Department of Advanced Research in Technology,
MetaSapiens.tech (DARATM)

Author: Girish Bansode,
Co-founder and CTO,
Metasapiens.tech
Email: Girish@tradixnetwork.com

Blockchain-Based Smart Contracts: Opportunities and Challenges for Automating Legal Agreement

ABSTRACT

In recent years, the rapid development of blockchain technology and cryptocurrencies has influenced the financial industry by creating a new crypto-economy. Then, next-generation decentralized applications without involving a trusted third-party have emerged thanks to the appearance of smart contracts, which are computer protocols designed to facilitate, verify, and enforce automatically the negotiation and agreement among multiple untrustworthy parties. Despite the bright side of smart contracts, several concerns continue to undermine their adoption, such as security threats, vulnerabilities, and legal issues. In this paper, we present a comprehensive survey of blockchain-enabled smart contracts from both technical and usage points of view. To do so, we present a taxonomy of existing blockchain enabled smart contract solutions, categorize the included research papers, and discuss the existing smart contract-based studies.

1. INTRODUCTION

For more than a decade, the blockchain is established as a technology where a distributed database records all the transactions that have happened in a peer-topeer network. It is regarded as a distributed computing paradigm that successfully overcomes the issue related to the trust of a centralized party. Thus, in a blockchain network, several nodes collaborate among them to secure and maintain a set of shared transaction records in a distributed way without relying on any trusted party.

In 2008, Satoshi Nakamoto introduced Bitcoin [69] that was the first proposed cryptocurrency introducing the blockchain as a distributed infrastructural technology. It allowed users to transfer securely crypto-currencies, known as "bitcoins" without a centralized regulator. Besides, Ethereum [16], NXT [71], and Hyperledger Fabric [4] were also proposed as blockchain-based systems used for the cryptocurrency. Unlike Bitcoin, they can use smart contracts (SC). Blockchain technology overlaps traditional contracts by including the terms of agreements between two or more parties, but surpasses them thanks to smart contracts by automating the execution of agreements in a distributed environment when conditions are met. Smart contracts are executable codes that run on top of the blockchain to facilitate, execute, and enforce an agreement between untrustworthy parties without the involvement of a trusted third-party [16]. Smart contracts gave network automation and the ability to convert paper contracts into digital contracts.

Compared to traditional contracts, smart contracts enabled users to codify their agreements and trust relations by providing automated transactions without the supervision of a central authority [89]. In order to prevent contract tampering, smart contracts are copied to each node of the blockchain network. By enabling the execution of the operations by computers and services provided by blockchain platforms, human error could be reduced to avoid disputes regarding such contracts. Although smart contracts have made progress in recent years, they still face many challenges. For instance, one infamous malicious attack took place in 2016 when the Decentralized Autonomous Organization (DAO) smart contract was manipulated to steal around 2 million Ether 1(50 million USD on the time) because of its reentrancy vulnerability [103]. In addition to the vulnerability problem, smart contracts face several challenges including privacy, legal, and performance issues.

To understand current topics on smart contracts, we conduct a comprehensive survey, with the aim of better identifying and mapping research areas that need further studies. The focus of this survey is studying smart contracts from the technical point of view (e.g., codifying, security, performance issues) and the usage point of view (e.g., smart contract applications in finance, healthcare, etc). The major contributions of this paper are summarized as follows:

1.1.1. We propose a taxonomy of studies based on blockchain enabled smart contracts including two categories, namely SC improvement and SC usage.

1.1.2. We categorize 200 papers that we have extracted from different digital databases and discuss the existing smart contract-based studies.

1.1.3. Based on the findings from the survey, we identify a set of smart contract challenges and open issues that need to be addressed in future studies. Therefore, this survey provides a helpful reference to the researchers who want to target smart contract improvement or usage in their future studies.

1.1.4. Finally, we discuss future trends of smart contracts and explain how they provide better solutions to the open research challenges. Considering the above contributions, the remainder of this paper is structured as follows. Section 2 discusses background information about blockchain and smart contracts technologies. Section 3 discusses existing reviews studying smart contract-based approaches. Section 4 describes the adopted survey methodology and the solution taxonomy used to categorize existing smart contract-based solutions. In Sections 5–8, we present existing advances in modelling-driven smart contract improvement, optimization-driven smart contract improvement, resource-driven smart contract usage, and cross-organizational collaboration-driven smart contract usage. Section 9 discusses the study results by introducing challenges and future trends in the studied field. Finally, Section 10 concludes the paper.

2. Literature Survey

The Bitcoin whitepaper (Nakamoto, 2008) was published in 2008, and the related blockchain was started in 2009. Since then, blockchain technology has continued to show several advantages (e.g., decentralization, trust, immutability, transparency Golosova and Romanovs, 2018) and different areas of applicability. One of the most relevant applications of blockchain is smart contracts (i.e., self-executing contracts containing the terms of the agreement between the parts). Smart contracts allow trusted transactions and agreements to be carried out among different anonymous parties.

The result of a smart contract execution on the nodes of a blockchain corresponds to a change of status in the blockchain itself. Such a change of status is triggered by a transaction posted to the blockchain. Transactions are aggregated in blocks, and nodes must reach a consensus to add a new block to the blockchain. In particular, due to the absence of a central authority, blockchain technologies make use of consensus algorithms to validate and verify the transactions. To reach such consensus, well-known algorithms are typically used (e.g., the Proof of Work and the Proof of Stake algorithms Bach et al., 2018).

Blockchain applications and smart contracts can be used in various fields: from insurance refunds to financial transactions, from corporate operations to the traceability of goods and the protection of intellectual property. Thus, the number of companies using blockchain and smart contract applications continues to grow. However, for satisfying high performance, scalability, and security requirements, blockchain applications need to be well-designed and thoroughly tested. This is especially true if we consider that smart contracts are developed through non-standard software life-cycles, in which delivered applications can hardly be updated or bugs resolved by releasing a new version of the software (Destefanis et al., 2018). In general, the development of smart contracts is very different from traditional software development, raising new problems and challenges (Marchesi et al., 2020). For instance, on the one hand, (i) developers must ensure code security for smart contracts due to the immutability of blockchain and the sensitiveness of digital information often managed, on the other hand (ii) they must pay special attention to gas consumption, as the execution of smart contracts in blockchain platforms like Ethereum is implemented through the gas mechanism (Zou et al., 2019). It should be considered that the blockchain technology requires specific constraints and characteristics of the applications that will run on it, the product lifecycle and the development software process of smart contracts and blockchain-based applications. All these changes to the software product and process must be identified and studied in order to develop a comprehensive body of knowledge of blockchain based software engineering.

Although the increasing popularity of smart contracts and the research efforts that have been posed to tackle some of these issues, the approaches proposed are still far from being consolidated. For these reasons, it urges to identify the software engineering tools, techniques, best practices, as well as testing approaches, specially designed to address the novel features introduced by decentralized programming on the blockchain (Chakraborty et al., 2018). To fill this gap and have a clearer picture of the research efforts that have been carried out to improve the implementation, the security, and the reliability of this kind of applications, in this paper we perform a systematic review of the literature concerning the software engineering tools, techniques, and practices envisioned for dealing with the peculiarities posed

by smart contracts and blockchain development. Moreover, we also try to identify possible future research directions and open issues that need to be addressed. In particular, we pose the following general research question:

What is the current state of the art in research and which are the main challenges faced in the development, testing, and quality assessment of blockchain-oriented software?

In particular, this research question aims at reviewing the specific methods, techniques, and tools proposed for improving the design, construction, testing, maintenance, and quality of smart contracts and decentralized apps. Additionally, our goal is to also identify the specific challenges of blockchain-oriented software engineering that are still open and need further research. To answer our research question, several aspects of software engineering have been considered, such as testing, security, and source code quality of blockchain-based applications.

During the life cycle of software, the testing phase is useful to verify if the software produced corresponds to the expected specifications and, above all, if it does not present bugs, errors, or other defects. Concerning software testing, we specifically analyze (i) approaches and frameworks for generating test cases (such as Zeus Kalra et al., 2018), (ii) approaches to identify code smells present in the source code (Chen et al., 2020b), and (iii) tools based on fuzz testing (such as Fuse Chan and Jiang, 2018, Contractfuzzer Jiang et al., 2018, Evmfuzz Fu et al., 2019 and ReGuard Liu et al., 2018).

Another aspect to consider in software engineering is the analysis of the source code with the aim of evaluating its quality. For this purpose, we discuss the existing solutions aimed at detecting problems in the code, (e.g., Smartcheck Tikhomirov et al., 2018, Slither Feist et al., 2019, KEVM Hildenbrandt et al., 2018). In particular, we analyze the proposed solutions to identify which of them is more useful for identifying specific problems.

