money is spent
4. creating opportunities for economic growth, bolstering SMEs and increasing employment
5. reducing tax fraud

Other uses for blockchain are proposed every week – often with little technical or business credibility.



Will Bitcoin and the Block Chain change the way we Live and Work?

- I think the Blockchain and Distributed Ledger Technologies (DLTs) *will* change how we live and work, because they enable organisations to reduce or eliminate costs, errors and delays in very many transactions.
- DLTs **could** be used to give individuals far greater control over the way their personal data is used – but I'm not optimistic about that.
- As usual with new technology, the people who eliminate costs will be the winners and the people who **were** the costs will be the losers.
- If Bitcoin continues on its current path, it will change how we live by accelerating climate change!
- DLT's will further increase our dependence on software – which will need to be highly reliable and should be ***correct by construction*** and not merely tested.

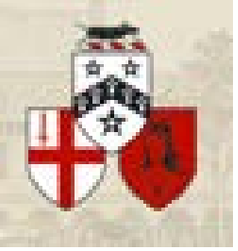
Conclusion

- Distributed Ledgers and the *Internet of Value* are likely to be disruptive to surprisingly many businesses.

- Cryptocurrencies will probably be around for ever but Governments will try very hard to regulate them – probably by licensing the exchanges that convert them into other currencies.

- Bitcoin probably won't be the leading cryptocurrency, by capitalisation or by number or total value of transactions.

- Blockchains depend on correct software and there have been major failures already. This is yet another reason why the world needs to invest in far stronger software engineering.



Questions?