A CCA-PKE Secure-Cryptosystem Resilient to Randomness Reset and Secret-Key Leakage

R G Vidhya[1], Uttamkumar chourawar[2], Indumathi. M[3], Divya.S[4], Umashree chourawar[5]
[1,2,3,4,5]*HKBK College of Engineering, Department of ECE, Bangalore – 45, Karnataka, India*

Abstract **- Organizations appear to implement blockchain solutions based on fear of missing out instead of a clear understanding of blockchain usefulness. Actually, ninety percent of current blockchain projects do not need a blockchain to meet their requirements. Therefore, we employ a Design Science Research approach to develop a framework for evaluation of blockchain implementations. The framework incorporates common factors of blockchain decisions, including blockchain innovation, blockchain design, inter- organizational integration, and implementation environment. We contribute to the scientific literature by structuring previous research efforts in a four-step framework, which provides a fruitful ground for future conceptual and empirical studies. For practitioners, the framework is useful to identify blockchain projects that facilitate purposeful blockchain adoption.**

Index Terms **- Blockchain, distributed ledger technology, Bitcoin.**

INTRODUCTION

Blockchain is an interesting technology that promises to convert agreements, processes, companies, and financial models into digital codes that are stored and distributed and shared on unalterable accounts, identified and authenticated through cryptographic signatures (Beck et al., 2016). Blockchain can redefine business and economy by relying on distributed user networks, which can change enterprise structures and affect the way businesses generate value. At least one blockchain-based innovative business is expected to reach 10 billion by 2022 and could grow to 3.1 trillion by 2030 (Farlanger & Valdes, 2017).Organizations are interested in blockchain networks to reduce costs, speed up existing processes, exchange data with partners, and generate new revenue streams. However, current blockchain applications are often driven by fear of losing rather than understanding the usefulness of blockchain (Furlonger and Valdes, 2017). Like many projects based on new technologies, blockchain projects are driven by political issues in organizations (for example, how to please a CEO) or aimed at improving the company's image. The long-term commercial value of blockchain networks is often overlooked. As a result, ninety percent of current blockchain projects either do not require blockchain to meet their needs or lead blockchain solutions that are not suitable for implementation on existing IT infrastructure (Furlonger and Valdes, 2017).Blockchain design components and business outcomes differ from traditional technologies and business models because the infrastructure, is decentralized and relies on peer-to-peer information exchange, business value is collectively created by nodes, and collaboration is needed within and between organizations. Take full advantage of technology (Beck and Miller-Bloch, 2017). In order to implement blockchains into the current ecosystem, several factors of IT infrastructure, inter-organizational governance, and social interaction must be considered together (Glaser, 2017). For example, technical blockchain limitations need to be considered in blockchain implementation. Transactions) and performance measures for various blockchain designs (Walsh et al., 2016; Xu et al., 2017). At the same time, requirements for blockchain interaction with other systems, user behavior and regulations may affect the outcome of blockchain projects (Peters, Panayi and Chapel, 2015; Schlegel, Javolokina and Schwabe, 2018). Furthermore, the interconnection between blockchain integration and nodes is not limited to a single entity but requires collaboration between entities (Friesen, Schweizer, Regner and Arbach, 2018; Olivera et al., 2018). The lack of a comprehensive framework for evaluating blockchain applications leads to confusion regarding the basic objectives of blockchain, inconsistencies between blockchain design components, failure to interact with existing IT

solutions, and future prospects for technology (Furlonger and Valdes, 2017).

In the context of this discussion, the purpose of the manuscript is to gather technical and management knowledge about blockchain and to operate it in a way that evaluates blockchain applications. We answer the research question: What are the common factors of blockchain decisions to evaluate blockchain applications and how do these factors relate to each other?

This study follows a design science research approach (Hefner, Mars, Park & Ram, 2004). To collect data, we use scientific literature that helps us access a range of blockchain evaluation factors. Building on blockchain IT tools, we organize outcome factors into a framework that evaluates blockchain applications into four semantic categories: blockchain innovation, blockchain design, inter-organizational integration, and implementation environments. We evaluate the framework by conducting interviews with experts and reviewing the implementation of the framework in the Brooklyn microgrid project (Lacity, 2018; Mengelkamp et al., 2018).

The study contributes to the scientific literature by synthesizing and mobilizing previous research efforts in the framework of evaluating blockchain applications. Moreover, the manuscript itself contributes to the structure. Entrepreneurs can use the framework to understand in advance the key factors for the success or failure of blockchain applications.

We created the manuscript as follows. We start with the blockchain background and highlight the importance of DSR in the blockchain space. Next, we define our DSR methodology. Then we introduce the developed framework. In addition, we show the application of the framework in the Brooklyn Microgrid project. Next, we discuss key findings, implications for theory and practice, limitations of our study, and areas for future research.

