**Towards a Framework for Understanding the Performance of Blockchains**

M. Touloupou, K. Christodoulou, A. Inglezakis, E. Iosif and M. Themistocleous, "Towards a Framework for Understanding the Performance of Blockchains," 2021 3rd Conference on Blockchain Research & Applications for Innovative Networks and Services (BRAINS), 2021, pp. 47-48, doi: 10.1109/BRAINS52497.2021.9569810.

Abstract— Blockchain and Distributed Ledger Technology (DLT) appears to be at a worldwide threshold of acceptance and adoption. Since their inception, several innovative projects have been proposing solutions to the blockchain trilemma, improving blockchain features and its technical limitations. However, the adoption of blockchain as a technology or a software component, requires a comprehensive understanding and characterization of their technical principles and characteristics. The latter introduces an uncertainty for an organization to decide which blockchain protocol best meets its needs and demands. In general, there is a lack of proper testing and software engineering practices for assessing the usage of blockchains usage and understanding their performance. Towards that direction, this paper presents an architecture for a blockchain benchmarking framework which aims at the deployment and evaluation of different blockchain protocols, focusing on different aspects such as security and scalability. A set of modules is introduced for testing and evaluating the behaviour of blockchain protocols under different test scenarios.

A distributed ledger is often described as a shared distributed database which is accessed and maintained by a set of independent, possibly untrusted participants (i.e., nodes). Each participant owns an identical copy of the database of transactions (i.e., the ledger) maintained over a peer-to-peer (p2p) network. All modifications or additions to the ledger are expressed immediately and agreed among the participants using a consensus algorithm. Blockchain, which is considered as a type of a Distributed Ledger Technology (DLT), was first introduced within the concept of a cryptocurrency (i.e., Bitcoin), while by then has received a lot of attention due to the unique characteristics it offers, i.e. security, anonymity, transparency, and decentralization [1]. The decentralized nature of a blockchain, lacks of a central authority to synchronize the state of the processes. For this reason, such systems implement consensus algorithms, which are responsible for (i) the coordination of the distributed nodes, and (b) the validation of the state of transactions propagated in the network. Moreover, consensus algorithms provide reliability and liveness to the network and defend it against malicious (aka byzantine) attacks. Nowadays, blockchain technology has been introduced as a software component in many domains such as healthcare, supply chain, finance, and energy [2], while many enterprises and academic institutions are conducting research on how blockchains can be used for solving real-world challenges (e.g., identity theft, mismanagement in healthcare, digital copyright & piracy issues etc.). Still though, the wide adoption of the technology still remains an ongoing task. On the technical side, choosing which blockchain protocol to deploy, and which type (public, private or consortium) is challenging.

Before deciding which blockchain protocol to deploy several questions need to be explored such as: Why a blockchain infrastructure is required? How is the blockchain infrastructure improving current processes? Which blockchain protocol is suitable based on the requirements at hand? and to what extend does the selected blockchain protocol handles security and scalability concerns? In an attempt to answer the aforementioned questions, this paper introduces an architecture for a proposed blockchain benchmarking framework that aims to be: (a) generic, in terms of the deployment of different blockchain protocols, (b) reliable in terms of achieving close-to-real data, and (c) scalable. The proposed benchmarking framework aims to serve as a staged environment for supporting blockchain researchers and developers to test and validate the performance of a blockchain protocol under various settings and synthetic scenarios. In brief, the aim of this work is to provide a benchmarking environment for monitoring and comparing the behavior of each blockchain protocol in the presence of faults. In addition, the proposed modules enable the user to monitor different metrics and to identify potential performance bottlenecks within the network.

II. RELATED WORK

Currently, there are multiple studies regarding measuring the performance of blockchain protocols. Some of these studies are targeting public blockchains while others private ones. BlockBench [3] is a framework for analyzing private blockchain protocols. It is considered adaptable in terms of integrating any private blockchain while it can measure throughput, latency, scalability, and fault tolerance against different workloads. Additionally, the authors in [4] have considered the scalability of blockchain protocols as an urgent concern. Thus, they have studied how different bottlenecks in the Bitcoin network can affect the overall throughput of the network. In the work conducted in [5], the authors have studied the propagation time of blocks and transactions in the network concluding to the fact that the latter is the primary cause for blockchain forks. They have also demonstrated what can be achieved while pushing the network to its limit, by introducing unilateral changes to the client’s behavior. Furthermore, the authors in [6], have introduced a framework for analyzing existing Proof of Work (PoW) based deployments and PoW blockchain variants, in an attempt to compare the trade-offs between their performance and security provisions.

III. BLOCKCKHAIN BECNHMARKING FRAMEWORK PROPOSITION

Blockchain-based protocols are complex systems that comprise of many components ranging from the underlying communication network, cryptographic libraries, gossip protocols, consensus, virtual machines, and game theoretical aspects. In most cases, bootstrapping a private blockchain network on a local deployment and use it for testing is a challenging task. It is even more challenging to compare various private blockchain implementations in terms of transactions throughput, latency, fault-tolerance, and scalability. Moreover, having an isolated environment where you can introduce changes to the source code, test and debug the system without affecting the implementation of the production blockchain, is essential. Implementing a blockchain infrastructure considers several design choices such as network performance, network anomalies, node’s misbehavior, etc. However, the latter introduces several challenges, while a blockchain network usually consists of several nodes running in different machines around the world (i.e., high level of distribution and decentralization). The proposed implementation of our benchmarking framework is open-source, and it is published under our GitHub repository [7]. Currently, it is capable of deploying a full-mesh XRP ledger network with a given number of nodes/validators. Moreover, different scripts are developed for generating traffic in the network (e.g., in the form of payment transactions), a monitoring framework for capturing and visualizing data produced by the network, as well as, a connectivity manager, aiming for the adaptation of the network rules at different nodes during runtime. We note that the current deployment is generic, and it could be adapted to support the deployment of any blockchain protocol.

1. Architecture Overview

As depicted in Figure 1, the proposed architecture is comprised of four main building blocks. These are: (a) the Control & Configuration components, (b) the Validators Network, (c) the Accounts Management and Traffic Generator, and (d) the Monitoring Services. Figure 1: Blockchain Benchmarking Framework Architecture Control and Configuration: This module considers the deployment process of the network (e.g., generation of configurations files, bootstrapping the network, adapting the connectivity between the nodes/validators etc.)