Software metrics are useful measurement units for quantifying, measuring, and evaluating the different aspects of software development. Such metrics can be divided into different categories according to their use, including metrics related to software products, metrics related to software development processes, metrics related to software quality, Object-oriented metrics. We analyze the literature concerning the adoption/proposition of metrics to deal with issues specifically posed by blockchain-oriented development.

Another very important aspect is the security of the source code. Since the most popular and successful applications of smart contracts are tokens and decentralized exchanges (i.e., peer-to-peer trading of cryptocurrencies) moving money for tens of billions of dollars (Oliva et al., 2020), there is a need for improved security practices. Source code might contain critical security defects or vulnerabilities, which, if exploited, in the case of blockchains, smart contracts, and virtual currencies, can lead to financial losses. Thus, we consider both techniques and tools aimed at identifying fraudulent behaviors and security flaws in smart contracts (e.g., TEETHER Krupp and Rossow, 2018, MAIAN Nikolić et al., 2018, Oyente Luu et al., 2016). We also discuss solutions aimed at measuring Dapp (decentralized application) performance. In particular, benchmarks for performing such evaluations are analyzed. In addition, to better understand the specific applications that use the blockchain beyond cryptocurrency, we also consider the Dapps, which have been created by developers for being used in a plethora of different scenarios (e.g., social platforms, casino, and financial exchange, etc.). In particular, analyzing such applications, we are interested in better comprehending which specific problems are addressed through the adoption of the blockchain technology.

Results of our literature review highlight that most of the techniques investigated and tools/frameworks implemented have a focus on the Ethereum platform, with few exceptions as Bitcoin and Hyperledger. However, many of these techniques and tools only deal with specific aspects and issues of blockchain-oriented software engineering. For these reasons, further research is needed for more comprehensively targeting the different constraints and challenges posed by blockchain-based software development, testing, and quality assessment.

In summary, the contribution of the current paper is twofold:

we provide the community with a common knowledge base enumerating the approaches for improving smart contract and blockchain application development that have been proposed so far; and we identify the specific blockchain software engineering challenges that are still open and need further research.

Paper structure. The paper is organized as follows. Section 2 compares existing literature review in the field of blockchain and our proposal regarding software engineering. Section 3 presents the research methodology used. Section 4 discusses the findings of our literature review, while Section 5 highlights future research directions and open issues that have emerged from the analysis of the collected papers. Section 6 deals with the main threats that could affect our findings and, finally, Section 7 concludes the paper. The interest of the research community towards issues concerning applications based on the blockchain technology is increasingly growing. Unfortunately, a literature review systematically examining the specific aspects of Software Engineering is still lacking. In fact, the literature reviews realized till now regards mainly the application of the blockchain technology to specific domains such as security, biomedical, intellectual property. Among the topics covered in the identified literature

Research methodology: Our systematic literature review on blockchain based Software Engineering has been carried out following the guidelines of Kitchenham and Charters (2007). In this section we will introduce how the examined papers have been selected, prepared for the analysis and an overview of the produced research (who are the main authors, how the papers are distributed over time and on the types of publication).

Results: The different studies have been classified into six categories. The first four concern smart contracts and consider the aspects of testing, security, analysis and metrics relating to the source code. The rest concerns Dapps and blockchain applications. Table 1 reports the distribution of analyzed articles by year, while in Table 2 the considered papers are divided by publication types. Based on the 96 papers considered, Table 3 indicates the 10 authors who authored (or co-authored) the largest

Discussion: By analyzing the current literature on blockchain-oriented software engineering, it emerges that most of the research focuses on the Ethereum platform with a few exceptions as Bitcoin and Hyperledger. Consequently, while there is a large convergence of results concerning this specific platform, replications and new studies on the other platforms are necessary for generalizing the results.

3. Motivation

Every new innovation is the result of an attempt to solve a problem. Blockchain technology is no exception. It's quite evident after learning about the evolution of blockchain technology that it arose because of a need to address the inevitability of uncertainty in the existing economy.

Uncertainty could never be eliminated, but only lowered: there have always been institutions that have acted as third-party lawmakers to lower uncertainty, or lack of trust, whenever there was a need for an agreement between parties. A typical example would be buying an item on eBay. You would always need as much certainty as possible about the trade. One party expects fair goods, and the other expects agreed money. Now, though the buyer and seller have no reason to trust each other, they complete their trade as they trust the third party, which is eBay, who assures them both of a legitimate trade. Again, there was a need to trust these "medium" institutions. Trusting an institution requires a lot of research and knowledge. Blockchain promised to overcome these issues by implementing applications in a decentralized and secure way, assuring some level of certainty. This was one of the main reasons behind the widespread adoption of blockchain in a trustless society.

We know that blockchain is an ideal technology for implementation in trustless environments. However, the blockchain alone is not responsible for the success of the complete implementation. It's assisted by several other protocols that make it the robust and resilient technology it is. Blockchain can be implemented in trustless networks mainly due to the decentralization of computation in dense P2P networks and the maintenance of a secure and publicly distributed ledger that gives complete transparency over the entire blockchain. The P2P protocol makes sure that every node holds the latest state of the blockchain.

The need for decentralization is the key motivation behind the blockchain technology, and decentralization is achieved by distributing the computation tasks to all the nodes of the blockchain network. Decentralization solves several problems of traditional systems; the single point of failure is one such problem. For example, in a centralized system such as a bank, the user would always communicate with the same third-party bank to fetch their account details. This downtime is something that's inevitable, even in perfectly architected servers. If the same scenario was faced in a decentralized network, it wouldn't be an issue, because all the transaction data would be distributed across all the nodes, meaning that each node can act as a backup node in case of failure, maintaining the integrity of the data (another key benefit of blockchain-based solutions). This is something that's achieved by maintaining a distributed ledger of blockchain data. Blockchain immutability, which is a key factor in trusting the integrity of the blockchain, ensures the integrity of the ledger, which is publicly accessible to all nodes.

4.Problem Definition

Scalability: A long blockchain can produce challenges for an organization as it runs into trouble with scalability. There are several factors at play here.

First, each computer on the network working to confirm transactions and keep accurate records of the blockchain must store data starting from the genesis block to the most recent block. These computers -- called nodes -- must have the capacity to store that data. The redundancy creates a more secure system, but it also becomes increasingly inefficient as the network and blockchain grow. Next, when creating a new block on the blockchain, the node that confirms the transactions must broadcast the new block to every other node on the network. They can then verify the transactions and add the block to the blockchain. This can use substantial network resources as the network grows in size.

In big public blockchains such as Bitcoin (CRYPTO:BTC) and Ethereum (CRYPTO:ETH), the scaling issue can translate into nodes demanding higher transaction fees to process transactions on the blockchain. They need to see an adequate return on their investment into computing resources. Energy consumption: Blockchains that use a proof-of-work system to determine which node wins the right to confirm the next block in the chain can become extremely energy-intensive. Both Bitcoin and Ethereum use the proof-of-work model where nodes compete to solve a complex equation fastest. As the network grows, the number of competitors increases, and there's a fight for more computer power, which consumes energy. The energy consumption is extremely inefficient because ultimately just one node will win the right to confirm the next block.

The proof-of-stake model is held up as a solution to the energy consumption problem faced by blockchains. However, such a system poses challenges in itself. For one, the code required to put together a good proof-of-stake system is much more complex than a proof-of-work system. That can lead to more bugs and vulnerabilities. Second, it may be easier for a single party to take control of a majority of the staked cryptocurrency, allowing it to exercise too much control over the blockchain. The latter vulnerability is less likely in a proof-of-work model since a single party would need to obtain a majority of computer power on the network. Additional computer power could be obtained by other parties to wrest away control and ensure that the blockchain remains decentralized. Despite those drawbacks, Ethereum is migrating from a proof-of-work model to a proof-of-stake model.

4.1: Speed: Blockchain transactions are relatively fast for account-to-account transfers, but the decentralized nature of blockchain can make it a poor tool for everyday transactions. When you swipe your debit or credit card at a store, you can confirm the transaction in a matter of seconds. Behind the scenes, a network of payment processors works to move money from your account to the merchant's account, but the whole process can actually take a day or two. In the meantime, the merchant can trust that the issuing bank of the payment card will make good on the payment. This trust allows payment card networks to process thousands of transactions per second. Since a blockchain like Bitcoin's is fully decentralized, there are no guarantees on a transaction until it's confirmed on the blockchain. That can take a long time since the Bitcoin blockchain can only process a handful of transactions per second. A

merchant might not know whether a transaction really went through for an hour. That makes it impractical for most retail transactions even if there are plenty of useful blockchain applications in the financial sector.

No universal standards: Almost every implementation of blockchain technology is unique. That creates a couple of challenges for businesses and developers working on various applications. First, it makes interoperability between blockchains difficult. If one company wants to share data with another company's blockchain, they'll likely need to develop additional tools to allow data to flow between the two blockchains. There are dozens of blockchain interoperability solutions already in use, but the fact that no one solution fits all highlights the fragmented standards of blockchain implementations. The second challenge comes about when developers create something on a blockchain (for example, a smart contract or a decentralized finance app). Since there are no universal standards, a developer will have to rework everything to offer the same product on another blockchain. The lack of standards may also open up vulnerabilities in code as developers work with less familiar platforms.