Blockchain Background

The blockchain Bitcoin blockchain was introduced by Satoshi Nakamoto in 2008 - a transparent, global and openly accessible shared property account that maintains a history of financial transactions between members of a decentralized peer-to-peer network (Nakamoto, 2008). Over time, other types of blockchain have emerged that differ in their approach to blockchain governance (Table 1).[1] Unauthorized public bitcoins are fully decentralized blockchains where everyone can read, write and authenticate information (Beck, Miller-Bloch and King, 2018). This blockchain is useful for applications with a large number of untrustworthy participants as there are no access restrictions and no authentication is required for authentication. Unlicensed public blockchains require proof of working consent mechanism or wager consent mechanism to obtain agreements on system updates.[2] Examples of applications are cryptocurrencies, where participants do not have to trust each other but the blockchain itself (Nakamoto, 2008). Public authorized blockchains are more centralized blockchains, where only authenticated and pre-defined users can read and write transactions. However, all nodes in the network participate in seeking consensus. Participants identify consensus mechanisms. Consortiums of entities (e.g., Ripple) are examples of publicly licensed blockchains, where predefined nodes in the network are trusted entities and interact directly with each other to support peer-to-peer transaction exchange (Walsh et al., 2016).

Licensed private blockchains are fully centralized blockchains that do not require access authentication permissions, which require additional authorization rights that are usually granted only in small numbers.[3] Nodes that are authorized to read data also need to be authorized to transmit transactions. In licensed private blockchains, many highly trusted nodes are involved in seeking consensus (for example, practical Byzantine fault tolerance) based on the provision of resources. Typically, companies use licensed private blockchains (for example, Hyper-Laser) for their implementation. A private blockchain does not apply. No apps selected

Table 1. Blockchain Types

Blockchain Types	Description	Applications
Public Permissionless Blockchains	Everyone can read, write, and validate the information. The consensus is enforced by proof-of-work or proof-of-stake. Users are usually anonymous and pseudonymous.	Cryptocurrencies (Bitcoin)
Public Permissioned Blockchains	Only authenticated and pre-defined users can read and write transactions. All nodes participate in consensus finding. Identifiable nodes determine consensus mechanisms.	Organizational consortia (Ripple, R3)
Private Permissioned Blockchains	Access authorization does not entail validation permissions, which require additional authorization rights given to several nodes. Consensus (e.g., practical Byzantine fault tolerance) is enforced by trustful nodes.	Enterprise projects (Hyperledger)

Design Science Research in the Blockchain Domain

In recent years, interest in the blockchain has grown far beyond Bitcoin. The financial and other sectors are

searching for prototypes of the blockchain proof concept. For example, blockchain prototypes for financial transactions can replace trust-based payment solutions (Beck et al., 2016). Automated execution of blockchain-based financial contracts can move from natural languages to the official languages of smart contracts (Elsman, Egelund-mu, Henglein and Ross, 2017). If the workflow is managed across institutions affiliated with a German bank, it can be run on blockchains (Fridgen, Radszuwill, Urbach, and Utz, 2018). In addition, blockchain prototypes can reduce the cost of client authentication processes and revolutionize loyalty programs (Wang, Luo, and Xu, 2018). In the public sector, blockchain prototypes aim to double tax investors in dividend payments and transfer land records from paper to the blockchain (Hyvärinen, Risius and Friis, 2017). Public health services can benefit from health care value chain audits to manage medical records on blockchain, improve critical health care, and improve patient outcomes. For the energy sector, the most researched implementation is its integration into electric vehicles and microgrids (Albrecht et al., 2018; Hua et al., 2018; Lacity, 2018; Mengelkamp et al., 2018). Logistics is exploring prototypes for transforming documents central in transportation (for example, bills of lading) into blockchains into smart contracts (Naerland, Müller-Bloch, Beck and Palmund, 2017). Other blockchain proof-of-concept concepts enable automated transactions of real-world assets such as diamonds (Notheisen, Cholewa and Shanmugam, 2017; Loebbecke, Lueneborg and Niederle, 2018). For social companies, the blockchain is the core technology of crowdfunding platforms and social networking practices (Schweizer et al., 2017; Ciriello, Beck and Thecher, 2018).

In contrast to the specific proof concept, the conceptual framework guides the integration of blockchain applications across industries and markets. The basic idea of the proposed framework focuses on several layers of blockchain technology and its environment (Glaser, 2017). For example, the blockchain market engineering approach introduces the macro elements of blockchain-based platforms and the surrounding factors (such as legal, social and economic barriers) that represent the underlying macro layers of the infrastructure (Notheisen, Hawlitschek, and Weinhardt, 2017).[4] The infrastructure layer implements blockchain protocols that define the basic elements of blockchain system design, including distributed databases . Approval mechanism and encryption protocol. The infrastructure level, in turn, influences the application logic for implementation and is the basis of microeconomic design. Based on these envisioned applications, social factors and individual user behavior in decentralized networks can be analyzed.

