Equipment Life-cycle Management based on Private Blockchain and Smart Contract

Guicang Peng, Songpu Ai, Li Zhang, Chunming Rong and Tore Markeset

September 18, 2018

Equipment Life Cycle Management Based on Private Blockchain and Smart Contract

Guicang Peng[1], Songpu Ai[2], Li Zhang[3], Chunming Rong[4], Tore Markeset[5]

Abstract: Equipment management is gradually becoming more decentralized, and, in many cases, the equipment owner, operator, maintainer and inspector are not the same legal entity. This slows down equipment data transmission between stakeholders and reduces business and technical process automation. In this paper, we discuss how the application of distributed ledger concept based on private blockchain and smart contract technology can resolve these challenges and create a more automated and surveillance-free equipment life cycle management process.

1 Introduction

Conventional equipment ledgers are hosted by the equipment owner - often as a central database. It is the owner's responsibility to maintain the central database so that other stakeholders can retrieve updated data. However, different stakeholders may use different systems and protocols to store and share equipment data, and the different systems and protocols cause data transmission lags and inaccuracies between stakeholders. This would not only reduce business and technical process automation, but also create challenges for data verification and validation which contract execution and regulatory auditing largely depend on. A typical example of this deficiency is the aviation industry: It costs about 1 billion USD annually to transfer aircrafts between operators, with a large part of the expenses being caused by aircraft records transmission and approval (Canaday, 2017).

To resolve these challenges, the use of a distributed equipment ledger can be the first step. As UK Government Chief Scientific Adviser Mark Walport described in

[1] G. Peng (✉)
University of Stavanger, e-mail: guicang.peng@live.com

[2] S. Ai (✉)
Songpu Ai, University of Stavanger, e-mail: songpu.ai@uis.no

[3] L. Zhang
University of Electronic Science and Technology of China, email: zhangli240@uestc.edu.cn

[4] C. Rong
Chunming Rong, University of Stavanger, email: chunming.rong@uis.no

[5] T. Markeset
Tore Markeset, University of Stavanger, email: tore.markeset@uis.no

his report: "A distributed ledger is essentially an asset database that can be shared across a network of multiple sites, geographies or institutions" (Walport, 2016). However, a distributed ledger alone is not capable of solving the existing challenges; questions remain, such as: Based on a distributed ledger, how can we enhance business and technical process automation whilst ensuring stakeholder consensus and data authenticity? One answer is the private blockchain (Chowdhury et al., 2018). With its advantages, such as decentralization, transparency and anti-tampering, it provides a solid foundation for distributed ledger implementation. Moreover, together with the smart contract, the distributed ledger can be used to automate business and technical processes without third-party surveillance (Walport, 2016).

The rest of the paper is organized as follows: Section 2 will explain what the distributed ledger concept, private blockchain and smart contract are, and how they can be implemented together for general business scenarios. Section 3 will discuss how equipment life cycle management can be improved by the blockchain and smart contract. Section 4 will conclude on the pros and cons of the proposed solution. However, due to page limitations, we will not discuss the technical details of the private blockchain and smart contract to a research level; instead, we will only discuss how to customize and apply them to improve the equipment life cycle management process.

2 Distributed equipment ledger, blockchain and smart contract

2.1 Distributed Equipment ledger

A distributed equipment ledger is owned by all stakeholders as an auto-convergent database, in which every stakeholder maintains the part of the database that is relevant only to themselves, according to certain contract and regulation requirements. Equipment data can be recorded accurately and in a timely way by data generators themselves on their own premises; also, because a distributed ledger has to implement a unified data-storing and -sharing protocol for collective usage, the unified protocols will further enhance data transmission efficiency and accuracy between stakeholders. The distributed equipment ledger concept is illustrated in