Validators Network: This module enables the dynamic spawn of a blockchain network of n number of nodes that act as validators. Accounts Management and Traffic Generator: This module is responsible for creating new accounts and for injecting traffic (in form of transactions) towards the network participants.

Monitoring Services: This module enables several monitoring services. In brief this module gathers data and enables different data visualizations by looking at the transactions performed in the network. Furthermore, the module reads data regarding the health of the nodes that participates within then network.

CONCLUSIONS

This paper introduces the architecture of a blockchain benchmarking framework with the aim of monitoring and measuring the performance of various blockchain deployments in the presence of faults. An implementation of the architecture is provided under [9] to showcase an instantiation of the framework with the deployment of the rippled daemon. A comprehensive evaluation of the deployment is set as a future work. Currently, we are working towards extending the framework with providing support to other blockchain protocols (e.g., Stellar, Ethereum). The aim of this work is ultimately to act as a common ground for performing benchmarks while stress testing the behavior of different blockchain protocols against different scenarios that simulate close to real environments.

**Peer Review Aggregation utilizing blockchain technology**

J. Lawton, K. Uzdoğan and P. Cox, "Peer Review Aggregation utilizing blockchain technology," 2021 3rd Conference on Blockchain Research & Applications for Innovative Networks and Services (BRAINS), 2021, pp. 8-11, doi: 10.1109/BRAINS52497.2021.9569802.

Abstract—It is widely accepted that peer review is important to maintain the quality and integrity of scholarly communication [1]. However, recognition and discoverability of peer reviews in a systematic way is challenging because of the multitude of stakeholders and discrepancies between systems that report peer review statistics. We propose a blockchain-enabled application called PeerView that empowers researchers, publishers, and other stakeholders to integrate and access peer review information in a decentralized data structure, such as a blockchain. Furthermore, due to the cryptographic, immutable, decentralized, and autonomous nature of a blockchain, we can support data security, privacy, and provenance. Ultimately, this ensures that no central or individual entity will have complete ownership over the valuable data contained within, while still ensuring that peer review metrics can be properly attributed. We provide the initial prototype application along with an integration with an open peer review journal, F1000Research.

1. PROBLEM STATEMENT & OVERVIEW

Peer review can help to ensure the quality and soundness of scientific work [2]. Additionally, it is widely accepted in the scientific community to be an important part of scientific publishing [1], [3]–[5]. However, as vital as peer reviews are to scientific publishing, the process still has ongoing problems such as bias [6], general inconsistency [7], [8], and is ineffective in detecting errors [9]. Due to the nature of blinded peer reviews, many are publicly unavailable, thus it is also difficult to credit reviewers, and research peer review in detail and at scale [10]. Furthermore, incentivizing peer reviewing via proper attribution and recognition can help encourage more researchers to participate in the peer review process [1]. Peer review is generally not considered when evaluating scientists [11], [12]. The metrics used to evaluate scientists are publication based such as h-index, citation counts or the Journal Impact Factor of the journals published in [12]. Many aspects of the peer review process, for instance peer review count or quality, could also be utilized to give a more holistic overview of a scientist’s scholarly contributions [13]–[15].

However, peer reviews generally have limited discoverability, difficultly in providing attribution, and innate problems due to the usual confidential nature of the review process [16]–[22]. By solving or minimizing these problems, we aim to give better insight into a researcher’s scholarly body of work in order to better effectively evaluate a scientist, as well as bring more recognition to the peer review efforts of researchers.

Many organizations are working to solve these aforementioned issues in peer review. The majority of them use a centralized solution, such as a database, to aggregate peer review information from various sources [23]–[25]. This means that a single entity controls access to this information, decides what constitutes a peer review, or who can add new peer reviews. In a diverse stakeholder setting such as peer review, potential stakeholders in this ecosystem could include funding organizations, governmental bodies, scientific journals, research institutes, and individual scientists. These stakeholders have a variety of requirements, along with the necessity to access and analyze this aggregated peer review information to properly perform evaluation of a researcher. However, in the current setting, the authors and publishers are effectively relinquishing control while these third-party entities hold monopoly over the data. An improved peer review infrastructure should be built with this multitude of stakeholders and a shared governance in mind [26].

We construct our system upon blockchain technology which is a decentralized, distributed, and immutable ledger of information. Blockchain has been shown to be effective in improving discoverability [27], [28], enhancing data provenance and attribution [29]–[31], as well as ensuring no single point of failure or authority to restrict information access exists [32], [33]. Building a peer review aggregation system on a decentralized infrastructure ensures that no single stakeholder holds a monopoly on the aggregated peer review data. This could encourage these stakeholders to open their own centralized data silos of peer review information to a larger ecosystem. The distributed nature of the blockchain also ensures redundancy in case of failure of any single node. Lastly, the immutable nature of a blockchain facilitates a long term outlook for peer review data in regards to persistence and preservation. Specifically, we utilize the bloxberg [34] blockchain which is a scientific infrastructure governed by scientific institutes and organizations. In comparison to other blockchain networks such as Ethereum [35] or Bitcoin [32] that use proof of work for their consensus algorithm, bloxberg uses a proof-ofauthority consensus called AuRa [36]. This alternative consensus algorithm is more energy efficient, faster, and ensures that every node that validates blocks in the network is publicly known and non-anonymous. Each node that validates blocks in the chain, is a research organization. This governance model works to support scientific infrastructure, such as peer reviews, will be continually maintained and in line with scientific norms.