Other process-based tools investigate the dynamics of blockchain implementation (Beck and M ₹ ller-Bloch, 2017; Albrecht et al., 2018) or offer ways to develop blockchain use cases (Friesen, Redszuville, Rigger, and Arbach, 2018). Researching the topologies and classifications of blockchain-related concepts (such as cryptocurrencies) for market factors affected, such as the potential for restriction and competitive pressure (Kazan, Tan and Lim, 2014). Patterns and patterns of blockchain business networks formalize concepts and characteristics to describe integral parts of blockchain business models and values (Rückeshäuser, 2017; Seebacher, 2018). Management studies obtain combinations of business factors for the implementation of block chains (Lacity, 2018; Mengelkamp et al., 2018). Also, there are classifications of new events causing blockchain, for example, economics (Friesen, Schweizer, Regner & Arbach, 2018; Olivera et al., 2018). The Blockchain Economy and Decentralized Autonomous Organizations (DAOs) are of interest to various governance structures.[5]

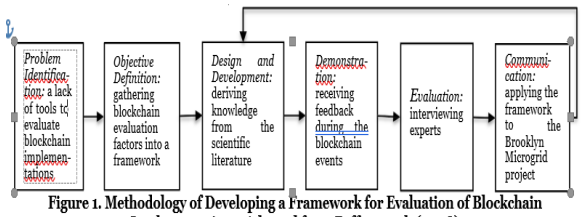


Figure 1. Methodology of Developing a Framework for Evaluation of Blockchain Implementations. Adopted from Peffers et al. (2008)

METHODOLOGY

Defining the problem The blockchain field is still in the early stages of development and is related to the lack of specific tools to guide the evaluation of blockchain applications. This results in a large number of failed blockchain applications (Labazova et al., 2019).

Objective definition. To explore the potential use of our framework, we asked experts in informal negotiations if a solution was needed. The authors

systematically participated in thematic blockchain programs to come up with solutions.

Design and development. We've redesigned and refined our solutions based on access data analysis. For data analysis, we applied open-pivot cryptography to remove the initial classification and overlapping concepts of blockchain concepts while performing conceptual redundancy testing against data (Strauss and Corbin, 1990). If available, we also coded the theoretical bases that were used to explain the interrelationships and structure of factors. Next, we grouped the factors into broad categories drawn from analysis and counted the number of documents and expert data on blockchain evaluating factors and their interrelationships (Appendix A). Interrelationships between concepts have been determined based on the semantic implications of one concept over the other found in scholarly texts from literature reviews. Correlations given in scholarly texts and interviews were encoded with descriptive information, such as text excerpts from which the interrelationships were derived. One researcher coded the resources twice in spring/summer 2018 and winter/spring 2019 for initial coding and validation of results (Strauss & Corbin, 1990). The dispute was resolved during the discussion. Finally, we translated the data into a framework for assessing blockchain implementation by literally grouping factors into four categories – blockchain innovation, blockchain design, inter-organizational integration, and implementation environment. Clusters arise from semantic similarities and are based on related artifacts (Notheisen, Hawlitschek, et al., 2017). Subsequently, the four categories are aligned with the four main evaluation steps that guide the evaluation of blockchain applications performance. We have demonstrated the framework developed during blockchain-friendly audiences at scientific conferences, consortia, and other thematic events evaluation. To evaluate our results, we conducted our first set of interviews (seven semi-structured interviews) in April and May 2018. We sought experts in a variety of fields, including computer science, finance, and the social sciences, as our results covered a wide range of aspects of blockchain. The interviews were conducted face-to-face via Skype and telephone and lasted an average of 74 minutes. The interviewees had an average of eight years of work experience and were involved in an average of three blockchain projects. We used the interview guide. We first discussed with the interviewees the appropriate factors for evaluating blockchain applications, and then presented the first versions of the developed framework. The researchers followed the framework in discussing the proposed blockchain evaluation factors and their interrelationships. The interview was transcribed and encoded using NVivo software. In all, we collected ninety-eight pages of interview transcripts.[6]

Subsequently, we modified the framework according to the interview and new literature. Therefore, we asked the same experts for feedback by phone or email on newer versions. All experts answered.

communication. We reconnected the framework developed on the basis of knowledge, demonstrating the usefulness of the framework in implementing a randomly chosen blockchain. The breaches include a generalized abstraction of the framework, which should evaluate any blockchain implementation.[7] For these purposes, we had a caption for well-known blockchain projects. The first author took a piece of paper and said: “Brooklyn microgrid” (Albrecht et al., 2018; Lacity, 2018; Mengelkamp et al., 2018). Subsequently, we examined secondary resources for the Brooklyn Microgrid Project, including the project's website, published scientific documents, and other resources. In total, we searched over 100 pages of secondary data.

