Position Paper on Blockchain Technology: Smart Contract and Applications

Weizhi Meng[1(✉)], Jianfeng Wang[2], Xianmin Wang[3], Joseph Liu[4], Zuoxia Yu[5,6], Jin Li[3], Yongjun Zhao[7], and Sherman S. M. Chow[7]

[1] Department of Applied Mathematics and Computer Science, Technical University of Denmark, Copenhagen, Denmark
weme@dtu.dk

[2] State Key Laboratory of Integrated Service Networks (ISN), Xidian University, Xi'an, People's Republic of China

[3] School of Computer Science, Guangzhou University, Guangzhou, China
{xianmin,jinli71}@gzhu.edu.cn

[4] Faculty of Information Technology, Monash University, Melbourne, Australia

[5] Department of Computing, The Hong Kong Polytechnic University, Hung Hom, Hong Kong SAR

[6] Department of Computing, The Hong Kong Polytechnic University Shenzhen Research Institute, Shenzhen, China

[7] Department of Information Engineering, The Chinese University of Hong Kong, Shatin, Hong Kong SAR

Abstract. Blockchain technology enables a transaction to be handled in a decentralized fashion. In this position paper, we aim to introduce the background of blockchain technology, discuss one of its important component — smart contract, and present its recent applications in many fields such as cryptocurrency, financial services, risk management, and Internet of Things.

Keywords: Blockchain technology · Smart contract
Practical applications · Financial services · Internet of Things
Risk management

1 Blockchain Background

Cryptocurrencies refer to digital currencies in which cryptographic techniques are used to regulate the generation of the currency units as well as securing their transaction. Research on cryptocurrency begins in the 1980's. The first electronic cash scheme was proposed by Chaum [9]. While extensive researches have been conducted (e.g., [3,14]), real-world deployment of cryptocurrency has seen little success.

The situation has changed dramatically with the invention of Bitcoin [32], which has become the most popular cryptocurrency to date. The main problem of previous cryptocurrencies is that they failed to be decentralized. Bitcoin

M. H. Au et al. (Eds.): NSS 2018, LNCS 11058, pp. 474–483, 2018.
https://doi.org/10.1007/978-3-030-02744-5_35

overcomes this problem by introducing a distributed ledger technology known as blockchain. Specifically, every Bitcoin transaction is recorded on blockchain with an underlying distributed consensus mechanism that can be compromised only if the attacker controls the majority of the whole world's computation power. Double-spending can be detected at the time of spending by referring to the blockchain. Bitcoin differs from some of the existing cryptocurrencies in the sense that it does not support offline transactions. However, since Bitcoin network is fully decentralized, peers can transact directly among each other within the network, without any centralized party such as the bank. According to CoinMarketCap[1], the total market cap of over 1700 cryptocurrencies exceeds 267 billion US dollar. The blockchain market size, according to a recent report published by Markets is expected to grow from 411 million USD in 2017 to 7683 million in the next five years.

Blockchain has attracted a lot of attention from both the industry and the academia. In a nutshell, blockchain offers a promising building block for applications which were otherwise only known to hold with the help of (offline) trusted third party (e.g., [15]). As a decentralized, append-only distributed ledger, blockchain technologies find applications beyond electronic currencies, money related applications such as trading, and other FinTech applications. Integrating with other techniques, it also allows recording, managing, and tracing of goods or spare parts, or in general, complicated procedures in the logistics process. Ethereum[2], the second largest cryptocurrency, introduces general computability into the blockchain platform. This makes blockchain-based applications more versatile.

1.1 Different Layers of Blockchain

Blockchain applications can be divided into several layers, namely, consensus, data structure, and ledger (or application). The consensus layer ensures different nodes in the network share the same view of the current blockchain and governs who is authorized to append a new block to the current blockchain. The data structure layer specifies how data are recorded and arranged while the application layer defines the format and meaning of the data recorded. Below we discuss how cryptography plays an important role in each of these layers in the Bitcoin blockchain.

