Emerging Technologies: Blockchain and Smart Contracts

Aristeidis Davelis, Usman Javed Butt, Gemma Pendlebury, and Khaled El Hussein

Abstract This chapter begins by briefly covering the history of Blockchain and introducing its core elements, continuing to explain the fundamentals of Blockchain technology and Smart Contracts. A discussion is made on nodes, consensus mechanisms, digital signatures and cryptographic hashes, types of blockchains, Ethereum, and Smart Contracts benefits. After that, it explores the distributed ledger technology (DLT) and blockchain as a subset of DLT in greater detail, discussing the benefits and challenges of DLT with Blockchain. It then presents us with some of the interesting use cases of Blockchain within various industries including financial, healthcare, manufacturing, and agriculture. Furthermore, it provides a roadmap for successfully implementing Blockchain in modern business, with recommendations on preparation, design and planning, implementation, and review. Finally, it explores future trends in DLT, blockchain and Smart Contracts.

Keywords Blockchain · Smart contracts · Distributed ledger technology · Bitcoin · Ethereum · Consensus · Blockchain use cases · Blockchain implementation · Blockchain benefits and challenges · Future of blockchain

1 Introduction

The emergence of Bitcoin and various other cryptocurrencies over the first two decades of the twenty-first century, gave birth to the first implementation of Blockchain. In its conventional form, Blockchain can be perceived as a set of immutable and tamper-proof data, arranged in cryptographically linked discrete sets

A. Davelis · U. J. Butt (✉) · G. Pendlebury · K. E. Hussein
Northumbria University Engineering and Environment, London, UK
e-mail: usman.butt@northumbria.ac.uk

A. Davelis
e-mail: aris.davelis@northumbria.ac.uk

K. E. Hussein
e-mail: khaled.el-hussein@northumbria.ac.uk

H. Jahankhani et al. (eds.), *Blockchain and Other Emerging Technologies for Digital Business Strategies*, Advanced Sciences and Technologies for Security Applications,
https://doi.org/10.1007/978-3-030-98225-6_6

Table 1 The value at stake from blockchain varies across industries adapted from: Carson et al. [3] (McKinsey & Company)

Industry	Revenue potential	Cost reduction potential
Agriculture	Average-High	High
Automotive	High	Average
Financial	Average-High	High
Healthcare	High	High
Insurance	Average	High
Real estate	High	High
Public	High	High
Media and communications	High	Average
Transport and logistics	Low-Average	Average-High
Utilities	Average-High	High

of information called blocks [1]. Data on the Blockchain is shared among participants via a distributed ledger, similar to a database stored in a decentralised system [2].

Growing beyond cryptocurrency, Blockchain found applications in various sectors with huge potential impact, due to its traceability, trust, immutability and decentralisation properties. Additionally, Blockchain technology quickly evolved with the inclusion of "Smart Contracts", which allow for programmable instructions that can be set to automatically trigger when specific conditions are met [3]. These benefits provide Blockchain with the ability to increase revenues and reduce costs in multiple industries. Some of the most impacted industries in terms of benefiting from Blockchain can be seen on Table 1.

1.1 From Conception to Implementation

Although Blockchain is considered an emerging technology, the concept of Blockchain is far from new. The idea of a distributed, secure, trusted system which would replace the need for mutual trust between varying parties, was introduced as early as 1979 [4]. Chaum's suggestions followed the basic principles behind Distributed Ledger Technology (DLT), with the later-conceived Blockchain being a specific type of DLT.

Later in 1990, the use of linked cryptographic hash functions had been suggested as a means to providing a "digital document time-stamping service", which could work under a "distributed trust" environment [5]. The proposal aimed to digitally sign and timestamp documents, in order to ensure they have not been tampered with. This essentially described the fundamental idea behind Blockchain. Very soon afterwards, cryptographer Nick Szabo introduced the idea of Smart Contracts, as a

means of securely and reliably automating contract execution over a network. Under this concept, a contract's clauses could be "embedded" in hardware or software components and make the breach of the contract nearly impossible or prohibitively expensive [6].

It wasn't until over a decade later however that the Blockchain concept started materialising. In 2008, a cryptographer using the alias "Satoshi Nakamoto" published a paper on a distributed digital currency system called "Bitcoin", utilising a timestamp server and cryptographic hash functions. These were used to link immutable "blocks" of transactional and other data in the form of a chain, which were verified by a "Proof-of-Work" consensus process [7]. Bitcoin was quickly implemented and the first Bitcoin transaction took place in 2009, giving birth to multiple cryptocurrencies over the following years.

Finally, the Ethereum cryptocurrency and blockchain implementation actually incorporated Smart Contracts upon its release, as mentioned in its white paper in 2014. In Ethereum, as Buterin [8] describes, Smart Contracts could be perceived as programmable entities on top of the blockchain, similar to "cryptographic 'boxes' that contain value which only unlocks when certain conditions are met".

Since the emergence of Ethereum, Blockchain has been undergoing constant development and improvement, evolving beyond cryptocurrency and establishing itself in multiple business applications in numerous sectors as mentioned earlier.

1.2 Core Elements

Some of the main concepts of Blockchain and DLT are presented in summary on Table 2, and will be discussed in greater detail in the following sections.

Table 2 Core elements of blockchain and DLT

Concept	Description
Decentralisation	The fact that no single entity or institution controls the operation of Blockchain [9]
Blocks	Discrete linked sets of transactions (or other information) stored on the Blockchain
Distributed Ledger	The record of all transactions, stored and shared across all devices on the Blockchain network
Consensus	The process of verifying new transactions [2], in order to agree on the addition of new blocks and the new state of the ledger
Nodes	Devices participating in the Blockchain network and the consensus process, holding copies of the ledger
Miners	The nodes competing to add new blocks to a cryptocurrency blockchain, and be awarded cryptocurrency if successful [10]
Smart contracts	Programmable instructions stored on the chain, that can be set to automatically trigger when specific conditions are met [3]

2 The Fundamentals of Blockchain

The Bitcoin cryptocurrency could be considered the first significant practical implementation of blockchain technology. It is an open-source, public, global, peer- to-peer (P2P) Distributed Ledger Technology, where users request transactions which are placed on the Bitcoin network, while being authenticated using their personal digital signature. Sets of financial transactions are pooled and then recorded in a 'block' that is added to a chain of similar blocks, in chronological order. Each block contains a cryptographic hash of the previous block's header information, to link the blocks in a chain. This is performed by decentralised Bitcoin nodes (miners) who hold a record of the blockchain ledger [7]. The Bitcoin nodes act collectively as a decentralised time-stamp server that uses Proof of Work (PoW) computation for the consensus mechanism, proving the chronological order of transactions and allowing blocks to be added to the chain once tested and confirmed by other nodes in the network [11].

2.1 Node Architecture

Blockchain is a type of DLT, which as mentioned earlier is a term for any shared databases, which are distributed amongst various parties. It is important to note however, that not all DLTs use blockchain technology.

In their purest implementations, blockchain systems are both distributed and decentralised. Nodes on a distributed system communicate with each other directly to fulfil a shared aim as a single platform; node coordination and fault tolerance however remains a concern. To protect themselves against issues caused by faulty nodes, blockchain systems utilise consensus mechanisms with varying fault tolerance levels. While distributed systems can still be controlled by a central authority, blockchain's decentralised concept means that no one central authority controls the network; it is instead controlled by the computations of the distributed nodes through the consensus model. This formation without a centralised controller is known as peer-to-peer (P2P) architecture [12] (Fig. 1).

2.2 Consensus Types

Blockchain uses consensus mechanisms, for nodes on the network to reach agreement on the blockchain state at any given time. This is challenging, as the algorithms must handle security of transmissions, synchronisation, failure, performance, and malicious nodes, as Chicarino et al. note [13]. Consequently however, consensus is critical to blockchain security [14].