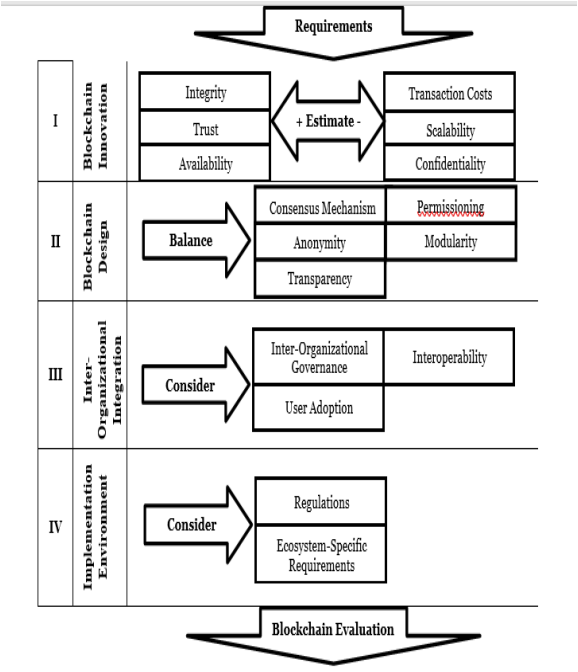


Figure 2. A Framework for Evaluation of Blockchain Implementations

BLOCKCHAIN INNOVATION

First, it is necessary to estimate the suitability of the blockchain for implementation. The suitability of a blockchain category includes six factors that represent the advantages or challenges of specific blockchain applications.

Integrity ensures that information is protected from unauthorized modifications, that is, it preserves its original state (Wüst and Gervais, 2017). Applications can take advantage of data integrity across blockchains to review the validity and demonstrate the immutability of the entire history of continuous transactions between nodes in the network (Glasser, 2017). Increased network fraud is achieved by removing any focal point of security failure and increasing the number of nodes. To attack, a malicious actor requires 51% of network power (Yli-Huumo et al., 2016), which is difficult to achieve on large networks with a large number of competing nodes. Laser immutability can support implementations that require data to be off-chain stored (for example, to verify that data remains unchanged in the cloud). However, there are many ways to deal with blockchains, for example, using arbitrage bots, which exploit the weaknesses of decentralized networks, pay higher transaction fees, and improve network latency (Daian et al., 2019).

Blockchains can provide trust in a network of selfish and potentially corrupt agents by replacing any central point of administration with cryptographic evidence (Nakamoto, 2008). Smart contracts provide additional functionality in blockchain transactions by ensuring that pre-defined agreements between users are maintained without the need for intermediaries (such as lawyers). Smart contracts can be useful in enforcing policies, for example, "launching smart contracts that prevent everyone from sharing malicious files" (I2).[8]

Availability measures the likelihood of the system becoming accessible when needed (Xu et al., 2017). In blockchain systems, availability is provided by replicating data on nodes (Wüst and Gervais, 2017) by reducing the "probability of each node closing and data disappearing" (I7). In centralized systems, there is availability This is usually achieved through replication on physical servers and backups and is an expensive solution for most applications (Wüst and Gervais, 2017).

Blockchain implementation relies on transaction costs (or fees) as tokens representing internet-based pricing (Glasser and Beisenberger, 2015) to reward contracts for processing transactions. Token commodification refers to the assignment of tokens with assets so that blockchain transactions can be used in a variety of contexts. If tokens are not used as assets, there is no common language for integrating blockchains into regulatory workflows and with other systems (I5). There are two main types of tokens that have different commodity levels: stock tokens and utility tokens. Stock symbols are in the form of coins (for example, Bitcoin) and are aimed at higher commodities. Utility tokens are not converted into cash and represent more specific assets (for example, company stock). Since blockchains operate on closed networks (Glasser, 2017), tokens are subject to cost fluctuations because the markets for tokens (such as cryptocurrencies) can change rapidly and dramatically. Additionally, one should be able to withdraw tokens from the system.[9]

Scalability refers to the ability of the blockchain to handle increasing workloads. The size of the blockchain network must be scalable enough to meet the requirements of the execution environment. For example, the blockchain for electronic medical records should be scaled to allow all stakeholders to participate in the blockchain-based information exchange. Throughput is the number of transactions that can be successfully delivered and validated during a given period of time in the network (Yli-Huumo et al., 2016). When the frequency of transactions on the blockchain increases, the throughput of the blockchain network should be able to validate the submitted transactions with minimal latency.[10] Transaction size represents the amount of data stored in a single transaction. The number of transactions contained in each block is limited by the bandwidth of the nodes participating in the network (for example, the bandwidth of each bitcoin block is 1 megabyte) and the specific block size (for bitcoin, on average 500 transactions per block) (Xu et al.). Al, 2017). The delay is the time between sending a transaction to the blockchain and the secure integration after a certain number of blocks. For Bitcoin, the response time is close to 1 hour with a block interval of 10 minutes and 6 blocks after confirmation; For Ethereum, this is close to three minutes with a 14-second block interval and confirmation after 12 minutes (Xu et al., 2017).