Consensus. The consensus mechanism underlying Bitcoin is later known by the name of Nakamoto consensus, attributing to the original Bitcoin proposal of Nakamoto [32]. The longest chain rule specifies that the nodes to decide locally the current view of the blockchain by following the longest chain. This layer also defines the rules governing who is authorized to produce the next block to be appended to the current blockchain. In Bitcoin, this is enforced by proof-of-work. A node which wishes to publish a new block must find a

[1] https://coinmarketcap.com.

[2] https://www.ethereum.org.

nonce such that the hash value of this newly produced block is less than a certain threshold. Finding such a nonce requires a certain amount of work which explains the name proof-of-work. The actual amount of work is adjusted dynamically to ensures that new blocks are proposed at a constant rate on average. There are recent proposals [23,29] that aim to achieve higher block creation rate when more peers participate. Nevertheless, further research is needed to balance efficiency, security, and other requirements [16].

Data Structure. Data items in the Bitcoin blockchain are grouped into blocks. Each block is linked to the previous one through the use of a cryptographic hash function. Specifically, each block contains the hash of the previous block. As this structure forms a chain, hence the name of blockchain.

Application Layer. The original purpose of the Bitcoin blockchain is to support Bitcoin transaction. The original data format for the records in each block is rather simple. Each record is simply a Bitcoin transaction with an input and an output, except that the first transaction recorded on each blockchain does not require an output. This special transaction, sometimes known as the coinbase transaction, serves as an incentive mechanism for nodes to create new blocks, and also for Bitcoin unit creation. An output is merely (a hash of) a public key of a digital signature scheme and an amount, while the input is an unspent output of some previous transaction. The input-output has to be signed, using a secret key that matches the public key of the output to be spent. Transactions recorded in the same block are arranged into a Merkle tree. The block only stores the root of the Merkle tree to save storage space.

1.2 Privacy Aspects of Blockchain-Enabled Cryptocurrencies

Achieving security and privacy simultaneously has been the design goal for cryptocurrencies since its introduction [9]. Despite being regarded as highly anonymous by the general public, the privacy guarantee provided by Bitcoin is inferior to traditional cryptographic electronic cash. In particular, transactions in Bitcoin are linkable. For an example of analyses, it is possible to correlate Bitcoin address and IP address in Bitcoin blockchain [24].

To address the privacy issue, several new cryptocurrencies have been proposed. Created in 2014, Monero is an open-sourced decentralized cryptocurrency which employs linkable ring signatures [27] to hide the sender of the transaction. A ring signature scheme is a special kind of digital signatures which can convince a verifier that one out of several possible signers generated the signature, without revealing exactly whom. The linkability mandates that the signatures issued by the same signer for the same "context" can be publicly linkable[3]. This allows the actual sender to hide the fact that money is transferred from his account. Double-spending is prevented through the use of the one-time key in a way that signatures generated by the same key can be detected. Subsequently, Monero upgrades its protocol to ring confidential transaction, which also hides transaction amount and receiver [30].

[3] There are other variants of linkability. For example, escrowed linkability [17] only allows a designated party to link.

Zcash is another privacy-preserving cryptocurrency that makes heavy use of cryptographic techniques. It is based on Zerocash [5]. The core underlying cryptographic technique is zero-knowledge succinct non-interactive arguments of knowledge (ZK-SNARK), which allows a prover to produce a short proof to convince anyone that he knows some secret without revealing it. In Zcash, ZK-SNARK is employed to allow a spender to prove that he is spending a valid coin to a receiver without revealing any extra information. In general, ZK-SNARK is a powerful cryptographic technique which implies many other cryptographic primitives, such as multi-key homomorphic signatures unforgeable under insider corruption [25].

As more people consider applying blockchain for applications beyond cryptocurrency, the privacy issue attracts more and more attention. Improved cryptographic techniques are required to cope with these new use cases in an efficient manner.

