Evaluating Suitability of Applying Blockchain

Sin Kuang Lo
University of Malaya
Kuala Lumpur, Malaysia
dnllo36@gmail.com

Xiwei Xu
Data61, CSIRO
Sydney, Australia
Xiwei.Xu@data61.csiro.au

Yin Kia Chiam
Faculty of *Computer Science and Information Technology, University of Malaya*
Kuala Lumpur, Malaysia
yinkia@um.edu.my

Qinghua Lu
China University of Petroleum(East China)
Beijing, China
qinghualu@upc.edu.cn

***Abstract*—Blockchain is an emerging technology for decentralized and transactional data sharing across a large network of untrusted participants. It enables new forms of distributed software architectures, where agreement on shared states can be established without trusting a central integration point. As a database and computational platform, blockchain has both advantages and disadvantages compared with conventional techniques. Blockchain may be an appropriate choice for some use cases while conventional technologies will be more appropriate for other use cases. A major difficulty for practitioners to decide whether or not to use blockchain is that limited product data or reliable technology evaluation available to assess the suitability of blockchains. In this paper, we propose an evaluation framework that comprises a list of criteria and a typical process for practitioners to assess the suitability of applying blockchain using these criteria based on the characteristics of the use cases. We then use several existing industrial trails to evaluate the feasibility of our framework.**

***Keywords*—blockchain, suitability, evaluation**

I. INTRODUCTION

Blockchain is the technology behind Bitcoin [1], which provides an append-only data store of transactions replicated between peers and enables new forms of distributed software architectures, where agreement on shared state for decentralised and transactional data can be established across a large network of untrusted participants.

Blockchain has unique properties. When data is contained in a committed transaction on the blockchain, it eventually becomes *immutable* in practice. The immutable chain of cryptographically-signed historical transactions provides *non-repudiation* of the stored data. Cryptographic tools also support data *integrity*, the public access to blockchain provides data *transparency*, and *equal rights* allow every participant the same ability to access and manipulate the blockchain. *Trust* in the blockchain is achieved from the interactions between nodes within the network. The participants of blockchain network rely on the blockchain network itself rather than relying on trusted third-party to facilitate transactions, which has the power to control and manipulate the system and is a single point of failure.

Applications built on blockchains can take advantage of these properties of the blockchain. Many banks are involved in trials of blockchain technology, including through the global R3 consortium[1] which is applying blockchain to trade finance and cross-border payments. Financial transactions are the first, but not the only use case being investigated for blockchain technology. A blockchain implements a distributed ledger, which can verify and store any kind of transactions, in general [2]. Many startups, enterprises, and governments [3] are exploring blockchain applications in areas as diverse as supply chain, electronic health records, voting, energy supply, ownership management, identity management, and protecting critical civil infrastructure.

Data privacy and *scalability* are two points of criticism of blockchain. The privacy setting is limited since there are no privileged users, and every participant can join the network to access all the information on the blockchain. For throughput scalability, mainstream public blockchains to date can only handle on average 3-20 transactions per second[2], whereas mainstream payment services, like VISA, can handle an average of 1,700 transactions per second[3].Thus, blockchains cannot by themselves meet the requirements for all usage scenarios, for example, applications that require real-time processing or used within a single organizational unit. Gartner estimated that 90% of enterprise blockchain projects launched in 2015 would fail within 18 to 24 months [4].

In practice, there is a gap where no proper evident-based guideline that could be used to evaluate the suitability of blockchain use cases. Hence, this paper provides insights on the trade-offs on non-functional requirements when implementing blockchain-based applications and develops a blockchain suitability evaluation framework based on a list of criteria. Several industrial trails are selected to validate the suitability of blockchain using our evaluation framework.