Privacy is defined as protecting information from unnecessary disclosures. Data encryption provides privacy in block chains. For example, on the Bitcoin network, all transactions will be publicly visible and user privacy may be compromised. However, Monero and Zcash use advanced encryption architectures to protect users' privacy.

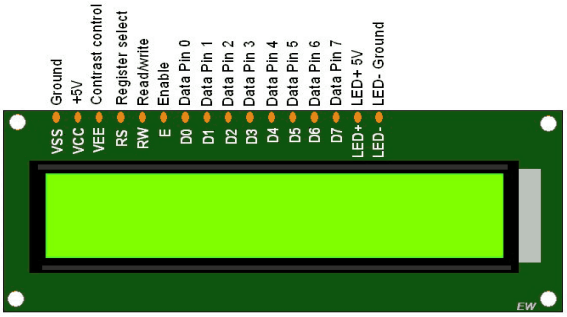


Figure 3 : Schematic View of LCD

Blockchain Design

Blockchain designs are aimed at minimizing losses and maximizing the benefits of the blockchain in accordance with the project's requirements. The first and most important factor is the approval mechanism that ensures that only valid and unique transactions are added to the blockchain (Walsh et al., 2016). There are three main consensus mechanisms. Proof of work requires resources from me (eg processing time) to produce relatively solid data. (delegated) Proof-of-Stack distributes the ability to create new blocks based on user participation in the system. Practical Byzantine fault tolerance combines individual decisions made by trusted nodes in a network that together define system-wide agreements. “This consensus part is the hardest part when designing a blockchain because it will affect everything. You make key decisions about the consensus mechanism here, and it’s hard to change them later. The right choice of consensus is to move from thinking about design to thinking about implementation.”.

The anonymity of users determines the accuracy with which users can be matched against certain identities. For example, users are anonymous in the case of Bitcoin and anonymous in the case of Zcash, while users are often identified on business blockchain networks (for example, hyperlaser). Anonymity of users is considered according to project requirements. "If you're thinking of existing blockchains for clinical data, they prefer anonymity. But if you're thinking of a pharmaceutical company, you need to de-identify the users at some point" (I2).Transparency represents the accessibility of block chain information or data (Yli-Huumo et al., 2016). The transparency of blockchain networks gives end users a degree of control over the programs they run. In some scenarios, the processors in question may act as a black box and may not reveal how they reached specific results(for example, Oracle):

The results are published in series. However, this goes against the basic understanding of how the blockchain works. Transaction transparency represents the degree of openness of data in block chains. There are no restrictions on reading blockchain data on a public blockchain; Private blockchains restrict virtual users' access to blockchain data (Walsh et al., 2016). If the transparency of the transaction is public, anyone can retrieve the transaction history and retrieve sensitive information (Walsh et al., 2016). For shared economies, for example, transparency can predict signals and thus predict economies; “For medical records, transparency is harmful because one must first follow the law” (I2).

The permission determines whether all users can participate in the network or whether participation in a small community is limited. Permitted blockchains restrict the processing of transactions on pre-selected nodes, while unauthorized blockchains do not restrict the identification of authentication nodes (Walsh et al., 2016). As for implementation, the differences emerge when solutions target external communication with customers (eg online services) or when the blockchain is used to manage inter-organizational processes (eg supply chain management).

Blockchain modularity may be required to separate different types of transactions stored in the blockchain to reduce system complexity or improve scalability. Side chains allow assets to be moved between multiple block chains. This allows users to access new systems using assets they already own (Xu et al., 2017). By reusing assets, these systems can interact with each other to avoid lack of liquidity and market volatility. Some data should not be stored in block chains and chain decisions should be made during the project. To support off-chain decisions, other storage systems (eg interplanetary file systems) are required. For mobile devices, the concept of light nodes can be considered versus full nodes. Full nodes copy the entire transaction history and this history must be downloaded. Lightweight nodes authenticate

transactions using simple payment authentication methods that just download the headers of all blocks in the blockchain. Full nodes support lightweight nodes by allowing and transmitting transactions across the network and by notifying light nodes when a transaction is affected.