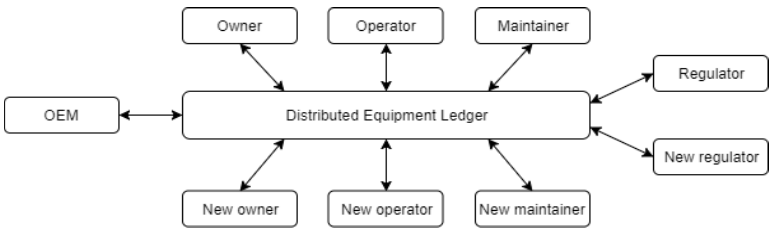

Figure 1 Distributed equipment ledger

Figure 1, with boxes representing stakeholders, and arrows representing data flow between stakeholders and the distributed ledger.

2.2 Private blockchain

Blockchain: A blockchain is a decentralized ledger with record groups stored simultaneously on multiple computers. A group of records is called a block. Once a block is entered into the ledger, it is immutable and linked using cryptography (Yaga *et al.*, 2018). A basic blockchain structure is illustrated in Figure 2. Each block has at least three core elements: 1) Block hash value generated by cryptography function; 2) Previous block's hash value; and 3) Data stored in the block (Conte de Leon *et al.*, 2017).

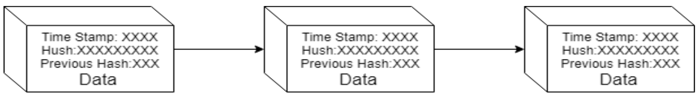

Figure 2 Basic Structure of a blockchain

A sound blockchain has three features which are relevant to our discussion here: 1) The blockchain is immutable and data stored in the blockchain is not changeable; 2) Blocks can only be added to the blockchain after passing consensus mechanism; 3) After a new block is successfully added to the blockchain, the new blockchain will auto-synchronize itself across the network to ensure the updated blockchain copy prevails. These three features of the blockchain are the backbone of anti-tampering and timely convergent distributed ledger system (Conte de Leon *et al.*, 2017).

Decentralized network: The peer to peer network without central administration, anyone within the blockchain decentralized network keeps an updated copy of the blockchain. A blockchain decentralized network is illustrated in Figure 3.

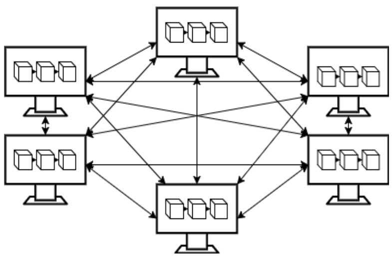

Figure 3 Blockchain Decentralized Network

Consensus mechanism: A consensus mechanism is a pre-defined protocol to maintain the consistency of the blockchain among the computers within the decentralized network. A proposed block can be added to a blockchain only after passing through the blockchain's consensus mechanism. (Pilkington, 2016).

Public blockchain: Anyone connected by Internet can download a public blockchain and to be an “endorsing peer” to add new block to the blockchain. The decentralized network of a public blockchain is limitless and can be extended to any computer connected by Internet.
Private blockchain: Access to the private blockchain network is governed and only consists of people who are within the same business process or generic endeavors. For example, nodes with certain rights and obligations bounded by relevant regulations, contracts and agreements can access a private blockchain. (Jayachandran, 2017).

2.3 Smart contract

Smart contract: A computer program intended to digitally facilitate, verify, or enforce the negotiation or performance of a contract(Tar, 2017), smart contracts embedded in blockchain serve the same purposes as anywhere else, the only specificity of them is that they are executed automatically and impartially without needs for human intervention(Walport, 2016). A typical process of private blockchain and smart contract integration are illustrated in Figure 4:

- **Stakeholder selection and consensus mechanism definition:** This step selects eligible stakeholders to establish private blockchain network according to relevant regulations, contracts and agreements. It is also practical to define or adjust the consensus mechanism based on the stakeholders being selected.
- **Pack smart contract and data into blocks:** Data generated during collaborations are packed into proposed blocks; automatable business and technical process are converted to smart contract and embedded into proposed blocks as computer programs. The proposed block will be added to blockchain only after passing pre-defined consensus mechanism.
- **Smart contract execution:** Smart contracts embedded into blocks are auto-executed based on block data and external inputs. Updated blockchain together with smart contract executing results is looped back to support stakeholder decision making and generating new blocks when necessary.