II. SUITABILITY EVALUATION FRAMEWORK

The first step of architecting a blockchain-based application is to assess the suitability of applying blockchain against the requirements of use cases. Fig. 1 shows the framework proposed based on existing industrial products, technical forums, academic literature and our own experience of using blockchains and developing prototypes. The process to evaluate the suitability of blockchain comprises mainly seven questions that need to be answered, which are denoted as white

[1] http://www.r3cev.com/

[2] https://blog.ethereum.org/2016/01/15/privacy-on-the-blockchain/

[3] https://usa.visa.com/run-your-business/small-business-tools/retail.html

978-1-5386-2431-9/17 $31.00 © 2017 IEEE
DOI 10.1109/ICECCS.2017.26

decision nodes. The subquestions derived from the main questions are denoted as grey decision nodes.

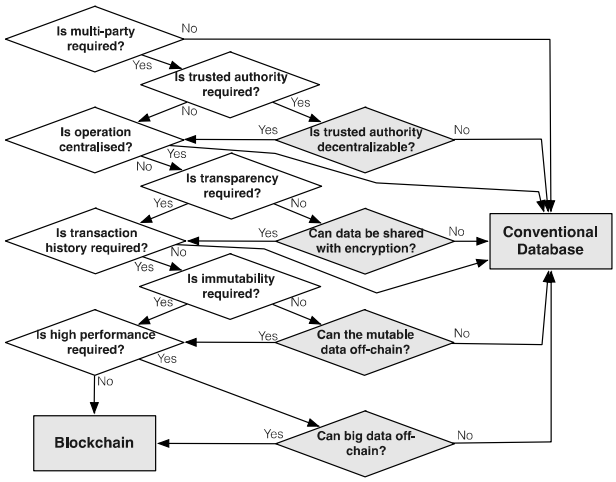

Fig. 1. Suitability evaluation framework.

A. Multi-party

The first question is whether multiple parties are involved in the scenario. The operations or transactions between parties are normally governed by intermediaries. Supply chain is one of the examples as it consists of complex, dynamic, multi-party arrangements with regulatory and logistical constraints spanning across different jurisdictional boundaries. Blockchain provides a shared infrastructure with a neutral stand where none of the participated organization dictates it. Thus, blockchain is suitable for scenarios involving multiple parties, potentially where there are intermediaries acting within the current systems. It would break down the silos of information controlled by individual parties while at the same time make the process faster and cheaper. A system within a single entity can use other relatively cheaper mechanisms to achieve the same properties provided by blockchains.

B. Trusted authority

The second question is whether a trusted authority is required in the scenario. Trusted authority is an entity that is authorized to execute a certain operation or alter a policy or configuration of an operation. Examples of the trusted authorities would be the bank and government. The issue arises from having a trusted authority is that it may become a single point of failure. When the trusted authority experiences problems, all the users accessing the services from it would be affected. Blockchain is suitable for scenarios without any trusted authority or the current trusted authority has potential to be decentralized. Using a blockchain does not remove trust because users are still exposed to risk in their use of blockchain technology. Users are shifting their trust from the third-party intermediaries or central governing organization to the blockchain software, the incentive that motivates "good behavior" of the processing nodes, and the trusted third parties that act as "oracles" which record information about the external world on the blockchain. Blockchain removes the need to trust a single specific third party to maintain the ledger of a transaction, and so is sometimes called a "distributed trust".

C. Centralized operation

The third question is whether the operations on the application is centralized. In blockchain-based systems that use smart contracts, system operation is harder to implement for the smart contracts than regular distributed systems. This is because smart contracts comprise code that regulates the interactions between mutually untrusting parties; trust is derived from the fact that the code cannot be changed easily. By implementing the blockchain-based system, no single party controls the system but every single user is in control of their own data and assets, which inherently creates challenges for governance. The management of the evolution of blockchain-based systems is more like diplomacy than traditional risk management or conventional product management. Hence, the current configuration of blockchain is not suitable for a system that requires centralized operation.