4.2: Privacy: Blockchain was designed to be publicly distributed. That means anyone can see the data written to the blockchain. Although the information is anonymized using blockchain wallet addresses as identifiers, the other details of a transaction are plain to see. Nobody's going to care about the $20 worth of Bitcoin you send to a friend, but some data and transactions require a greater level of privacy. A private blockchain is one way for a business to implement blockchain technology without fear of leaking any information to the public, but it has its disadvantages. Since a private blockchain has an authority that delegates who can and cannot participate, it's not truly decentralized. That can reduce trust from the public in a blockchain-based product.

5. Scope of the project

This is not the full potential of the blockchain and smart contracts, though. These boundaries can be pushed. The transactions can be deeper than just logic-based.

5.1. Sophisticated smart contracting

Smart contracts can be smarter. The code has the potential to offer more. The basic logic that it offers now could be slowly transformed into something much more complex. It could be used in negotiations to reduce time-spend. The contract could stipulate that if a vendor offers a product at a specific price, then another price could be offered based on that vendor price. This could be extended to many more factors than price, including indemnity, fallback clauses, and other various redlines and markups. In short, the blockchain is programmable and rules can be built into it that execute under data-based conditions. This removes the need for advisors, consultants, and lawyers and enables companies to hastily make their way through negotiations in a much more pain-free way.

5.2. The creation of digital trust in procurement

The central issue that blockchain addresses is trust. It creates it without the need for an intermediary. Due to the inherent lack of trust in business transactions, when a house is being sold or bought, proof needs to be provided that the buyer and seller are who they say they are, the house is what it has been represented as, the seller owns the house, and the buyer has the means to purchase the house. These processes that are traditionally very lengthy, can be sped up with the blockchain and remove the necessity for a trusted intermediary. And this concept can be extended far beyond real estate, reaching into supply and value chains.

5.3. The ability to build on top of data

Historically, databases have logged transactions. And they have been good at it. They are even better at it than the first generation of blockchain—it was slow, did not have effective query support, and had a low throughput, among other issues. Once blockchain was advanced, it could keep up with databases. This, combined with the fact that it has an immutable audit trail and cannot be altered by a single individual, makes it more trustworthy than traditional databases can be. Because of the confidence that businesses and individuals can have the data in the blockchain, it can be built on to help optimise business systems and processes.

For example, many paper-based business processes could be streamlined. Instead of paying with checks, B2B businesses could implement blockchain options. Another example directly in the supply chain is harnessing the technology to allow members of a supply chain to easily and safely exchange documents, track shipments, and oversee import and export paperwork.

5.4. Strengthening the platform economy

The platform economy is growing. Apps like southeast Asia's Grab are putting more power and freedom into the hands of consumers. Blockchain could add to this platform economy. It could be integrated into these applications in order to help identify openings and surpluses in order to match consumers to these offerings.

5.5. The enhancement of regulation

Currently, much of the discussion around blockchain is that governments are trying to find effective ways to regulate the processes that it accomplishes. In the near future, however, this conversation will change into how the government will harness blockchain to regulate. Smart contracts will be the instrument that governments around the world use to implement everything from laws and regulations to directives and treaties. In the end, this will lower the cost of compliance for individuals and businesses, as well as making it much more effortless. It will also lower the cost and burden of oversight.

5.6. A cleaner supply chain

Supply chains have a tendency to get messy. It can be nearly impossible for retailers to know exactly how their product was sourced. They can not guarantee that slave labour was not used. They cannot be sure that detriment to the environment did not occur. They can not make a promise that the raw materials in the product were conflict free. Blockchain has the potential to change this. Every transaction and exchange within the supply change could be stored and recorded. This type of traceability empowers businesses to be more responsible, as well as making it easier to be ethical. This type of real-time traceability is especially lucrative for industries that have strict regulations, such as the pharmaceutical and food and beverage sectors. Additionally, counterfeit products would become obsolete under a blockchain-enhanced supply chain.

5.7. Better machine-to-machine cooperation in procurement

Because the data in blockchain can be fully trusted, offers additional data collection opportunities, and allows smart contracts to execute programs, this creates a distributed system where machines can fully trust each other. This means that more and more automation can happen with less and less risk, whether that be corrupted data, latency due to intermediaries, or poor execution. In the future, IoT will be utilising this benefit, especially in the supply chain. For example, IoT could track product movements in real-time. If something goes wrong or is not on time, an immediate investigation can be launched. During the whole process, though, smart contracts that are powered by blockchain can use automation to execute various actions and all supply chain activity can be permanently and immutably recorded. This could be extended to everything from product requisitioning and ordering to inventory tracking and management. It can all be automated and operate consistently.

5.8. Better human-to-human cooperation in procurement

Human-to-human cooperation is no different to machine-to-machine cooperation in that it needs trust. This can become a problem in supply chains. Not all of the partners know each others' identity or reputation. Blockchain fixes this. It guarantees that users are who they say they are. In the future, this will likely look like a digital resume on the blockchain. It will allow business partners to fully trust each others' credentials.

To dive more deeply into reputation, though, blockchain will offer immutable reputations. They will be based on an individual's or business' history of transactions. As the blockchain expands, this reputation will become more and more reliable. In the end, this can significantly lower the risk of working with new partners. Instead of spending more money to work with a select few suppliers that a business trusts, they can start extending their reach and working with new partners that offer lower prices.

5.9. Audits will happen

In the past, bugs and glitches came part and parcel with software. With blockchain, this can not happen. Smart contracts represent capital. If there is a bug or problem with the system, this could lead to businesses losing large sums of money. Therefore, many organizations, in order to fully trust blockchain and smart contracts, will require security audits.

5.10. Predictions in supply

One of the issues that supply chains face on a continuous basis is all of the unknowns that can happen. There can be a shortage of materials. There can be drops in demand. Blockchain could be used to predict these events. These decentralised predictions would be objective and based on past events. When this happens, release dates could be more precisely estimated, hedging could be more accurate, and automation of payments could be tied to the probability of an event occurring.

6. Existing System

A key concern in the supply chain and logistics sector is the lack of communication and transparency due to the plethora of logistics companies within the industry. Furthermore, data is skewed or manipulated as every logistics company uses their own terms, making it hard for non-specialists.

A joint study by Accenture and DHL found that more than 500,000 shipping companies in the US alone are causing data siloing and transparency issues. The report says blockchain can solve many problems plaguing supply chain and logistics management. The research argues that because blockchain enables data transparency by indicating a single source of verifiability, it can build greater trust within the sector. Blockchain applications have the bonus of making the logistics process leaner and automated, saving the sector billions of dollars a year. Supply chain blockchain applications will reimagine how the supply chain sector and all those who function within it will work.

6.1. Healthcare blockchain applications

Though early in its adoption, blockchain in healthcare is already showing some promise. Early blockchain solutions have demonstrated the potential to reduce healthcare costs, improve access to information across stakeholders, and streamline business workflows. An advanced ecosystem for accumulating and sharing private information could be what medical healthcare professionals need to ensure an already inflated industry trims exorbitant costs. An example is the Estonian X-Road solution that connects different information systems for various services. A blockchain network is used in the healthcare sector to preserve and exchange patient data through hospitals, diagnostic laboratories, pharmacies, doctors and nurses. Healthcare blockchain applications can accurately identify severe mistakes and can improve the performance, security and transparency of sharing medical data in the healthcare industry.

6.2. Retail & eCommerce blockchain applications

The most common blockchain technology used in e-commerce is the Ethereum virtual machine, which provides a platform for eCommerce brands to manage their blockchains. The cryptocurrency Bitcoin allows customers to make purchases on sites and apps that accept Bitcoin as payment. Because online financial transactions on the blockchain are more secure, using blockchain applications is a win-win for both brands and consumers. Furthermore, it has added advantages of cutting costs, improving business processes, making transactions faster, and improving the overall customer experience.

Because of its immutability, retail blockchain applications can ensure that manufacturers can't substitute your purchase with a cheaper product when you buy products, and retailers can't try to sell you a different, more expensive product. This also means that you can't return a 'fake' product and get a replacement. If the product is what you ordered, it will be what you received.

6.3. Finance blockchain applications

With its advantages, blockchain could have a massive impact on the financial services industry. Blockchain can make payment processes more efficient. For instance, blockchains like Polygon and Solana and sidechains like Arbitrum can settle transactions in split seconds at $0.01 or less, which is considerably cheaper when compared with Visa, Mastercard and Amex. Finance blockchain applications

like Ripple reduce costs for financial organisations and their clients and customers. Finance blockchain applications help financial institutions save on international transactions, with banks potentially saving $27 billion on cross-border transactions by 2030.

