MODULE 3 UNIT 1

Blockchain technology and its use cases

UNIVERSITY OF CAPE TOWN

FINTECH: DISRUPTION IN FINANCE

IN COLLABORATION WITH getsmarter

Table of contents

Learning outcome:

LO1: Describe the foundations of blockchain technology and its uses.

1. Introduction

Traditionally, centralised decision-making authorities like banks, businesses, and governments have played an instrumental role in organising markets and governing countries. For centuries, banks have kept ledgers that record the inflow and outflow of customers' money, while businesses distribute resources, products, and services. Governments arrange elections, collect taxes, and enforce the rule of law through legislative and judiciary bodies. With the increasing globalisation of societies, central authorities have concentrated power among themselves by merging across industries and borders, often at the expense of the individual (Wright & De Filippi, 2015).

The advent of the internet in the 1990s signalled the potential disruption of this social order. Those who supported the disruption of traditional power structures argued that an interconnected world could facilitate smaller communities that function independent of central authorities. While the internet facilitated the liberation of information and more open markets, expectations of independence from centralised authorities have not been met. In fact, the distributive power of the internet has made governments and large corporations bigger and more powerful (Wright & De Filippi, 2015).

The emergence of blockchain technology has the potential to disrupt the current social power structure, as the technology reduces the need for centralised authorities. Transactions are administered on a decentralised database where users act as a collective middleman. Distributed ledger technology, which this set of notes covers, updates information instantaneously and enables users to interact directly with one another while remaining pseudonymous. Hence, blockchain technology can enable interaction on platforms that are not governed by the centralised authorities that dictate interaction on traditional platforms.

2. The foundations of blockchain technology

Blockchain technology is an amalgamation of various technological applications such as distributed ledger technology (DLT), peer-to-peer (P2P) networking, and cryptography. This section of the notes explores these technological applications in more detail. The composition of these various technological applications that form a blockchain depends on the inefficiencies (or problem) the blockchain aims to solve.

2.1 A distributed ledger

A distributed ledger is a database that is shared and maintained across a distributed network of participants called nodes. A blockchain is one type of data structure that is used in distributed ledgers. In a blockchain, data is stored and transmitted in blocks that are connected to each other in a digital chain. While the records in a centralised ledger are transmitted to nodes by a central authority, records in a distributed ledger are independently constructed and held by each node in the network, as illustrated in Figure 1 (Bryzek, 2018).

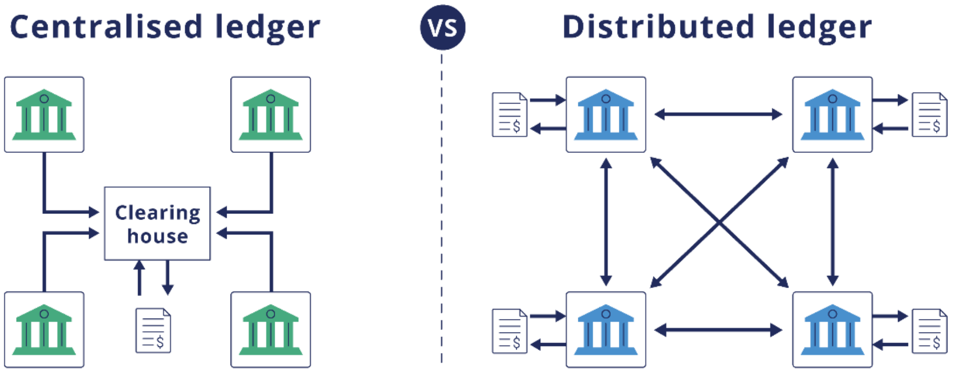

Figure 1: The difference between a centralised and a distributed ledger. (Adapted from: Bryzek, 2018)

Explore further:

In Module 1, you were introduced to the concept of blockchain as the solution to the Byzantine Generals' Problem. The distributed ledger technology can also be described as another layer to the internet.

2.2 Distributed consensus

Every transaction created on the distributed ledger must be processed and verified by each node or participant on the network. Nodes verify the authenticity of each transaction and, ultimately, reach consensus when a transaction is approved by more than 50% of the network (Bryzek, 2018). This process of verification is referred to as distributed consensus, or consensus protocol. Once consensus is established, the distributed ledger is updated and reflects identically for all users of the network.