D. Data transparency vs confidentiality

The fourth question is whether data transparency or confidentiality is required. Blockchain provides a neutral platform where all participants can see the published data. With all the published information, transactions can be validated by all processing nodes. In a cryptocurrency blockchain, miners can use the public data to check if a sender account has enough value to process a transaction. In a blockchain running smart contract, miners are able to check any conditions that could be programmed as smart contracts. Encrypting data before storing it on a blockchain may increase confidentiality, but may reduce performance, transparency or independent auditability. Storing only a hash of data on-chain and keeping the raw data off-chain improve confidentiality and performance, but partly undermines the distinctive benefit of blockchains in providing distributed trust. Greater transparency is in tension with commercial confidentiality, even if pseudonyms are used, and even if encryption is used. Consortium and private blockchains can provide read access controls, but this does not provide commercial confidentiality between competitors on a consortium blockchain. The main trade-off is between the benefits of sharing data within the group of collaborators (visibility) and retaining confidentiality towards competitors where needed.

E. Data integrity

The fifth question is whether the integrity of transaction history is required. Data integrity in the historical transactions is key for creating provenance, which can be used to track physical assets through changes in ownership and handling. Using blockchain to achieve integrity may be relatively expensive compared to other persistence mechanisms. There are existing mechanisms available to prove the origin of data, like hashing technology, and to cryptographically sign data. An architecture with existing tracking mechanism may not benefit from the provenance information added by using a blockchain.

F. Data immutability

The sixth question is whether data immutability is required. In economies where third-party service providers are not always trustworthy, a significant benefit of blockchain systems may be in a strong support that they can provide for immutability and non-repudiation. The linking of blocks in a

chain of cryptographic hashes supports a kind of immutability for historical transactions. In practice, data on blockchain cannot be changed easily because it is continually replicated across many different locations and organizations; attempts to change it in one location will be interpreted as an attack on integrity by other participants, and is rejected. This is normally a good thing but can cause problems. In real world blockchain systems, problems may arise such as disputed transactions, incorrect addresses, exposure or loss of private keys, data-entry errors, unexpected changes to assets tokenized on the blockchain or if a court orders illegal content to be removed from the blockchain. The concerns around the historical transactions need to be considered during the system design. The immutability of blockchain ledgers may make them less adaptable than conventional technologies controlled by trusted third party organizations that support rollback.

G. *High performance*

The seventh question is whether high performance is required. While blockchains are currently not highly scalable, this is not necessarily an inherent limitation, and may be overcome in near future. Consortium and private blockchains with careful design and performance tuning have much better performance compared with public blockchain. Blockchain is not suitable for storing Big Data due to large volumes of data and high velocity data. This is an inherent limitation of blockchains, because of the massive redundancy from a large number of processing nodes holding a full copy of the distributed ledger. The current workaround is to store the large amount of data off-chain to avoid duplication of the data to all the connected peers.

III. USE CASE EVALUATION

We have created an evaluation framework based on our investigation for the Australian government on the use of blockchains in various use cases, and our experience from implementing proof-of-concept blockchain-based systems [13]. We used the proposed evaluation framework to evaluate four of the industrial blockchain trails to assess the suitability of using blockchain for those use cases. Table 1 gives the summary of the evaluation results based on the seven questions (A - G) from the framework which are discussed in Section II.

TABLE I. RESULT OF SUITABILITY EVALUATION

	Supply chain	**Electronic health records**	**Identity**	**Stock Market**
A	Required	Required	Required	Required
B	Not required	Decentralized	Not required	Not required
C	Not required	Not required	Not required	Not required
D	Transparent	Confidential	Transparent	Confidential
E	Required	Required	Required	Required
F	Required	Required	Required	Required
G	Not required	Not required	Not required	Required
Result	**Blockchain**	**Database**	**Blockchain**	**Database**

A. *Use case 1: Supply chain*

Supply chain is the connection of all the processes involved in creating and distributing goods, from raw material to completed products and to consumers in the end. According to Deloitte survey, 42% of the companies in consumer goods and manufacturing plan to spend at least $5 million on blockchain technology in 2017 [5]. Walmart tested blockchain technology for their supply chain management. Their pilot project that started on the first quarter of 2017 on tracking the pork in China and in U.S [5].