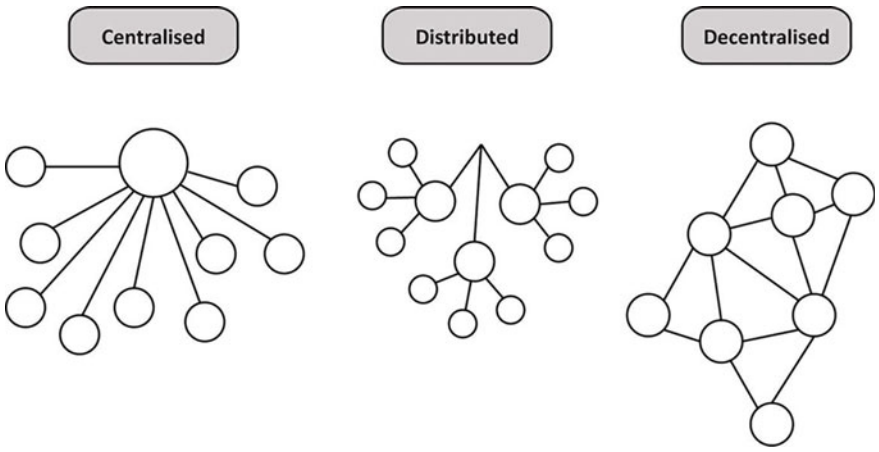

Fig. 1 Comparison of centralised, distributed and decentralised systems. Adapted from: Bashir [12]

There are many consensus mechanisms. The Bitcoin consensus type is called Proof of Work (PoW) and it uses the SHA-256 hash algorithm. The computing power required to complete PoW directly correlates with the economic value gained, aiming to disincentivise attackers. In Bitcoin's PoW consensus, a computed block hash must result in a number lower than the latest network target, in order for the hash to be valid. The average number of attempts to achieve this is the difficulty rating, and network hash rate is the times per second it takes to produce a valid hash. The target is changed over time depending on the nodes' processing power, to maintain a block generation time of approximately 10 min [15].

PoW is problematic due to the computing power it requires leading to a high consumption of energy and potentially negative environmental impact. Various consensus mechanism alternatives have been proposed as a solution to this issue. As Shibata [11] mentions, one alternative for cryptocurrency is Proof of Stake (PoS) which consumes less energy than PoW. With PoS, miners must prove their ownership of the currency to validate in consensus, working on the assumption that people who own more of the currency would be less likely to compromise the system. Some PoS solutions combine stake size with currency age or randomisation, to mitigate unfairness in the likes of the richest owner dominating the blockchain.

Delegated Proof of Stake (DPoS) is similar to PoS, but stakeholders elect the nodes delegated to produce blocks.

Another popular consensus mechanism is Practical Byzantine Fault Tolerance (PBFT), which is designed to tolerate byzantine faults (unknown percentage of faulty nodes) and malicious nodes, requiring every node to be visible to the network. It is managed by a primary node which is selected to sequence the transaction phases; pre- prepared, prepared, and commit. Each phase transitions to the next when at least two thirds of nodes have agreed [16].

2.3 Digital Signatures and Cryptographic Hash

In Bitcoin, digital signatures are used to prove that a transaction was legitimately initiated by a specific user. When a user requests a transaction, they must sign it with their private key to encrypt the transaction before it is broadcast to the network. Then the mining nodes validate the signature's authenticity using the public key, in order to confirm that the funds belong to the user who made the request, thus ensuring non-repudiation and data origin authentication. Bitcoin uses the Elliptical Curve Digital Signature Algorithm (ECDSA) to generate the key pairs, which is based on the standard Digital Signature Algorithm (DSA). As Raj [17] notes, the ECDSA uses a mathematical equation to create points on a graph curve, which are then used with a randomly generated number to calculate a private and public key pair.

In general, cryptographic hashes are integral to the Bitcoin blockchain. A cryptographic hash function converts input data, to output a corresponding string of fixed length known as a 'hash' or 'message digest'. To complete PoW and add a block to the chain, Bitcoin miners must use computing power to solve a complex mathematical puzzle, in the form of discovering the value of a pseudo-random generated number called a nonce (number only used once). As Bitcoin [18] states, the nonce is a random number which miners need to guess to produce the correct hash output and add the block to the chain. The nonce is then passed through a SHA- 256 cryptographic hash function in combination with transaction data to produce the result. Once complete, the result is broadcast to the other miners who verify whether it is correct, and if it is, the new block is added.

Whenever a new block is added to the chain, it also contains a link to the previous block using a cryptographic hash of the previous block header. This makes it almost impossible to tamper with, as changing one block would mean all previous blocks would need to be altered. Bitcoin blockchain headers contain the block version, the previous block header's (SHA256) hash (which ensures previous block headers cannot be altered without altering this), the Merkle root (SHA256) hash (computed from the block's transactions and thus ensuring they cannot be altered without altering the header), a timestamp, nBits (a value that the header must be equal to or less than), and the verified nonce. As Maleh et al. [19] point out, the distributed users' need for consensus, alongside the cryptography, protects blockchain against malicious alterations of the chain.

2.4 Types of Blockchains

There are different types of blockchain networks, each with its individual attributes:

Public (or permissionless) blockchains are transparent and open to the public to use, without a central authority governing them. The system is governed by the

blockchain network itself, with Bitcoin and most common cryptocurrencies being a widely known example.

Private (or permissioned) blockchains, where access to the system is restricted by a centralised authority and network transactions are not transparent to unauthorised parties [20]. These blockchains are common in corporate environments.

Consortium blockchains, which are controlled by a group of organisations [21]. As Maleh et al. [19] note, in this type of blockchain the network nodes are predetermined and controlled by the consortium. This essentially creates a semi- private blockchain concept, where the system is divided into a private section accessed by known entities and a public part available to anyone.

Another type of blockchain, based on architecture rather than access permissions and governance, is the sidechain (or pegged sidechain). As Bashir [12] highlights, sidechain refers to a blockchain linked to another blockchain using a two-way peg, to allow assets to be moved across the two chains (Fig. 2).

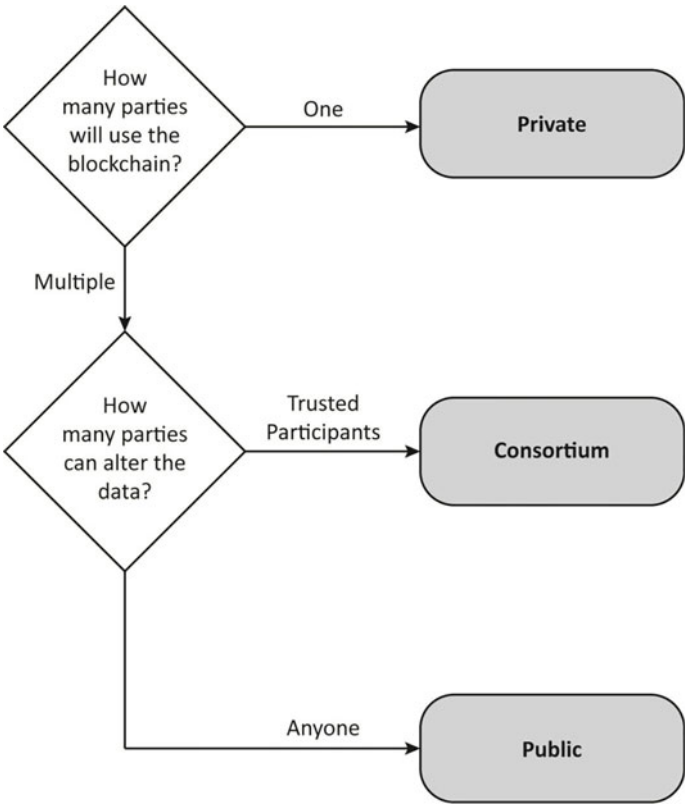

Fig. 2 Types of blockchains. Adapted from: Maleh et al. [19]

2.5 Ethereum and Smart Contracts

As Staples et al. [22] note, Smart Contracts store pre-programmed instructions that automatically execute transactions on the blockchain, when certain criteria are met. This negates the need for a centralised trusted third party, which would otherwise be required to perform clearing, settlement, or funding from issuers. Smart Contracts are programmed with predefined functions that determine what is the correct output based on input, in the execution of an agreement between multiple parties. The contract is hosted on the blockchain and after development is complete, the final code is stored on the blockchain to be invoked by relevant transactions. There are multiple platforms that facilitate Smart Contracts (e.g., Ethereum, Hyperledger Fabric, and NXT). Ethereum is the most popular platform implementing Smart Contracts; programmers can use Solidity to write decentralised apps (DApps) which are compiled using the Turing-complete runtime environment of the Ethereum Virtual Machine (EVM), and funded through a payment of Ethereum called 'gas' [23]. As Khan et al. [24] mention, the amount of 'gas' depends on the complexity of the contract. Furthermore, as Petrov [25] states, because the contract can be programmed to span the entire process of the agreement on the blockchain, all transactions are secure, immutable, and clearly auditable.

