GRESHAM COLLEGE

9 JANUARY 2018

WILL BITCOIN AND THE BLOCK CHAIN CHANGE THE WAY WE LIVE AND WORK?

PROFESSOR MARTYN THOMAS

Introduction

This lecture is about the *blockchain* — a novel way of recording and sharing data that has the potential to revolutionise the way that we manage and control everything from money to medical records to physical assets such as land and electronic components.

Recent reports from the UK Government Office for Science[i] and the World Economic Forum[ii] describe blockchain as highly disruptive and revolutionary. They say that systems that use the blockchain could remove the need for central banks, notaries, registrars and other intermediaries and make it much quicker, safer and cheaper to buy and sell houses, to pay taxes, to trade internationally and to deliver overseas aid whilst greatly reducing the opportunities for fraud and corruption.

The blockchain was invented to support Bitcoin, which is a form of digital money that exists without any central bank. It has been successful because its technology allows its users to have confidence that a bitcoin they are offered in payment really does belong to the person offering it and that it has not been forged or already spent. I shall use the example of Bitcoin to explain what the blockchain is, because we all understand and use money and the power of the blockchain will become clearer through a real example.

The strength of the blockchain depends on cryptography, so Bitcoin is known as a *cryptocurrency* or *cybercurrency*. It has become popular with criminals because it can be transferred anonymously over the internet. This has given blockchain a negative image that is undeserved.

I shall explain how Bitcoin evolved from the earlier ideas of digital fingerprints and digital signatures, so I shall need to explain these technologies too so that you can see that the blockchain is built on strong foundations.

What is money?

Money is a way of storing value and passing value around. Without money, all trading would be reduced to barter - swapping something that I have for something that you have. My cow for your corn, or my day's work for your fish. Money gives us a way of storing the value that we create with our labour so that we can use it later to get whatever we need.

Trust

Of course, we need to have confidence that the money we receive will be accepted by someone else later. The value of money therefore depends on the trust placed in the institution that guarantees its value. UK banknotes are guaranteed at face value by the Bank of England and carry a promise and signature from the Chief Cashier; other nations' currency is guaranteed by their own central banks. Such currencies are called *fiat money* because they

have been given value by the decision and action of a Government. Forgeries are made as difficult as possible and when forgery levels are thought to be high, the coin or note is withdrawn from circulation and replaced, as happened with the UK one-pound coin in 2017.

Cash is also trusted because you can see that a cash buyer really does have enough money and that they have not already spent it. The buyer loses the ability to spend the cash in the same instant that the seller gains it. But cash is inconvenient for major purchases or for anything other than face-to-face transactions.

Credit and debit cards are a form of electronic money and they are trusted because the issuers are trusted and because they offer some guarantees. But credit and debit cards must have a central bank or a credit card company behind them, which means that we have to give up some control over our money. For example, credit card companies take a percentage of every transaction, and accumulate vast quantities of personal information about us all.

Cash is different from credit cards and bank transfers because it is private and uncontrollable. You can give me cash if you choose to do so and no-one can stop you, or demand a percentage. If you only spend cash, no-one needs to know who you are, where you are or what you have been buying. Payment by bank transfer or credit card is different because it goes through an intermediary – your bank or credit card company – an intermediary that records the transaction and that can reveal the details, prevent it, reverse it later, charge a commission or deduct tax from it if the Government tells them to. Criminals use cash to be anonymous and to avoid taxes and other interference. Governments have responded by withdrawing very high value banknotes and they would like to eliminate cash and the cash economy entirely. Not surprisingly, governments and law enforcement agencies view the rise in cryptocurrencies with growing concern.

Bitcoin

Bitcoin was invented precisely to create a currency that had anonymity of cash but the convenience of debit cards without having to rely on trust. A currency that could be exchanged across the internet safely without any possibility of interference by governments or anyone else.