1. SYSTEM DESIGN

We developed an initial prototype application along with integrations with other service providers as a proof of concept in order to overcome the aforementioned issues in peer review, particularly discoverability and attribution. Our target users are scientists and researchers from a wide variety of fields, many of whom are unfamiliar with blockchain technology and any complexities this may entail. Therefore, a primary goal of our architecture design is to ensure a usability experience similar to typical web applications that don’t utilize a blockchain. From this prototype, we plan to further test usability of the application, as well as explore additional features. The architecture of the application is shown in Figure 1. Firstly, in order to interact with a blockchain, a user must have access to a Web3 compatible wallet. One of the options, Magic [37] (previously Fortmatic [38]), is a passwordless identity solution with web3 functionality that is injected into the application using a common login mechanism, such as an email. This greatly enhances the user-friendliness by abstracting away the blockchain processes at the cost of custodying the keys to a service provider. Users who are willing to manage their own keys are also given the option to use a Web3 browser wallet such as Metamask [39]. We build the PeerView application on top of the bloxberg scientific blockchain infrastructure which is ideal for an application in the area of scientific research. The primary component of the application is the smart contract [35] on the bloxberg blockchain written in Solidity language. The contract serves as the back-end of the application enabling the storage of and the interaction with the peer review data. The contract also declares a basic peer review data model which includes attributable information such as the author, publisher, and a URL of the review. The number of attributes are kept minimal to accommodate different peer review processes.

Besides the contract, personally identifiable information and larger data is stored in a MongoDB [40] database. However, the system is fully functional without it. The database in future could be replaced with alternative decentralized file storage systems such as IPFS [41]. To enable interactions with the database and the integrations with the external services, an Express [42] server is developed. In order to ensure high performance that users expect in a web application, we also integrate an indexing server which indexes smart contract events from the blockchain into a server. This allows high volume querying of the indexing server to strengthen scalability and usability.

To demonstrate the feasibility of integrating a live publishing platform into PeerView, we utilized the API of F1000Research (https://f1000research.com/developers), an open peer review publishing platform [43]. F1000 Research provides a post-publication, open peer review and open access publication model which allows for all elements of the publication and review process to be accessed publicly. This includes all versions of articles as well as all peer review feedback and author responses. Users can import all previously done peer reviews on F1000Research into PeerView. Lastly, we identified a typical problem that users encounter when interacting with a blockchain-based application, namely managing gas [35]. In order to alleviate this issue, we instantiate a Gas Station Relay Network [44] which abstracts away the necessity of a user holding cryptocurrency in their wallet. The peer review smart contract is simply funded with enough cryptocurrency to pay for the user gas costs of the application. A user simply needs to sign a transaction to add a peer review to their profile in lieu of holding and managing cryptocurrency.

**Research on Digital Finance Based on Blockchain Technology**

Y. Zhu, "Research on Digital Finance Based on Blockchain Technology," 2021 International Conference on Computer, Blockchain and Financial Development (CBFD), 2021, pp. 410-414, doi: 10.1109/CBFD52659.2021.00089.

Abstract—Blockchain has many technical characteristics such as distributed, traceable, trustless, difficult to tamper with, and multi-centralized. Blockchain can effectively establish a financial asset management system based on digital technology, automatically docking assets of different industrial forms into a digital financial framework. It can realize the automatic mapping and circulation of assets under the chain, and create an economic network integrating financial asset digitization and asset management. Blockchain technology has attracted much attention, but in its development process, there are still problems such as inconsistent standards, chaotic derivative markets, threats to security, and difficulty in supervision, so that the current blockchain and physical business docking products that can be implemented in the market less. This paper analyzes the application cases of digital financial asset transactions based on blockchain technology, studies the current pain points of blockchain technology in various digital financial asset transaction industries, and provides corresponding solutions.

1. INTRODUCTION

Blockchain technology is considered to be one of the most representative achievements of the fourth industrial revolution, and is "the core technology with the most potential to trigger the fifth wave of disruptive revolutions." In recent years, China's digital finance has developed rapidly. "Digital finance generally refers to the use of digital technology by traditional financial institutions and Internet companies to realize financing, payment, investment and other new financial business models." It first appeared mainly to make up for the shortcomings of traditional finance, and then gradually became an important force in China's financial service market, especially in the field of payment. Digital finance breaks the time and space constraints, cost constraints, information barriers, and customer exclusion of financial services, making finance better serve the real economy. After the previous technology accumulation, the blockchain is now rapidly extending its application to industrial Internet, Internet of Things, smart manufacturing, intelligent investment advisory, digital finance, supply chain management, asset trading, regulatory supervision, contract management and other fields. At the same time, because the potential of blockchain applications is far from being fully released, it has received more and more attention and attention from the international community. Major countries in the world, including China, are seizing the opportunity to compete for the commanding heights of blockchain development. At present, news and start-ups about blockchain technology in digital currency and digital asset trading are emerging one after another, but there are still few products that can really be introduced to the market and have been tested by the market. This article will analyze Bubi's innovative methods from multiple perspectives through the case of Bubi in digital asset transactions, hoping to bring more enlightenment to the implementation of blockchain technology in digital asset transactions.

1. BLOCKCHAIN CONCEPT AND CHARACTERISTICS.

A)The concept of blockchain

Blockchain is a decentralized distributed database. The database is formed by linking data blocks generated by cryptographic methods in chronological order. The blocks contain data generated within a certain period of time and cannot be tampered with. In a distributed network system, each node has complete database information, all information is open and transparent, and the rights and obligations of each network node are equal. The system data is maintained by the entire network node, and the authenticity and consistency of the information can be verified without a third party. The industry generally believes that the financial market mainly relies on financial intermediaries to reduce adverse selection and moral hazard, so as to effectively allocate resources, improve market efficiency, and ultimately achieve economic growth. Since blockchain technology relies on cryptography to realize global value transfer and gets rid of the dependence on trust, blockchain distributed ledger technology challenges this established logical thinking.

B) Characteristics of blockchain

1) Decentralization: The blockchain database is a peer-topeer autonomous network that can create trust between nodes. Each network node has equal rights and obligations. The storage and management of information is maintained by the entire network node. All nodes follow the same rules. The participation of third-party intermediaries will not affect the operation of the system because any single node is attacked or cannot be controlled. We organically combine a centralized system with a decentralized network, which is a practical and feasible path for blockchain to land. Not only that, there are different degrees of decentralization, which specifically include four degrees of decentralization, weak center, multi-center, and centralization. You can choose the appropriate degree of decentralization based on business characteristics and needs.