2 Smart Contract

The concept of smart contracts was proposed by Szabo in 1994 [36]. With the great success of Bitcoin, Blockchain 2.0 introduces the support of smart contracts for executing diverse applications other than cryptocurrency [26]. In particular, Ethereum, the second largest blockchain, supports Turing-complete smart contracts. There are already more than 4 million smart contracts on Ethereum. Besides Ethereum, there are also some other blockchain systems supporting smart contracts [4], such as Counterparty, Stellar, Lisk, Monax, etc.[4]

A smart contract can be considered as an autonomous program that can be automatically executed according to the predefined program logic. Developers usually design and implement smart contracts using high-level languages, such as, Solidity, Serpent, LLL, etc. Then, the smart contract will be compiled into EVM (Ethereum virtual machine) bytecode and deployed to the Ethereum blockchain. Once the smart contract is invoked by a user or another smart contract, it will be executed in the EVM on every Ethereum node. EVM is a register-based virtual machine and its specification can be found in the Ethereum yellow paper [37]. For security consideration, EVM is sandboxed and the smart contract running in EVM cannot access the important resources (e.g., network, file system, etc.) of each Ethereum node. Different from traditional virtual machines, Ethereum introduces the *gas* mechanism such that the execution of each EVM operation costs a certain amount of money equal to the multiplication of the gas price and the gas cost of the operation. This indirectly guarantees that the execution of a smart contract will eventually stop.

The most severe threat to smart contracts is its software vulnerabilities. Nicola et al. carried out a systematic study on the attacks on Ethereum smart contract [2]. Loi et al. designed Oyente [28], a symbolic execution tool which identified four kinds of security vulnerabilities —

[4] `counterparty.io`, `stellar.org`, `lisk.io`, `monax.io`.

1. The reentrancy vulnerability results from the fact that when an Ethereum smart contract invokes another one, the current execution will wait until the invocation finishes. If the callee is malicious, it could exploit the intermediate state of the caller to launch attacks. Such vulnerability has led to 60 million USD worth of Ether theft [8].
2. The mishandled exceptions may happen when one smart contract calls another one. In particular, if the exception in the callee is not propagated to the caller or the caller does not take care of the return value from the callee, the execution logic of caller will be affected.
3. The transaction-ordering dependence refers to the potential attacks resulting from the unexpected order of transactions. Note that the miner that mines the block can determine the order of the transactions.
4. The timestamp dependence refers to the potential vulnerability in smart contracts that use the block timestamp to control the execution of some important operations. A malicious miner may change the block timestamp to affect the execution of those important operations.

Recently, Kalra et al. proposed a tool, named Zeus [22], which employs abstract interpretation, symbolic model checking, as well as constrained horn clauses to quickly discover security issues in smart contracts. Besides the above four security issues [28], they further investigated how to detect new vulnerabilities, such as unchecked send, failed send, integer overflow/underflow, etc. Further research is needed to improve the detection rate of vulnerabilities and decrease the false positive rate.

Attackers can also use smart contracts to conduct malicious activities and even attack the Ethereum platform. Juels et al. [21] showed that the criminal smart contracts can facilitate the leakage of confidential data, theft of private keys, and various "calling-card" crimes, such as murder, terrorism, etc. Malicious smart contracts have also been used to launch denial-of-service (DoS) attacks on the Ethereum platform [6,7]. Chen et al. designed a measurement approach to assess whether the gas price is properly set by Ethereum [11]. Unfortunately, their results show that although Ethereum has adjusted the gas prices of some operations to defend against known DoS attacks, there still exist underpriced operations that can be exploited by attackers to launch DoS attacks. To address this problem, they proposed an adaptive gas cost mechanism to defend against known and unknown DoS attacks. They further conducted the first systematic study on Ethereum and employed three types of graphs, including money flow graph, smart contract creation graph, and smart contract invocation graph to characterize the major activities on Ethereum. By conducting graph analyses, they revealed stealthy attacks on Ethereum [13]. Further research is desired to capture more stealthy attacks with low false positive rates.

Besides security issues, there are also various performance issues in Ethereum. Dinh et al. proposed the first evaluation framework to measure the performance of private blockchains in terms of throughput, latency, scalability, and fault-tolerance [19]. Zheng et al. designed a lightweight performance monitoring framework for blockchain systems, which can visualize detailed and real-time performance data [39]. Since the execution of smart contracts cost money, Chen et al. [10] found that gas-inefficient patterns are prevalent in existing smart contracts. In other words, a smart contract with gas-inefficient patterns costs more gas than necessary. They further designed GasReducer, a tool which automatically eliminates such gas-inefficient patterns in smart contracts [12]. Further research is needed to automatically identify and remove more gas-inefficient patterns.