Fig 4: Piezo Buzzer

Integration Between Organizations

Cross-organizational governance assesses whether blockchain capabilities enhance competitiveness between organizations (Beck et al., 2018). The vision, strategy, and tactics may differ or be affected by the blockchain due to its nature between organizations. For example, open source strategies must provide universal access to development rights. The value of the trade depends on the specific use case. Other project-specific features (such as project size) may affect blockchain adoption. It is necessary to consider the transfer costs arising from blockchain adoption. However, these research guidelines are still in their infancy and should focus on how governance differs or is affected by other IT solutions versus blockchain. User interactions are at the heart of blockchain, and users need to be careful about blockchain adoption. "I believe that organizational influence is simply the social structure of people, which produces value" (I1). User acceptance is driven by ignorance of the hype and technical knowledge surrounding blockchain and the implications of blockchain. "In the future, people will start to realize that blockchain was a good idea for some things, but also a very bad idea for everything else, like Facebook" (I1). A user's dependence on a blockchain may depend on utility (the quality of ease of use to effectively accomplish a specific task), which is currently an issue with the blockchain. For example, Bitcoin API is difficult to use in development services (Yli-Huumo et al., 2016). Acceptance of technology and related combinations, such as ease of use and usefulness, and cultural and age differences, as well as concepts from the broader acceptance literature, such as technology acceptance theory and integrated technology acceptance theory, can provide additional insights for assessing user adoption. An important question is whether current theories about user adoption will hold up to blockchain technologies as well.

Interoperability is defined as the interoperability between block chains, and the interoperability of the block chain with other systems. The interactions between block chains are related to the interaction of tokens. Blockchain platforms (such as Ethereum) that use their own currency make it difficult to interact with other platforms. If someone is on the blockchain network and uses their tokens, it increases the value of the tokens. "The worst thing that can happen in five years is to use Ethereum only because the whole point of the blockchain is not a single pivot point and that is the reason for failure" (I2). Interactions between blockchains and other systems should come naturally when they adhere to data standards.

Implementation Environment

The blockchain must comply with regulations and other requirements in the implementation environment. Blockchain compliance with current regulations is the biggest hurdle. Data standards have not been proposed to deal with blockchains. "I think governments and regulators, in general, are far behind in terms of data in blockchain and data market-driven economies" (I2). One of the problems with block chains is that they have a cipher layer that can allow for ambiguity in the actions that occur in block chains. Only a handful of governments have enforced blockchain rules, for example, in Singapore, China, Japan and South Korea. The requirements for an ecosystem can vary in the suitability of the blockchain to the market and industry. Ecosystem self-sufficiency depicts closed systems where the exchange of values occurs without external interactions (Glaser, 2017). Achieving a high degree of ecosystem self-reliance requires the support of customers and value providers within the ecosystem. Institutionalization involves the extent to which blockchains are integrated into social structures, for example, those of issue value (for example, central banks or community currency issuers). "In some cases, you need to have a locked

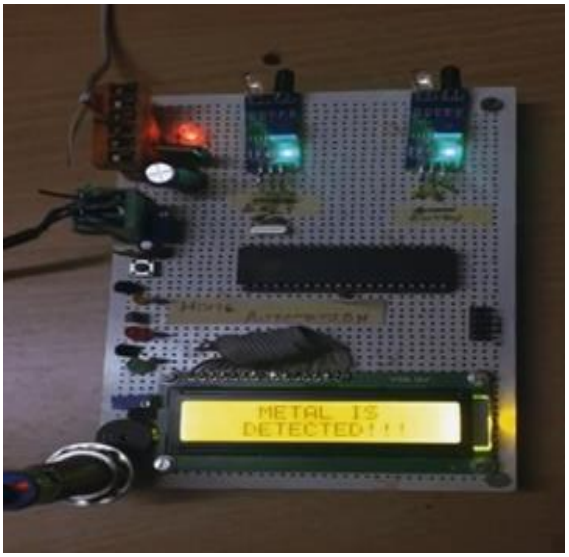
blockchain, for example, Fedcoin, if federal states decide to start their own currencies to bypass banks and waive certain taxes" (I2). Other economic constraints, including the potential for industry disruption or distribution of market power, and competitive pressures, can be considered along with related principles (for example, principles of competition and market performance) to further inform blockchain.

