MOTT MACDONALD

Blockchain

A very disruptive new technology

November 2017

10 Fleet Place
London EC4M 7RB
United Kingdom

T +44 (0)20 7651 0300
F +44 (0)20 7248 2698
mottmac.com

Blockchain

A very disruptive new technology

November 2017

Issue and Revision Record

Revision	Date	Originator	Checker	Approver	Description
0.1	3/3/17	A. Wheen	S. Clayton-Mitchell		Initial draft for review
0.2	14/3/17	A. Wheen			Address review comments
0.3	14/11/17	A. Wheen			Further updates
0.4	15/11/17	A. Wheen			Version for web site review

Information class: Standard

Contents

1 Blockchain Technology

Blockchain regularly appears on published lists of new technologies that are disrupting established markets and business models. This section provides an introduction to blockchain technology and explains why it is significant.

1.1 Introduction

Although similar data structures had been used in computing for many years, the concept of a "blockchain" was first described in a white paper published in 2008 by Satoshi Nakamoto[1]. The blockchain was initially proposed as an integral part of the design of the Bitcoin cryptocurrency, but it soon became clear that the concept could be used to solve a much wider range of problems associated with distributed online applications. Today, blockchain technology is widely used in the financial sector, but has also found applications ranging from ride sharing in cars to the ownership of diamonds. The blockchain revolution has started, but it still has a long way to go.

1.2 Why do we need blockchains?

The blockchain was originally devised to avoid the need for any form of centralised control over the Bitcoin cryptocurrency. Before considering how a blockchain might be useful in other contexts, it is useful to understand the problem that it was originally designed to solve.

In any normal financial transaction that is conducted over the internet, there is a trusted intermediary required between the buyer and the seller. That intermediary is often a bank or a credit card company, but it could be a lawyer or some other organisation that is trusted by both parties. The primary role of the intermediary is to ensure that transactions can take place between complete strangers in a secure and transparent way. They provide a record of transactions that is accepted by both parties, and they help to ensure that both parties play by the rules. If such trusted intermediaries did not exist, then the internet would not be used for business because the risk of fraud would be unacceptably high. Blockchains are revolutionary because they eliminate the need for a trusted intermediary to support online transactions.

Blockchains are revolutionary because they eliminate the need for a trusted intermediary to support online transactions.

In the case of a currency, the trusted intermediary is ultimately the central bank. Amongst other things, the central bank controls interest rates and the supply of money in the system to ensure that the currency is not undermined by either inflation or deflation. It can also issue notes and coins if there is a requirement for cash transactions. Examples of central banks include the Bank of England (for the Pound Stirling), the Federal Reserve (for the US Dollar) and the European Central Bank (for the Euro).

[1] "Bitcoin: A Peer-to-Peer Electronic Cash System", Satoshi Nakamoto, https://bitcoin.org/bitcoin.pdf

However, to the original proponents of Bitcoin, a central bank is synonymous with central control. They wanted a currency that provided a secure store of wealth but was not subject to the whims of government or other pillars of the state. Consequently, they wanted a cryptocurrency that did not depend upon any centralised facility (such as a database of transactions) that could be shut down by state intervention. The blockchain was designed to provide a secure, distributed, online database that was not vulnerable to outside interference.

Whilst the motives of the Bitcoin proponents may have been idealistic, their creation provided a very convenient platform for illegal transactions relating to terrorism and drugs. The reputation of the Bitcoin currency suffered as a result of these unsavoury connections, but the traffic that they generated proved the viability of the underlying blockchain technology. It is quite possible that blockchains will live on long after Bitcoin has disappeared into history.

1.3 What is a blockchain?

To illustrate how a blockchain works, let's consider the blockchain used by the Bitcoin cryptocurrency.

As the name suggests, a blockchain consists of blocks of data arranged in the form of a chain. Each block holds a batch of valid transactions along with a timestamp, a link to the previous block in the chain and a "hash" of the previous block. The hash is rather like a checksum that can be used to confirm the integrity of a block of transactions. If anyone tampers with a block in the blockchain, then the hash stored in the following block will no longer be correct.