Smart Contracts can cover the entire agreement or accompany a traditional contract, and just handle the execution of certain actions, like the movement of funds. Like any software code, the parameters and functions of Smart Contracts need to be clearly defined, and often relatively simple requests are actioned. For example, if one rule of a contract between parties X and Y is honoured by party X, that triggers the contract to transfer some agreed funds from party Y to party X. However, developers are also using Smart Contracts to invoke other Smart Contracts which increases the potential complexity. Even so, Smart Contracts are not suitable for subjective decision making on contracts where there is any ambiguity involved, but they are very suitable for paying funds when certain events take place, or forfeiting fund as a penalty for commitments not being met. As Levi and Lipton [26] highlight, because the Smart Contract runs automatically on the blockchain, an intermediary (e.g. a judiciary or escrow holders) is not required to action or enforce the contract. Moreover, the enforcement of Smart Contracts is anonymous because there is no centralised control over the blockchain [27].

There are several variations of Smart Contracts; some have terms which are primarily written in natural language, but can use code to automatically perform the actions required by the agreement. Other contracts are only written in code, without any natural language describing the terms. Finally, hybrid contracts are a combination of the two to a greater or lesser extent. For example, the terms are mainly code based, but some provisions are written in natural language [28].

3 Beyond Blockchain

3.1 Distributed Ledger Technology

Distributed Ledger Technology (DLT) emerged before the development of blockchain and Bitcoin. As mentioned, early development of DLT was identified in the works of Bayer et al. [29] and Haber and Stornetta [5], wherein the chain of cryptographically linked data blocks was developed for secure and efficient handling of the digital data with the inclusion of hashing functions and Merkle Trees. In addition, DLT can be considered as an umbrella term wherein multiple systems operate without any central authority or operator. Furthermore, blockchain technology can be considered as a subset of the DLT environment, because of the use of hash-linked data blocks.

The definition of DLT as per Natarajan et al. [30] is a broad category of shared ledgers, which are defined for sharing records amongst multiple parties. On the other hand, the European Central Bank defines DLT as a technology that provides the benefit of storing and accessing information associated with specific assets to the users and holders within a shared database [31]. Regardless of definition specifics, as Rozario and Thomas [32] state, the use of DLT reduces the dependency on a central validation system, which consequently provides the users with the ability to settle their transactions independent of information of securities and cash within the distributed system.

There is no central coordinator existing in a DLT which operates in the traditional form. Figure 3 depicts that DLT provides multiple controls to different parties, making the system more preferable as compared to any other distributed or centralised database.

DLT also includes linking of cryptographic hashes for developing tamper evidence, and the result sharing helps in building an authoritative aspect of the records. It is also important to understand the concept of Ledger within DLT because

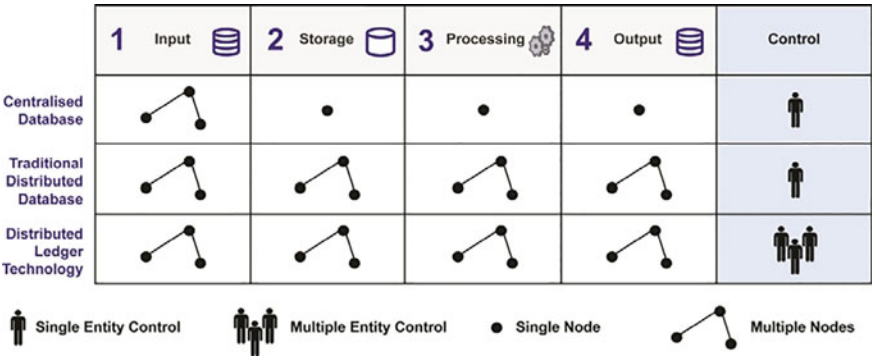

Fig. 3 Centralised databases and DLT

it is one of the most significant components of the system. The ledger would hold different meanings as per the application of DLT system, but as Hewa et al. [33] state, it is mainly developed through the data collected by an individual node, and the data that is commonly held by the majority of the nodes (Fig. 4).

Another significant aspect of the DLT system is the private key which is often referred to while making authorised transactions in the system [34]. This private key is a cryptographic sign of the initiator, which helps in changing the record state and fulfils the transaction instructions [35]. As Alharby et al. [36] highlight, private keys are very significant because they provide validation and guarantee that the transaction has been initiated by a true holder, proving there is no compromise with the safety of the ledger or the overall system.

DLT systems are also composed of multiple actors, which are interacting in the system. These actors are grouped into four significant categories as depicted on Fig. 5.

DLT systems are based on three core layers; the Network, the Protocol and the Data layer, which include sets of components and processes that enable the overall system to function [37]. The system view of the DLT is depicted on Fig. 6. This demonstrates that the foundation of DLT is based on the protocol layers, wherein the

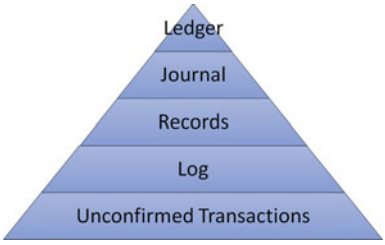

Fig. 4 Transactions to records—Development of a ledger in DLT

Fig. 5 Actors of DLT

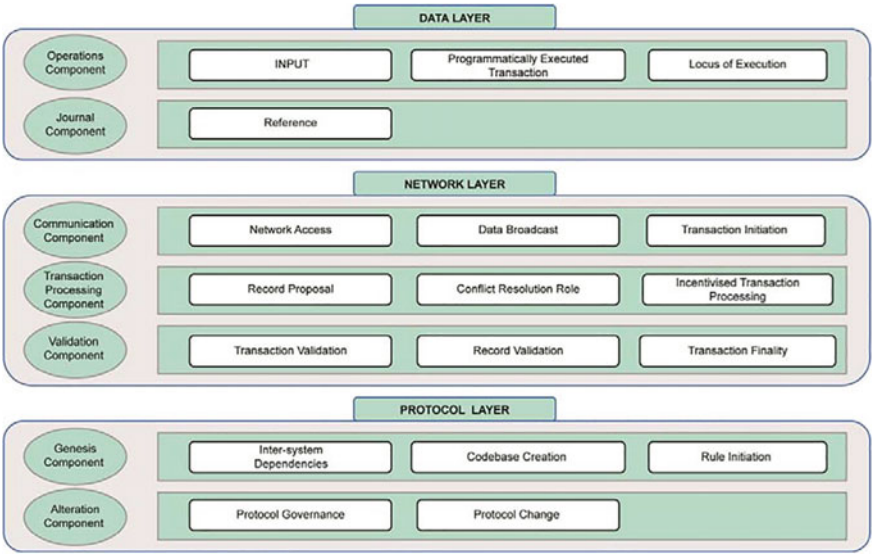

Fig. 6 DLT system layer view. Adapted from: Rauchs [39]

formal rules and the governing codes are established. The two components of the Protocol layer, Genesis and Alteration, are responsible for the network launch and the evolution of the system on time respectively [38].

Secondly, the Network layer is based on the implementation of the protocols that are defined in the foundational layer, and contains the identification of the ways through which data would be shared and updated in the network and the ledger. This layer also has three significant components. These are the Communications, Transaction Processing and Validation components, which enable better incorporation of the authorisation in the records [31]. Finally, the third layer of the DLT system is the Data layer, where the Operations and the Journal components are found. These are governing the flow of data in this layer, along with the storage of records as per the references and engagement of the nodes [40].

3.2 Benefits of DLT and Blockchain

DLT and blockchain systems provide the benefit of independent validation, wherein each participant in the system has the independency to verify the transaction state and maintain the integrity of the system [41]. Furthermore, they offer the benefit of shared recordkeeping, since multiple parties are collectively maintaining, creating and updating the records as per their level of authority.

Additionally, the system in the form of blockchain is capable of developing tamper evidence and censorship resistance, which indicates that a single party performs

the transactions or processes unilaterally [42]. The censorship resistance can also appear with the blocking or censoring of the transactions, or the change in the rules of the overall system within blockchain. Moreover, the decentralisation feature of DLT systems can be enabled at the desired degree at the different layers, as per the requirement of the system actors [43]. This implies that there is higher tamper resistance along with higher censorship resistance and low trust requirement, which makes the DLT a more desirable and reliable system as compared to fully centralised ones.