Since blockchains provide distributed, unalterable transaction records, financial institutions can use them for keeping records and bookkeeping and comply with regulatory agencies. The more immediate transaction settlements offered by finance blockchain applications can improve existing financial services. For instance, lenders will be able to fund loans faster, vendors will receive payments quicker, and stock exchanges can immediately settle securities purchases and sales.

6.4. Property & real estate blockchain applications

Exclusive real estate investments will become available as an investment opportunity for everyone. For the first time, real estate-based security tokens enable proportional ownership of a plot of land or building, increase market participation for all, and open up new financing opportunities for developers. Another factor that real estate blockchain applications can achieve is the highly efficient evaluation of property investments based on anonymous and comparable data. The parties involved in a transaction can thus save themselves from financially expensive, independent real estate valuations, as all parties can access all available data on the blockchain. The entire property history is both transparent and traceable. When buying a property and taking out a mortgage, all property buyers will find the current process tedious and labour-intensive. With several parties involved in the process, like notaries, estate agents and financial institutions, the mortgage process is highly vulnerable to human errors and thus could accrue additional costs. With the introduction of property blockchain applications, the need to rely on paper-based and individual communication is reduced, reducing costs and human errors and speeding up the process. Thanks to a leaner lending process, this removal of intermediaries benefits borrowers and financial institutions that can offer more competitive pricing and lower staff costs.

6.5. Media blockchain applications

Key concerns within the media relate to data privacy, royalty payments, and intellectual property piracy. According to research by Deloitte, the digitisation of media has caused widespread content sharing and has caused copyright infringement. Deloitte believes media blockchain applications can offer the sector a much-needed facelift regarding data rights, piracy and royalty payments.

Media blockchain applications offer the media sector the ability to avert a digital asset, like an mp3 file, from duplicating in multiple locations. It can be shared and distributed whilst preserving ownership, making piracy virtually impossible through a transparent blockchain ledger system. Additionally, media blockchain applications maintain data integrity, allowing advertising agencies to target the right customer demographics and musicians to receive appropriate royalties for their original works.

6.6. NFT marketplace blockchain applications

Non-Fungible Tokens (NFTs) have been the hottest blockchain application since the early years of cryptocurrencies. Recent years have brought a rise in these digital items that are currently taking the

world by storm. NFTs are unique (forgery resistant) tokens used to prove digital, physical or intellectual property ownership. Remember the Nyan Cat meme? That memorable GIF sold for $600,000 in Ethereum in April 2021 on an NFT marketplace. Before his digital work *The First 5000 Days*, the artist "Beeple" never sold any artwork over $100. And yet, his *The First 5000 Days* sold for an astounding $69 million! NFTs allow buyers to own digital moments, art, and culture that will outlive us all.

6.7. Heavy industry & manufacturing blockchain applications

As factories worldwide become increasingly interconnected, the influence of blockchain is becoming more prevalent. The factory of the future spans a whole network of machines, parts, products and value chain participants, including machinery providers and logistics companies. Now, more than ever, manufacturers and heavy industry face sharing data concerns securely internally and externally of factory walls. Equipped with detailed data that understands the challenges and opportunities they face, manufacturers can then choose the most appropriate option from technology solutions. Manufacturing blockchain applications can scale transparency and trust through all stages of the industrial value chain, from sourcing raw materials to producing the finished product ready for supply chains. Furthermore, manufacturing blockchain applications can eradicate counterfeit production, engineer high complexity products, identify management, asset tracking, quality assurance and regulatory compliance.

6.8. Music blockchain applications

Music blockchain applications will save the music industry billions by revolutionising the rights and royalties process, ensuring that writers, artists, publishers, and everyone associated with the industry are rewarded appropriately. Adding music blockchain applications across the music industry would streamline the management of royalties and rights with a unique version of the artist's work, regardless of location and ownership rights - ensuring musicians are paid the correct amount more quickly. Ultimately, this will save the music industry billions in lost revenues, delayed payments and legal costs. But for this to happen, the music sector must come together to determine a common practice and place trust in each other and the blockchain technology.

6.9. Cross-border payments blockchain applications

Pioneered by the world's first-ever cryptocurrency, Bitcoin, money transfer apps have exploded in popularity. Cross-border payment blockchain applications are proving extremely popular in fintech for the reduced fees and speed it can help individual consumers and newer businesses. For instance, money transfer blockchain applications can save the most significant banks $8-$12 billion a year by eliminating bureaucratic red tape, making digital ledger systems in real-time, and reducing third-party fees.

6.10. Internet of Things blockchain applications

The Internet of Things (IoT) is an obvious location for new IoT blockchain applications. IoT devices have millions of applications open to security and hacking concerns. An increase in IoT products means

more opportunities for hackers to steal your data or make you a victim of fraud or scams on everything from smart home devices to online passwords. IoT Blockchain applications will add a higher level of security by preventing data breaches by utilising transparency and virtual incorruptibility of the blockchain technology.

6.11. Gaming blockchain applications

Just as in an online Role-Playing Video (RPG) game like World of Warcraft, World of Freight or Fortnite, there are facets within the game that are familiar, special, unique, epic, and *legendary*. The legendary items are the rarest. In gaming blockchain applications and blockchain-based games, you can determine how many legendary items are available in the game, such as 25. After this amount has been reached, there can be no more legendary items of this type. Even if these 25 items are identical, each unique item is remarkable since it will include the entire records of how that item has been used. The game's best player might have owned it, and this knowledge will always remain with the item, even if someone else purchases it from them. But what if the game you're playing stops working? Well, your item, on the other hand, will not stop working. This is because it can be transferred from one blockchain to another in the metaverse - the item is a non-fungible token and can be used in a new game. You need to store it in a cryptocurrency wallet. NFTs are a type of content that can live on in the metaverse forever.

6.12. Personal identity security blockchain applications

Data from LifeLock and identity theft experts show that more than 16 million Americans complained of identity fraud and theft alone, with an identity being stolen every two seconds! Deception on this scale can occur via forged documents to hacking into personal files. Governments who use personal identity security blockchain applications could see a massive drop in identity theft by keeping birth certificates, birth dates, and social security numbers; in fact, any sensitive information on a decentralised blockchain ledger.

6.13. Voting & government blockchain applications

Government blockchain applications can improve local political engagement, improve bureaucratic efficiency and accountability, and reduce massive financial burdens. Like Illinois, some state governments in the USA are already using the technology to secure government documents. Government Blockchain applications have the prospect of cutting millions of hours of bureaucracy each year, holding public officials accountable through smart contracts and digital ledgers providing absolute transparency and producing public records, according to the New York Times. Voting Blockchain applications could also revolutionise electoral processes. Blockchain-based voting could improve civic engagement and reduce voter apathy by providing a level of security and incorruptibility that allows voting to be done on mobile devices.

6.14. Anti-money laundering blockchain applications

Anti-money laundering blockchain applications possess inherent characteristics that can potentially prevent money laundering. Every transaction done over blockchain leaves behind a permanent trail of unalterable records. Thus, it makes it easier for authorities to track the source of the money's origin. A public blockchain ledger can supervise, validate, and record each transaction's complete history. If all the transaction phases, including destination wallet, departure wallet, currency type and amount, are left unverified, the transaction gets immediately blocked. Blockchain also enables money laundering risk analysis and reporting mechanisms. It allows overall system analysis rather than monitoring just entry and exit points.

6.15. Advertising blockchain applications

Advertising blockchain applications are a distributed digital ledger technology that promotes decentralisation and provides the ultimate security, traceability and transparency.

Once a digital record is stored on the blockchain, it is unchangeable, meaning that those with access can view the transactions but can't modify them. Since a blockchain records information and transactions in real-time, advertisers can leverage it to keep track of ad spending. Ultimately, this can provide the transparency that current methods can't replicate. Transparency isn't the only benefit. Speed is vital in advertising. It's complicated to follow inventory and ensure high-quality merchandise. Blockchain technology can keep up with the pace.

6.16. Content creation blockchain applications

6.16.1. Whilst there are some incredibly successful Instagrammers, YouTubers, TikTokers and Facebook streamers reaping the rewards of social media fame, many content creators struggle to make ends meet. This is because many challenges are involved in this industry. Such challenges centre around the following issues:

6.16.2. Plagiarism: Content creators often spend an astonishing amount of time on a project only for it to be stolen or replicated by someone else.

6.16.3. Intermediaries: Whilst digital platforms offer content creators the opportunity to earn money from advertisers for their efforts, the media platform they post on will significantly cut their profits. For instance, Facebook's Watch feature consumes around 45 per cent of all revenue. The industry is currently structured to favour the platform or intermediary instead of the creators. Creators only receive a small portion of the profit a piece of content generates, or creators need to have a considerable following to see any actual monetary returns. To solve the current challenges of content creation and create a fairer and more rewarding ecosystem, blockchain technology may be the answer to enrich and empower artists through its content sharing social media ecosystem.

