Decentralized Applications: The Blockchain-Empowered Software System

Presented by
Byoung Wook Kwon

OUTLINE

I. Introduction

II. Background: Classic Blockchain Systems

A. Prehistory

B. Double Spending Issue

C. Broader Definition of Blockchain Systems

III. Evolution of Blockchain Systems

A. Decentralizes Smart Contract

B. Decentralizes Applications

IV. State-of-the-art dapps

A. Games

B. Internet of things

1) Smart Hardware

2) Supply Chain

V. Desirable Characteristics of dapps

A. Better Performance

1) Low Latency

2) High Throughput

3) Fast Sequential Performance

B. Enabling Offline Transactions

VI. Considerations When Selection a Blockchain Implementation

VIII. Conclusion

I. INTRODUCTION

- By definition, a blockchain is a continuously growing chain of blocks, each of which contains a cryptographic hash of the previous block, a time-stamp, and its conveyed data.

- Due to the existence of the cryptographic hash, the data stored in a blockchain are inherently strong to modification.

- Maintenance of peer-to-peer (P2P) ledgers for cryptocurrencies has become the first application of blockchain.

I. INTRODUCTION

- Thousands of cryptographic tokens, or coins, were delivered to the public market, after the huge leap in market cap of Bitcoin.

- Due to the lack of legal regulation, a large number of scams also brought bad reputations to blockchain technology.

- this paper surveys the state-of-the-art of blockchain technology and introduces **decentralized Applications(dApps)**, which is a novel form of the blockchain-empowered software system.

II. BACKGROUND: CLASSIC BLOCKCHAIN

A. PREHISTORY

- The blockchain concept, the fundamental form of public ledger, was first introduced for time-stamped digital documents in 1991.
- Was incorporated into the cryptographically secured chain by allowing several documents to be collected into one block, which improves the system efficiency and reliability.
- Such a ledger implemented with a chain of blocks is still a centralized database, which relies on the maintenance of a trusted third party financial institute.

II. BACKGROUND: CLASSIC BLOCKCHAIN
B. DOUBLE SPENDING ISSUE

- Thanks to the hash-linking feature of the blockchain, each coin in the ledger can be traced back to the first record when it was created.

- Therefore, forgery on a non-existing coin is impossible in a public decentralized ledger. However, different from a physical coin, a digital coin can be easily replicated by duplicating the data.

- If a dishonest use of the public ledger is capable of performing a Sybil attack, the coins that the user double-spends will be legalized by the majority of parties, which diminishes user trust as well as the circulation and retention of the currency.

II. BACKGROUND: CLASSIC BLOCKCHAIN
C. BROADER DEFINITION OF BLOCKCHAIN SYSTEMS

- Thanks to the hash-linking feature of the blockchain, each coin in the ledger can be traced back to the first record when it was created.

- Therefore, forgery on a non-existing coin is impossible in a public decentralized ledger. However, different from a physical coin, a digital coin can be easily replicated by duplicating the data.

- If a dishonest use of the public ledger is capable of performing a Sybil attack, the coins that the user double-spends will be legalized by the majority of parties, which diminishes user trust as well as the circulation and retention of the currency.