Apart from the aforementioned benefits, a DLT system or blockchain provides flexibility and freedom in deploying applications with a customised perspective. The distributed ledger has opaqueness and high-performance capabilities which enable efficient use of time and resources over the computers [44]. On top of this, the security of the distributed ledger is quite high because there is no compromise of stored data and easier access achieved through everyday practice.

The DLT system implemented in the form of blockchain would also be providing benefits like cost reduction within the organisation, due to easier reporting and auditing. The institutions would be able to perform multiple tasks through the use of blockchain which provides the benefit of speed and efficiency. Transactions are performed in seconds or less, which would be contributing to better management of time and efficiency requirements.

3.3 Challenges of DLT and Blockchain

The adversarial environment is considered as a strong indicator for the DLT system to have malicious actors as part of the system [45]. This environment depicts that the system is not used for the purpose it was intended for and there is exploitation of the consensus in the system, due to unauthorised authentication and disrupted network transferred transactions [46]. In other words, the intrusion in the system through unauthorised access will be affecting the DLT system's transactions.

The DLT systems are subjected to the challenge of compromise when the private keys are stolen and there is no security available for the transactions that are initiated with authorised attempts [47]. This provides an opportunity to the hackers to steal the data through engagement in the transactions without the knowledge of the true owners and authorised parties in the DLT.

The organisations with slow and cumbersome technological developments can experience the challenge of lack of scalability. Additionally, the difficulty in integration of the blockchain will be affecting the overall performance and complexity of the system. Additionally, the scalability and transaction speed of public blockchain systems is quite low, as compared to the private and consortium blockchains, making them less reliable. The governance of the private and consortium blockchains is also stronger compared to public ones [48]. This indicates that there is higher susceptibility to the environment, regarding the functioning of blockchains and DLTs without centralised administration.

Finally, contradictory to the advantages and benefits explored for DLT and blockchain, there is a technological challenge due to DLT still being the early stage of development. There are significant concerns prevailing in terms of the resilience and robustness which can affect the functioning of large software and the volumetric transactions [49].

4 Use Case Examples

A few use case examples based on real life applications of Blockchain and Smart Contracts are discussed in this section. This list is in no way exhaustive, aiming to provide a better view of how blockchain has already started adding value to a multitude of sectors, industries and markets.

4.1 Bitcoin and Cryptocurrencies

Bitcoin cryptocurrency could be considered the original implementation of blockchain, and has been recognised as a legitimate means of payment for goods and services in certain industries. As Raj [17] points out, cryptocurrencies differ from traditional currency, in that their creation and transference is decentralised and does not require an intermediary. Along these lines, Bitcoin was designed to solve the previous digital payment systems' weaknesses (including double spending) and remove the need for trusted intermediaries to mediate financial disputes, by creating a peer-to-peer system which relies on cryptographic proof of immutably recorded transactions taking place and their chronological order, rather than trust [7].

Blockchain has been described as the Internet of Value and Bitcoin became the first unit of value therein. It has proven blockchain's usefulness in transferring, and accounting for, value on a decentralised ledger across a peer-to-peer network. The first real world payment using Bitcoin was in 2010; since then Bitcoin's success has been followed by the creation of a multitude of alternative cryptocurrencies. A prominent example is Ethereum. Ethereum was developed by Vitalik Buterin, whose fascination with Bitcoin led him to start a project in 2013 to develop a blockchain platform (with a built-in cryptocurrency—Ether) on which developers can build applications [20].

4.2 Smart Contract Implementations

As a digital alternative to traditional contracts detailing agreements between parties, Smart Contracts are useful in multiple industries, including logistics, shipping supply chain, insurance and charities. Especially with regards to cross-organisational agreements, they can increase profit by accelerating processes, reducing real-time tracking

costs and enhancing cross-border payments. Crowdsourcing can also benefit from Smart Contracts, for the purpose of raising funds for a project through small donations from a large number of people. Additionally, charitable organisations could benefit in showing how contributions from various sources are handled so that performance data could be audited.

Due to their transparency, Smart Contracts can also be used for proving the provenance of data, managing access and sharing, as a reliable trust-less alternative to trusting a centralised intermediary for data handling. Apart from data provenance, other uses involve product tracing, with asset tracking from food to vehicles being typical examples. Another use case example for Smart Contracts is device management, in order to ensure synchronisation, authentication and data integrity for devices deployed on a decentralised network, rivalling the traditional client–server model. This is particularly useful in the case of IoT devices.

Furthermore, as Khan et al. [24] observe, non-fungible tokens (NFT) are a way to prove a unique asset's ownership using Smart Contracts on Ethereum. NFTs can be used to record ownership for real-estate, collectables, and art. The concept of NFT extends to anything non-fungible as the name suggests, meaning unique and not simply interchangeable with something else, unlike currency which is a fungible item. NFTs create a way to represent uniqueness, scarcity, and proof of ownership in digital form. The ownership is on public record, so it can be easily verified, and items can be exchanged in ways that could be difficult with physical assets without an intermediary. Similar to creating limited print runs of artwork, NFT creators can decide the scarcity by creating limited or numbered replicas, each with a unique ID. NFTs can also be programmed to stipulate if the creator is to receive royalties if the asset is sold on [50].

Another promising application of Smart Contracts is Decentralised Finance (DeFi), which refers to financial services built on blockchains like Ethereum, driven by Smart Contracts. An example is Compound, which is an open-source platform for lending and borrowing cryptocurrency built on Ethereum using Smart Contracts. As Leshner and Hayes [51] note, Compound allows users to earn interest on their cryptocurrency and tokenise assets using native tokens ('cTokens'), which are created from Ethereum ERC-20 tokens. Another example is Stellar, which is an open source blockchain-based system for trading multiple currencies affordably and efficiently. Like Ethereum 'gas', Stellar requires payment to use services in the form of the cryptocurrency 'lumens' [52].

4.3 Financial Services

One key aspect of blockchain is that it can be relatively cost-efficient to maintain financial services on it. This is a quality that could aid poorer jurisdictions, in extending financial services to previously excluded members of society, thus promoting financial inclusivity. By sharing transaction information via a blockchain ledger, blockchain can assist with reducing the cost and time of reconciliation,

which currently suffers from lack of visibility between reconciling organisations. The immutability of blockchain adds an extra layer of security against altering records and makes transactions easily auditable [53].

Under the context of Financial Services, blockchain can also be used for workflow automation with the possibility to script workflows across organisations, using Smart Contracts to validate data and action workflow steps. This could be also combined with an off chain 'oracle' for data inputs to the workflows through a third-party service. In addition, blockchain can increase the security and efficiency of systems where information needs to be shared between financial institutions about customers, providing them with a unique ID and immutably stored information that they can choose to share (e.g. customer identity verification). This also applies to any document sharing, which can be added to the chain with a hash signature for verification and can be linked to transactions for auditing purposes. Furthermore, because of its decentralised architecture, blockchain is well suited to building financial exchanges, offering settlement time and cost reduction while increasing transparency. As Roy [53] mentions, other financial applications of Blockchain include trade finance, cross-border remittance, secure IPOs and asset tracking.

4.4 Anti-Money Laundering

Regulated organisations and financial institutions currently must comply with anti-money laundering (AML) laws by conducting Know-Your-Customer (KYC) checks, which verify an individual's identity at the start of the business relationship and then performing Customer Due Diligence (CDD) throughout the business relationship to ensure they are not facilitating financial crime. The KYC process in itself can be time consuming and disjointed. FATF [54] also points out that financial institutions experience issues with financial inclusion, integration, legacy systems, data sharing and accuracy, when implementing AML solutions.

KYC systems built with blockchain technology can enhance this process by providing a distributed source for customer verification on a consortium blockchain, shared privately among financial institutions. Such systems utilise blockchain's immutability, transparency, and distribution to pool data in a single solution from multiple legacy systems. As Bashir [12] points out, this in turn results in reducing costs and the complexity associated with the KYC process. As an example to this aspect of the technology, ConsenSys and the Codefi product suite is an already established anti- money laundering solution built on blockchain. Codefi is designed to assist organisations with KYC and KYT blockchain monitoring and security auditing tools for smart contracts on Ethereum [55].

4.5 Healthcare and Pharmaceuticals

Blockchain has the potential to address issues currently experienced in the healthcare industry, surrounding control, integration, complexity and auditability. It could help increase availability and trust, decrease expenditure, and protect privacy.