3 Blockchain Applications Beyond Cryptocurrencies

The original application of blockchains is Bitcoin [32]. With the increasing number of adoptions, it has diverse application scenarios related to finance, Internet of Things, risk management, etc. Below we highlight some of these applications or the vision behind.

3.1 Financial Field

Blockchain technology is expected to optimize the global financial infrastructure and build an efficient economic system. Cocco et al. [18] noted that many banks are focusing on blockchain technology to promote economic growth and accelerate the development of green technologies —

> "Sustainability strategies try to minimize the impact on the environment, starting from making people more efficient, improved recording of environmental key performance indicators, efficient building technology, green travel to sustainable purchasing, and from the end-to-end management of resources and waste."

That is, they appreciate the effort of saving energy while using blockchains.

In addition, Hong Kong's de-facto central bank had planned to evaluate blockchain distributed ledger solutions by building an innovation hub [34]. The Hong Kong Monetary Authority (HKMA) is also working with the Hong Kong Applied Science and Technology Research Institute (ASTRI) to enhance such hub as a blockchain testbed. They believe that this innovation hub can be acted as a "neutral ground" for evaluating financial technology prior to its eventual release in near future.

3.2 Internet of Things (IoT)

The Internet of Things (IoT) represents a kind of network environment that consists of various Internet-enabled physical and embedded devices with electronics, software, and sensors, etc. Recently, blockchains have become a popular means to help address issues in an IoT environment. For example, Sharma et al. [35] proposed a blockchain-based distributed cloud architecture with a software-defined networking enabled controller at the network edge, providing low-cost, secure, and on-demand access to the most competitive computing infrastructures in an

IoT network. Novo [33] introduced an IoT architecture for arbitrating roles and permissions based on blockchain technology, which is a fully distributed access control system for IoT. Their method can operate in a single smart contract, simplifying the whole process in the blockchain network and reducing the communication overhead between the nodes.

IoT may involve many financial factors. Zhang and Wen [38] introduced an E-business architecture designed specifically for IoT through the Bitcoin protocol. They adopted distributed autonomous corporations as the transaction entity to handle the paid data and the smart property. In their e-commerce architecture, users can obtain IoT coins through P2M and DACs. How to combine blockchains and various IoT scenarios is one popular topic in both industry and academia.

3.3 Risk Management

Blockchain technology allows verification without a central authority or a trusted third party. It can be useful to enhance the existing risk management, including intrusion detection and trust computation.

Intrusion Detection. To examine system or network threats, intrusion detection system (IDS) is an important and commonly available tool for different organizations. Meng et al. [31] discussed how to combine distributed or collaborative IDSs (CIDS) with blockchain technology. They identified that blockchains can be used to solve data sharing and better establish mutual trust among collaborating parties by working as a permanent public ledger of contracts between data owners and other parties. Gu et al. [20] introduced a multi-feature detection method for detecting and classifying malware by establishing a fact-base of distributed Android malicious codes by blockchain technology. In particular, they proposed a framework, called "consortium blockchain for malware detection and evidence extraction, which is composed of two parts of mixed chains: detecting consortium chain by test members and public chain by users.

Trust Computation. It is an essential and critical task to evaluate the trustworthiness of nodes in a distributed IDS network environment. Traditionally, trust computation needs a certified third party or a central server, which may suffer from many attacks, especially insider attacks, where the intruders have authorized access to the network. With the advent of blockchains, it become feasible to perform a trust evaluation without any trusted third party. Alexopoulosetal et al. [1] described a blockchain-based CIDS framework, in which they considered the raw alerts generated by each IDS node as transactions in a blockchain.

4 Concluding Remarks

There is an increasing number of blockchain applications in various fields. This position paper briefly introduces what are blockchain and smart contract, and presents their recent applications in finance, IoT and risk management. More research is still needed to investigate how to design a robust, efficient, and privacy-preserving blockchain-based security mechanism.

Acknowledgement. Sherman S.M. Chow is supported by the General Research Fund (CUHK 14210217) of the Research Grants Council, University Grant Committee of Hong Kong.