Supply chain is one of the most complex multi-party systems that span across different participants such as farmers, production factories, retailers. Current trusted parties can be decentralized among all participants. The operations are distributed and come from all participated organizations. Data transparency is desired because other participants need to know what step or sequence the transferred item reach to react or be prepared for their part. Transaction history and data immutability are desired, which enables tracing back the origin of the transferred commodity and auditing the condition of the item. Current supply chain systems, especially the ones that use paper-based documents, are not being updated in real time. A short delay is allowed in this circumstance hence blockchain performance issue can be neglected in supply chain. Supply chain is a promising area for blockchain-based applications [11], as it will benefit from digital nature of blockchain while not affected by its current limitations.

B. *Use Case 2: Electronic Health Records(EHRs)*

Electronic Health Records (EHRs) contain collections of patient medical records. It contains clinical related data such as the blood type, vital signs past medical records, medications and radiology report of a patient [6], which is maintained by specific healthcare providers over the time. Most of the existing EHRs are normally silos systems which are not connected to other EHRs. MedRec is an initiative to explore on blockchain architecture in contributing to secure and interoperable EHRs systems [7].

Multiple parties from different medical jurisdictions and patients are involved in the data exchange to allow efficient health care and research. The decentralized healthcare providers are the trusted authority where they have access to the patient's data and the authority to make the changes on patients' data. The main operation of the EHRs is also distributed across different health care centers. Data transparency remains one of the main issues in existing EHRs. In MedRec, the patients' data is still up to the patients whether or not to allow their data to be published across other EHRs in the blockchain. If all patients choose not to transfer their data, interoperability between EHRs can never be achieved. EHRs contains one's very important health data that are not supposed to be modifiable without properly reviewed by a doctor or healthcare expert. Besides, history of the changes serves the audit purpose. In regards to the requirement of a high performance system, EHRs does not need real time data update, hence the current performance limitation of blockchain does not affect the operation of an EHR. MedRec stores a pointer to patients' data in the blockchain and allow patients to choose when and who to share their data [7]. Current blockchain initiative serves as a bridging technology to connect EHRs. Blockchain could be used as the native storage for EHR when patients are willing to give up their data privacy in the future.

C. *Use Case 3: Identity* Management

Identity management drives every single business and social interaction. There is a vast area of identity applications such as passport, wedding certificates and online login account. Blockchain has been used to manage the identity of an individual in term of authorization, authentication, user role and privileges within or across an enterprise system [8] [9].

Identity Management System (IDM) manages all user identity within the enterprise system. All the operations of the existing system are centralized and being managed by a trusted authority. The authority sets permission and role to users to ensure they only access to the parts of the system that are relevant to them. Blockchain allows the roles, permission and privilege of users are being verified by the distributed peers connected to the same network, which removes the need of having a centralized admin and avoiding to have all operation centralized at one place. Data on blockchain is transparent to everyone on the network by default. The immutable transaction history is duplicated to all connected peers. A transparent IDMs ensure all users of a certain enterprise system behave as intended following the permission and role being set. Immutable IDMs with all the history will ensure all the role and authorization will not be altered without authorization. Despite the fact that current blockchain performance does not match up with the existing systems, it is still viable to implement IDMs on blockchain because performance will not affect the standard operation of IDMs. IDMs are suitable to be implemented on blockchain because it can make sure of all benefits from digital nature of blockchain while not being affected by its current limitations.

D. *Use Case 4: Stock market*

Stock market is a place where trading of stocks, bonds and securities happen. It involves complex procedures that can be time-consuming, expensive, and prone to risk [10].