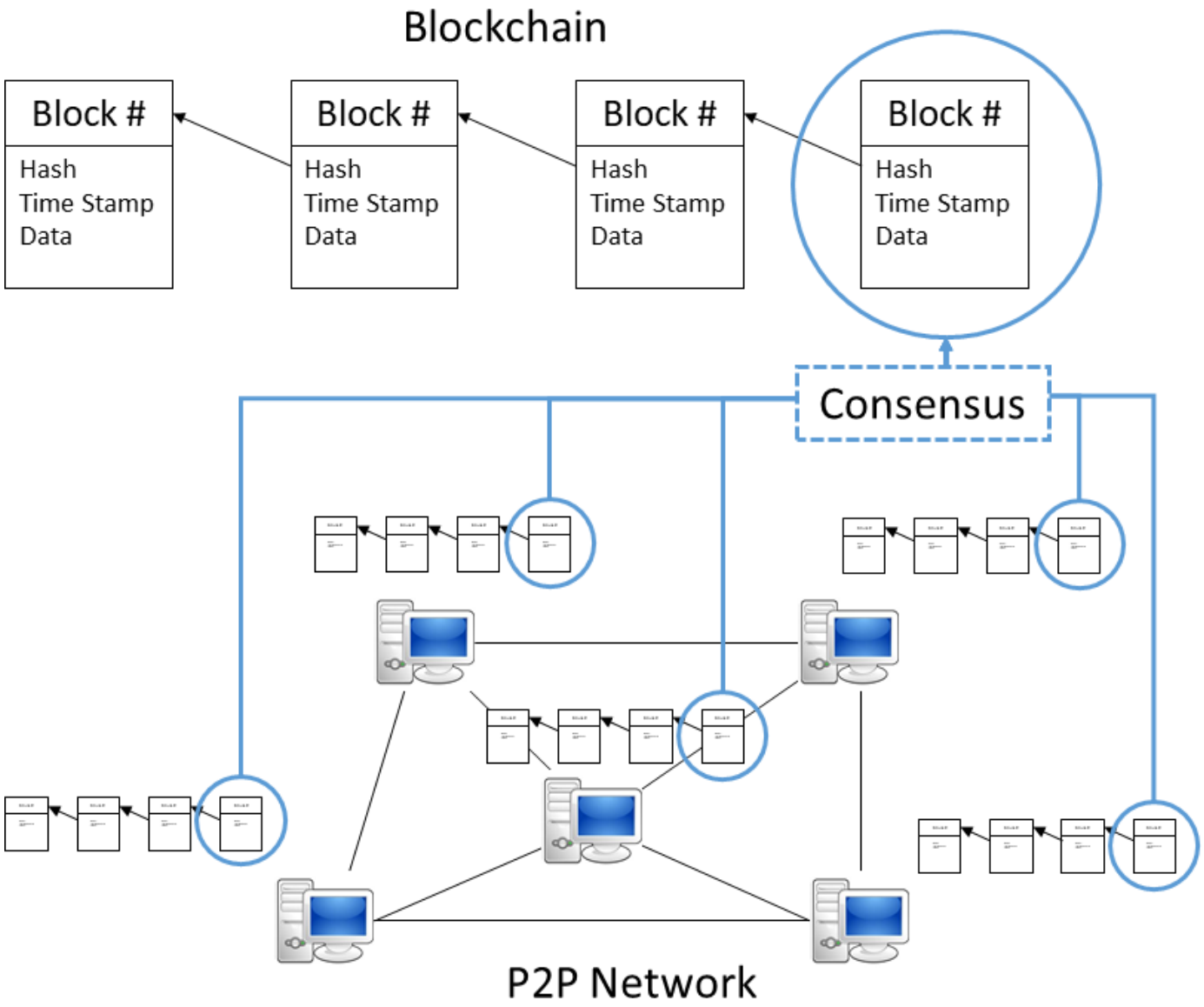

FIGURE 1. Key elements of blockchain systems.

III. EVOLUTION OF BLOCKCHAIN SYSTEMS
B. DECENTRALIZED SMART CONTRACT

- In order to add more values to the blockchain ecosystem, Ethereum [10] is designed to be a platform to facilitate decentralized smart contracts via Ether, its own currency vehicle.

- Smart contract [11] refers to the idea that legal contracts can be notarized and executed automatically. Equipped with Solidity [12], a Turing-complete programming language, Ethereum developers are able to implement a series of smart contracts, which are executable programs written into blocks.

- Therefore, publishing a smart contract creates a set of public trusted functionality for public users.

III. EVOLUTION OF BLOCKCHAIN SYSTEMS
C. DECENTRALIZED APPLICATIONS

- Current blockchain-based applications are still limited to utilizing smart contract for core data and functionality that should be resistant to modifications.

- An ideal blockchain application or service should be operable without any human intervention, which forms a Decentralized Autonomous Organization (DAO) [13].

- DAO is an organization that is run through rules encoded as smart con- tracts running on the blockchain. Due to its autonomous and automatic nature, a DAO's cost and profit are shared by all participants by simply recording all activities into the blocks.

C. DECENTRALIZED APPLICATIONS

- Open Source: Due to the trusted nature of blockchain, dApps need to make their codes open source, so that audits from third parties become possible.

- Internal Cryptocurrency Support: Internal currency is the vehicle that runs the ecosystem for a particular dApp. With tokens, it is feasible for a dApp to quantify all credits and transactions among participants of the system, including content providers and consumers.