6.17. Automotive blockchain applications

For those working in car sales and manufacturing, a lack of operational transparency is a daily struggle. By implementing automotive blockchain applications for payments, the industry can create a unified platform to quickly track down and pay for vehicle parts, services and manufactured vehicles. Compared

to traditional paper-based systems and digital web2 databases, automotive blockchain applications are immune to accidental data loss, human error or deletion. The popularity of ridesharing and carsharing services has increased as car ownership has become more expensive than sharing one. But what matters here is using blockchain technology to process automation and prevent fraud. Fraud is the biggest challenge for both providers and recipients of automotive services. With smart contracts, blockchain technology can help all parties create binding financial agreements that they will execute with a guarantee after all agreement conditions are satisfied.

6.18. Smart contracts blockchain applications

Smart contracts are like regular contracts, except the contract rules are enforced in real-time on a blockchain without ambiguity, eliminating the middleman and adding accountability for all parties involved in a way not possible with traditional agreements. This saves businesses time and money while ensuring compliance from everyone involved. Blockchain-based contracts are becoming more and more popular as sectors like government, healthcare, and the real estate industry discover the benefits.

7. Proposed System (System Architecture)

7.1. Proposed System Architecture

In this section, we discuss our proposed architecture based on blockchain for a tamper-proof cloud-based EHR management system. The architecture is depicted in Figure 7.3. There are four key components in our proposed architecture: *user application*, *blockchain handshaker*, *cloud*, and *public blockchain network*. Each component is explained as follows:

7.2. User Application

User application is a software module that provides two functionalities. Firstly, it provides application interfaces for users. In our system, there are several types of users such as doctors, nurses, system administrators, pathologists, etc. Each type of user has different role. Hence, the user application provides specific user interfaces based on a user role. Secondly, user application builds an initial transaction(T_I) based on data inserted by a user (e.g. patient blood pressure) and some system generated data (e.g. timestamp). T_I is sent to blockchain handshaker for verification purposes. In summary, user application establishes a link between users and blockchain handshaker.

7.3. Blockchain Handshaker

Blockchain handshaker (*BH*) is the key component of our proposed architecture. This component acts as a wrapper component that connects user application, cloud-based EHR system and public blockchain network in our proposed architecture. *BH* has three sub-components, namely transaction template manager (*TTM*), transaction generator (*TG*), and transaction validator (*TV*). The internal architecture of *BH* is illustrated in Figure 3. Description of each component of *BH* is described below:

7.3.1. Transaction template manager (TTM): contains a set of predefined transaction templates for blockchain network. Transaction templates are generated by the system administrator following specifications of the blockchain network platform and set of attributes in corresponding smart contracts.

7.3.2. Transaction generator (TG): builds a blockchain transaction (T_C) from an initial transaction (T_I) following one of the templates in *TTM*. *TG* does the mapping between T_I and a suitable template in *TTM*.

7.3.3. Transaction validator (TV): is the core component of *BH* that controls the overall interactions among international blocks of *BH* and handshaking user applications, blockchain network and cloud. *TV* receives an initial transaction T_I from user application, sends it to *TG* and waits for receiving a blockchain transaction *TC* from *TG*. Upon receiving a *TC*, *TV* sends it to blockchain network for validation. The blockchain network returns validated transaction T_I . If the validation is true, *ACK* is sent as valid transaction to the cloud for storing in cloud database. Otherwise, *ACK* is sent as invalid transaction and stored for future audit tasks.

7.3.4. Public Blockchain Network

We use a public blockchain network (e.g. Ethereum) in our proposed architecture. The public blockchain network comprises blockchain nodes, distributed ledger and smart contracts. Blockchain nodes are in fact miners that are responsible for maintaining blockchain according to the consensus mechanism. In other words, blockchain nodes receives transactions and validate based on smart contracts. If a transaction is found as valid, data are converted to blocks and added in the distributed ledger. Public blockchain network sends an acknowledgement as true or false to the transaction validator (TV) of the blockchain handshaker.

7.3.5. Cloud

The cloud provides two services in our proposed architecture that are similar to the traditional cloud-based EHR management system. The first service includes hosting the EHR management system. The second service is the storage service. The cloud provides a database for storing all health records. EHR management system receives transactions T_I from BH, performs all tasks related to it and stores

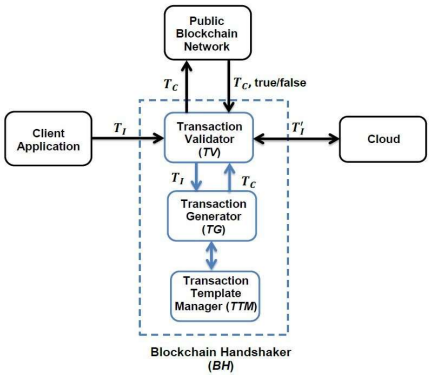

Figure 7.3: Internal Architecture of Blockchain Handshaker (BH).

transaction data in the cloud database. The cloud responds with appropriate data in response to access requests from users.

7.4. System workflow

In this section, we discuss the system workflow of our blockchain and cloud-based EHR management system. Figure 7.4 shows an overview how the system components interact with each other. Initially, user application sends an initial transaction (T_I) that contains patient health data inserted by a user. Next, T_I is sent to Blockchain Handshaker (BH) for communicating with public blockchain network. BH generates a blockchain transaction (T_C) using its internal components transaction generator (TG) and transaction template manager (TTM). Another component of BH, transaction validator (TV), sends T_C to public blockchain network for validation. Further, the public blockchain network validates transaction using smart contracts and mines to add transaction data into the blockchain. Finally, the cloud stores data in the cloud database at the end of processing.

According to our proposed architecture, each and every record related to patient health is passed to Blockchain Handshaker (*BH*) first for validation. One or multiple smart contracts are created and distributed among public blockchain nodes. Whenever a transaction is sent to the public blockchain network, transactions are validated against smart contracts anonymously. At the end of validation, data of the transaction is stored in the blockchain or distributed ledger. As the blockchain nodes are anonymous, none of them can be compromised. Proof-of-Work (PoW) consensus mechanism ensures secure mining of blocks. Hence, our proposed system architecture ensures tamper-proof data ledger. Moreover, transactions are stored in cloud database as per validation of public blockchain network.

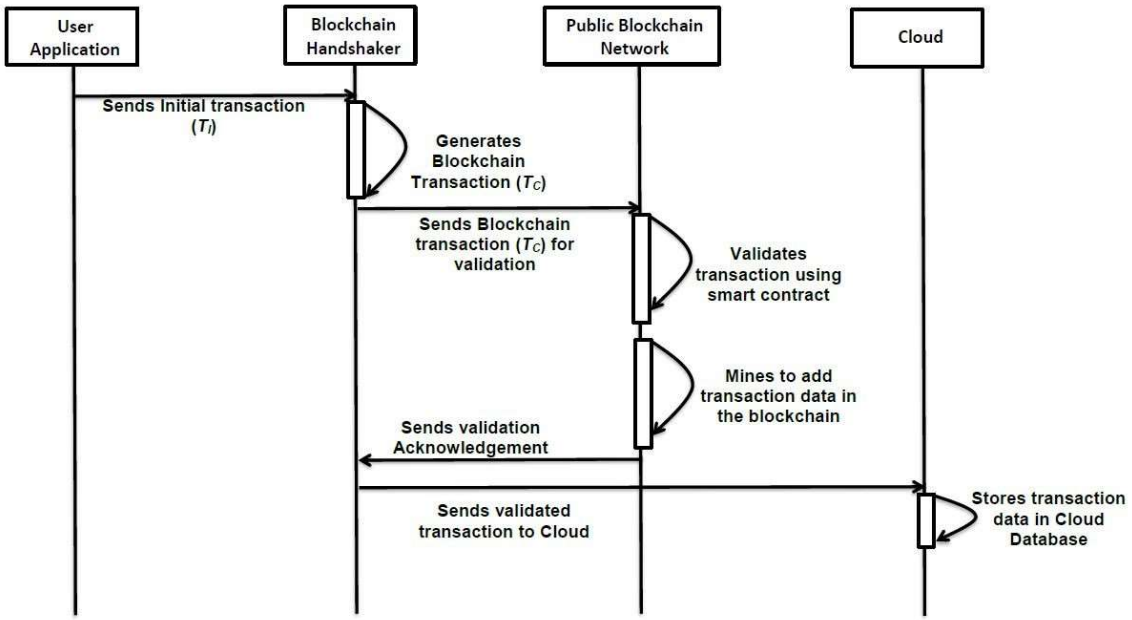

Figure 7.4: Communication Among Components of Proposed Blockchain and Cloud-based EHR Management Systems.

The usage of *ACK* along with transaction data ensures which transaction are faulty and which are not. From there, data modification can be tracked and traced. Therefore, data accountability is ensured. As the system ensures tamper-proof data storage and accountability, it can be said as immutable system.