Bitcoins therefore need these properties:

- 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
- The validity of coins and transactions should never have to rely on trust.
- There should be no need for a central institution or any user with more rights or powers than others have
- 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

The solution was novel and at first sight might seem impractical, but it worked. It involved keeping a universally available, unchangeable, unforgeable, indestructible record of every transaction with every bitcoin from the very first time it was created through to the instant at which its current owner wishes to spend it, forever, without requiring that the real identity of any bitcoin owner is ever recorded.

The blockchain is the ledger that records this data and, for it to be universally available, every bitcoin user must be able to have their own copy and to have certainty that their copy is identical to every other copy of the blockchain. The blockchain is therefore a *distributed ledger* that contains the entire incorruptible history of every bitcoin.

As we shall see later, when you can do this for bitcoins, you can do it for anything and because it is digital you can use the same infrastructure to automate a lot of processes securely that can currently only be done manually, slowly and expensively.

Before we look in detail at the technical implementation, I want to make a brief diversion, to see why an innovation in managing ledgers could affect so much of society.

Ledgers

A ledger is a physical record of ownership and of transactions, and people have created and used ledgers for thousands of years. Ancient ledgers have been found that record harvests, the sale and purchase of grain or animals or houses or slaves and the collection of taxes, for example.

Today, ledgers are at the heart of business management, book-keeping, accountancy and audit. The Land Registry is a large ledger that records the ownership of land and buildings and the associated transactions of mortgages, sale and purchase, and legal rights and obligations attached to land.

Traditional ledgers have an owner that controls and authenticates changes to the ledger. For example, your bank and credit card accounts are ledgers that are managed and controlled by your bank or other financial service provider. Your passport and driving license are authenticated and managed through ledgers controlled by the Government. Your medical records and the deeds of your house are stored and managed in ledgers.

Wherever you look in a modern economy you will find ledgers and their controllers, and the controllers bring costs and overheads and employ a lot of people. All of which means that an effective way of managing ledgers without controllers could disrupt a lot of the economy and society.

The challenge for bitcoin was to create a ledger for a digital currency without relying on any central authority to create new money or for the control and authentication of transactions. Instead, bitcoin relies on digital signatures and these depend on public key cryptography and hash functions, so let's see how these work.

Cryptography, hashing and digital signatures

Cryptography is the world of secret codes. The objective is to translate any readable text ("plaintext") into an unreadable sequence of characters that can only be decoded and read by someone who has the key to the code. But this means that if Alice wants to send a coded message to Bob, they first have to exchange the key to the code, which has the disadvantage that their secret key may be intercepted, or the parties may have to meet to exchange the secret key.

Public key cryptography overcomes that problem through some mathematical magic. It uses uses two keys instead of one and these two keys are carefully designed so that they have the remarkable property that any plaintext that is encrypted with one of the two keys can only be decrypted with the other key, and yet you cannot calculate either key even if you know the other key and have a large amount of text that has been encrypted with either one of the keys. (The mathematics used to generate a pair of keys with this remarkable property relies on the difficulty

of factorising a number that is the product of two 100-digit primes - a task that has been shown to take impractical amounts of computer power – although that will change when quantum computing becomes a practical reality).

Now Alice and Bob can communicate in secret without ever having to meet or to exchange a secret key. They each generate their own pair of keys and they keep one completely private (their *private key*) and they publish the other one (their *public* key) on the internet, linked to their email address. When Alice (or anyone else) wants to send a secret message to Bob, they just have to encrypt it with Bob's public key, knowing that only Bob will be able to read it because no-one, but Bob knows Bob's private key. When Bob wants to send a secret reply to Alice, he encrypts it with Alice's public key and only Alice will be able to read it.

Anyone can use public key cryptography. It is freely available, for example as the *Enigmail* add-on to the Thunderbird mail client (which is what I use). The public keys are stored on *key servers* on the internet and the software will find them for you automatically.