- Decentralized Consensus: The consensus among decen- tralized nodes is the foundation of transparency.

- No Central Point of Failure: A fully decentralized sys- tem should have no central point of failure since all com- ponents of the applications will be hosted and executed in the blockchain.

IV. STATE-OF-THE-ART DAPPS
A. GAMES

- As one of the most successful blockchain games and even a milestone in the development of Ethereum, **CryptoKitties** may be the most well-known blockchain game nowadays.

- In CryptoKitties, players can buy, sell, and breed cats by using a smart contract on the Ethereum Blockchain.

- Blockchain-based games benefit from the features of non-fungible tokens and system transparency.

IV. STATE-OF-THE-ART DAPPS
C. INTERNET OF THINGS

1) SMART HARDWARE

- Automation is a key concept in IoT applications.

- Smart hardware that connects to the network should be able to perform predefined actions without human intervention. This requires- ment perfectly fits the nature of smart contracts running on blockchains.

- With transparent and immutable smart contracts, multiple parties in an IoT platform can establish trustful relationships without complicated conversations and regulations.

IV. STATE-OF-THE-ART DAPPS
C. INTERNET OF THINGS

2) SUPPLY CHAIN

- In the blockchain era, the integration of smart contracts with supply chains will further optimize the systems.

- Multiple levels of suppliers, manufacturers, service providers, distributors, and retailers make record-keeping and communications inefficient.

- IoT and smart contracts can simplify the whole procedure by coordinating sensory data, documentation, and transparency to regulations.

V. DESIRABLE CHARACTERISTICS OF DAPPS

A. BETTER PERFORMANCE

1) LOW LATENCY

- Long transaction delay has been a critical issue since the birth of Bitcoin.
- Since the average time for the Bitcoin nodes to mine a block is 10 minutes, the average transaction confirmation time is around an hour.
- In fact, longer delays frustrate users and make dApps less competitive with existing non-blockchain alternatives.

V. DESIRABLE CHARACTERISTICS OF DAPPS
A. BETTER PERFORMANCE

2) HIGH THROUGHPUT

- Modern web-based systems, e.g., social networks, massive multi-player online games, online shopping malls, require the blockchain platform to support millions of active users on a daily basis.

- Therefore, the capability of handling a large amount of concurrent traffic is critical in a dApp platform.

- However, current blockchain platforms still suffer from throughput bottlenecks.

V. DESIRABLE CHARACTERISTICS OF DAPPS
A. BETTER PERFORMANCE

3) FAST SEQUENTIAL PERFORMANCE

- In system designs, dependencies among software components or logical steps restrict the execution of an application.

- Some procedures in certain applications, such as updates on one particular piece of data, cannot be implemented in parallel, due to the sequential dependent on the results produced by previous steps.

- In blockchain systems, the sequential performance of a dApp is determined by the response delays from all nodes in the network, since all transactions/operations should be executed and verified by all nodes to reach a consensus..

V. DESIRABLE CHARACTERISTICS OF DAPPS

A. BETTER PERFORMANCE

- As one of the most successful blockchain games and even a milestone in the development of Ethereum, **CryptoKitties** may be the most well-known blockchain game nowadays.

- In CryptoKitties, players can buy, sell, and breed cats by using a smart contract on the Ethereum Blockchain.

- Blockchain-based games benefit from the features of non-fungible tokens and system transparency.

VIII. Conclusion

- Blockchain systems leverage cryptography technologies, P2P networking and consensus models to provide infrastructures for decentralized applications.
- We have presented the application scenarios of dApps, which in our opinion is the subject matter of future blockchains.
- We have discussed the desirable characteristics of dApps and recent directions in blockchain development, including payment channels, novel consensus models and non-public blockchains.
- We believe that networked computing systems are on the edge of a new era of the decentralized ecosystem, which will eventually lead to the next-generation Internet services..