2.3 Peer-to-peer (P2P) networking

A P2P network facilitates a distributed ledger. While a centralised network stores the network's information at a central point, such as a server, information on a P2P network is constantly recorded and shared between all users on the network. Examples of P2P networks include an intranet on which folders are shared among employees in an office or company and file-sharing applications on the internet.

2.4 Cryptography

Cryptography:

> [I]nvolves creating written or generated codes that allow information to be kept secret. [It] converts data into a format that is unreadable for an unauthorised user, allowing it to be transmitted without unauthorised entities decoding it back into a readable format [and] compromising the data.
>
> (“Cryptography”, n.d.)

Cryptography is used for identity verification and data encryption.

Cryptographic keys are complex cryptographic formulas or puzzles. To solve these puzzles, and thereby approve transactions on the system, users need to dedicate computer hardware and software to the task of solving the puzzle. Once the first user solves the cryptographic puzzle, that user is rewarded (usually with tokens) and receives Proof of Work (PoW). This forms the basis for every transaction that follows in that particular blockchain. PoW and other consensus mechanisms like Proof of Stake (PoS) are covered in more detail later in this module.

When a digital asset is transferred, a distributed ledger utilises public key cryptography to verify the transaction. To protect the asset, the user transferring the asset creates a unique digital signature – an algorithmic formula known as a private key – to which only that user has access. The other users in the distributed network then validate the asset transfer with a matching public key, which is another algorithmic formula available in a public depository. The users in the network verify the asset transfer by decrypting it using the public key. Public key cryptography is covered in more detail in the video in this unit.

3. Public versus private blockchains

A blockchain can be either public or private. In public blockchains, the network is open, and anyone can participate and execute consensus protocol. In private blockchains, users can only join a network by being invited and validated by the creator of the network. Both public and private blockchains are decentralised P2P networks in which users share distributed ledgers, but they are implemented for different purposes.

The operators of private blockchains, also called permissioned blockchains, decide who has access to the ledger, and who submits and verifies transactions. The implementation of private blockchains includes land and physical asset registries, commodities trading, and private equity distribution (Berke, 2017).

Currently, consensus protocol on the bitcoin blockchain takes about 10 minutes (Berke, 2017). Transaction verification on a blockchain is designed to take time for a reason. After consensus is established, transactions are only fully verified after an hour or two. This delay makes it too computationally expensive for a malicious party to introduce an altered variation of the ledger, known as a fork, and thus diverge the blockchain away from the main chain. However, this security measure can be a significant obstacle in fast-paced systems like stock trading. To address this obstacle, the operators of private blockchains can assign specific users to verify transactions and speed up the process of consensus and verification.

3.1 Suitability of private and public blockchains

Private blockchains are most often used for networks where parties want to interact, but do not fully trust one another. Private blockchains have mainly been implemented in the financial industry.

Private blockchains are most suitable for a system that requires:

- Central control over the verification of transactions;
- Quick processing of transactions; and
- The possibility of transaction reversal.

Public blockchains are preferable for a system that requires:

- Transparency;
- Widespread participation; and
- Third-party verification.

(Berke, 2017)

In the same way that businesses decide to host some of their systems on a secure intranet and others on the internet, businesses are more likely to implement a combination of both private and public blockchains This choice depends on a specific network's priorities.

4. Current applications of blockchain technology

The potential applications of blockchain technology are numerous, ranging from digital authentication to voting systems. One major focus of blockchain technology is to improve the way digital assets are stored, transferred, and recorded. Some of the most successful applications of blockchain, so far, have been in digital currencies, smart contracts, and global payment systems, which are explored in the following sections.

4.1 Digital currencies

As discussed in Module 1, blockchain was introduced as the underlying technology of the cryptocurrency bitcoin. As a result, blockchain has emerged and grown right alongside cryptocurrencies. Introduced in 2009, bitcoin is a digital currency that uses a decentralised blockchain. Unlike fiat currencies, bitcoin is not regulated by a central bank or government. Instead, the system is “completely decentralised, with no central server or trusted parties, because everything is based on crypto proof instead of trust” (Nakamoto, 2009).