Hashing is a way to create a unique digital fingerprint of anything that can be stored on a computer, such as a block of data or a photograph. This "fingerprint" is a number (called the *hash*) with the property that it is extremely difficult (and for strong hash functions impossible in practice) to create another block of data or photograph that has the same hash. The input to the hash function can be as big as you like, but its hash will always be short.

So, if you are sent an original text or photo and its hash, and if you know what hash function has been used, you can easily check that the original was not altered after the hash was created by simply running the hash function on the original and comparing the resulting hash with the one you were sent.

Even the smallest change to the original will change the hash. For example, the hash of the sentence "The quick brown fox jumps over the lazy dog" using the SHA224 hash function is 730e109bd7a8a32b1cb9d9a09aa2325d2430587ddbc0c38bad911525 in hexadecimal notation. Adding a full stop at the end of the sentence changes the hash to 619cba8e8e05826e9b8c519c0a5c68f4fb653e8a3d8aa04bb2c8cd4c.

We can use public key cryptography and hash functions together to create a *digital signature* as follows.

Suppose you wish to digitally sign an email. You create the email and generate its hash and you then encrypt the hash with your private key and send the encrypted hash with the email.

Anyone who receives the email and its hash can check that the message really was created by you and that it has not been altered or corrupted in any way. All they have to do is to use your public key to decode the hash and then regenerate the hash of the message themselves and compare the result. If they match, then they know that the message has not been altered and that it must have come from you, because no-one else should have access to your private key. In other words, the message has been digitally signed. If the recipient is using *Enigmail* or a similar system, this checking is carried out automatically.

Many software providers sign their software updates in this way (and all of them *should* do so), so that the users know that the software update is genuine and that it hasn't been corrupted, since even a single bit change would invalidate the hash.

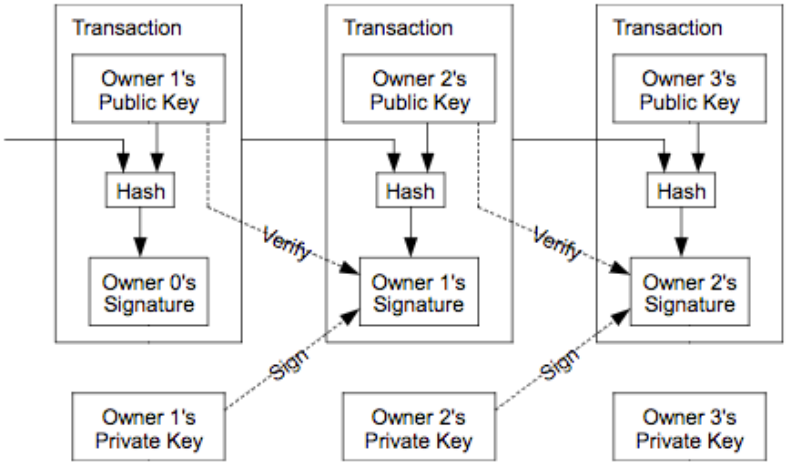
As we shall see, Bitcoin uses digital signatures to secure all the transactions in the blockchain.

Who invented Bitcoin and what is the Blockchain?

The acknowledged inventor of Bitcoin was Satoshi Nakamoto[iii]. This name is believed to be a pseudonym and there is no agreement about who (or even how many) people this really is[iv]. He, or they, may even be dead, as the bitcoin account linked to their public key is worth around many billion dollars and has been inactive for years.

Satoshi Nakamoto's original paper defined electronic money as follows

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.



This structure provides two essential guarantees. By checking that the public key in the coin is able to decrypt the signed transaction and that the hashes match, the we know that the coin has not been forged and that it belongs to the owner of the public key.

That leaves one further question before we can accept the coin in payment – how can we tell that the coin has not been spent already, without a central authority that can decide on the order of transactions?