Reference

1. M. Nofer, P. Gomber, O. Hinz, and D. Schiereck, ‘‘Blockchain,’’ Bus. Inf. Syst. Eng., vol. 59, no. 3, pp. 183–187, Mar. 2017.
2. S. Nakamoto. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. [Online]. Available: https://bitcoin.org/bitcoin.pdf
3. D. Chaum, ‘‘Blind signatures for untraceable payments,’’ in Advances in Cryptology. Boston, MA, USA: Springer, 1983, pp. 199–203.
4. S. Haber and W. S. Stornetta, ‘‘How to time-stamp a digital document,’’J. Cryptol., vol. 3, pp. 99–111, Jan. 1991.
5. R. C. Merkle, ‘‘Protocols for public key cryptosystems,’’ in Proc. IEEE Symp. Secur. Privacy, Apr. 1980, p. 122.
6. D. Bayer, S. Haber, and W. S. Stornetta, ‘‘Improving the efficiency and reliability of digital time-stamping,’’ in Sequences II, R. Capocelli, A. De Santis, and U. Vaccaro, Eds. New York, NY, USA: Springer, 1993, pp. 329–334.
7. L. Lamport, R. Shostak, and M. Pease, ‘‘The Byzantine generals problem,’’ ACM Trans. Program. Lang. Syst., vol. 4, no. 3, pp. 382–401, Jul. 1982. [Online]. Available: http://doi.acm.org/10.1145/357172.357176
8. J. R. Douceur, ‘‘The sybil attack,’’ in Peer-to-Peer Systems. Berlin, Germany: Springer, 2002, pp. 251–260.
9. A. Back. (Aug. 2002). Hashcash—A Denial of Service Counter-Measure. [Online]. Available: http://www.hashcash.org/papers/hashcash.pdf
10. V. Buterin. (2013). Ethereum White Paper: A Next Generation Smart Contract & Decentralized Application Platform. [Online]. Available: https://github.com/ethereum/wiki/wiki/White-Paper
11. N. Álvarez-Díaz, J. Herrera-Joancomartí, and P. Caballero-Gil, ‘‘Smart contracts based on blockchain for logistics management,’’ in Proc. 1st Int. Conf. Internet Things Mach. Learn., New York, NY, USA, 2017, pp. 73:1–73:8.
12. C. Dannen, Introducing Ethereum and Solidity: Foundations of Cryptocur- rency and Blockchain Programming for Beginners. New York, NY, USA: Apress, 2017.
13. H. Green. (May 2016). Introducing the DAO: The Organisation That Will Kill Corporations. [Online]. Available: http://www.cityam.com/ 240198/introducing-the-dao-the-organisation-that-will-kill-corporations
14. S. Raval, Decentralized Applications: Harnessing Bitcoin’s Blockchain Technology, 1st ed. Newton, MA, USA: O’Reilly Media, 2016.

Reference

15. (Mar. 2018). Blockchain Games: A Surprising New Player in the Industry. [Online]. Available: http://bitcoinist.com/blockchain-games-a-surprising- new-player-in-the-industry
16. (Feb. 2018). How Blockchain Games Can Change the Gaming Industry. [Online]. Available: https://plarium.com/en/blog/blockchain-games
17. (Feb. 2018). Introduction to Blockchain Games and Dragonereum. [Online]. Available: https://medium.com/@dragonereum/introduction-to- blockchain-games-and-dragonereum-fd5380b8ffc2
18. (Aug. 2017). Steem: An Incentivized, Blockchain-Based, Public Content Platform. [Online]. Available: https://steem.io/steem-whitepaper.pdf
19. K. O. R. O'Reilly. (2017). Gems Protocol. [Online]. Available: https://gems.org/whitepaper.pdf
20. S. Ranger. (Aug. 2018). What is the IoT? Everything You Need to Know About the Internet of Things Right Now. [Online]. Available: https://www.zdnet.com/article/what-is-the-internet-of-things-everything- you-need-to-know-about-the-iot-right-now/
21. K. Shaik. (Jan. 2018). Why Blockchain and IoT are Best Friends. [Online]. Available: https://www.ibm.com/blogs/blockchain/2018/01/ why-blockchain-and-iot-are-best-friends
22. K. Christidis and M. Devetsikiotis, ''Blockchains and smart contracts for the Internet of Things,'' IEEE Access, vol. 4, pp. 2292–2303, 2016.
23. A. Jeppsson and O. Olsson, ''Blockchains as a solution for traceability and transparency,'' Packag. Logistics, Lund Univ., Lund, Sweden, Student Paper, Tech. Rep., Jun. 2017.
24. J. Pouwelse, P. Garbacki, D. Epema, and H. Sips, ''The bittorrent P2P file-sharing system: Measurements and analysis,'' in Peer-to-Peer Systems IV, M. Castro and R. van Renesse, Eds. Berlin, Germany: Springer, 2005, pp. 205–216.
25. J. Ernst et al. (Mar. 2018). The Power of Connectivity in the Hands of the People. [Online]. Available: https://steem.io/steem-whitepaper.pdf
26. T. Rightmesh. (Mar. 2018). Rightmesh is Starting a Revolution With Blockchain and Mesh Networks. [Online]. Available: https://yourstory.com/2018/03/rightmesh-blockchain-mesh-networks
27. D. P. Anderson, ''BOINC: A system for public-resource computing and storage,'' in Proc. 5th IEEE/ACM Int. Workshop Grid Comput., Nov. 2004, pp. 4–10.