METAL DETECTION

Selected interrelationships between factors

Developers and blockchain integrators also need to consider the interrelationships between factors when evaluating blockchain applications. We found 48 correlations between factors, however, we only discussed the mentioned factors more than twice. In general, trade-offs between all factors must be specifically considered for each implementation.Consent mechanism and modularity Integrity and scalability: Consensus mechanisms are closely related to issues of integrity and scalability, and trade-offs are required. Different approval mechanisms have different delays related to transaction confirmations (Walsh et al., 2016) and need to manage the speed of transactions according to appropriate integrity levels (Risius and Spohrer, 2017; Xu et al., 2017). Blockchains are not suitable for high-frequency transactions but ensure high data integrity when using Proof of Work as an approval mechanism (Albrecht et al., 2018). However, blockchains with consensus mechanisms such as proof of stake and practical Byzantine fault tolerance achieve higher scalability but are less secure against unauthorized modifications to data. The use of multiple connected block chains improves scalability (for example, hashing). Many chains are used for specific tasks and types of transactions, as all chains are linked to the main blockchain. These multiple chains can build a blockchain ecosystem based on the main blockchain to reduce transaction load on the main chain (Xu et al., 2017). However, "If we keep more data on the string, the integrity of the data will increase"

Approval Mechanism Transparency of Permission Anonymity: There are trade-offs between these four factors for blockchain design. While 96% of unlicensed blockchains use Proof of Work or Proof of Stake approval mechanisms (Salviotti, Rossi, & Abitmarco, 2018), licensed blockchains typically use lightweight approval mechanisms, for example, the Byzantine Practical Fault Tolerance and Recovery 2017; Salvioti et al., 2018). On public and unauthorized networks, users act anonymously or anonymously, while on authorized and private networks all users are identified (Notheisen, Hawlitschek, et al., 2017; Salviotti et al., 2018). All transactions on unauthorized blockchains can be viewed in public, which creates complete network transparency; Permissible blockchain can sacrifice information transparency (Riccius and Spohr, 2017; Albrecht et al., 2018).



User adoption Confidentiality, integrity, transaction cost, and scalability: Fear of being able to identify in a fully transparent network and being associated with a transaction prevents users from adopting blockchains. Information about blockchain integrity violations (for example, financial losses) can prevent an eclipse from happening because in most cases people "believe themselves in the blockchain" (i5) without understanding the technical work. Integrity-related issues can also be mediated through cultural or age-related differences (Riccius and Spohrer, 2017). If data integrity is not strong, people will be less inclined to adopt blockchains, "if they are secure it will increase user acceptance".

DISCUSSIONS

The blockchain implementation assessment framework includes important things to consider before starting blockchain projects. The factors are grouped into four semantic categories in blockchain

suitability, blockchain design, integration between organizations, and implementation environment. First, the benefits of blockchain implementation - integrity, reliability, and availability - and challenges - transaction costs, scalability, and confidentiality - and inconsistencies with project requirements must be weighed. Second, the five blockchain design components — approval mechanism, anonymization, transparency, authorization, and modularity — can be combined into different blockchain designs to maximize benefits and minimize challenges. Third, blockchain-based systems must be integrated into organizational processes, which requires governance, user adoption, and the interaction between the blockchain and other information systems. Fourth, the blockchain must be compatible with its implementation environment, including compliance with regulations and other requirements specific to the ecosystem (for example, competitive pressures).

This research contributes in four ways based on scientific knowledge. Previously, previous research on blockchain suggested computer science (Glasser and Beisenberger, 2015; Walsh et al., 2016), user-related and enterprise-related factors (Glaser, 2017; Salvioti et al., 2018) but less. Yes. Consider their mutual influence. Our study complements previous research by providing clear concepts of specific blockchain evaluating factors and their interrelationships. The determinants bridge the gap between existing research centered on technology and centered around regulation in block chains and serve as the basis for further synthesis of findings. Second, we have proposed an integrated framework for evaluating blockchain implementation. The framework brings together expert insights on the development and implementation of blockchain-based systems in regulatory and environmental contexts. Third, an overview of current research can accelerate future conceptual studies in blockchain adoption across different industries (for example, case studies, expert interviews, Delphi studies) that can identify new interrelationships between factors not addressed in the current literature. Fourth, further analysis.Theoretical and empirical results in various industries will allow the development of blockchain performance and measurement indicators, which will be useful in reducing the prevailing uncertainty about the commercial value of the blockchain.

Our research contributes to practice by providing a detailed set of factors that may influence implementation outcomes. We have proposed an integrated framework for evaluating blockchain applications that is useful for practitioners to gain knowledge about key factors before starting projects. For example, our manuscript highlights blockchain designs other than the widely known public blockchain, which are useful if a public blockchain is impossible. For many projects, companies should consider implementing private blockchains that store information more predictably and confidentially than public blockchains. Private blockchains lose the advantages of fully decentralized networks; However, they keep updated data with an unchanging history of changes available to all network members. In addition, the framework can support project management by providing project teams with the necessary expertise and insights into objective KPIs for blockchain projects.