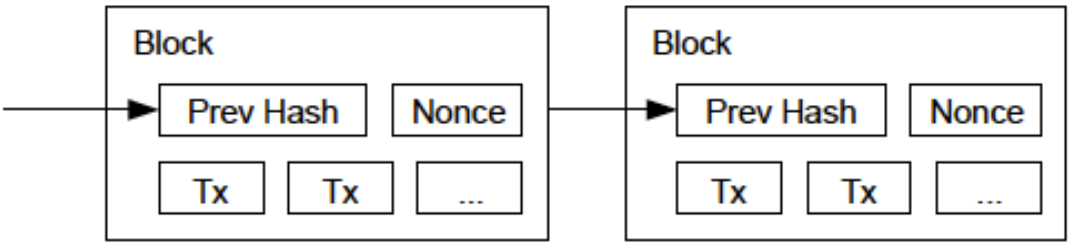
Satoshi Nakamoto's solution is that all transactions must be timestamped and published (which means that everyone can have a copy of the ledger – making it a *distributed ledger*) and that there must be a way in which all bitcoin users can agree which transaction happened first. In Satoshi Nakamoto's words "The payee needs proof that at the time of each transaction, the majority of nodes [in the Bitcoin network] agreed that it was the first received". It then becomes straightforward to check whether a coin has already been spent and to reject a new attempt to spend it if it has.

In this way, everybody can be sure that their copy of the distributed ledger has been agreed to be the truth.

The way in which this consensus is formed is a key technology at the heart of Bitcoin. It works like this, using as an example a customer spending a bitcoin in an online shop.

The customer sends the proposed transaction to the Bitcoin network to verify. Many network nodes (known as *Bitcoin Miners*) will then compete to verify the transaction, because they earn bitcoins by being the first to verify. When the transaction has been verified, the shop delivers the purchase.

Verification involves building the proposed transaction (usually but not necessarily with many others) into a new block in the blockchain, which has to have this structure (I have copied the diagram below from Santoshi Nakamoto's original paper):



The Tx fields are the bitcoin transactions in this block. In principle, there could be a new block for each individual transaction but, for efficiency, many transactions are usually included in each new block.

The Nonce (the name comes from "a Number used ONCE") is an arbitrary and meaningless number chosen by the verifier – I'll come back to what this is for in just a moment.

The Previous Hash field is a cryptographic hash of the previous block, using a standard hash function such as SHA-256[v] twice. As we have seen, the hash function generates a short digital fingerprint for a block in such a way that it isn't feasible to create another block that will have the same fingerprint. So, including this hash in the following block means that any change to a block somewhere in the chain would require that every block that followed it in the chain had to be recalculated. So, he verifiers start with the last block in the blockchain and check that the previous hash value is correct. If there is more than one version of the blockchain, they always use the longest one, which kills off any attempt to split the chain.

The security in Bitcoin comes from the great difficulty of creating a new block, which makes it extremely time-consuming and costly to forge even a short part of the blockchain. To make it difficult enough to be really secure, the Bitcoin rules require that a valid hash must have a minimum number of leading zeroes and the number of zeroes required is increased from time to time to make sure that the difficulty of creating a valid new block keeps up with the rate of improvement in computer hardware. The aim is to ensure that a new block takes about 10 minutes of computing on the fastest computers available, so that only about 10 new blocks can be created each hour. The requirement at the end of 2017 was that there must be 17 leading zeroes in the hash.

How do you create a block with a hash value that has at least 17 leading zeroes? Only by chance, because you cannot predict what the hash function will generate and the only thing you have that you can change is the nonce value (because everything else in the block has been digitally signed), So that's what a verifier has to do, increasing the nonce repeatedly and checking the resulting hash value. On average, it takes many trillions of attempts and calculations before happening on a nonce value that generates a hash with 17 leading zeroes (in blockchain jargon this is known as "proof of work").

The verifiers include a transaction that awards themselves 12.5 bitcoins. The first verifier to succeed in creating a block with enough leading zeroes broadcasts their new block to the Bitcoin network where it is checked by all the nodes that need to use it as the latest for extending the blockchain. When enough verifiers have accepted it by using the new block, its creator has these 12.5 new Bitcoins worth (as of November 2016) about 100 thousand US dollars, which is why people are willing to design special purpose hardware, to buy rooms full of powerful computers and to set up bitcoin nodes and act as verifiers. It's also why verifiers are known as "Bitcoin Miners", by analogy with digging for gold.