2) Safety: Each node of the blockchain has complete database information. When a new block is to be added, a consensus algorithm will be implemented on all nodes in the entire network to update the entire block information. Data information will be stored forever, and the proof-of-work mechanism makes it possible to change the information of the database at least to control 51% of all nodes. Therefore, as the scale of the blockchain continues to grow, so does the security.

3) Openness: The blockchain system is highly open, except that the private information involving transaction nodes will be encrypted, the technology, data, and access rules are all public; the entire system information of the blockchain is highly transparent and open. If a node wants to query the relevant data of the blockchain or wants to develop blockchain-related applications, it can use the public interface.

C. The application of blockchain in digital finance

At present, there are not many applications of blockchain in the financial field. Among these applications of blockchain, micro-enterprise chain, ZRobot, and bank draft system are several typical application frameworks.

III. THE DEVELOPMENT DILEMMA OF DIGITAL FINANCE BASED ON BLOCKCHAIN TECHNOLOGY

1. The lack of special laws on digital finance

Blockchain technology has not been included in the current financial legal framework. From the perspective of legal supervision in recent years, there are major deficiencies in the supervision of Internet finance, and it is in a relatively vague state, almost impossible to rely on. In this case, once there is a related loss of interest, it will seriously affect the enthusiasm of related participants. First of all, there is a conflict between the basic principles of the existing contract law and the implementation of smart contracts under the blockchain. The relevant laws of Internet finance need to resolve the legal attributes of smart contracts. Second, it is necessary to do a good job in determining the legal effect of undisclosed data, and whether undisclosed data has legal effect, use it as the basis for fulfilling relevant obligations. Finally, for the stability and prosperity of the financial market, it is necessary to formulate more detailed and applicable laws and regulations regarding digital assets and digital currencies. China's "Cyber Security Law" stipulates that individuals have the right to require network operators to delete or correct their personal information in accordance with the law. To modify data in the blockchain, more than 51% of the nodes need to be controlled. Once any data is written into the blockchain, it is difficult to delete or modify. Therefore, the application of blockchain technology hinders the relevant legal entities from exercising the right to delete and fulfilling the obligation to delete, and has a certain impact on the governance of cyberspace.

1. Blockchain digital financial application technology is low

At present, the application of blockchain technology in the field of digital finance is still in its infancy, and large-scale and large-scale implementation has not yet begun. For traditional financial institutions such as banks, blockchain may not be able to meet the basic technical requirements required for the development of blockchain finance. For the securities industry, the blockchain seems to have achieved decentralization in the settlement of the securities industry, but it still needs the help of intermediate companies. For the insurance industry, every customer's information and data needs to be recorded, saved and copied. The more node participants on the blockchain, the greater the network and node computing pressure. Mass data may bring hidden dangers such as data transmission errors and network paralysis, which will further increase the cost of insurance companies. Moreover, the distributed nature of the blockchain makes insurance claims take more time, which greatly reduces the operating efficiency of the insurance industry.

1. Blockchain digital financial supervision system is not sound

The healthy operation of digital finance is inseparable from effective supervision. At present, the blockchain still has certain problems in digital financial supervision. On the one hand, blockchain has certain regulatory loopholes in digital financial supervision. Blockchain technology can improve the security and controllability of the blockchain system by controlling membership, but it cannot ensure that all parties will not conspire to tamper with the basic agreement and ultimately harm the interests of other participants. On the other hand, blockchain has certain technical defects in digital financial supervision. The corresponding secret key is required when using blockchain technology to conduct digital financial transactions. Once there is a problem with a certain transaction, the supervisory authority cannot find the key corresponding to the transaction chain in a short time, which further increases the difficulty of supervision. If the key of a blockchain user is lost, it may cause irreparable losses to the user. Because after the blockchain key is lost, its tamper-proof modification prevents users from recovering assets and recovering identities by changing data, unable to read and store information, and unable to conduct transactions, let alone declare property ownership, which may cause huge assets to users’ loss. Therefore, blockchain not only provides technical means for digital financial supervision, but also raises supervision problems for it.

IV. COUNTERMEASURE ANALYSIS

1. Improve the blockchain digital financial legal system

At present, although China has made preliminary attempts in the theory and practice of blockchain legislation, because the application of blockchain in China is still in its infancy, relevant laws and regulations cannot be formulated in time. To this end, efforts must be made from the following aspects: First, improve the legislation in the field of computer and information technology related to blockchain. At present, China has promulgated laws such as the Cyber Security Law, the Electronic Commerce Law, the Electronic Signature Law, and other administrative regulations such as the Regulations on the Security Protection of Computer Information Systems, and the Measures for the Administration of Internet Information Services. As a new technology, blockchain needs constant regulation by law. Due to the relative lag in the formulation and implementation of laws, with the emergence and gradual promotion of blockchain technology, we must continue to improve the related upper laws to better regulate the application of blockchain technology at the macro level. Second, formulate rules and regulations are related to blockchain in a timely manner. At present, the Central Bank of China has formulated the Implementation Measures for the Protection of the Rights and Interests of Financial Consumers, and the State Internet Information Office has also issued and implemented the Regulations on the Management of Blockchain Information Services. These "methods" and "regulations" are of great significance for maintaining financial security and regulating the application of blockchain technology. However, with the continuous integration of blockchain and digital finance, more detailed rules and regulations need to be formulated to better guide the healthy and orderly development of digital finance. Third, new rules for blockchain digital finance applications will be issued in a timely manner. At present, the Supreme People's Court of China has issued a judicial interpretation of the "Regulations on Several Issues Concerning the Trial of Cases by Internet Courts", which provides for the development of electronic evidence such as blockchain. The relevant competent authorities have also issued notices such as the "Notice on Preventing Bitcoin Risks", "Announcement on Preventing the Risk of Token Issuance Financing", and "Risk Tips on Preventing Illegal Fund-raising in the Name of "Virtual Currency" and "Blockchain"" or announcement. Blockchainrelated industries have made advance explorations on the standardization and related specifications of the blockchain field, and released materials such as "China Blockchain Technology and Application Development White Paper", "Blockchain Reference Framework", and "Blockchain Data Format Specification". This has important guiding value for the development of blockchain digital finance. With the deepening of blockchain digital finance, this field requires more detailed rules and regulations. For this reason, relevant departments and industries must pay full attention to the development trend of blockchain digital finance, formulate relevant rules in a timely and effective manner, and guide and regulate the healthy and orderly development of blockchain digital finance.