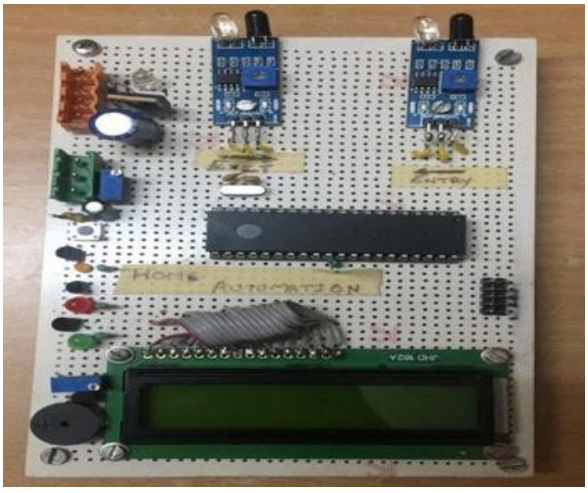
This study is not without limitations. First, we focus on the blockchain as a type of distributed account where a persistent transaction history is kept in blocks. Other types of distributed computations, for example, directed non-periodic graphs (IOTA) are beyond the scope of the manuscript. Second, we don't go into the technical details of blockchain factors. For example, our discussion of honesty can go into more detail about encryption algorithms. Cryptographic algorithms must also be exchanged or strengthened with increased processing power once attackers or exploits are detected. However, this seems appropriate because our goal was to provide an overview of the factors that can guide projects that take into account blockchain users. Future research may duplicate our research approach with more scientific or industrial data to refute or disprove our findings. Identification of additional blockchain evaluation factors expands the use of the developed framework. In addition, future research can expand the proposed concepts for specific industries, markets, and countries. Studies in different industry contexts will allow the development of appropriate measurement and performance indicators for blockchain systems. This, in turn, will reduce the current uncertainty

CONCLUSION

Blockchain is an emerging technology that is unlikely to be widely used. Currently, knowledge of blockchain varies greatly, which hinders the integration of blockchain-based systems into organizations. Our work integrates research into the technical, cross-organizational, and environmental perspectives of blockchain as a framework for evaluating blockchain implementation. The framework considers blockchain assessment factors grouped into four categories: blockchain suitability, blockchain design, cross-organizational integration, and implementation environment. This research contributes to the foundation of scientific knowledge by compiling information on blockchain evaluating factors and highlighting their interrelationships. It complements the blockchain classification and blockchain integration framework, i.e. the scientific literature on DSR in the blockchain field. Overall, the Blockchain Applications Evaluation Framework captures the current state of knowledge in aspects of blockchain and their interrelationships; At the same time, it serves as the basis for future theoretical and empirical research on how to integrate blockchain into industries and markets.

ACKNOWLEDGEMENT

We would like to thank Alexander Hervix (University of Cologne), Tobias Dilling (Karlsruhe Institute of Technology), Nicholas Käneser (Karlsruhe Institute of Technology), Benedict Nothiesen (Texas), and Karlsruhe Institute of Technology. Ali Sunyaf (Karlsruhe Institute of Technology) for helpful comments on previous editions of this work.



REFERENCE

[1] D. Kornack and P. Rakic, “Cell Proliferation without Neurogenesis in Adult Primate Neocortex,” Science, vol. 294, Dec. 2001, pp. 2127-2130, doi:10.1126/science.1065467.

[2] M. Young, The Technical Writer’s Handbook. Mill Valley, CA: University Science, 1989.

[3] R. Nicole, “Tally Stick retrieved from http://www.edubilla.com/invention/tally-stick.

[4] Heath, S. (2003), Embedded systems design, Second Edition, Burlington: Newnes.

[5] D.Saravanan, J.Surendiran,”A new framework for video data retrieval using hierarchical clustering technique”, International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249 – 8958, Volume-8, Issue-6S3, September 2019.

[6] D.Saravanan, J.Surendiran .”Video Data Retrieval using Image Color Histogram Technique”, International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249 – 8958, Volume-8 Issue-6S3, September 2019

[7] S. P. Anandaraj, N. Kirubakaran, S. Ramesh, J. Surendiran,”Efficient Way to Detect Bone Cancer using Image Segmentation”, International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249 – 8958, Volume-8, Issue-6S3, September 2019

[8] U. Satheeshwaran, N. Sreekanth, J.Surendiran,”X-RAY CT Reconstruction by using Spatially Non-Homogeneous ICD Optimization”, International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249 – 8958, Volume-8, Issue-6S3, September 2019

[9] R.G.Vidhya, R. Saravanan, K.Rajalakshmi (2020), ‘Mitosis Detectionfor Breast Cancer Grading’, International Journal of Advanced Science and Technology. Vol.29, No. 3, pp. 4478-4485.

[10] M.Niranjana Priyadharshini, S.Sathyadevi, R.G.vidhya (2018), ‘Unit Selection based Speech Synthesis using Consonant-Vowel Units’, Jour of Adv Research in Dynamical & Control Systems, Vol. 10, No.09, pp. 2708-2712(scopus).