This means that anyone wishing to tamper with one of the blocks in a blockchain also has to modify the hashes in all the subsequent blocks in the chain. In the case of Bitcoin, the process of calculating the hash for a block requires the solution of a complex mathematical problem. This process is called "mining", and it has deliberately been made computationally intensive so that any attacker wishing to attack the blockchain needs access to a huge amount of computer power.

Every network node that supports the blockchain database will maintain its own copy of the blockchain. However, some nodes will inevitably hold a more up-to-date version than others as new transactions take place and new blocks are added to the blockchain. Each node therefore compares its own blockchain with those held by its neighbours, and the network of nodes will continually converge towards the version containing the largest number of validated blocks. This is done because it is assumed that the majority of network users are honest, so the majority of computer power in the network has been used to develop the variant of the blockchain that required the most work to create.

The probability of a new block being subsequently rejected goes down as more blocks are added to the blockchain and the number of nodes accepting that version of the blockchain increases. If an attacker tries to tamper with one of the blocks in the blockchain, they would have to re-mine the hashes in all the subsequent blocks. Furthermore, they would have to add additional blocks to the blockchain, because the other nodes will not accept the modified blockchain unless it is longer than the blockchains that they already hold. Since mining is computationally-intensive, and the attacker's node would be no match for the combined computer power in all the other nodes, it is very unlikely that such an attack would succeed in an established network.

This means that adding data to a blockchain is far simpler than deleting or changing existing data. The blockchain therefore provides a widely-available, difficult-to-attack, permanent and tamper-resistant distributed database. Since every node in the system holds a separate copy of the blockchain, there is no central point of failure and the system is highly resilient.

Since every node in the system holds a separate copy of the blockchain, there is no central point of failure and the system is highly resilient.

So far, we have only considered blockchain technology in the context of the Bitcoin crypto-currency. Alternative blockchains (also referred to as “altchains”, “consensus protocols” or “consensus platforms”) attempt to improve on the original Bitcoin concept, and typically offer some combination of: better performance, lower cost, more scalability, privacy, support for applications or other advanced functionality.

1.4 Public vs private blockchains

There are essentially two different types of blockchain:

- Public blockchains (also referred to as “permissionless” or “unpermissioned” blockchains) are useful when no central entity is available to verify a transaction. A public blockchain provides a permanent, immutable, verifiable and censorship-resistant record of transactions that everyone can see. However, these advantages come at the cost of computational complexity and slower transactions. Both Bitcoin and Ethereum are public blockchains.
- Private blockchains (sometimes referred to as “permissioned blockchains”) are restricted to a limited number of trusted participants. Restricting the blockchain to trusted participants avoids the need for some of the overheads associated with public blockchains. Private blockchains are typically preferred by large corporations (including financial services) for applications requiring simplicity, speed, and “controlled transparency” (i.e. transactions that have restricted visibility). However, it could be argued that private blockchains are effectively performing the same job as a distributed database, and are equally vulnerable to tampering by operational staff.

1.5 Standards

The development of blockchain technology will best be served by standard protocols and open source implementations to ensure interoperability. Links to well-known blockchain consortiums and collaborative projects can be found at: http://www.blockchaintechnologies.com/blockchain-definition#consortiums .

The Linux foundation has taken code donated by IBM and others to form an open source blockchain implementation called Hyperledger that can form the basis for further development. Microsoft has formed a working group called Kinakuta to exchange best practices on smart contracts and to work on improving security. The Smart Contracts Alliance is an industry initiative to promote smart contracts and provide a forum to develop industry standards.

2 Blockchain Applications

Since the blockchain concept originated in a cryptocurrency, it is not surprising that most of the initial applications for blockchain technology were in the financial sector. However, it has now become clear that the technology is applicable to a much wider range of distributed online applications in which there is a need for a reliable record of transactions that does not require the participation of a trusted third party. This section describes some current and future applications for blockchain, and identifies some key characteristics of successful applications.