Explore further:

Bitcoin might be the most well-known cryptocurrency, but there are other cryptocurrencies with unique aspects worth reading up on.

4.2 Smart contracts

Smart contracts are self-executing digital contracts and are an application of blockchain that could revolutionise the practice of law (Wright & De Filippi, 2015). Legal provisions and contractual agreements are embedded in a smart contract’s source code, which means that the legally bound parties can confirm whether conditions have been met without using an independent third party. Therefore, the confusion around legal terms that sometimes hinder contracts are eliminated, making contractual relationships potentially more effective.

Smart contracts have been implemented to facilitate the sale of goods between unrelated parties online and to automatically execute options, derivatives, futures, and swaps. Increasingly, sophisticated smart contracts are being developed by companies like Ethereum, Counterparty, and Mastercoin. Smart contracts and the programming language that underpins them could be used to create contracts that ensure employees are paid hourly, that taxes are paid to governmental agencies in real time, and that music royalties are distributed to composers as songs are played. Smart contracts could potentially replace the roles of trustees and testament administrators (Wright & De Filippi, 2015).

Pause and reflect:

Consider musicians who only upload their music to streaming services, such as Spotify and Apple Music, and use smart contracts to earn royalties. In this case, they could circumvent the process of using a lawyer altogether. Can you think of other industries where smart contracts could have a similar impact?

4.3 Global payment systems

Blockchain presents the opportunity to improve the security, speed, and cost of digital payments. As a result, blockchain technology is increasingly being implemented in global payment systems. For example, BitPesa in Kenya uses blockchain to facilitate payments without the need of a third party. This is particularly useful in countries that do not have established banking infrastructure.

Explore further:

While cryptocurrencies have made inroads as an alternative payment platform, most cryptocurrencies have not been successful at effecting one of the industry's most important objectives: banking the unbanked. Read about how BitPesa is solving the problem of banking the unbanked, one bitcoin transaction at a time.

As covered in Module 1, companies like Ripple are finding innovative ways of implementing the technology to find better solutions in the payments and settlements space. Many large financial institutions like Mastercard and Visa have also started to implement blockchain to facilitate cross-border payments, which currently take a long time to clear, and payments on business-to-business platforms.

Explore further:

In 2017, Mastercard announced the launch of its own blockchain. Read the linked article to find out why the credit card giant decided not to use any cryptocurrencies on its blockchain.

5. Conclusion

Blockchain technology presents the opportunity to eliminate the need for centralised intermediaries. It requires network users to verify transactions. Therefore, the network is maintained by all its users, rather than a central body. A blockchain can be public or private, depending on its purpose. Blockchain has enabled the implementation of decentralised ledger technology for networks that benefit from decentralised control. Current applications of blockchain can be found in digital currencies, smart contracts, and global payment systems. In the class-wide forum that follows, share examples of where you have seen blockchain technology applied in innovative ways.

6. Bibliography

Berke, A. 2017. *How safe are blockchains? It depends*. March 7. Available: https://hbr.org/2017/03/how-safe-are-blockchains-it-depends [2018, October 3].

Brown, C. 2018. *Blockchain continues to advance into the payment environment*. Available: https://www.forbes.com/sites/forbestechcouncil/2018/06/20/blockchain-continues-to-advance-into-the-payment-environment/#476ea13d24c9 [2018, October 3].

Bryzek, P. 2018. *The ultimate newbie guide to distributed ledgers*. Available: https://medium.com/@bryzek/the-ultimate-newbie-guide-to-distributed-ledgers-f8cc6950c826 [2018, October 3].

"Cryptography". *Techopedia.* n.d. Available: https://www.techopedia.com/definition/1770/cryptography [2018, October 17].

Jayachandran, P. 2017. *The difference between public and private blockchain*. Available: https://www.ibm.com/blogs/blockchain/2017/05/the-difference-between-public-and-private-blockchain [2018, October 3].

Nakamoto, S. 2009. *Bitcoin open source implementation of P2P currency*. Available: http://p2pfoundation.ning.com/forum/topics/bitcoin-open-source [2018, October 3].

Wright, A. & De Filippi, P. 2015. Decentralized blockchain technology and the rise of lex cryptographia. *SSRN Electronic Journal*. January 2015.