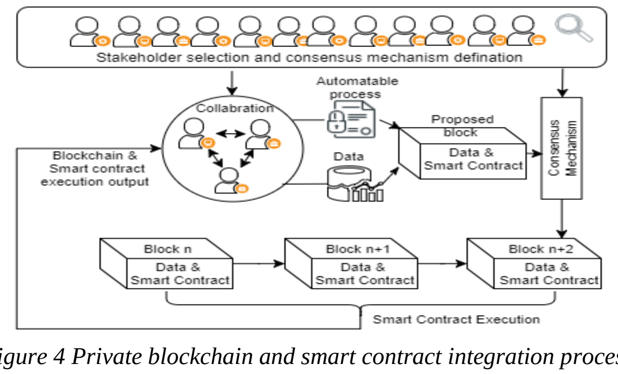

Figure 4 Private blockchain and smart contract integration process

3 Equipment life cycle management by private block-chain and smart contracts

Because equipment life cycle management is conducted by a limited number of stakeholders and is subject to confidentiality requirements in general, we follow a private blockchain and smart contract integration process in Figure 2 to model the equipment life cycle management process. There are many blockchain platforms that can run smart contracts on blockchain, Ethereum Foundation and IBM Block-Chain Platform are two well-known examples. However, due to page limitations, we will only discuss major function requirements and the technology roadmap to realize them.

3.1 Stakeholder selection and consensus mechanism definition

There are in general eight types of stakeholders who participate in equipment life cycle management, their roles are described below:

1. The original equipment manufacturer (OEM) design and manufacture equipment, supplies spare parts, provides technical upgrades and overhaul services.
2. The regulator approves equipment's design, issues equipment market access certificates, establishes equipment operation, maintenance and scrapping baseline.
3. The dealer sells equipment and provides value-added services under distributor contract.
4. The owner owns equipment and may operate the equipment with their own personnel or lease it out. If the equipment is leased out it may be leased out including operators, or the leaser may have their own operators. The user may also buy the function of the equipment as in a functional product(Markeset and Kumar, 2005).
5. The operator operates equipment under ownership, commission or lease agreements.
6. The service provider/ contractor provides consultation, inspection, maintenance, repair and scrapping services etc. under service contracts. A service provider may also own or operate the equipment
7. The supplier provides equipment consumables and spare parts.
8. Third-party auditor provides auditing services when necessary.

The eight types of stakeholders are selected and collaborate with each other according to equipment management regulations, contracts and agreements etc. The decentralized private blockchain network formed by them are illustrated in Figure 5, where computer icons represent stakeholders, arrows between computer icon represent collaborations between stakeholders. Any stakeholder in the network is allowed to propose new blocks, stakeholders who generate data are generally responsible to generate the associated blocks. In situations where data and documents are generated by more than one parties, the associated block can be generated by any party since the consensus mechanism will ensure the data is accepted by all relevant stakeholders. When to generate blocks is mainly depending on when data is generated. For example, equipment condition monitoring data may be posted at some fixed period, then the associated block can be generated at end of each period when data is available – the schedule-based block generation. On the other hand, inspection and maintenance report is produced only after certain failure detection and repairing job is done, then the report associated block is generated based on a specific event - the event-based block generation. Actual block generation is a mixture of both situations.