8. Flow Diagram (UML Diagram, State Diagram ER diagram)

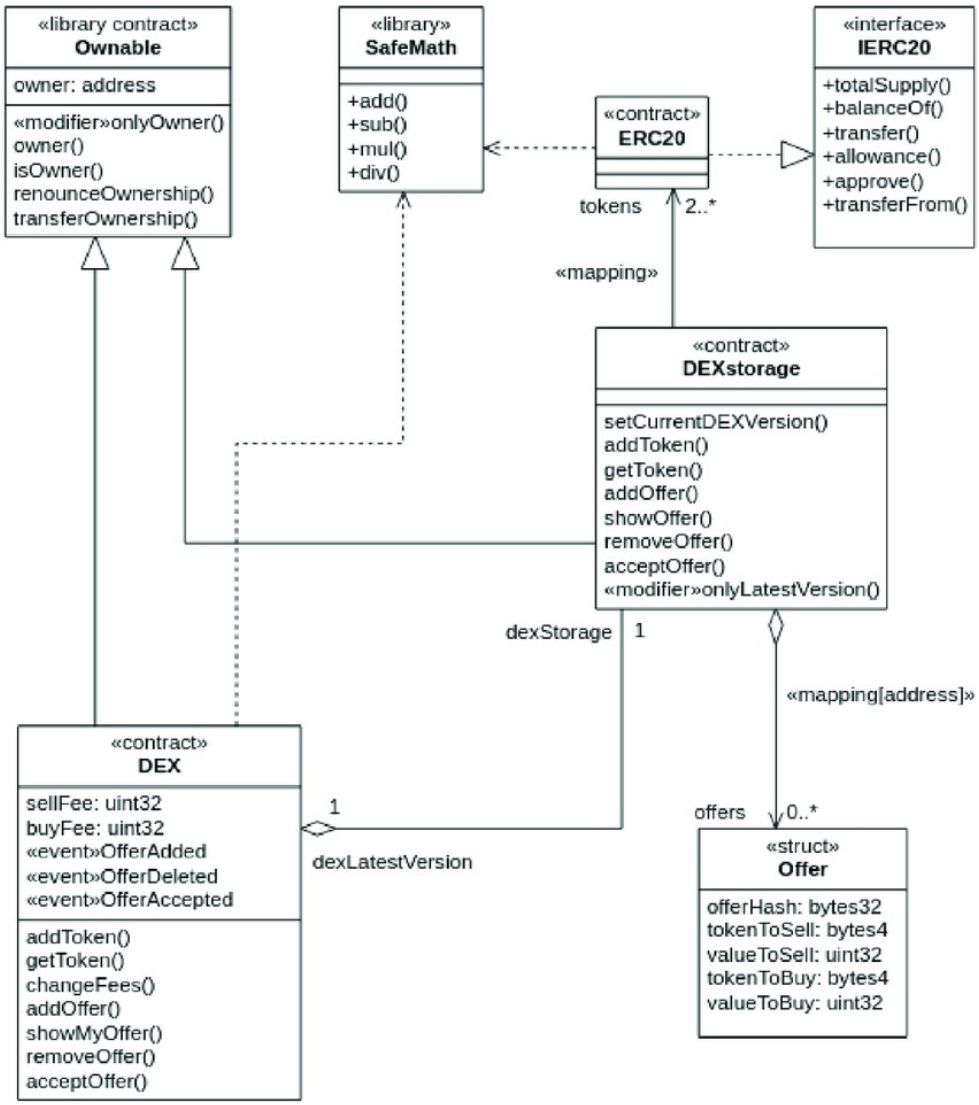

Figure 8.1: UML Diagram of Blockchain

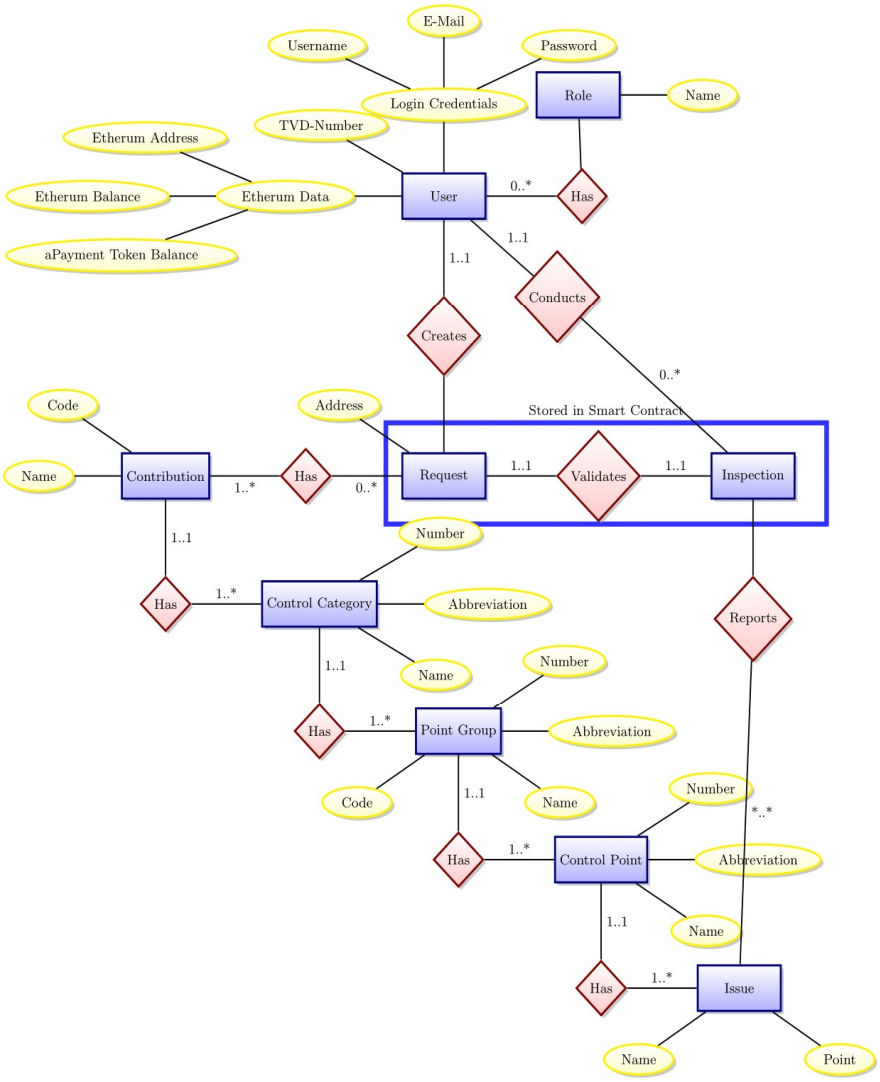

Figure 8.2: ER Diagram of Blockchain

9. Functional and Non-functional requirements

9.1. Functional

9.1.1. Look & Feel

Business Stakeholders are obsessed with the "look and feel" of an application, and for good reason. Studies have shown that an exceptional user experience will lead to greater user adoption. The greater to user adoption, the greater the ROI. When gathering requirements from the Business stakeholders, our team makes sure to put emphasis on the functional requirements like Business Logic, what should the application do, and how to stay within brand guidelines.

9.1.2. Technologies Involved

While Business Stakeholders focus on the functional requirements, IT Stakeholder's main area of concern is around the technical requirements. These are the Stakeholders that understand the technology plumbing that is currently keeping the company afloat. During technical requirement gathering sessions, our team makes sure to cover areas such as performance, availability, security, regulatory, data integrity, etc.

9.1.3. Integrations Required

End-to-End blockchain solutions have the power to reimagine existing technology. We don't believe that blockchain is here to take place of legacy systems, but rather add value and transform these systems. In your Use Case scenario, you may need to keep certain technologies as they play a critical role business processes. Our team of experienced solution architects will help intertwine related systems by focusing on areas such as data flow, APIs, streaming or batch processes, relationships, etc.

9.2. Non-functional

To make a system successful, it is very important to develop and consider the non-functional requirements properly. On system can work just fine based on its functionality but can also fail for not handling the non-functional requirements (NFR) appropriately. Non-functional requirements are product constraints or the features the system provides. They include constraints on timing, technology limits, and limitations imposed by standards. In certain cases, non-functional specifications refer to the device as whole systems or facilities, rather than individual device functions. This specific description, which describes something crucial in terms of what it is not, is not ideal, as many authors have discussed. Our aim here is not to satisfactorily define NFRs but to explore their application to blockchain-based systems. NFRs can be treated as quality and the functional requirements can be recognized as an entity. For example, a bus reservation system can be used to book seats using a secured transaction gateway. Here, booking the seats is functional requirements or entity of the system and security is the non-functional requirements or quality.