1. Strengthen technological innovation

The core issue hindering the development of blockchain finance is technical issues. Technological instability will affect the operation of financial platforms and the security of users’ assets and information, which will result in slow or stagnant development of new things. We must further strengthen the R&D and application of the core technology of the blockchain financial platform, break through the core technology bottleneck, build a consensus mechanism system, realize the interconnection of system information, and do a good job in information security management. Research and develop key technologies such as consensus mechanisms and smart contracts, and formulate Chinese standards and systems. At the same time, when we invest the developed blockchain technology in finance for practical applications, we should analyze various technical problems in a timely manner, including analyzing possible situations and finding solutions. In addition, China has many blockchain patents, but generally lacks core technologies. It is recommended that key domestic financial technology companies, related scientific research institutions and universities work together to research and develop core technologies, such as research and development of key technologies such as smart contracts and consensus mechanisms. We develop a reasonable and implementable standard system. At the same time, when this system is specifically put into the financial industry for practical applications, specific problems need to be analyzed in detail, and specific and adjustable solutions can be formulated for different situations and different technical requirements that may arise.

1. Improve the blockchain financial supervision system

"Holding the bottom line that systemic financial risks do not occur" is the core principle of financial supervision. As a subdivision form of financial technology, blockchain finance should follow the core guidelines of the financial industry. From the current point of view, there are few application cases of blockchain technology, and there is a lack of long-term practical experience and time test. The risks and challenges that this technology may bring to the financial system still have large uncertainties, so in this while technology continues to evolve, it is also necessary to continuously improve the supervision of the financial system. At the early stage of the development of new technologies, government policies should focus on support, and its supervision should be appropriately relaxed. An overly strict regulatory system will not be conducive to the development of emerging technologies and hinder the development of financial technology. However, emerging technologies have too many unknowns and will generate a lot of hidden risks. Too loose policies will encourage risks to be amplified. Therefore, it is necessary to set up an audit mechanism in the early stage to ensure that industry risks are within the government's controllable range. This requires regulatory agencies to plan in advance to help emerging industries establish mature industry standards and enable them to develop soundly. In addition, a reasonable access mechanism can trap risks in a cage, and it needs to cooperate with in-event and post-event supervision to form a complete system. At the same time, we can learn from international methods, such as the sandbox supervision model, to promote the steady development of the industry.

V. CONCLUSION

Blockchain technology has developed from the Bitcoin Enlightenment era to the present, and has undergone continuous development and exploration. At present, blockchain technology is still in the stage of theoretical verification. The application of blockchain technology in the financial field is still in the exploratory stage, and many aspects still need to be improved and developed; although it is still unable to have a disruptive impact on the production relations of the financial industry, it provides a new operation plan for the trading and circulation of digital financial assets. Blockchain technology is an important driving force leading the transformation of the industry. It can undertake the conversion of new and old kinetic energy. It is an emerging technology in the national strategic plan. Its future may generate immeasurable value. As a "strategic source", the blockchain will continue to provide impetus for technology and model innovation, and from becoming an important infrastructure in the era of the new Internet, the "Internet of Value", leading the world's technological and industrial changes. Blockchain is a catalyst in the process of credible digitization. Blockchain not only accelerates the development of this process, but also promotes better financial services to the real economy, making the relationship between the two closer, and at the same time deepening Deep integration between the two.

**E-Chain Learn: A Degree Certification System Based on Blockchain**

T. Kuang, W. Zou, H. Qi and S. Zou, "E-Chain Learn: A Degree Certification System Based on Blockchain," 2022 International Conference on Blockchain Technology and Information Security (ICBCTIS), 2022, pp. 225-229, doi: 10.1109/ICBCTIS55569.2022.00058.

Abstract:

Most of the existing academic certification systems are based on the traditional B/S structure and Web technology, and most of the functions and permissions are in the central server. The data may be unreliable due to data tampering and other reasons. In response to the above problems, this article uses the advantages of blockchain in decentralization, non-tampering, and traceability to construct a blockchain credit management platform for college student archives. Combining with smart contract technology and CA certification technology, the platform provides identity verification, degree certification, and performance certification involved in college student files in decentralized security pattern.

## Introduction

Academic certification is a complex process involving students, universities, enterprises, and the Ministry of Education. Its main manifestation includes the issuance, identification, and inquiry of academic certification reports. The Education Certification Center of the Ministry of Education will issue an academic certificate after review according to the user's academic certification requirements, electronically registering the report and providing online auerv.

With rapid development, it still exists many problem in degree certification. Due to easy fraud, hard certification, and weak privacy, it becomes an increasingly common phenomenon in the world, including academic or degree fabricating.

In June 2020, according to many authoritative reports such as Sohu.com, more than 200 people in Shandong, China, entered school with imposters. Meanwhile, a number of job recruitment websites leaked job applicants' resumes for profit, like landing.zhaopin.com, liepin.com, etc.

The two major issues of “fake” and “privacy” in academic degree certification have made such a huge negative impact on society. It becomes an certain tendency to design a degree and diploma certification management system, with high reliability, simple storage, hard falsifying and strong privacy[1]. For these, we, this paper, propose a degree certification system based on blockchain to lessen the degree fraud and improve the privacy security in authentication process.

With decentralized characteristics, the blockchain realizes a distributed ledger for trusted management of data and provides a trusted authentication method that does not require a third party [2]. Therefore, in recent years, some researchers have also used the blockchain to design the certification system, among which degree certification is also a high-frequency scenario of blockchain + certification[3].

Chuntian Zhou et al. adopts a credibility measurement model related to time factors, which might avoid the tampering after generated certification, with efficiency improved. However, the employer is as a third party at the end of the authentication chain which cannot guarantee the authenticity.

In the solution given by[5], the storage structure is divided into the blockchain part and the off-chain distributed storage part. However, the security of the off-chain part is not as well as blockchain, without any privacy protection.

MIT Media Lab released a blockchain certificate project called Blockcerts, which is an open standard for digital academic certificates based on the Bitcoin blockchain. Regrettably, this project is based on the Bitcoin chain which might need amount of Bitcoin to pay off, even illegal in many countries.