2.1 Application examples

A blockchain-based distributed ledger can be used to disrupt many existing business models. Some examples are given in Table 1 below:

Table 1: Blockchain applications

Application	Description
Financial Applications	In 2015, Nasdaq launched a blockchain-based service called Linq to support share trading in privately-owned companies. Swiss bank UBS is leading a team of some of the world's largest banks to develop a blockchain-based settlements system to support trading in stocks and other financial instruments. Blockchain has also been used for crowdfunding applications such as Swarm. In addition to Bitcoin, there are now many other blockchain-based cryptocurrencies including BlackCoin, Dash, DigitalNote, Omni and Ripple XRP. Chain is a platform that enables organisations to build blockchain-based financial services.
Ownership of property	Everledger provides an immutable record of the ownership of diamonds. A diamond's serial number is registered on a blockchain along with its ownership and insurance details, so the blockchain provides a secure, public record of the diamond's ownership history. If a stolen diamond is recovered anywhere in the world, the police can quickly identify the rightful owner. The same approach can be used to record the ownership of paintings, land, houses, vehicles and just about anything else that can be owned and traded – including low-value or short-lived assets such as vouchers and tickets. It can also be used for the ownership of financial assets such as stocks and bonds, as discussed above under Financial Applications. Openchain is a blockchain-based platform that enables organisations to issue and manage digital assets in a robust, secure and scalable way.
Ownership of intellectual property	In addition to recording the ownership of physical property and financial assets, blockchain technology can also be used to manage ownership of intellectual property. A blockchain can create a permanent, public, transparent ledger for storing rights data and controlling payments to content creators based on usage. Examples from the music industry include Mycelia and Resonate.
Traceability	Since a blockchain can record the history of a product, it can be used to generate an audit trail for traceability purposes. For example, a blockchain can be used to certify the origins of organic and fair-trade produce, and can record information about prices paid to the original producer. Storing this information in a blockchain makes it possible to prove that the information existed at a specific moment in time, and that it has not subsequently been altered.
Identity verification	The need to verify a user's identity is an essential part of many online transactions. These include banking and other financial transactions, log-in to online accounts, access to medical records and other personal data, job applications, benefit applications, voting, tax returns and digital passports. With blockchain-based solutions, consumers can use an app for authentication instead of a username and password. The solution will store their encrypted identity, allowing them to share their data with companies while managing it on their own terms. This is done by combining two different technologies: blockchains and digital signatures. The digital

Application	Description
	signatures (typically based on public key cryptography) provide irrefutable identity verification, and the only check required is whether or not the transaction was signed with the correct private key. The blockchain provides a secure public record of transactions without the need to divulge the actual data and without the need for a trusted central authority. This approach allows users to control access to their personal data and to know who has accessed it. Since 2013, the Estonian government has used Guardtime to authenticate all citizen-related and business-related information in its databases. Other examples include BlockStack and Keybase.
Credit Rating & Online Reputation	Blockchain technology can be used to maintain a permanent and public record of an individual's past behaviour and reliability. This could range from relatively informal systems (such as Uber drivers refusing to pick up passengers with too many bad reviews) to formal credit rating and criminal record systems. The permanent nature of blockchain records might make it difficult to remove "spent" convictions or youthful irresponsibility, and could lead to litigation from people who feel that their reputation has been unfairly tarnished. However, the long-term consequences of getting a bad online reputation could also lead to improved behaviour.
Smart contracts	In addition to recording value and ownership, a blockchain can be used to execute software programs concurrently on multiple computers without the need for any centralised control. A smart contract is a program that is stored (typically in encrypted form) on the blockchain. The input data used by the smart contract, and the outputs that it generates, can also be stored on the blockchain. Since each computer will be executing the same code, they can compare their results in the same way that new additions to the blockchain are checked. In effect, the smart contract creates a distributed computer system that nobody controls and everyone can trust. A smart contract uses a programming language (such as C++ or Java) to define the contractual terms agreed by the contracting parties in essentially the same way as a traditional contract. The smart contract adds a layer of logic above the data stored on the blockchain that defines how particular eventualities should be handled. Whilst conventional contracts can contain ambiguities that require arbitration or the public judicial system to resolve, smart contracts can specify actions such as "in this situation, then this must happen" in a way that is unambiguous and can be implemented automatically. As an example, companies can use smart contracts to manage the insurance premiums that they pay more effectively. Inventory held by logistics companies constantly changes, so sometimes they are over-insured and sometimes under-insured for what they have in stock. A smart contract can link to an RFID tagging system that automatically registers stock in a warehouse, allowing the level of insurance to constantly match what is required. Organisations supporting smart contracts include Expanse, Etherium, Tezos and Monax.
Rental & sharing services	Slock.it is an application running on the Etherium blockchain that can be used to rent, sell or share a physical item. Access to the item (which could be, for example, an apartment, a car or a bicycle) is controlled by a smart lock. An advertisement offering use of the item can be placed on the blockchain, and responses will be recorded on the blockchain. The blockchain can then support a smart contract that controls access to the item and sorts out the associated payments. No middleman is involved, but both parties can be assured that the transaction is secure. Indeed, the process is so highly automated that it raises the possibility of completely autonomous companies that manage processes of this type without any human intervention at all.
Ride sharing	Peer-peer ride sharing applications such as Arcade City and La'Zooz connect drivers with customers and handle the associated payments. However, the use of blockchain technology eliminates the need for a centralised intermediary (such as Uber), so the rates charged can be controlled by the drivers themselves.
Internet of Things	The Internet of Things (IoT) requires a very large number of cheap, network-connected devices. This inevitably raises a number of security concerns, but public blockchain technology could provide a suitable distributed database on which IoT security could be based. In addition to holding device authentication information (model, serial number etc), the blockchain could also hold records of any data that a sensing device (eg a pressure sensor) generates, or a log of any commands sent to an actuating device (eg a smart lock). Blockchain technology would provide a secure, resilient platform that could scale to support billions of connected devices.