Stock market system is a complex system that involves multiple entities and currently being controlled and maintained by a centralized registrar. Blockchain technology allows trades to be settled by peer confirmation, removing the need for centralized operation and centralized authority to verify trades. Data transparency, however, is an issue in the context of the stock market. All investors and market participants are exposed to the public as the trading identity is openly shared to the public. This could be a disadvantage to the investor. For example, a super fund sells a large position on a gradual basis for a long period [10]. Transaction history is important because it keeps track of the ownerships of shares and also any changes that happen. Data Immutability is also crucial as it ensures that all successful transactions cannot be tampered by anyone. Looking at the scalability of existing stock exchange, blockchain technology might not be suitable for this use case until the performance of blockchain can match up with the current legacy system. Currently, blockchain is not suitable for high volume stock trading in general, not until the scalability and privacy issue resolve. But there are some blockchain solutions in stock exchange domain have been explored and used in big stock exchanges. Nasdaq with its Nasdaq Linq blockchain ledger managed to reduce settlement time and potentially expediting trade clearing [11]. ASX is also exploring blockchain to replace their current Clearing House Electronic Subregister System, on core modules such as trade registration and settlement process [12].

IV. Conclusion

In this paper, we proposed a suitability evaluation framework based on considerations to be made before implementing blockchain-based applications. The framework is important and useful as a starter guide for organizations to examine the suitability of blockchain based on the intended use case. By evaluating four different industrial trails using blockchain technology, we found that supply chain and identity management would benefit from using blockchain while EHRs and stock market is not suitable yet due to the nature or limitation of blockchain. This framework would serve as a guide for practitioners that plan to apply blockchain and help to reduce the waste of effort on the unviable use case.

References

[1] S. Nakamoto. Bitcoin: A Peer-to-Peer electronic cash system, 2008.

[2] F. Tschorsch and B. Scheuermann. Bitcoin and beyond: A technical survey on decentralized digital currencies. IEEE Communications Surveys & Tutorials, 18(3):464, 2016.

[3] Distributed ledger technology: beyond blockchain. Technical report, 2016. UK Government Chief Scientific Adviser.

[4] S. Omohundro. Cryptocurrencies, smart contracts, and artificial intelligence. AI Matters, 1(2):19–21, Dec. 2014.

[5] Kharif, O. Wal-Mart Tackles Food Safety With Trial of Blockchain. [Online]. Available at: https://www.bloomberg.com/news/articles/2016-11-18/wal-mart-tackles-food-safety-with-test-of-blockchain-technology [Accessed 2017 May 24]

[6] Cms.gov. Electronic Health Records - Centers for Medicare & Medicaid Services. [online] Available at: https://www.cms.gov/Medicare/E-Health/EHealthRecords/index.html?redirect=/ehealthrecords/ [Accessed 2017 June 29]

[7] Azaria, A., Ekblaw, A., Vieira, T., & Lippman, A. MedRec: Using Blockchain for Medical Data Access and Permission Management. 2016 2nd International Conference on Open and Big Data (OBD). Available at: doi:10.1109/obd.2016.11 [Accessed 2017 May 24]

[8] J. Arun. It's all about trust: Blockchain for identity managemet. 12 May 2017. [Online]. Available at: https://www.ibm.com/blogs/blockchain/2017/05/its-all-about-trust-blockchain-for-identity-management/ [Acessed 2017 May 24]

[9] Mesropyan, E. 21 Companies Leveraging Blockchain for Identity Management and Authentication. [online] Lets Talk Payments. Available at: https://letstalkpayments.com/22-companies-leveraging-blockchain-for-identity-management-and-authentication/ [Accessed 2017 June 29]

[10] Adrian. L. How Blockchain Tech is About to Transform Sharemarket Trading. [Online]. Availabe at: http://www.coindesk.com/how-blockchain-technology-is-about-to-transform-sharemarket-trading/ [Accessed 2017 June 12]

[11] Nasdaq.com. Nasdaq Linq enables first-ever private securities issuance documented with blockchain technology. [Online]. Availabe at: http://ir.nasdaq.com/releasedetail.cfm?releaseid=948326 [Accessed 2017 June 29]

[12] Asx.com.au. ASX Chess Replacement. [online] Available at: http://www.asx.com.au/services/chess-replacement.htm [Accessed 2017 June 30].

[13] Staples, M., Chen, S., Falamaki, S., Ponomarev, A., Rimba, P., Tran, A. B., Weber, I., Xu, X., Zhu, J., Risks and Opportunities for Systems Using Blockchain and Smart Contracts. Data61 (CSIRO), Sydney, 2017