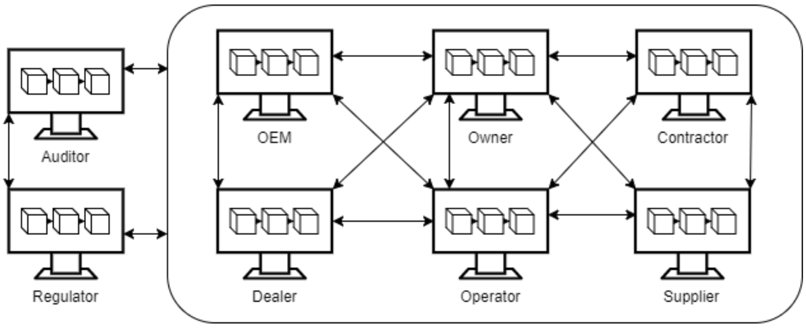

Figure 5 Equipment lifecycle management private blockchain network

Only blocks passing consensus mechanism can be added into blockchain. In our case, the consensus mechanism depends on stakeholders' rights and obligations bounded by contracts and regulations within the equipment management process. For example, the equipment operator proposes a block with operation commission charges data to the blockchain, only equipment owner as commissioner can approve the proposed block rather than anyone else, this type of consensus mechanism is called "Selective Endorsement"(Lucas, 2017). Selective endorsement relationship between stakeholders within equipment life cycle are illustrated in Table 1:

- N means having no rights for endorsement, for instance, stakeholders for specific projects usually do not have rights to endorse regulations, standards, statements and reports generated by regulators, similarly stakeholders have no rights to endorse their competitors or other stakeholders they have no collaboration with.
- ER means endorsing based on regulations, regulators endorse blocks based on relevant regulations and standards, auditors usually do the same when commissioned by regulators but also endorse blocks based on contracts as third party.
- EC means endorsing based on conditions such as regulatory, contractual or technical requirements etc. Contract-based endorse rights are always mutual between contracting parties.

Block endorsement process can be automated or manually executed. Many of nowadays business scenarios still need manual endorsement, yet automate endorsements are gradually taking holds because of technology advancement such as IoT and 5G etc. enable it. For example, block with equipment delivery confirmation can be automatically endorsed by data sent from warehouse's barcode scammer.

Table 1 Block Selective Endorsement Relationship

Selective Ensdorsement		Block Endorsed by							
		Regulator	OEM	Dealer	Owner	Operator	Contractor	Supplier	Auditor
Block Generated by	Regulator	N	N	N	N	N	N	N	N
	OEM	ER	N	EC/N	EC/N	N	N	N	ER/EC/N
	Dealer	ER	EC	N	C	N	N	N	ER/EC/N
	Owner	ER	EC/N	EC/N	N	EC/N	EC/N	EC/N	ER/EC/N
	Operator	ER	N	N	EC/N	N	EC/N	EC/N	ER/EC/N
	Contractor	ER	N	N	EC/N	EC/N	N	EC/N	ER/EC/N
	Supplier	ER	N	N	EC/N	EC/N	EC/N	N	ER/EC/N
	Auditor	ER	EC/N	EC/N	EC/N	EC/N	EC/N	EC/N	N

3.2 Pack smart contract into blocks

Smart contract can largely improve operation efficiency because it can be used to automate business and technical process without needs for third-party surveillance. For equipment life cycle management, it is possible to automate the following process by running a smart contract in combination with a blockchain.

1. **Regulatory compliance process:** a smart contract can automate regulation enforcement process such as: equipment market access certification based on third-party auditing results; equipment operation and service contractor qualification auditing based on stakeholder's online profiles; equipment environmental protection auditing based on IoT data.
2. **Business process:** a smart contract can automate contracts execution process such as: equipment operation commission charges approval based on equipment running parameters; equipment service contract payment approval based on equipment running parameters; spare parts and consumables procurement and logistic automation based on warehouse IoT data.
3. **Technical process:** a smart contract can automate technical process such as: equipment condition monitoring data processing and storage; activate equipment inspection, maintenance, repair or scrapping process based on equipment running parameters; suspense or continue equipment operations based on operating parameters; issuing equipment reports and notifications.

Smart contracts automating process described above are embedded into proposed block as relatively simple computer programs, together with other information within the proposed blocks, embedded smart contracts has to pass through consensus mechanism before execution on blockchain network.