Source: Mott MacDonald

2.2 Application characteristics

It can be seen from the examples given in the previous section that blockchain applications typically have some or all of the following characteristics:

Table 2: Characteristics of blockchain applications

Characteristic	Blockchain Implementation
The same set of data must be accessible to a number of different users.	The same blockchain is stored separately on each participating computer in a network.
It must be possible to control who has access to the data.	The blockchain data can be encrypted. Digital signatures can be used to validate user identities.
It must be possible to ensure that the data has not been tampered with so that all users can depend upon its integrity.	Blockchains on the participating computers are kept in alignment. If there are enough separate computers, then tampering with the data becomes effectively impossible.
It must be relatively simple to store new data with an associated time stamp that can be relied upon.	An application is used to add data to the blockchain so complexity is hidden from the user. Once the data and the associated timestamp are added to the blockchain, they are protected from tampering in the same way as any other date held on the blockchain.
The implementation must be highly resilient so that the stored data is always available.	Since every participating computer holds a separate copy of the blockchain, there is no central point of failure.
No one person or organisation should have effective control over the stored data.	This is an inherent characteristic of public blockchains, and was one of the key objectives for the original Bitcoin implementation.
The data storage must be scalable to meet the needs of the applications that it supports.	The issue of blockchain scalability is discussed in Section 3.
It must be possible to use smart contracts to handle commercial transactions based on the stored data.	Smart contracts can be written in standard programming languages. The code and the associated data can be stored on the blockchain.

Source: Mott MacDonald

3 Blockchain Challenges

Despite the excitement that blockchain has generated, it is worth noting that there are still some significant problems that need to be solved.

3.1 Blockchain scalability

In January 2017, the size of the Bitcoin blockchain was approximately 100GB and was growing at 5MB/hour[2]. By November 2017, it had reached 140GB. If every user of the Bitcoin network were to store a full version of the blockchain, then this would raise some serious scalability issues – both in terms of the amount of memory required and the amount of network bandwidth required to keep all the nodes synchronised. Although memory and bandwidth costs are falling fast, this is an issue that will become increasingly serious if it is not addressed.

In the Bitcoin system, there is a small number of "full-node" clients that store a copy of the entire blockchain including the details of all transactions. These nodes are fundamental to the security of the Bitcoin system. However, most clients do not need to store the full details of every Bitcoin transaction that has ever occurred; instead, they store a summary of previous transactions that provides a verified representation of the current state. These clients are known as Simple Payment Verification (SPV) clients. SPV clients are much smaller and faster than full-node clients, while still following the same decentralised, peer-to-peer architecture.

The blockchain was originally devised to prevent any form of centralised control over the Bitcoin cryptocurrency, but the need to make the system scalable means that a degree of centralisation has become necessary to keep the system viable. Such compromises are more likely to be required in public blockchains (such as Bitcoin) than in private blockchains because the former are more likely to be characterised by a large number of relatively low-power nodes. However, there is a balance to be struck; if the number of full-node clients becomes too small, then it raises the risk of collusion between the owners of these clients to exert centralised control or manipulate the system for their own financial gain.