Reference

28. A. L. Beberg, D. L. Ensign, G. Jayachandran, S. Khaliq, and V. S. Pande, ‘‘Folding home: Lessons from eight years of volunteer distributed com- puting,’’ in Proc. IEEE Int. Symp. Parallel Distrib. Process., May 2009, pp. 1–8.
29. B. Dickson. (Dec. 2016). How Blockchain Can Create the World’s Biggest Supercomputer. [Online]. Available: https://techcrunch.com/2016/12/27/ how-blockchain-can-create-the-worlds-biggest-supercomputer
30. Z. Hong, Z. Wang, W. Cai, and V. C. M. Leung, ‘‘Connectivity-aware task outsourcing and scheduling in D2D networks,’’ in Proc. 26th Int. Conf. Comput. Commun. Netw. (ICCCN), Jul./Aug. 2017, pp. 1–9.
31. Z. Hong, Z. Wang, W. Cai, and V. C. M. Leung, ‘‘Blockchain-empowered fair computational resource sharing system in the D2D network,’’ Future Internet, vol. 9, no. 4, p. 85, 2017.
32. A. Beikverdi and J. S. Song, ‘‘Trend of centralization in bitcoin’s dis- tributed network,’’ in Proc. IEEE/ACIS 16th Int. Conf. Softw. Eng., Artif. Intell., Netw. Parallel/Distrib. Comput. (SNPD), Jun. 2015, pp. 1–6.
33. C. Natoli and V. Gramoli, ‘‘The blockchain anomaly,’’ in Proc. IEEE 15th Int. Symp. Netw. Comput. Appl. (NCA), Oct./Nov. 2016, pp. 310–317.
34. K. O’Hara, ‘‘Smart contracts–dumb idea,’’ IEEE Internet Comput., vol. 21, no. 2, pp. 97–101, Mar./Apr. 2017.
35. N. Atzei, M. Bartoletti, and T. Cimoli, ‘‘A survey of attacks on Ethereum smart contracts (SoK),’’ in Proc. 6th Int. Conf. Princ. Secur. Trust, vol. 10204. New York, NY, USA: Springer-Verlag, 2017, pp. 164–186.
36. M. Wohrer and U. Zdun, ‘‘Smart contracts: Security patterns in the Ethereum ecosystem and solidity,’’ in Proc. Int. Workshop Blockchain Oriented Softw. Eng. (IWBOSE), Mar. 2018, pp. 2–8.
37. K. Bhaskaran et al., ‘‘Double-blind consent-driven data sharing on blockchain,’’ in Proc. IEEE Int. Conf. Cloud Eng. (IC2E), Apr. 2018, pp. 385–391.
38. K. Croman et al., ‘‘On scaling decentralized blockchains,’’ in Proc. Int. Conf. Financial Cryptogr. Data Secur. Berlin, Germany: Springer-Verlag, 2016, pp. 106–125.
39. S. Rouhani and R. Deters, ‘‘Performance analysis of Ethereum transactions in private blockchain,’’ in Proc. 8th IEEE Int. Conf. Softw. Eng. Service Sci. (ICSESS), Nov. 2017, pp. 70–74.
40. A. Rosic. (Oct. 2017). Proof of Work Vs Proof of Stake: Basic Mining Guide. [Online]. Available: https://blockgeeks.com/guides/proof-of-work- vs-proof-of-stake
41. G. Greenspan. (2015). Multichain Private Blockchain–White Paper. [Online]. Available: https://www.multichain.com/download/MultiChain- White-Paper.pdf

Thank you.