References

1. Alexopoulos, N., Vasilomanolakis, E., Ivánkó, N.R., Mühlhäuser, M.: Towards blockchain-based collaborative intrusion detection systems. In: D'Agostino, G., Scala, A. (eds.) CRITIS 2017. LNCS, vol. 10707, pp. 1–12. Springer, Cham (2018)
2. Atzei, N., Bartoletti, M., Cimoli, T.: A survey of attacks on ethereum smart contracts (SoK). In: Maffei, M., Ryan, M. (eds.) POST 2017. LNCS, vol. 10204, pp. 164–186. Springer, Heidelberg (2017). https://doi.org/10.1007/978-3-662-54455-6_8
3. Au, M.H., Chow, S.S.M., Susilo, W.: Short E-cash. In: Maitra, S., Veni Madhavan, C.E., Venkatesan, R. (eds.) INDOCRYPT 2005. LNCS, vol. 3797, pp. 332–346. Springer, Heidelberg (2005). https://doi.org/10.1007/11596219_27
4. Bartoletti, M., Pompianu, L.: An empirical analysis of smart contracts: platforms, applications, and design patterns. In: Brenner, M., Rohloff, K., Bonneau, J., Miller, A., Ryan, P.Y.A., Teague, V., Bracciali, A., Sala, M., Pintore, F., Jakobsson, M. (eds.) FC 2017. LNCS, vol. 10323, pp. 494–509. Springer, Cham (2017). https://doi.org/10.1007/978-3-319-70278-0_31
5. Ben-Sasson, E., et al.: Decentralized anonymous payments from bitcoin. In: Proceedings of 2014 IEEE Symposium on Security and Privacy, SP 2014, 18–21 May 2014, pp. 459–474 (2014)
6. Buterin, V.: A state clearing FAQ (2016). https://goo.gl/x5QRrd. Accessed 30 July 2016
7. Buterin, V.: Transaction spam attack: next steps (2016). https://goo.gl/uKi9Ug. Accessed 30 July 2016
8. Castillo, M.: The DAO attacked: code issue leads to $60 million ether theft (2016). https://www.coindesk.com/dao-attacked-code-issue-leads-60-million-ether-theft
9. Chaum, D.: Blind signatures for untraceable payments. In: Chaum, D., Rivest, R.L., Sherman, A.T. (eds.) Advances in Cryptology: Proceedings of CRYPTO 1982, Santa Barbara, California, USA, August 23–25, pp. 199–203 (1982)
10. Chen, T., Li, X., Luo, X., Zhang, X.: Under-optimized smart contracts devour your money. In: Proceedings of SANER (2017)
11. Chen, T., et al.: An adaptive gas cost mechanism for ethereum to defend against under-priced DoS attacks. In: Liu, J.K., Samarati, P. (eds.) ISPEC 2017. LNCS, vol. 10701, pp. 3–24. Springer, Cham (2017). https://doi.org/10.1007/978-3-319-72359-4_1
12. Chen, T., et al.: Towards saving money in using smart contracts. In: Proceedings of ICSE (2018)
13. Chen, T., et al.: Understanding ethereum via graph analysis. In: Proceedings of INFOCOM (2018)
14. Chow, S.S.M.: Running on karma – P2P reputation and currency systems. In: Bao, F., Ling, S., Okamoto, T., Wang, H., Xing, C. (eds.) CANS 2007. LNCS, vol. 4856, pp. 146–158. Springer, Heidelberg (2007). https://doi.org/10.1007/978-3-540-76969-9_10
15. Chow, S.S.M., Hui, L.C.K., Yiu, S.-M., Chow, K.P.: Practical electronic lotteries with offline TTP. Comput. Commun. **29**(15), 2830–2840 (2006)