3.2 Blockchain power consumption

Energy consumption is a significant concern for public blockchains such as Bitcoin. As explained in Section 1.3, the process of adding a new block to the blockchain requires a "mining" operation in which different computers compete to find the solution to a complex mathematical problem. This uses a great deal of computer power, and the Bitcoin network was probably consuming about 350MW of electricity in November 2017. Projections for future energy consumption vary widely depending upon the energy efficiency assumptions used; for a worst-case scenario, one researcher has calculated that Bitcoin could consume as much electricity as Denmark by 2020[3]!

It might seem strange that the process for adding a new block to the blockchain requires Bitcoin nodes to undertake a task that has deliberately been made computationally-intensive. The reason is that the nodes in the network need to agree on which Bitcoin transactions are valid,

[2] https://blockchain.info/charts/blocks-size

[3] https://motherboard.vice.com/en_us/article/aek3za/bitcoin-could-consume-as-much-electricity-as-denmark-by-2020

and achieving consensus across a network of nodes without resorting to centralised decision-making is not easy – particularly if some of the nodes may be faulty or controlled by criminals.

The mining approach used by Bitcoin requires “Proof of Work” before a new block can be added to the blockchain. Since making a change to a block in the blockchain requires the work done to create that block – and all subsequent blocks – to be repeated, the risk of any block being changed becomes increasingly small as further blocks are added to the blockchain.

However, Proof of Work is not the only reliable method of achieving distributed consensus. For example, cryptocurrencies such as ShadowCash, Nxt, BlackCoin and Nav Coin use “Proof of Stake” algorithms in which the creator of the next block is chosen by factors such as wealth, age or random selection. Other possible approaches are based on Proof of Burn, Proof of Capacity, Proof of Activity, Proof of Storage, Proof of Space or Proof of Elapsed Time.

Ethereum (ETH) is currently working to migrate their blockchain implementation from Proof of Work to Proof of Stake, and it is likely that other public blockchains will migrate towards more environmentally-friendly ways of achieving distributed consensus. Energy consumption is not normally an issue for private blockchains because they are restricted to a limited number of trusted participants so achieving consensus is less of a problem.

3.3 51% attacks

As explained in Section 1.3, it is always possible for more than one version of the blockchain to be present in the Bitcoin network. If this happens, then the network will adopt the longest valid version of the blockchain.

However, if a fraudulent version of the blockchain were to be promoted by more than half the network users, then they would have more computer power than the honest users. As a result, they would be able to mine faster and their version of the blockchain would grow faster. Eventually, this would enable them to impose their fraudulent version of the blockchain on the rest of the network. If they did this repeatedly, then they would effectively have control of the blockchain. This is known as a “51% attack”.

This form of attack used to be considered infeasible because of the large number of fraudulent network users required. However, economic factors are causing mining activities in the Bitcoin network to consolidate into pools, and the four largest pools now control more than 50% of total mining capacity[4]. It would only take a small number of pool owners to work together for such an attack to become a realistic possibility.

[4] https://blockchain.info/pools

4 Conclusions

Blockchain technology has its origins in the Bitcoin cryptocurrency, and Bitcoin provided a large-scale demonstration of the benefits of blockchain. The many new applications and business models that can be enabled by blockchain technology will ensure that innovation will continue at a rapid pace. The blockchain revolution has started, but it still has a long way to go.

The blockchain revolution has started, but it still has a long way to go.

Despite all the excitement, there are still some significant problems to solve. One of these is the energy consumption of public blockchains such as Bitcoin. There are also concerns about the scalability and security of blockchain-based systems. Smart contracts have already been hacked and money has already been stolen. A “51% attack” on Bitcoin was once dismissed as infeasible, but is now looking increasingly possible as Bitcoin miners consolidate into pools.

Nobody is saying that these problems cannot be solved, but the features of public blockchains that were designed to prevent tampering or centralised control may make it more difficult to fix design problems once the blockchain is operational. New blockchain applications will need to avoid unnecessary complexity in order to manage the risk, but this will require the kind of restraint that is not characteristic of rapidly-evolving technology markets.