The “Micro-credentials” and “openbadges” can record distributed user education data and help store electronic archives[6]. However, the blockchain only participates in the recording of data in this mode. Once needed further authenticate, other authentication nodes and contracts will also be required, that makes inefficiency being the main factor limiting the system performance.

The above research cases show that the blockchain-based certification system is becoming a trend, especially for degree certification, which is feasible, safe and efficient. The following will introduce the structure of our system.

## Degree Certification System Based on Blockchain

The overall structure of the program is divided into three parts: Based on the blockchain technology, the three underlying modules of “blockchain architecture”, “CA certification”, and “zero-knowledge proof” are designed. Through mobile client and web client, it is convenient for students and management Operators, third-party units and other nodes conduct operation management to form a complete chain.

This section will focus on technologies such as hybrid chain, CA certification, and zero-knowledge proof, and introduce the technical principles and workflow of the proposed certification system.

### A. Mixed Mode Blockchain

The “main chain + side chain” dual-chain hybrid mode is adopted, combing with the “off-chain state channel”, to design three types of blockchain channels to ensure that each transaction can be verified in the blockchain network regardless of whether it needs to participate in the verification of the blockchain network[7]. The system can words, it is not necessarily that every transaction must be verified by the main chain, and the validity can also been guaranteed.

The main chain is constructed by the consortium chain, which is jointly initiated by several organizations. Some nodes can be accessed at will, and the other part must be authorized to access. It is between the public chain and the private chain, with multiple centres or parts, giving consider to the characteristics of public and private chains. At the same time, the side chain is used to expand the blockchain on the basis of the alliance chain, to meet the needs of each node's information and reduce the pressure on the main chain[8]. The identity types of nodes on the chain are shown still certificate normally without invalid records. In other in

#### 1) Alliance Chain Node Type

The nodes in the alliance chain of this system are divided into management nodes, user nodes and private nodes[9].

* The management node is mainly the education department. The management node can write data to the underlying blockchain, update data, and also assign permissions to user nodes.
* The user node only participates in the transaction to enjoy the service, and does not participate in the update record of the underlying data. But ordinary nodes can view the data recorded on people's chains and read the corresponding transaction records.
* Private nodes refer to users who contribute private resources to join the alliance chain[10]. Users have the right to create nodes, modify the underlying data of the nodes they own, update data, etc., but do not participate in the record update of all the underlying data.

#### 2) State Channel

All nodes of the blockchain perform equivalent calculations and store equivalent data. Such a system that allows redundancy to process transactions is very slow and expensive. This article deploys small and multiple trading contracts to the state channel.

The work of the state channel is mainly off-chain interaction and on-chain clearing, avoiding small transactions on the chain, and only need to submit the final state to the chain, which reduces the workload on the chain. When both parties have no objections, the settlement can be completed quickly, realizing immediate finality. In addition, due to the off-chain transactions in the channel, faster transaction speed, lower handling fees, and better privacy can be achieved.

### B. CA Certification

Considering the shortcomings of node security and electronic certification, this article decided to introduce CA certification to ensure security and improve anti-counterfeiting performance[11].

The system adopts CA certification for:

#### 1) Third-Party Node Certification

There are many nodes that join the system, and it is difficult to ensure the officiality of the nodes. In order to prevent the nodes from malicious actions, CA certification is used to authenticate and manage third-party nodes.

#### 2) Electronic Degree Certificate Certification

Considering the many problems in the current electronic certificate authentication, the combination of CA authentication and blockchain “digital signature” is used to verify and authenticate electronic certificates to prevent electronic fraud and improve anti-counterfeiting.

The CA certification process adopts a distributed CA certification mode, and the CA certification process is operated on the chain to eliminate the risk of attacking the centralized CA ecosystem.

### C. Zero-Knowledge Proof

For a long time, a number of students' personal information on the academic degree and degree information is the main evidence for their “verification”. To maintain the validity of authentication under the premise of ensuring privacy and security, this paper adopts a zero-knowledge proof mechanism for protection. It is stipulated that “students” shall be the “providers”, and employers or other verification nodes shall be the “verifiers”.

#### 1) System Zero Knowledge Proof

After applying the zero-knowledge protocol to the system, the process is as follows:

* The student wants to send the information M to the employer. The system network acts as a trusted third party and uses the private key to generate digital signature information r and s and send it to the student.
* When the student receives the digital signature r and s, he chooses a series of random numbers, like r0,r1,…,ri∈R,Zg. ‘ starts to use his key to perform secret calculations, and then generates a zero-knowledge proof {c, d, …, s }.
* Students send zero-knowledge certificates to employers through safe tunnels {c, d, …, s }. • When the employer receives the zero-knowledge certificate, it uses the shared information p, q, g, y, M, z, b to verify whether the user student is a legitimate user. If the student is legal, the employer will establish a connection with the student for communication.

### D. Authentication Forwarding Workflow

The three-layer blockchain channel method described in this article can realize the separation of verification and query. Verification and query can be different, and the verified can be forwarded through the alliance chain to ensure the validity and achieve multiple verifications at the same time. There is also a work flow of the system application in this article, with verification as the core forwarding and auxiliary inspection methods.

## System Test

After the deployment of the blockchain at the bottom of the system, this article conducted a test based on the system's functional characteristics. The test items are as follows:

### A. Test Setup

#### • Parallel Execution Efficiency of Smart Contracts

Use multiple nodes to execute different contracts at the same time, and count the average time to execute a contract.

#### • Transaction Success Rate

Under the state channel, perform a few multiple transactions at the same time, and count the transaction success rate within a period of time.

#### • Contract Security

Use integer overflow, double- spending attack, symbolic execution, taint analysis and other methods to conduct security test attacks against smart contracts;

## Conclusion

For the first time, the model of “alliance main chain + alliance side chain + state channel” is adopted, and the characteristics of blockchain is utilized to solve the problem of degree fraud. All query verification records are locked on the main chain, and the main chain links the side chains through smart contracts to realize data decentralization and parallel processing. Using CA certification, the certificate can be verified anytime and anywhere on the basis of public trust; the zero-knowledge protocol can ensure the validity of the certification while reducing the possibility of privacy leakage.