As Bashir [12] mentions, a strong example use case in healthcare is stopping the distribution of counterfeit medicine. Counterfeit medicines can contain incorrect levels of active ingredients with unpredictable effects on the body. According to the World Health Organisation, 0.2 of 1 million deaths are caused by drug tampering and research has shown that 10–15% of global medicines are counterfeited. Studies have shown that blockchain technology can be used to authenticate medicine and enhance the monitoring of their production and distribution, to combat counterfeiting and tampering. One example is using blockchain to establish medicine provenance, tracking each medicine from manufacturer to distributor, then from carrier to hospital or pharmacy. The distributors are registered with a unique ID in the blockchain, and each delivery is recorded, time and location stamped, using their key to sign for verification. Furthermore, sensors are attached to each package that monitor factors like humidity and temperature to ensure the medicine is not spoiled. At the destination, QR codes can be scanned by the consumer to reveal the provenance of the medicine.

In a separate example application, Quzmar et al. [56] discuss that researchers devised a system that recorded information including hospital, administering doctor, drug dosage, dispensing pharmacy, and specific patient data—in addition to the delivery information which could be shared among hospitals which required the data. It used Smart Contracts to define the access permissions for security and confidentiality. As Wilson [57] mentions, British hospitals have already utilised the distributed ledger technology Everyware, developed by Hedera, to track and monitor COVID-19 vaccines. Similarly, researchers are investigating the use of blockchain for COVID-19 vaccine and contact tracing. One obvious challenge is maintaining the balance between transparency and privacy, although as Ricci et al. [58] propose, cryptographic techniques could be utilised to protect highly sensitive data while maintaining auditability.

4.6 Supply Chain

As Hewett et al. [59] discuss, the COVID-19 pandemic highlighted issues with the reliability of existing supply-chain processes for tracking, financing, authenticating, and delivering goods. Blockchain can revolutionise supply chain and trade flows systems and is a major area of development. Warren et al. [60] highlight that trustless and decentralised platforms can maintain a reliable and shared source of data for stakeholder coordination and the supply chain networks' operations.

Blockchain's transparency of transactions and privacy through encryption makes it suitable for tracking the provenance of products, to provide reassurance to purchasers that they are genuinely ethically sourced. Products can be tracked from the source onwards to provide the purchaser with a complete picture, through historical records, of the product's journey thus far. One example is the Everledger platform, which is used to prove the provenance of diamonds and that they are from 'conflict free' sources. Utilising blockchain technology, the diamond is issued with an identifying number and traced, so that its history is transparent to any buyer who wants to verify the source and route that the diamond took, up to the point of purchase. Hargrave and Karnoupakis [20] point out that these benefits can also be applied to other luxury items, as well like designer goods.

While organisations are developing permissioned blockchains for purposes like trade finance platforms, system interoperability is currently limited. Interoperability is a major challenge and opportunity for development to meet the needs of global supply chain requirements, in order to facilitate the exchange of information between blockchain systems globally. As Hewett et al. [59] mention, this is crucial for systems to effectively track the transport of goods, globally across systems, with visibility for all parties involved (manufacturers, logistics, retail etc.). Khan et al. [24] note another example along these lines, with a UK firm who have partnered with developers to create a blockchain system that tracks halal livestock through the process, thus improving traceability and providing verification of halal meat.

4.7 Agriculture

Agriculture efficiencies can result from the use of blockchain for 'smart' agriculture. Distributed ledger technology and blockchain can be used to solve the issue of needing a dispersed single platform for the storage and sharing of agricultural data regarding climate and land that affects production. Transaction transparency can be used to tackle the issue of trust in food safety, providing a reliable source of safety information that cannot be tampered with once verified and added on the blockchain. This would assist in making issues traceable back to the root cause.

Furthermore, blockchain can assist the agricultural supply chain, recording real-time data and aid in balancing the transactions of farmers and markets, while helping supply meet demand. For example, as Dong and Fu [61] mention, blockchain is currently being used in China to aid collaboration across the industry. Scattered small scale farms are joining forces to share their production information, using the transparency and distribution of blockchain data, with Smart Contracts to automate management processes. This allows farmers to operate as a larger enterprise, improve precision, decision making, resolve management issues and share the provenance of products with the consumer.

5 Implementation in Modern Businesses

5.1 Discovery and Preparedness Assessment

Before designing, procuring, and implementing a blockchain solution, organisations must determine whether blockchain is a requirement and if the business is prepared to adopt it. They need to engage stakeholders to assess the suitability of blockchain, and detail any potential use cases in resolving problems that affect the business, while also identifying potential risks and assessing the proposed solution's Return on Investment (ROI). This stage also entails considering the solution's intrinsic qualities, and assessing if its implementation will help the organisation with cost savings and risk reduction (Fig. 7).

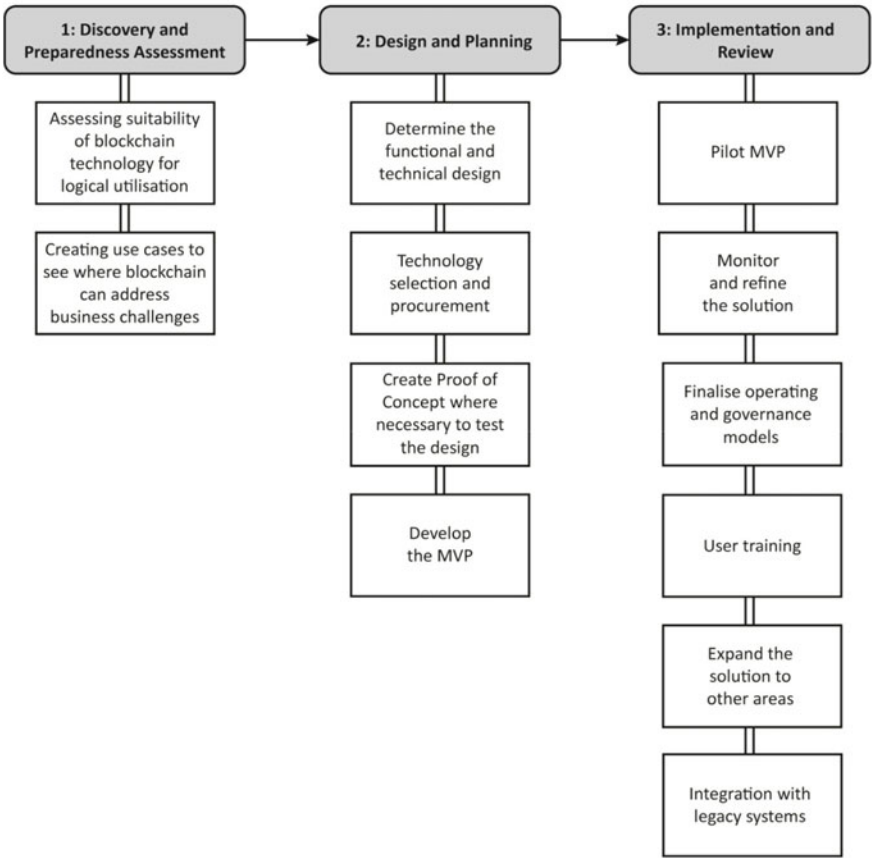

Fig. 7 Blockchain implementation roadmap

Once suitability has been determined, a Project Management Office (PMO) should establish a project team to organise the project and drive its phases forward, while monitoring milestones and risks, and coordinating all parties involved. Having the right team and skill sets is essential to a successful implementation, and to this end blockchain Subject Matter Experts (SMEs) should be engaged from the early stages, so that they can provide knowledgeable recommendations. Product and Business Owners need to monitor the development progress to ensure the solution is meeting their requirements, while existing enterprise architects and other technical staff should also be consulted and trained to address any skills gaps on implementation and maintaining the system. At the implementation stage, operational users need to be trained to interact with the technology, as ACT-IAC [62] suggests.

Organisations should also consider the adoption rate in the market they operate in, how this might impact their adoption strategy and if a blockchain solution is in line with their long-term business strategy. They need to evaluate their current technological environment and assess the complexity of integrating a blockchain solution in their ecosystem (including involving any participating partners), whether it will be an addition to existing systems, or whether it will fully or partially replace them. This evaluation also needs to consider the resulting impact on existing service, as well as the overall impact on the wider business and its processes, and what new policies and governance controls would need to be put in place. Governance and legal responsibilities need to be considered, and how they are affected if the solution needs to span multiple organisations in a consortium. Furthermore, the level of shared responsibility and trust that will be afforded to each involved party needs to be determined [63].