3.3 Pack data into blocks

Equipment life cycle data is generated with different sizes and formats, to store all data on blockchain demands tremendous data traffics and storage spaces because blockchain synchronizing updated copies on all computers in the blockchain network. To overcome this challenge, an off-chain encrypted storage plus on-blockchain access management methodology is proposed based on the well-known Inter Planetary File System (Swan, 2015). IPFS is a protocol and network designed to create a content-addressable, peer-to-peer method of storing and sharing hypermedia in a distributed file system(Finley, 2016). Below are the IPFS features that suit for blockchain implementation:

1. Decentralized data storage and hash searchable: IPFS do not use central server to store and share data, instead data is stored on private computers as local copies and published to IPFS with only a unique hash, the hash is then used to search and download data from any computers with the published data copy. The decentralization of IPFS provides great storage scalability and do not post any data format restrictions. Meanwhile because both blockchain and IPFS are decentralized data storage system, they can collaborate on the same decentralized network seamless without extra network configuration. Stakeholders only need to pack the data's unique hash into blocks rather than the data itself, other stakeholders can download data based on its hash from IPFS only when they need it. These data hash packed blocks are coming in a small and similar size which make blockchain synchronization much quicker. It also reduces data traffic and redundant storages within the blockchain network.
2. Data anti-falsification: Data is published to IPFS with unique hash, any changes made to a data copy after publication will make the changed data copy unsearchable by the given hash anymore, this feature makes data falsification impossible after publication to IPFS. If stakeholder download data based on data hash packed in blockchain from IPFS, they will get the unchanged data copy associated with the hash for sure.
3. Data access control: For data which is ought to be open for everyone, its ok to publish data to IPFS without encrypting it first. However, for technical and business sensitive data, stakeholders can fully or partially encrypt them before published to IPFS, then control data assess by broadcasting data hash and decryption key only to authorized stakeholders through blockchain and smart contract, only those who get both the data hash and the decryption key can download and review data.

IPFS provides anti-falsification, multi-level access control and decentralized data storage network that copes well with blockchain implementation in our case. Typical equipment life cycle data access control is illustrated in Table 2:

- F means full access, for example, equipment related design and operation guidelines stored on regulators' premises are generally available to everyone.

- C means condition-based access, for example, OEM has full access to the data stored on its own premises but may give partially or no access of its data to other OEMs under specific conditions such as regulations and contractual requirements. Equipment owner generally gives condition-based access of equipment data stored on its premises to the equipment operator and verse visa.
- R means regulation-based access, depends on regional and international regulations and standards, the regulator has certain access to data stored on other stakeholders' premises.
- N means no access, for stakeholders do not have any collaboration with each other, there is generally no access to each other's on-premises data neither.

Table 2 Decentralized data storage access control

Decentralized Storage Access control		Data accessed By							
		Regulator	OEM	Dealer	Owner	Operator	Contractor	Supplier	Auditor
Data stored on	Regulator	F	F	F	F	F	F	F	F
	OEM	R	F/C	C	C	C	C	C	C
	Dealer	R	C	F/C	C	N	N	N	C
	Owner	R	C	C	F/C	C	C	C	C
	Operator	R	C	N	C	F/C	C	C	C
	Contractor	R	C	N	C	C	F/C	C	C
	Supplier	R	C	N	C	C	C	F/C	C
	Auditor	R	C	C	C	C	C	C	F/C

3.4 Smart contract execution

After a block passing through consensus mechanism, smart contract embedded in the block will auto-execute desired business and technical process based on block data and external inputs from authorized stakeholders. Typical outputs of equipment management-related smart contract execution can be: equipment maintenance notifications and reports, service payment statements and invoices, taxing and fining statements, payments confirmations, authorizations for suspending or continue further operations etc., these outputs will be automatically looped back to support management decision making and generation of new blocks.