The reward for creating a new block halves roughly every four years. The new bitcoins that are awarded to miners are the only way that new bitcoins can be created, and the repeated halving of the reward means that after about 2150 no more bitcoins will be created.

To compensate for the reducing incentive to miners, transaction fees have been introduced so that Bitcoin users pay a fee to have their transactions verified. Those paying the minimum fee typically have to wait about 13 minutes for their transaction to be verified, though delays of up to 45 minutes have been experienced recently. Some Bitcoin users pay more so that their transactions are chosen preferentially by miners and verified more quickly.

The size of a Bitcoin block is limited to 1 Megabyte and this limit is controversial[vi], mainly because it slows down the number of transactions that can be verified per second (currently said to be 4.4) and this is an increasing problem as Bitcoin usage grows. Increasing the block size requires that most nodes in the network adopt new limits and create and accept larger blocks, which would require that every network node started new software and it would be the start of a changed blockchain - an event that is known as a "hard fork". This is a live issue and an alternative currency called Bitcoin Cash[vii] was created on 1 August 2017 from such a hard fork in the Bitcoin blockchain. If you are interested in the details,[viii] please follow the references in the lecture transcript.

This is a simplified explanation of the way Bitcoin works. More detail can be found in the references in the transcript[ix]. The effect of these rules is that anyone trying to forge a Bitcoin transaction successfully would need to control at least half of the computing power in the Bitcoin network to have any chance of success.

There are other cryptocurrencies, for example Ethereum, Ripple, Veritaseum, Litecoin, DigitalCash, NEM, IOTA, Gnosis, Monero, Wexcoin, and about one thousand others.

These use different mechanisms for verification and have many different features: you will be relieved to hear that I do not intend to explain how each of these works, though I shall return to Ethereum later to talk about a further development: *Smart Contracts.*

The exchange rate between cryptocurrencies and fiat currencies such as pounds and dollars is set by supply and demand and can move dramatically - the value of a Bitcoin in US dollars rose tenfold in 2017, by about 40% between October and November 2017 and by 12% in one day while I was writing this transcript. Before you all rush out and buy some, I should warn you that Bitcoin has been likened to the mania for Dutch tulip bulbs[x] that drove prices to absurd heights in the early 1600s before the price collapsed and ruined many speculators. The appearance of advertisements on the London Underground encouraging travellers to invest in Bitcoin suggests that the price rise is fuelled in part by a speculative bubble.

New cryptocurrencies are invented quite often and their development is increasingly funded by attracting investors with the promise that they will receive coins in the new currency. This method of funding has become known as an *Initial Coin Offering* or ICO, by analogy with the more traditional IPO or *Initial Public Offering* of shares in a new company. Some ICOs are fraudulent and all are high risk.

Blockchains without Miners

Santoshi Nakamoto chose to verify transactions through the consensus building and "proof of work" method that I have described above. This makes bitcoin transactions anonymous and free from interference, but it also makes bitcoin transactions relatively slow and expensive, because of the enormous amount of computation that is needed to slow down the process of creating each new block to prevent forgeries.

The bitcoin network uses a lot of electricity to power the computers that are competing to verify the latest transactions and to win the reward for creating the next block — and, of course, all but one of these attempts will fail and their computation will have been wasted. The present electricity used is said to represent 1.4% of the world's electricity consumption, or about the same as Morocco. An individual transaction takes about 260 kilowatt-hours, which is more than an average American household uses in a week[xi]. Citibank has calculated that the bitcoin network will ultimately use about as much electricity as Japan.