Figure 8 shows an example process flow for determining if there is a strong reason for an enterprise to adopt blockchain. As Knott [64] proposes, blockchain is most beneficial when a problem requires a decentralised, distributed solution that can transparently, securely, and immutably account for the history of assets and transactions. Blockchain will ultimately provide a permanent record that is easily audited and can prove the provenance of an asset; as a solution it is particularly suited to securing information between trusted parties, while allowing multiple parties to maintain a single source of truth for data sharing without an intermediary.

At this discovery stage, detailed technical planning is not required, but the higher-level technical aspects of blockchain should be considered to help assess its suitability and potential risks. By outlining the use cases in their organisation, the decision makers can consider the technical specifications of blockchain and its suitability. They should consider the type of blockchain, how accessible the data will be and if data is to be stored on or off the blockchain. What data validation requirements are there for adding data to the blockchain and if a 3rd party or notary will need to be involved to ensure data integrity. The size of the network, distribution and number of nodes should also be considered and how this will influence which consensus mechanism to adopt. Furthermore, the technical performance and scalability requirements for the solution need to be examined at this stage, such as transaction speeds and the amount of data to be processed.

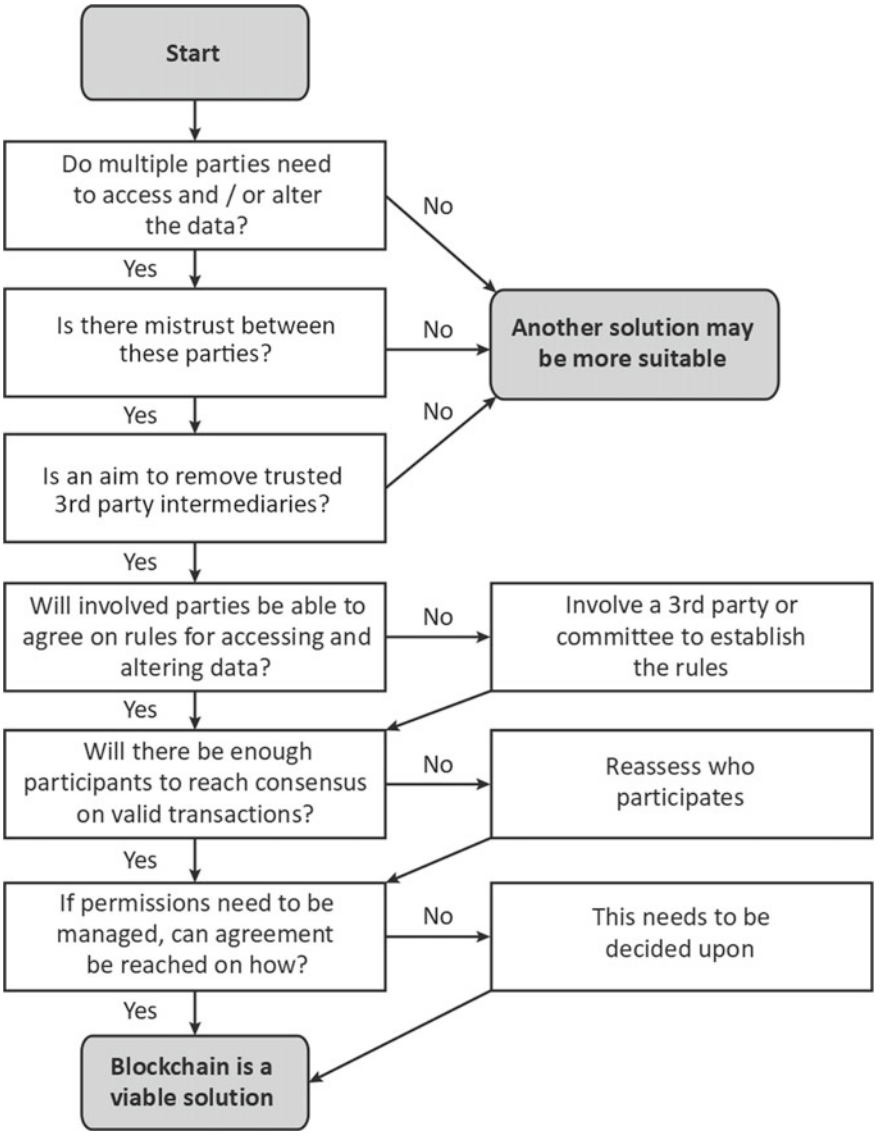

Fig. 8 Assessing blockchain's viability. Adapted from: Knott [64]

5.2 Design and Planning

Planning a Minimal Viable Product (MVP) is the recommended way to trial the blockchain solution on a smaller scale, within an area of the organisation that has been assessed for its suitability with a strong use case. Overall, a MVP can quickly

demonstrate the ROI a blockchain solution could bring, by testing it on a smaller scale and allowing for improvements while minimising turmoil for the business. It is also important however, to take a long-range approach when planning out future expansion and integrations with legacy systems and new technology [62]. This can be accomplished by adopting a phased approach, addressing different areas and needs within the organisation, and using a modular framework for blockchain projects that can be easily adapted for future developments as new standards emerge. Keeping the possibility of future interoperability with other systems in mind is beneficial. On top of this, as Hargrave and Karnoupakis [20] suggest, it is also important to consider the user experience when designing the solution, endeavouring to create a user focused design with simple interfaces for enthusiastic uptake and ease of adoption.

The planning phase should not only plan the technical details, but also map out the management of the solution's implementation, ongoing development, and maintenance. A change management plan should be of high priority, as it shapes the solution while users trial it and later use it, impacting the user engagement, adoption and ROI. It should also be adapted in consideration of specific blockchain qualities like immutability and automated Smart Contract execution. As Mpinyuri [65] suggests, a cross-functional team should also be appointed to deal with legal, compliance, and governance challenges (like privacy and jurisdictional responsibility), to work across all organisations involved with the solution. Other considerations during this phase include who is responsible for each aspect of the system, how the system will be governed, what the risks are, and what controls will be in place to mitigate them.

Before procurement, the blockchain technology specifications should be determined by assessing the business and technical requirements for the solution, considering the use cases identified in the discovery phase. Basic blockchain elements should be reviewed; for example, how transactions are performed, validated, and change the system. Furthermore, as ACT-IAC [62] states, the block composition and encryption mechanisms, the type of consensus and how any anomalies are handled, and how data is communicated between nodes should be examined. Among the technical considerations, it should be determined whether the network will be permissioned (private or consortium), permissionless (public) or a hybrid. Other standard operating requirements include the infrastructure platform (private, Software-As-A-Service/SaaS, Blockchain-As-A-Service/BaaS etc.), node location, user interfaces, reliability, and maintenance. Bashir [12] also points out that the organisation could use BaaS where blockchain services are managed externally and provide a platform ready for organisations to build their own Distributed Applications (DApps) onto. If an existing blockchain platform will be used, like Ethereum, any costs incurred (e.g., 'gas') will need to be taken into account [62]. In addition, choosing the consensus mechanism that best meets the performance requirements of the solution is very important, since it can impact transaction volumes, throughput and scalability. Moreover, as Staples et al. [22] note, another consideration is tied to whether all data will be stored on the chain (which can be more secure) or whether there will be use of indicators that point to a database located elsewhere (which can lead to better performance).

As a final consideration in this phase, the security specifications of the blockchain itself concerning encryption, consensus and data transport need to be defined. Organisations should research the different consensus methods (Proof of Work, Proof of Stake etc.) in the context of their network design, analysing the security risks related to each, in order to balance security with performance needs without compromising the system. Alongside that, user access must be considered (digital signatures, key management, authorisation, and authentication) to help preserve data integrity and mitigate unauthorised access, especially since this can be a major area of vulnerability with blockchain solutions. As Maleh et al. [19] note, any integrations with other systems, or applications, like Smart Contracts, will also need to be scrutinised for security risks.