16. Chow, S.S.M., Lai, Z., Liu, C., Lo, E., Zhao, Y.,: Sharding blockchain (Invited Paper). In: The 2018 IEEE Internal Conference on Blockchain (2018)
17. Chow, S.S.M., Susilo, W., Yuen, T.H.: Escrowed linkability of ring signatures and its applications. In: Nguyen, P.Q. (ed.) VIETCRYPT 2006. LNCS, vol. 4341, pp. 175–192. Springer, Heidelberg (2006). https://doi.org/10.1007/11958239_12
18. Cocco, L., Pinna, A., Marchesi, M.: Banking on blockchain: costs savings thanks to the blockchain technology. Future Internet **9**(3), 25 (2017)
19. Dinh, T.T.A., Wang, J., Chen, G., Liu, R., Ooi, B.C., Tan, K.: Blockbench: a framework for analyzing private blockchains. In: Proceedings of SIGMOD (2017)
20. Gu, J., Sun, B., Du, X., Wang, J., Zhuang, Y., Wang, Z.: Consortium blockchain-based malware detection in mobile devices. IEEE Access **6**, 12118–12128 (2018)
21. Juels, A., Kosba, A., Shi, E.: The ring of Gyges: investigating the future of criminal smart contracts. In: Proceedings of CCS (2016)
22. Kalra, S., Goel, S., Dhawan, M., Sharma, S.: Zeus: analyzing safety of smart contracts. In: Proceedings of NDSS (2018)
23. Kokoris-Kogias, E., Jovanovic, P., Gasser, L., Gailly, N., Syta, E. Ford, B.: Omniledger: a secure, scale-out, decentralized ledger via sharding. In: IEEE Symposium on Security and Privacy, pp. 583–598 (2018)
24. Koshy, P., Koshy, D., McDaniel, P.: An analysis of anonymity in bitcoin using P2P network traffic. In: Christin, N., Safavi-Naini, R. (eds.) FC 2014. LNCS, vol. 8437, pp. 469–485. Springer, Heidelberg (2014). https://doi.org/10.1007/978-3-662-45472-5_30
25. Lai, R.W.F., Tai, R.K.H., Wong, H.W.H., Chow, S.S.M.: Multi-key homomorphic signatures unforgeable under insider corruption. In: ASIACRYPT (2018, to appear)
26. Li, P.J.X., Chen, T., Luo, X., Wen, Q.: A survey on the security of blockchain systems. Future Generation Computer Systems (2017)
27. Liu, J.K., Wei, V.K., Wong, D.S.: Linkable spontaneous anonymous group signature for Ad Hoc groups. In: Wang, H., Pieprzyk, J., Varadharajan, V. (eds.) ACISP 2004. LNCS, vol. 3108, pp. 325–335. Springer, Heidelberg (2004). https://doi.org/10.1007/978-3-540-27800-9_28
28. Luu, L., Chu, D.-H., Olickel, H., Saxena, P., Hobor, A.: Making smart contracts smarter. In: Proceedings of CCS (2016)
29. Luu, L., Narayanan, V., Zheng, C., Baweja, K., Gilbert, S., Saxena, P.: A secure sharding protocol for open blockchains. In: Proceedings of CCS (2016)
30. Maxwell, G.: Confidential transactions (2015). https://elementsproject.org/elements/confidential-transactions
31. Meng, W., Tischhauser, E., Wang, Q., Wang, Y., Han, J.: When intrusion detection meets blockchain technology: a review. IEEE Access **6**, 10179–10188 (2018)
32. Nakamoto, S.: Bitcoin: a peer-to-peer electronic cash system (2008). https://bitcoin.org/bitcoin.pdf
33. Novo, O.: Blockchain meets IoT: an architecture for scalable access management in IoT. IEEE Internet Things J. **5**(2), 1184–1195 (2018)
34. Rizzo, P.: Hong Kong's central bank to test blockchain (2018). http://www.coindesk.com/hong-kongs-central-bank-test-blockchain. Accessed 30 July 2018
35. Sharma, P.K., Chen, M.Y., Park, J.H.: A software defined fog node based distributed blockchain cloud architecture for IoT. IEEE Access **6**, 115–124 (2018)
36. Szabo, N.: The Idea of Smart Contracts (1994). http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/idea.html
37. Wood, G.: Ethereum: a secure decentralised generalised transaction ledger. https://ethereum.github.io/yellowpaper/paper.pdf

38. Zhang, Y., Wen, J.: The IoT electric business model: using blockchain technology for the internet of things. Peer-to-Peer Networking Appl. **10**(4), 983–994 (2017)
39. Zheng, P., Zheng, Z., Luo, X., Chen, X., Liu, X.: A detailed and real-time performance monitoring framework for blockchain systems. In: Proceedings of ICSE (2018)