The system proposed in this paper has strong feasibility. As a new idea and new method of certification system, it can not only inspire innovation in degree certification, but also apply to the construction and innovation of other types of certification systems.

**A Smart Contracts Repository For Top Trending Contracts**

G. Ibba, "A Smart Contracts Repository For Top Trending Contracts," 2022 IEEE/ACM 5th International Workshop on Emerging Trends in Software Engineering for Blockchain (WETSEB), 2022, pp. 17-20, doi: 10.1145/3528226.3528374.

ABSTRACT

Blockchain technology spread very quickly during the last few years and has become one of the most popular trends among the research and developers community. In particular, the Ethereum blockchain is one of the most supported and used for developing smart contracts, which are informatics protocols that provide a higher level of security than traditional contracts and reduce other transaction costs associated with the bargaining practice. Nowadays, the transaction number associated with smart contracts deploying increased widely, and it is difficult for researchers and developers to keep track of programming trends. This work proposes a dataset containing only specific categories of smart contracts associated with the most popular trends of the last five years. Mainly, the proposed collection of programs contains Token and Non-Fungible-Token programs, whose popularity has increased a lot since their first appearance on the blockchain.

1 INTRODUCTION

Smart contracts are general-purpose programs that allow secure transactions without the help of third parties and reduce costs associated with the bargaining practice. Nevertheless, developers don’t take advantage of smart contracts (in particular, we are referring to the Ethereum ones) only to build programs [13] aiming to send and collect currency. Indeed, developers exploit Ethereum smart contracts also to create games (for both gambling and skill games), certificate documents, and build tokens. These are only a few smart contracts trends; indeed, there are many other usages for these versatile programs, and sometimes contracts developement is influenced by cryptocurrencies prices [2, 4]. One recent trend is the one of Non-Fungible-Tokens [16] (NFT). The first appearance of NFTs dates back to 2014, but they became popular when Cryptokitties 1 started to spread. NFTs aim is to certify a digital asset as unique and therefore not interchangeable; for this very reason, NFTs revolutionized copyright policies, and during the last three years, their popularity widely increased. Those listed previously, clearly, are not the only smart contracts categories. During the first two years of the Ethereum lifecycle, most of the contracts were programs whose aim was to manage or distribute money [1]. Other classes and design patterns include gambling games, contracts simplifying the interaction with blockchain, and others certifying data ownership. Meanwhile, Solidity programs design patterns [11, 17] evolved, and other categories [8] of smart contracts include:

• ICO (Initial Coin Offering): programs [6] used as crowdfunding platforms. Often, these types of programs are also related to token selling.

• Crowdsale: these programs are crowdfunding platforms like ICOs, but two main differences exist. The first one is that ICO is not used only for tokens but also for other goods, while network participants usually use Crowdsales for token selling. Another significant difference is related to token selling. In comparison, ICO is selling tokens linked to the value of the business, while Crowdsale is the sale of tokens used in the industry.

• Role Playing Games: smart contracts are not used only to set up gambling games such as roulettes, card games, etc., but also to set up role playing games, where it is possible to shop items with tokens.

• Token exchange: programs used exclusively for token exchanging.

• Token burn: programs used exclusively for token burn.

Previously, it was pretty common to find contracts whose only aim was to implement libraries (like SafeMath), but nowadays, it is very unusual since developers basically include the library they need in the main contract unless they are standard and well-defined libraries like SafeMath or Oraclize. Those listed previously are not the only smart contracts design patterns and categories. The direct consequence is that it is difficult for developers and researchers to spot the programs they need for practical and statistical purposes, primarily because the number of deployed smart contracts on the Ethereum blockchain is tremendous. It could be advantageous for developers to have datasets including specific categories of smart contracts. The alternative would be retrieving contracts and performing categorizations tasks, which could be tricky. This work proposes a dataset including four types of smart contracts, which correspond to top trending design patterns.

2 STATE OF ART

There are already existing smart contracts repositories containing a significant amount of programs. For example, Smart Corpus [12] is an organized, reasoned, and up-to-date repository where developers and researchers can efficiently and systematically access Solidity source code and other metadata about Ethereum smart contracts. Smart Bugs [7] contains vulnerable smart contracts and reports the vulnerability to which the contract is exposed for a subset of samples. This last contracts collection is interesting because it counts 47.398 contracts, which is impressive in terms of samples number. Another interesting dataset is Smart Sanctuary 2 , available on Reddit and contains only Ethereum verified contracts. Another existing dataset is available on Github 3 , a repository that contains smart contracts for both Binance and Ethereum. Many researchers and developers build their datasets by collecting existing contracts and taking advantage of existing repositories, but they are often unavailable. Therefore, it is pretty sure that many other repositories already exist, but since being private, researchers can’t take advantage of them. The available repositories could be beneficial to retrieve contracts in general, but researchers and developers often look for specific contracts categories. Actually, there are no repositories organized by smart contracts category. Given the number of smart contracts available on the Ethereum blockchain and the increasing number of transactions associated with contracts deploying, it could be quite a challenging task to retrieve specific contracts categories. For this very reason, it is essential to categorize smart contracts. Also, it is helpful for statistical purposes since it helps to keep track of contracts trends during the Ethereum lifecycle.

3 RESEARCH METHODOLOGY

The following chapter presents the research methodology to build the contracts dataset. This work aims to provide a dataset for which purpose is already known. So, the first step is to retrieve a sufficient amount of Solidity programs.

3.1 Exploratory Data Analysis

We merged three already existing datasets to perform this task: Smart Bugs and Smart Corpus, counting respectively 47.398 and 1.211 contracts, and Smart Sanctuary, which at the time included around 77k contracts. After incorporating these three datasets into one, we retrieved an amount of more than 125k contracts, which is a significant number. However, by merging three different datasets, one of the possible issues would be spotting duplicates in the collection. Another problem is that sometimes source code is unavailable for some contracts, so we must ensure that some Solidity files are not empty. After removing files with no source code, joining contracts with the same address and different source code, and removing duplicates (contracts with the same address and same source code), our samples were reduced from 125k contracts to 100040. Before starting to categorize the contracts collection to keep track of trends over time, we retrieved all the deploy dates of smart contracts. Figure 1 shows the number of samples representing each year. The most represented are 2018 and 2021, and the last one, in particular, is interesting to understand the most recent trends. Nevertheless, we lack a significant sample for years such as 2017, 2019, 2020 since SmartBugs includes mainly 2018 contracts and SmartSanctuary (which is the most recent) mostly 2021 and 2020. Besides, we lack all the contracts deployed in 2015 and 2016, and we could not retrieve the deploy date for some contracts, so we dated them as ’Unknown’; hence, we aim to collect more programs to add more representativeness to our dataset for future work.