Qualities for Blockchain Many works on blockchain have been described how blockchain works, how it is the most secure way to complete a transaction. These types of aspects are mainly analyzed and explained. Few works have been done regarding the non-functional requirements of a blockchain-based system. We are summarizing those works in this section. UX Design. One unique obstacle to the creation of blockchain is the complexity of the user interface. The query is, how much of blockchain should you disclose to your consumers, as the enabling infrastructure? Do people need to know where they communicate with a blockchain anywhere on the application? Will they need to know what public and private keys are? How will it be kept secret if people do not know their private keys? Do they know about tokens, and need them to communicate with the application? These questions are relevant because people trust their money into your blockchain application.

The value of the blockchain assets is usually backed by the value of a cryptocurrency coin, provided by an initial coin offering (ICO). If the customer's wealth is connected to the coin's value, then how do you tell them their net worth increases and decreases as the value of the cryptocurrency increases and declines? When they are using your website, are they now investors in cryptocurrency? It is critical from the perspective of the user experience, too. Applications should be user friendly. For a new consumer, this first experience is very significant.

Launching and cluttering a website with blockchain-related jargon is likely to put off most consumers. But dumbing it down can reduce the importance of it or the visibility of blockchain's main benefits that distinguish your application from the non-blockchain competition. Scalability [11]. If the platform is connected to an implementation of a blockchain such as Ethereum then it is also connected to the scalability of the underlying network. Ethereum currently runs up to a theoretical limit of 25 (based on proof of work) at 4 transactions a second. When the next Ethereum game begins, a lot of transactions are created, would this affect the consumers? If they needed it, could they get their assets out immediately? Consumers would like to realize that they are not bound to something and will be able to return to the non-digital world at any stage of their choosing. To this, it is important to choose the right underlying platform. Development Operations. As blockchain is still emerging, the technology to build a blockchain-based system is still evolving.

It takes time to integrate new functionality into the system and improve the DevOps experience. Therefore, there should be enough amount of time associated with the development phase. Managing

Stakeholders. There is a tendency to over-sell the benefits of governance while marketing the advantages of a blockchain program. Possibly the actors of governance (e.g. police, government, auditors) get the most benefits from being able to monitor what everybody is doing and use it to control or test enforcement. It is necessary but other stakeholders need opportunities to enter the network otherwise there would be no users and no regulatory or control transactions. And there is the question of persuading all the stakeholders to get involved so you can do market research and collecting requirements.

Modeling and smart contract concepts ensure that all various types of stakeholders recognize the company domains. It requires the views of several stakeholders to address the problem of what should be held in the blockchain [12]. Finally, who initiates and pays for the creation of the blockchain platform initiative? Blockchain's key advantage is that it can facilitate business and collaboration among organizations that have never met. Over the platform's lifespan, this would attract many organizations, but one company needs to take the initial step, see the benefit, and create the platform for everyone else to use

10. Hardware Requirements and Software Requirements.

10.1. Hardware requirements

Hardware that runs Blockchain Technology is often referred to as high-performance computers or HPCs. Financial Institutions (among many other businesses) depend on these powerful computers to perform a task at high speeds without errors or interruptions. A business, in most cases, will contact a computer manufacturer and provide a set of specifications and requirements that need to be met for the computer to be selected to perform the desired functions, including for blockchain applications. These specs and reqs can be anything from processing power, memory, storage, plug-ins to environmental restrictions such as shock, vibration, temperature fluctuations, and humidity ranges.All possible scenarios have to be accounted for think about it, what happens if the cooling system in the server room fails? Suddenly, your powerful computers become overheated and could face catastrophic failures. Something a financial institution like VISA (which runs an average of 150 million transactions per day) cannot afford.

10.1.2. The Core Component of a High-Performance Computer

In today's business/tech world, the focus is primarily set on CPUs (Central Processing Unit) aka Processors. Think of a CPU as the brains of the system. It performs high-level tasks that manage the entire computer. A better CPU means greater performance which equals faster completion of assigned tasks. *Simple*. But blockchain technology is changing the way we think about processing power altogether, especially, when it comes to latency and real-time transactions.

10.1.3. Blockchain and GPUs

Graphics Processing Units, commonly known as Graphics Cards. A GPU is specialized for handling display functions of a computer, such as video rendering. I'm sure you're wondering how a display device benefits blockchain technology. To explain, let's take another trip down memory lane. In the old days of Cryptocurrency Mining (which is done on a DLT like blockchain), the processing of blockchain code was assigned to the CPU. Things were okay but turned sour rather quickly. A CPU, although great at performing multiple high-level functions **simultaneously, simply could not** keep up with the demand of processing many streams of repetitive data at high speeds, such as executing blocks of code within a chain. As the problem became more apparent, the big question was: "What can perform repetitive calculations faster than a CPU?" Answer: GPU. A GPU is designed for high compute density, meaning more computations per second with one major caveat: the calculations cannot be too complex. Let's just say that, a CPU hires a GPU and offloads these tasks so it can focus on other important calculations a GPU simply cannot perform.

10.1.4. Nodes & Clients

Nodes are the core components of proof of stake infrastructure. A node is a computer that carries out the key functions of the network, such as validating transactions, storing

blockchain data, or submitting votes on network governance. The software that dictates how these key functions are performed is a client. A decentralized network can support multiple software implementations, or clients, dependent on the network's design. Clients can be built to leverage a variety of programming languages and can exist in a variety of implementations. For example, the Ethereum network consists of mostly Geth and Parity nodes, while eth2 will support a larger variety of clients including Prysm, Lighthouse, Teku, Nimbus, and Lodestar.

There are a few basic types of nodes that make up proof of stake networks; each node type is optimized to perform specific tasks. These node types include:

10.1.4.1. Participation nodes are the basic building block of proof of stake networks. They validate transactions and create blocks, and, in return for executing this work, earn block rewards. A set amount of value must be locked, or "staked," to the node for it to become an active participant, or validator, on the network. Only once it is active can a node produce useful work on-chain in exchange for rewards.

10.1.4.2. Read/write nodes can be used to verify transactions, obtain information about them (query), and write data such as transfers or smart contract interactions (transactions) to the chain.

10.1.4.3. Sentry nodes, sometimes called proxy nodes, are nodes that stand between a participation node and the blockchain, allowing the participation node to complete its function while staying private and hidden from the public internet. The participation node only communicates with the blockchain through its sentry nodes—when they are being used. The sentry nodes function to protect the participation node from attacks by creating an extra barrier between the public internet and the participation node. For example, rather than executing a denial-of-service attack on a participation node, an attacker would have to first execute a denial-of-service attack on the adjoining sentry nodes, during which time the validator could spin up a new, un-attacked sentry node and continue operating unharmed.

10.1.4.3. Relay nodes serve as hubs for the network's peer-to-peer (or node to node) communication layer. They connect to a participation node and maintain connections to many other nodes to reduce transmission time by maintaining open, efficient communication paths.

10.1.5. Clusters

10.1.5.1. The term cluster is used to describe a network-specific node (or a collection of nodes) and its supporting infrastructure, such as load balancing tools, monitoring, and alerting services.

10.1.5.2. Clusters are often made up of:

10.1.5.2.1. Load balancers distribute traffic across multiple servers to improve the responsiveness of a node. They ensure no single server bears an inordinate amount of network demand.

10.1.5.2.2. Failover protection ensures a node does not experience extended downtime if the system it runs on goes out of commission. The form that failover protection takes may depend on whether a node is cloud- or hardware-based.

10.1.5.2.3. Monitoring and alerting services ensure that nodes are healthy and participating optimally in the network. For example, monitoring the CPU use of a node shows us whether requests are processed effectively; a spike in CPU usage could be a sign of an attack or error in the code of a protocol update. Uptime is closely monitored to ensure all nodes are reliable, stable, connected to the protocol, and able to access data.

10.1.5.2.4. Container services enable mass actions within a cluster. They allow applications and their packages to be pulled together into a form that can be version controlled. Two primary use cases include maintaining multiple clusters and supporting Blockchain Client APIs.

10.2. SOFTWARE REQUIREMENTS FOR BLOCKCHAIN

10.2.1. Solidity

Solidity is, undoubtedly, one of the most popular languages used by Blockchain Developers. Influenced by C++, Python, and JavaScript, it was designed to target the Ethereum Virtual Machine(EVM). Solidity is statically typed, supports inheritance, libraries, and complex user-defined types. Solidity supports the OOP paradigm and CIS most commonly used for writing smart contracts. With Solidity, Blockchain Developers can write applications that can execute self-enforcing business logic embodied in smart contracts, thereby leaving a non-repudiable, and authoritative record of transactions. This comes in handy for creating contracts for voting, crowdfunding, multi-signature wallets, and blind auctions.

10.2.2. Geth

Geth is an Ethereum node implementation built using the Go programming language. It is available in the three interfaces, including JSON-RPC server, command-line, and an interactive console. Geth can be leveraged for Blockchain development on all three major operating systems – Windows, Mac, and Linux. Geth is used for a host of different tasks on the Ethereum Blockchain, such as transferring tokens, mining ether tokens, creating smart contracts, and exploring block history. After installing Geth, you can either connect to an existing Blockchain or create your own. The good thing is that Geth simplifies things by automatically connecting to the Ethereum main net.