4. Conclusion

This paper discussed how to apply private blockchain together with smart contracts and IPFS to improve equipment life cycle management process. The private blockchain provides decentralized business management framework, whilst the IPFS provides decentralized data storage, and the Smart contracts provide business and technical process automation. We believe the proposed solution would have the following advantages:

- Distributed equipment ledger enabled by private blockchain not only remove barriers for data transmission between stakeholders, it also provides a transparent and rigid collaboration framework without needs of third-party arbitration and surveillance.

- IPFS reduces tremendous data traffic and redundant data storage costs during equipment management process, IPFS also enable data storage and sharing much more efficient because it offers great scalability and posts no format restrictions for equipment data storage.
- Smart contracts enable highly rigid, transparent and surveillance-free technical and business process automation, which will increase equipment operation and maintenance performance considerably.

However, there are some disadvantages to the proposed solution as well. For example, IPFS is still at early stage of development, data access control is not a future-proof functionality of IPFS yet. For example, who gets the hush and download an encrypted data without decryption key cannot access the encrypted data, but maybe just for now since future computation power may be able to decrypt the encrypted data file anyway. This concern would intimidate many early adopters seriously. Moreover, blockchain and smart contract enable high degree of business and technical process automation, which is good for some scenarios, but maybe too rigid and robotic for the other scenarios where inherited deep uncertainties and huge risks require a certain level of human-interventions. Finally thanks Norwegian Research Council and Chinese Scholarship Association sponsor this research project.

References

Canaday, H. (2017) *Blockchain In MRO Could Happen Sooner Than You Think*. Available at: https://www.mro-network.com/big-data/blockchain-mro-could-happen-sooner-you-think , Accessed: 15 July 2018.

Conte de Leon, D. *et al.* (2017) 'Blockchain: properties and misconceptions', *Asia Pacific Journal of Innovation and Entrepreneurship*, 11(3), pp. 286–300. doi: 10.1108/APJIE-12-2017-034.

Finley, K. (2016) *The Inventors of the internet are trying to build a turly permanent web*. Available at: https://www.wired.com/2016/06/inventors-internet-trying-build-truly-permanent-web/.

Jayachandran, P. (2017) *The difference between public and private blockchain*. Available at: https://www.ibm.com/blogs/blockchain/2017/05/the-difference-between-public-and-private-blockchain/ , Accessed: 15 July 2018

Lucas, M. (2017) *The difference between Bitcoin and blockchain for business*. Available at: https://www.ibm.com/blogs/blockchain/2017/05/the-difference-between-bitcoin-and-blockchain-for-business/, Accessed: 25 July 2018

Markeset, T. and Kumar, U. (2005) 'Product support strategy: conventional versus functional products', *Journal of Quality in Maintenance Engineering*.

Emerald Group Publishing Limited, 11(1), pp. 53–67.

Pilkington, M. (2016) ‘11 Blockchain technology: principles and applications’, *Research handbook on digital transformations*. Edward Elgar Publishing, p. 225.

Swan, M. (2015) ‘Blockchain thinking: The brain as a dac (decentralized autonomous organization)’, in *Texas Bitcoin Conference*. Chicago, pp. 27–29.

Tar, A. (2017) *Smart Contracts, Explained*. Available at: https://cointelegraph.com/explained/smart-contracts-explained.

Walport, M. (2016) ‘Distributed ledger technology: Beyond blockchain’, *UK Government Office for Science*. Available at https://www.gov.uk/government/news/distributed-ledger-technology-beyond-block-chain

Yaga, D. *et al.* (2018) ‘Blockchain technology overview’, *Draft NISTIR*, 8202. Avaliable at https://csrc.nist.gov/publications/detail/nistir/8202/draft

Chowdhury, M. J. M., Colman, A., Kabir, M. A., Han, J. & Sarda, P. Blockchain Versus Database: A Critical Analysis. 2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/ 12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE), 1-3 Aug. 2018 2018. 1348-1353.