5.3 Implementation and Review

In this phase, the MVP is delivered, and the design, operational and governance models are refined. If the MVP has then proven to be successful and beneficial to the business, the solution is expanded and integrated with other systems as required. By this implementation stage, the organisation should confirm the solution design and other elements with a clear project plan which schedules activities, resources, budgets, and risks. This will enable the implementation of the selected deployment model, in order to create the core blockchain solution. It is recommended that the project goals and scope are finalised to identify the functional requirements that are being addressed, alongside the technical design and security controls, including technical details relating to the selected architecture and governance rules. Nevertheless, the project would benefit from taking an Agile and iterative approach to testing and quickly reworking any part of the solution that is not effective. As Welfare [66] suggests, it is important to recognise that the implementation is a continuous process of improvement, which will most likely require much revision.

The initial planning regarding the solution participants needs to be refined during the implementation phase and altered, particularly if more organisations join the project during this phase. Deciding who is authorised to access specific data and how they are authenticated to access the system is also of utmost importance, and the onboarding and off-boarding strategy for participating organisations should be refined, to ensure verification of entrants and mitigate security issues. Overall, security should be regularly monitored to ensure any vulnerabilities are detected early. Additionally, operational processes must also be defined, together with adequate training plans for all participants to support them in using the technology.

Another activity at the implementation stage is integrating the blockchain with other applications and databases. Extensive testing should be performed with any integrated systems that could experience negative consequences from the blockchain implementation or vice versa. As Koteska et al. [67] underline, these components should be identified, and a test strategy should be formulated for testing with the original use-cases and functional requirements in mind.

Expanding the solution beyond the initial MVP presents its own challenges, especially when increasing the number of parties involved. Consensus on governance matters should be regularly reviewed by an appointed steering committee and adapted, if necessary, as the network of collaborating organisations grows [66]. Deloitte [68] also recommends planning the wider roll-out and any technical requirement changes that come with operating at scale. This includes slowly increasing the number of participants on the Minimum Viable Ecosystem (MVE) by one partner at a time, with ongoing improvements made as size increases. Finally, a legal operational model is essential, with policies and guidelines on governance, including matters like technical updates, ownership rights, onboarding, legal requirements etc. Ultimately, clear governance principles which define the participants' roles and responsibilities are important for the success of a wider roll-out between multiple parties.

6 Future Trends

The evolution of DLTs and the increasing use of blockchain have increased the future potential for digital currencies and the transactions that take place in the digital environment. Future developments and trends in the context of Smart Contracts include research in the direction of formal verification, Smart Contract-based organisational management and the Layer 2 of Smart Contracts [69]. As Fox et al. [70] state, it is identified that Smart Contracts with formal verification will increase the confidence associated with the technology and overall user acceptance.

On the other hand, the rapid developments in technology associated with the Internet of Things and Artificial Intelligence, will lead to changes in the infrastructure associated with implementation of Smart Contracts. As Tarr [71] notes, there will be improvements in the conceptual frameworks and the fundamental theories associated with the use of blockchain and Smart Contracts due to the influence of AI, as well as the changing dynamics of organisational management. Due to their programmatic nature, Smart Contracts also bear the potential of transforming DLT systems and applications in the future, leading to the emergence of more complex blockchain architectures.

As Farahaniet et al. [72] suggest, DLT systems are expected to aid the development of governance frameworks in the future, which would be functional without the compromise of freedom and independence, as acquired via their decentralised attributes. Additionally, McCorry et al. [73] observe that future developments in blockchain would help in increasing performance and speed, and improving interoperability over multiple platforms. Finally, the implementations and research conducted in the context of DLT and blockchain, would aid in increasing the quality of system audits and reduce the expectation gap that exists between regulatory bodies, auditors and end users.

7 Conclusion

As discussed, the potential of blockchain and Smart Contract implementations is huge for a large number of industries, although they still emerge from their early development stages. The gradually increased adoption of blockchain projects as enterprise-level solutions have put the technology to the test, and will demonstrate its efficiency over the coming years. Furthermore, the integration of Smart Contracts in blockchain applications has enabled the technology to reach new levels of customisation and complexity, adapting to bespoke business needs, and meeting the elaborate demands of today's fast-paced industry.

At the end of the day, the ability to automate, secure and fortify the way transactions work in the online world is starting to be regarded as a necessity rather than an idealistic scenario. This is especially urgent in a digital environment where fraud, mistrust and lack of traceability have evolved into serious issues affecting individuals, organisations and governments on a daily basis.

References

1. Puthal D, Mohanty SP, Kougianos E, Das G (2020) When do we need the blockchain? IEEE Consum Electron Mag 10(2):53–56
2. Tasatanattakool P, Techapanupreeda C (2018) Blockchain: challenges and applications. In: 2018 international conference on information networking (ICOIN), IEEE, pp 473–475
3. Carson B, Romanelli G, Walsh P, Zhumaev A (2018) Blockchain beyond the hype: What is the strategic business value. McKinsey & Company 1–13
4. Chaum DL (1979) Computer systems established, maintained and trusted by mutually suspicious groups. University of California, Electronics Research Laboratory
5. Haber S, Stornetta WS (1990) How to time-stamp a digital document. In: Conference on the theory and application of cryptography. Springer, Berlin, pp 437–455
6. Szabo N (1997) Formalizing and securing relationships on public networks. First Monday 2(9)
7. Nakamoto S (2008) Bitcoin: a peer-to-peer electronic cash system. [Online] Available at: https://www.debr.io/article/21260.pdf. [Accessed 31 July 2021]
8. Buterin V (2014) A next-generation smart contract and decentralized application platform. Ethereum White Paper 3(37)
9. Kolb J, AbdelBaky M, Katz RH, Culler DE (2020) Core concepts, challenges, and future directions in blockchain: a centralized tutorial. ACM Comput Surv (CSUR) 53(1):1–39
10. Crosby M, Pattanayak P, Verma S, Kalyanaraman V (2016) Blockchain technology: Beyond bitcoin. Appl Innovation 2(6–10):71
11. Shibata N (2019) Proof-of-search: combining blockchain consensus formation with solving optimization problems. IEEE Access 7:172994–173006
12. Bashir I (2020) Mastering Blockchain—third edition. 3rd ed. s.l.:Packt Publishing
13. Chicarino V, Albuquerque C, Jesus E, Rocha A (2020) On the detection of selfish mining and stalker attacks in blockchain networks. Annal Telecommun, pp 1–10
14. Ren W et al (2020) A flexible method to defend against computationally resourceful miners in blockchain proof of work. Inf Sci 507:161–171
15. Lantz L, Cawrey D (2020) Mastering blockchain. s.l.: O'Reilly Media, Inc
16. Zheng Z, Xie S, Dai H, Chen X, Wang H (2017) An overview of blockchain technology: Architecture, consensus, and future trends. In: 2017 IEEE international congress on big data (BigData congress). IEEE, pp 557–564