3.2 Categorization

The smart contracts categorization step is the core of the research. As said previously, no works perform a massive analysis for contract categorization in literature. There are several ways to understand the aim of a particular Solidity program. The most trivial way is to check each contract manually and understand its logic. The approach is suitable only if the sample to analyze is pretty limited, but we are dealing with more than 100k contracts, so it is not feasible to manually check all the smart contracts. A possible approach, which is also the most viable, is machine learning. Some contract categories are very similar in their structure. For example, tokens, gambling games, and bank contracts have a standard pattern to follow, and this observation could help a lot in the analysis. So, the idea is to exploit developers’ source code and comments to categorize our collection of smart contracts. In particular, we used Natural Language Processing (NLP) techniques, and since we don’t have samples for which we know priorly the category, we used unsupervised learning techniques. The chosen approach is topic modeling [15], and in particular, we decided to use the Latent Dirichlet Allocation (LDA) model [3], assuming that each topic corresponds to a smart contract category. However, we are not dealing with human language but with code, so we had to perform preprocessing considering this fundamental aspect. First, we performed our analysis by computing coherence [14] and then finding the optimal number of topics by evaluating the topic coherence. Still, we noticed that some of the resulting categories could be aggregated into others. We decided to use a semi-supervised approach, taking advantage of a seeded LDA, assigning the highest topic probability to the topic associated with specific terms. The seeded LDA approach [10] consists of setting a dictionary of seed words such to predefine topics and biasing them according to the prior knowledge of the domain. The approach provides a set of seed terms of a domain topic, associating the a priori probability distribution of the words for that topic. The idea is that if a contract contains words like ’lock,’ ’start,’ ’end,’ ’time,’ ’deposit,’ ’deposit date,’ etc., it is almost sure that the program is a bank bound with time constraints.

• Bank contracts implement a virtual bank, allowing participants to store their Ether. A user can withdraw his money at any moment. This category is strictly correlated to Ether Lock / Time Constraints.

• Bid contracts implement auctions to buy a specific good. These contracts also include ICO and Crowdsales.

• Certification and NFT (CNFT) are contracts certifying the authenticity and the ownership of a digital asset.

• Chain Management (CM) programs implement chain operations, and simplify the interaction with the blockchain.

• Ether Lock / Time Constraints (ELTC) are like Bank contracts, but users cannot retrieve their Ether at any time. They must comply with time constraints.

• Gambling are programs implementing a gambling game.

• Game category differs from Gambling, because includes skill games, role playing games, etc. These contracts provide the possibility to use tokens for shopping particular items.

• The Money Investment category includes smart contracts where a user can invest his money to earn. This category also includes Ponzi schemes [9], which are scams.

• Token contracts implement tokens and specific operations to deal with them, like exchange and burn.

• Wallet programs act like wallets, performing transactions, storing Ether, etc. Sometimes these contracts simplify the interaction with the blockchain such as Chain Management category.

• We considered the documents unrelated to any of the categories above as Unknown (for example, Hello World, nonsense operations, and useless mathematical operations programs).

For each category divided by year, highlighting that the most popular trend is undoubtedly the token design pattern. It is interesting to notice that the number of CNFT contracts increased over time. Indeed, the spreading of NFTs overlaps with the launch of Cryptokitties in November 2017. We have fewer samples of CNFT representing 2019, but this is due to the lack of contracts for that particular year. Looking at the results, we can see that other exciting categories are Bank and ELTC, which are strictly correlated as shown by Figure 4. It is fascinating to notice that the trends of Bank and ELTC contracts over time almost overlap, giving proof of the correlation between these two categories. It is also interesting how the Erthereum blockchain has been overused to design Token contracts since its early years; it would be of great interest to analyze this particular trend in 2015 and 2016, for which we lack samples. As regards CNFT, their appearance increased hugely over time, and it is the most popular trend after the Token design pattern.

4 CONCLUSION AND FUTURE WORKS

As highlighted by the analysis, the two most popular trends are the Token and CNFT design patterns, which should not be surprising since the building token was one of the main trends since Ethereum’s early years, considering that the standards carried out over time contributed to token spreading. CNFTs also include NonFungible-Tokens, whose popularity increased exponentially over time; this is also witnessed by the fact that recently companies such as Nike and Adidas started to invest in NFTs. The number of samples representing other categories such as Chain Management, Money Investment, and Wallet decreased considerably over time. It should be emphasized that in 2017 smart contracts were a relatively new technology, and there was not a complete awareness of their potential use. Hence, developing programs simplifying the interaction with the blockchain and programs whose primary purpose was to manage money (along with tokens) were the most common way to use smart contracts. The dataset, which includes the most popular trends, is available on Github 4 . We organized the dataset by year, and for each year, we provided the corresponding top trending contracts. The repository also provides a CSV file reporting address, source code, category, and date for each smart contract. Currently, only the most popular trend contracts are available because we aim to collect and categorize more samples of the other categories. One of the future works is to collect more samples representing the lacking years (like 2015 and 2016). The process of gathering more smart contracts makes this work more valuable because: It allows gaining those smart contracts for which we don’t have many samples. It increases the representativeness of the dataset. It would allow confirming our findings of smart contracts trends or spot new categories. We plan to provide the remaining categories of contracts as soon as possible. Also, we spotted several vulnerabilities which affect many of the smart contracts samples. In future work, also, we aim to provide both the category and the exposure (or exposures) related to contracts.

Reference Links:

1. <https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9569810>
2. <https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9569802>
3. <https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9759174>
4. <https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9845121>
5. <https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9823368>