If we have an application that can use a cheaper form of verification (say by using one or more trusted verifiers) then we can gain all the rest of the blockchain's power much more cheaply. Many companies are therefore building or considering private blockchains for use in their businesses, and so are organisations that already verify transactions (for example the clearing banks and government agencies such as the Land Registry and the Passport Office). They can see the benefits that they could get from blockchain's security, audit trail, distributed ledger and smart contracts. So, let's see why these ideas have been recognised as having the power to change the way that we live and work.

Distributed Ledgers and Smart Contracts

The Blockchain is more than just a distributed database, because it can eliminate the need for trust and preserve anonymity

Marc Andreessen, a US software engineer and venture capitalist said

> *"The practical consequence [of the invention of the blockchain 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."*

A report[xii] from the World Economic Forum (WEF) said

> *Distributed ledger technology promises to have far-reaching economic and social implications. … … blockchain appears likely to transform a number of important industries that supply 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.*

The WEF report considers the invention of blockchain to be as significant as the invention of the World Wide Web, saying that the Web created the "internet of information" whereas blockchain is creating an "internet of value", where real assets are at stake.

The World Economic Forum report goes on to say

> *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.*

Of course, one of the things you can most easily express in computer code is software, so the blockchain can be used to hold transactions that can be made executable. The Ethereum cryptocurrency has been designed to make this particularly easy, with a standardised Application Programming Interface or *API*.

This API allows the creation of *Smart Contracts* that execute when some predefined conditions occur, such as the passing of a specified amount of time, or the receipt of a transaction with one or more specified signatures, or containing data that obeys some predefined rules.

As a simple example, consider the automatic compensation for a late-running train. Each ticket purchase is stored on a blockchain as a smart contract owned by the train company and identifying the account of the purchaser: the blockchain is also linked to the ticket gates on the stations, to record which ticket holders had actually travelled on that train. When the train is reported as over 30 minutes late, a trusted data source generates a transaction that causes the contract to be executed, compensating each purchaser who had a ticket for that train.

Or consider the sale of a car.

The car ownership record can be stored on the blockchain, authenticated by the Driver and Vehicle Licensing Authority DVLA and assigned to the owner (Alice) when she bought the car. To sell the car to Bob, Alice uses a smart contract that passes ownership of the car to Bob only when a transaction is received that transfers the selling price from Bob to Alice. Once the transfer of money from Bob to Alice has been verified by the blockchain network in the usual way, the ownership of the car will pass from Alice to Bob openly and securely by executing the contract. When Bob breaks the speed limit on the way home, the traffic camera will raise a transaction that automatically and instantly sends the infringement notice to the right owner.

More details of smart contracts can be found in a paper[xiii] written by Nick Szabo and published in 1998, ten years before the blockchain had been invented.

The Ethereum White Paper[xiv] provides examples of how smart contracts can be used for currency hedging, many forms of insurance, peer-to-peer gambling, electronic voting and much more. One American research organisation has even proposed[xv] using the blockchain to defeat attacks on the supply chains for critical national infrastructure, because the blockchain can be used to store and verify the origin and history of every component of a critical system.

But smart contracts are still just software and they can be wrong. The attack on the Decentralised Autonomous Organisation (the DAO) set up to fund Ethereum projects is the leading example and a fascinating modern detective story: the person who stole $55m of ether still has not been found. The story is entertaining, instructive and online[xvi].

Private Blockchains

You may be thinking "why would you use the blockchain instead of a conventional electronic ledger or database?". The answer is that the blockchain allows people and organisations to share data and to agree that they each have identical copies even if they do not completely trust each other, because they can each verify the data and every change that is made to it.

Often in business it is essential to share data with people we do not fully trust and where it is essential to be able to prove that transactions are valid and that no-one could have forged the records. Often it is necessary to share data across networks and across borders, so having a widely used common infrastructure reduces the costs involved in setting up and managing all the secure links and permissions.

The blockchain distributed ledger technology can be used to keep track of anything that can be uniquely specified by a digital identifier. Obvious examples include vehicles with chassis numbers, engine numbers and number plates, farm animals with ear tags, pets or other animals with microchips, and physical goods that have individual serial numbers. Banks and financial institutions can use blockchain technology to replace their existing ledgers and databases and then redesign their business processes to take advantage of the blockchain's properties.