17. Raj K (2019) Foundations of blockchain. Packt Publishing, s.l.
18. Bitcoin (2021) Block chain. [Online] Available at: https://developer.bitcoin.org/reference/block_chain.html [Accessed 31 July 2021]
19. Maleh Y, Shojafar M, Alazab M, Romdhani I (2020) Blockchain for cybersecurity and privacy: architectures, challenges, and applications. Taylor & Francis Group, ProQuest Ebook Central, s.l.
20. Hargrave SJ, Karnoupakis E (2019) What Is Blockchain?, s.l.: O'Reilly Media, Inc. As seen on: https://www.oreilly.com/library/view/what-is-blockchain/9781098114749/
21. Taskinsoy J (2019) Blockchain: a misunderstood digital revolution. Things you need to know about blockchain. SSRN Electron J
22. Staples M et al. (2017) Risks and opportunities for systems using blockchain and smart contracts. Data61 (CSIRO), Sydney
23. Ethereum (2021) Dapps [Online] Available at: https://ethereum.org/en/dapps/. [Accessed 19 Aug 2021]
24. Khan SN, Loukil F, Ghedira-Guegan C, Benkhelifa E, Bani-Hani A (2021) Blockchain smart contracts: Applications, challenges, and future trends. Peer- to-peer Networking Appl 1–25
25. Petrov D (2020) Blockchain Ecosystem in the Financial Services Industry. FAIMA Bus Manage J 8(1):19–31
26. Levi SD, Lipton AB (2018) An introduction to smart contracts and their potential and inherent limitations. [Online] Available at: https://corpgov.law.harvard.edu/2018/05/26/an-introduction-to-smart-contracts-and-their-potential-and-inherent-limitations. [Accessed 19 Sept 2021]
27. Kannengießer N, Lins S, Dehling T, Sunyaev A (2019) What does not fit can be made to fit! Trade-offs in distributed ledger technology designs. In: Proceedings of the 52nd Hawaii international conference on system sciences
28. Law Commission (2020) Smart contracts. [Online] Available at: https://www.lawcom.gov.uk/project/smart-contracts/. [Accessed 19 Sept 2021]
29. Bayer D, Haber S, Stornetta WS (1992) Improving the efficiency and reliability of digital timestamping. In: Capocelli R, De Santis A, Vaccaro U (eds) Sequences II. Springer, New York
30. Natarajan H, Krause S, Gradstein H (2017) Distributed ledger technology and blockchain. World Bank Group
31. Pinna A, Ruttenberg W (2016) Distributed ledger technologies in securities post-trading revolution or evolution?. ECB Occasional Paper No. 172. Available at: https://www.ecb.europa.eu/pub/pdf/scpops/ecbop172.en.pdf
32. Rozario AM, Thomas C (2019) Reengineering the audit with blockchain and smart contracts. J Emerg Technol Account 16(1):21–35
33. Hewa TM, Hu Y, Liyanage M, Kanhare S, Ylianttila M (2021) Survey on blockchain based smart contracts: technical aspects and future research. IEEE Access
34. Schulz KA, Gstrein OJ, Zwitter AJ (2020) Exploring the governance and implementation of sustainable development initiatives through blockchain technology. Futures 122:102611
35. Peters GW, Panayi E (2016) Understanding modern banking ledgers through blockchain technologies: future of transaction processing and smart contracts on the internet of money. In: Banking beyond banks and money. Springer, Cham, pp 239–278
36. Alharby M, Aldweesh A, van Moorsel A (2018) Blockchain-based smart contracts: A systematic mapping study of academic research (2018). In: 2018 International conference on cloud computing, big data and blockchain (ICCBB). IEEE, pp 1–6
37. Chowdhury MJM, Ferdous MS, Biswas K, Chowdhury N, Kayes ASM, Alazab M, Watters P (2019) A comparative analysis of distributed ledger technology platforms. IEEE Access 7:167930–167943
38. Kannengießer N, Lins S, Dehling T, Sunyaev A (2020) Trade-offs between distributed ledger technology characteristics. ACM Comput Surv (CSUR) 53(2):1–37
39. Rauchs M (2022) Ep. 71 – DLT Conceptual Framework - Insureblocks. [Online] Available at: https://insureblocks.com/ep-71-dlt-conceptualframework/. [Accessed 21 Mar 2022]

40. Cong LW, He Z (2018) Blockchain disruption and smart contracts. NBER working paper series. Working paper 24399. Available at: http://www.nber.org/papers/w24399.pdf
41. Ølnes S, Ubacht J, Janssen M (2017) Blockchain in government: Benefits and implications of distributed ledger technology for information sharing. Gov Inf Q 34:355–364
42. Okada H, Yamasaki S, Bracamonte V (2017) Proposed classification of blockchains based on authority and incentive dimensions. In: 2017 19th international conference on advanced communication technology (icact). IEEE, pp 593–597
43. Badr NG (2019) Blockchain or distributed ledger technology what is in it for the healthcare industry? In: KMIS, pp 277–284
44. Kuo TT, Kim HE, Ohno-Machado L (2017) Blockchain distributed ledger technologies for biomedical and health care applications. J Am Med Inform Assoc 24(6):1211–1220
45. Janowicz K, Regalia B, Hitzler P, Mai G, Delbecque S, Fröhlich M, Martinent P, Lazarus T (2018) On the prospects of blockchain and distributed ledger technologies for open science and academic publishing. Semant web 9(5):545–555
46. Wang S, Ouyang L, Yuan Y, Ni X, Han X, Wang FY (2019) Blockchain—enabled smart contracts: architecture, applications, and future trends. IEEE Trans Syst Man Cybern Syst 49(11):2266–2277
47. Rauchs M, Glidden A, Gordon B, Pieters GC, Recanatini M, Rostand F, Vagneur K, Zhang BZ (2018) Distributed ledger technology systems: a conceptual framework. Available at SSRN 3230013
48. Deshpande A, Stewart K, Lepetit L, Gunashekar S (2017) Distributed ledger technologies/blockchain: challenges, opportunities and the prospects for standards. Overview Rep Brit Stand Inst (BSI) 40:40
49. Benedict G (2019) Challenges of DLT-enabled scalable governance and the role of standards. J ICT Standard 195–208
50. Ethereum (2021) Non-fungible tokens (NFT). [Online] Available at: https://ethereum.org/en/nft/ [Accessed 12 09 2021]
51. Leshner R, Hayes G (2019) Introduction. [Online]. Available at: https://compound.finance/documents/Compound.Whitepaper.pdf. [Accessed 19 Sept 2021]
52. Stellar (2021) Intro to stellar. [Online] Available at: https://www.stellar.org/learn/intro-to-stellar. [Accessed 19 Sept 2021]
53. Roy I (2020) Blockchain Development for Finance Projects. Packt Publishing, s.l.
54. FATF (2021) Opportunities and challenges of new technologies for AML/CFT, s.l.: FATF
55. Consensys (2021) CODEFI COMPLIANCE: AML-CFT compliance for ethereum—Powered digital assets. [Online]. Available at: https://consensys.net/codefi/compliance/. [Accessed 22 Aug 2021]
56. Quzmar A, Qatawneh M, Al-Maaitah S (2021) Reducing counterfeit drugs with blockchains: A survey. s.l., 2021 Int Conf Inf Technol (ICIT), pp 143–148
57. Wilson T (2021) British hospitals use blockchain to track COVID-19 vaccines. [Online] Available at: https://www.reuters.com/article/uk-health-coronavirus- blockchain-idUSKBN29O0RW. [Accessed 11 Sept 2021]
58. Ricci L, Maesa DDF, Favenza A, Ferro E (2021) Blockchains for COVID-19 contact tracing and vaccine support: a systematic review. IEEE Access 9:37936–37950
59. Hewett N, van Gogh M, Palinczki L (2020) Inclusive deployment of blockchain for supply chains: Part 6–A framework for blockchain interoperability. In: Geneva, Switzerland: world economic forum
60. Warren S, Wolff C, Hewett N (2019) Inclusive deployment of blockchain for supply chains: Part 1—Introduction. World Economic Forum, Geneva
61. Dong N, Fu J (2021) Development path of smart agriculture based on blockchain. s.l., In: 2021 IEEE Asia-pacific conference on image processing, electronics and computers (IPEC), pp 208–211
62. ACT-IAC (2021) Blockchain playbook. [Online] Available at: https://blockchain-working-group.github.io/blockchain-playbook [Accessed 12 10 2021]
63. PWC (2016) Blockchain: key questions for your business. PWC, s.l.

64. Knott N (2019) Is your business ready for blockchain? [Online] Available at: https://bankingblog.accenture.com/does-your-fs-business-need-blockchain-how-to-get-started. [Accessed 13 Oct 2021]
65. Mpinyuri EB (2019) Beyond cryptocurrencies: financial applications of blockchain technology, University of Johannesburg, s.l.
66. Welfare A (2019) *Commercializing Blockchain.* s.l.: Wiley
67. Koteska B, Karafiloski E, Mishev A (2017) Blockchain implementation quality challenges: a literature review. Belgrade, SQAMIA 2017: 6th workshop of software quality, analysis, monitoring, improvement, and applications
68. Deloitte (2019) Business blockchains, s.l.: Deloitte
69. Byström H (2019) Blockchains, real-time accounting, and the future of credit risk modeling. Ledger 4
70. Fox MB, Glosten LR, Greene EF, Guan SS (2021) Distributed ledger technology and the securities markets of the future: a stakeholder survey. Columbia Bus Law Rev 2021(2)
71. Tarr JA (2018) Distributed ledger technology, blockchain and insurance: opportunities, risks and challenges. Insur Law J 29(3):254–268
72. Farahani B, Firouzi F, Luecking M (2021) The convergence of IoT and distributed ledger technologies (DLT): Opportunities, challenges, and solutions. J Netw Comput Appl 177:102936
73. McCorry P, Shahandashti SF, Hao F (2017) A smart contract for boardroom voting with maximum voter privacy. In: International conference on financial cryptography and data security. Springer, Cham, pp 357–375