10.2.3. Mist

Mist is the official Ethereum wallet developed by the creators of Ethereum. When it comes to Ethereum, before you can start using the platform, you must have a designated place where you can store your Ether tokens and execute your smart contracts. It is available for Windows (both 32- and 64-bit), Mac, and Linux (32- and 64-bit). While Mist is particularly suitable for deploying smart contracts, you must remember that it is a full node wallet – you have to download the entire Ethereum blockchain, which is larger than 1TB. Another critical thing to keep in mind is to remember your Mist password since you can never change it – it is a one-time setup ting.

10.2.4. Solc

Solc (Solidity Compiler) is a Solidity command-line compiler written in C++. Its primary purpose is to convert Solidity scripts into a more readable format for the Ethereum Virtual Machine. While Solidity is a slimmed-down, loosely-typed language with a syntax similar to JavaScript, the smart contracts written in it need to be converted to a format that can be easily read and decoded by the EVM. That's where Solc comes into the scene. There are two types of Solc – Solc (coded in C++) and Solc-js (it uses Emscripten to cross-compile from the Solc source code from C++ to JavaScript). Solc comes natively with most of the Ethereum nodes. It can be used for offline compiling, as well.

10.2.5. Remix

Remix IDE is a browser-based Blockchain tool used for the creation and deployment of smart contracts. Written in Javascript (so it can be accessed via any modern browser!), Remix can be used for writing, testing, debugging, and deploying smart contracts written in Solidity. It can be used either locally or in the browser. If you visit Remix's website, you can see a ready-to-use screen:

Apart from having excellent documentation, Remix can seamlessly connect to the Ethereum blockchain through Metamask.

10.2.6. Metamask

Metamask is a wallet designed to function that acts as a bridge between Ethereum Blockchain and a browser (Chrome or Firefox). Essentially, it acts as a browser extension. Metamask offers a software platform that allows you to serve Ether and other ERC-20 assets while also letting you interact with Ethereum Dapps. The best part – you can do so right from your browser. Metamask can be linked with Shapeshift and Coinbase to sell and buy ETH and ERC20 tokens. It can also save keys for ERC20 tokens and Ether. Since it can interact with different Ethereum test networks, it makes an ideal wallet for Blockchain Developers. Once you installed the app in your browser, you have a built-in Ethereum wallet ready to be used.

10.2.7. Truffle

Truffle is an Ethereum Blockchain framework designed to create a development environment for developing Ethereum-based apps. It comes equipped with a vast library that provides custom deployments for writing new smart contracts, developing complex Ethereum dApps, and helping tackle other challenging requirements of Blockchain development. Truffle can perform automated contract testing using Chai and Mocha. It can also enable smart contract development, including linking, compilation, and deployment. Plus, it offers a configurable build pipeline for performing custom build procedures.

10.2.8. Ganache

Ganache is a Blockchain tool from the Truffle Suite that allows you to create your own private Ethereum blockchain to test dApps, execute commands, and inspect state while taking full control of the operation of the chain. The greatest feature of Ganache is that it allows you to perform all the actions you would otherwise perform on the main chain, without incurring the cost for the same. Blockchain Developers use Ganache to test their smart contracts during development since it comes with many convenient options like advanced mining controls and a built-in block explorer.

10.2.9. Blockchain Testnet

When talking about Blockchain development, we cannot stress enough the importance of Blockchain Testnet. A Blockchain Testnet allows you to test dApps before making them live. Each blockchain

solution has its unique Testnet, and it is highly recommended that you use the respective Testnet for the optimal result. There are three kinds of Blockchain Testnets – Public Test, Private Test, and GanacheCLI. Testnets are extremely useful as it lets you test your dApps for bugs and errors without spending tons of cash or resources. For instance, Ethereum uses gas as the fuel for performing different operations. Spending on gas every time you need to do a test run can become a substantial financial burden. Thanks to Testnets, testing becomes feasible.

10.2.9.10. Blockchain-as-a-Service (BaaS)

Since it is not practical (or financially viable) for a company to implement a full end-to-end permissioned blockchain solution, it gave rise to the concept of BaaS. BaaS is modeled to function similarly to a SaaS model. It lets you leverage cloud-based solutions to build, host, and use your custom-made Blockchain apps, smart contracts, and other interoperability functions on the Blockchain, with the cloud-based service provider handling and managing all the essential tasks/functions required to keep the Blockchain infrastructure operational and agile.

BaaS can be a convenient tool for individual entrepreneurs or companies who wish to adopt Blockchain tech but haven't been able to do so due to operational overhead and technical complexities. Today, there are many BaaS service providers such as Microsoft (Azure), Amazon (AWS Amplify), SAP, IBM, and other stakeholders, to name a few. These services are usually more expensive due to higher transaction costs.

References

1. "IDC Digital Universe Study: Big Data, Bigger Digital Shadows and Biggest Growth in the Far East Sponsored by EMC.", 2011.

2. Lanier, Who owns the future?. London: Penguin Books, 2014, pp. 32-66.

3. H. Noman and J. York, "West Censoring East: The Use of Western Technologies by Middle East Censors, 2010-2011", Open Net Initiative, 2011.

4. Ghosh, "China Shut Down More Than 1M Web Sites Last Year", International Business Times, 2017. [Online]. Available: http:// www.ibtimes.com/china-shut-down-more-1m-web-sites-lastyear-298167.

5. T. Berners-Lee, Tim Berners-Lee Keynote: "Re-decentralizing the web - some strategic questions". 2016.

6. S. Driscoll, " How Bitcoin Works Under the Hood", Imponderable Things, 2013.

7. M. Dialysis, "How Does the Blockchain Work?", Medium, 2016.

8. A. Wenger, "Crypto Tokens and the Coming Age of Protocol Innovation", Continuations, 2016.

9. J. Benet, "IPFS - Content Addressed, Versioned, P2P File System (white paper)", 2014.

10. K. Nguyen, T. Nguyen and Y. Kucherov, "A P2P Video Delivery Network (P2P-VDN)", in 18th International Conference on Computer Communications and Networks, San Francisco, CA, USA, 2009.

11. F. Ehrsam, "The dApp Developer Stack: The Blockchain Industry Barometer", Medium, 2017. [Online]. Available: https://medium.com/ @FEhrsam/the-dapp-developer-stack-the-blockchain-industrybarometer-8d55ec1c7d4. [Accessed: 12- Dec- 2017]

12. Clearswift (2007), Demystifying Web 2.0, white paper, Clearswift Limited, July. Available at:http://resources.clearswift.com/ExternalContent/C12CUST/Clearswift/9514/200707(access ed 28 August 2013).

13. Cui-hong, H. Research on Web 3.0 Application in the Resources into Integration Portal; Southwest University of Science and Technology: Mianyang, China, 2012.

14. Pattal, M.M.I.; Li, Y.; Zeng, J. Web 3.0: A real personal Web! More opportunities & more threats. In Proceedings of the 2009 Third International Conference on Next Generation Mobile Applications, Services and Technologies, Cardiff, UK, 15–18 September 2009.

15. Dabit, N. What is Web3? The Decentralized Internet of the Future Explained. Free Code Camp. 8 September 2021. Available online: https://www.freecodecamp.org/news/what-is-web3/ (accessed on 5 January 2022). 4. Tran, K.C. What is Web 3.3 November 2019. Available online: https://decrypt.co/resources/what-is-web-3 (accessed on 2 February 2022).

16. Rudman, R.; Bruwer, R. Defining Web 3.0: Opportunities and challenges. Electron. Libr. 2016, 34. [CrossRef]

17. McCormick, P. The Value Chain of the Open Metaverse. Available online: https://ethereum.org/en/developers/docs/intro-toethereum/ (accessed on 25 January 2021).

18 . The Value Chain of the Open Metaverse. Available online: https://www.notboring.co/p/the-value-chain-of-the-open-metaverse (accessed on 10 January 2022).

19. Available online: https://docs.soliditylang.org/en/latest/ (accessed on 5 April 2022).

20. Alpert, J. and Hajaj, N. (2008), We knew the Web was big. Available at: http://googleblog.blogspot.com/2008/07/we-knew-Web-was-big.html (accessed 19 July 2013).

21. Anderson, A. (n.d), 10 Most Important Business Objectives, Demand Media. Available at: http://smallbusiness.chron.com/10-important-business-objectives-23686.html (accessed 9 September 2013).

22. Benjamins, R. and Contreras, J. (2002), Six Challenges for the Semantic Web, white paper,Intelligent Software Components, Intelligent Software for the Networked Economy (isoco), April. Available at: http://oa.upm.es/5668/1/Workshop06.KRR2002.pdf (accessed 2 October 2013).