Companies or groups can set up private blockchains with different privileges and security controls for different classes of user, and as described earlier, they can use a different mechanism than bitcoin's *proof of work* as the basis for achieving consensus on the validity of transactions. It is not necessary to follow bitcoin's design of distributed ledger or any other existing blockchain protocol, though it is likely be easiest and cheapest to build on top of one of the many open-source blockchain infrastructures that already exist.

The report by the UK Government Office for Science[xvii] observes that

> *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.*

The report describes in detail five particular use cases for blockchain in Government

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

New proposals come forward every week and companies have discovered that the mania for anything to do with blockchain can be very lucrative. A soft drink company changed its name in December 2017 to include the word *blockchain* – apparently with no in-house technology or technology partner – and their share price rose by 400%. This is very reminiscent of the dot-com boom and crash twenty years ago.

Conclusions

Distributed ledger technology is likely to change the way we run and use a wide range of services in society, ranging from banks to the National Health Service and beyond. We are in the very early stages of seeing how innovators will find ways to exploit the opportunities created by what the World Economic Forum report described as the Internet of Value.

Distributed ledgers have the potential to be far more resistant to cyberattack, because the data can be widely distributed and encrypted by default. The technology may often remove the need for a central authority or intermediary, taking away roles that have created whole professions.

Bitcoin is only one application out of the millions that will be built on top of blockchain technology but Bitcoin on its own could change the way we live and work - if only because its growing consumption of electricity will be a growing contributor to climate change!

Cryptocurrencies will probably be around forever, despite regulation by Governments but Bitcoin is unlikely to be the leading one.

There is much to be done to exploit these new opportunities and the integrity of blockchain systems depends, like the rest of our increasingly digital society, on software and therefore on far stronger software engineering than most software developers are currently using. That has been a pervasive theme of all my lectures and I hope that the adoption of distributed ledgers and blockchain technologies will stimulate a more rapid uptake of modern software development methods that lead to systems that can be proved to be Correct by Construction[xviii].

Until that happens, your Bitcoins, ether and other cryptocurrencies could disappear in an instant.

I have only been able to provide an introduction to the power of blockchain technologies. You will find much more detail in the references that I have provided in the transcript.

---

[i] https://www.gov.uk/government/news/distributed-ledger-technology-beyond-block-chain
[ii] https://www.weforum.org/whitepapers/realizing-the-potential-of-blockchain
[iii] *Bitcoin: A Peer-to-Peer Electronic Cash System*; https://bitcoin.org/bitcoin.pdf
[iv] https://www.coindesk.com/information/who-is-satoshi-nakamoto/
[v] http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.180-4.pdf
[vi] https://en.bitcoin.it/wiki/Block_size_limit_controversy
[vii] https://www.bitcoincash.org/
[viii] https://blockgeeks.com/guides/what-is-bitcoin-cash/
[ix] https://en.bitcoin.it/wiki/Block_hashing_algorithm
[x] http://www.investopedia.com/terms/d/dutch_tulip_bulb_market_bubble.asp
[xi] https://digiconomist.net/bitcoin-energy-consumption
[xii] https://www.weforum.org/whitepapers/realizing-the-potential-of-blockchain
[xiii] Secure Property Titles with Owner Authority, http://nakamotoinstitute.org/secure-property-titles/
[xiv] https://github.com/ethereum/wiki/wiki/White-Paper
[xv] http://www.defenddemocracy.org/content/uploads/documents/MEMO_Leveraging_Blockchain.pdf
[xvi] https://www.bloomberg.com/features/2017-the-ether-thief/
[xvii] https://www.gov.uk/government/news/distributed-ledger-technology-beyond-block-chain
[xviii] https://www.gresham.ac.uk/lectures-and-events/making-software-correct-by-construction