DLT and Blockchain Technology Outlook

IEEE Blockchain Technical Briefs (BCTB) 2024

Editor in Chief: Justin Y. Shi | justinshi@ieee.org
Editorial Board:
Boleslaw Szymanski | boleslaw.szymanski@gmail.com
Lakshmi Shankar Ramachandran | rlshankar@emory.edu
Imran Bashir | drequinox@gmail.com
Goga Nicolae | n.goga@rug.nl
Constantin Viorel Marian | constantinvmarian@gmail.com

April 2024

Transactions record histories and are mission critical. Transaction processors are the timeless essentials of all cyber infrastructures for mission critical applications. Traditional transaction processors are vulnerable to hacks, natural and malicious attacks. Since 2008, blockchain technology emerged as a new type of distributed ledger technology (DLT). It has demonstrated unprecedented service reliability and tamper resistance that outshined legacy transaction processing methods and centralized trust management systems. At IEEE BCTB2023, we have received many blockchain technology inspired application proposals from the community. Thank you!

From software architecture perspective, the starkest contrast of blockchain-based DLT methods compared to traditional transaction processing is the complete program and data decoupling from physical hardware components, such as networks, processors, and storage devices. Therefore, the blockchain service has no single-point failures. Storing the distributed ledgers in cryptographic proof chains afforded a level of security that is more reliable and less expensive than human-powered trust management systems. However, it is still not clear if all applications should be decentralized. For long term sustainability, the ledger immutability and scalable performance continued to be non-trivial challenges.

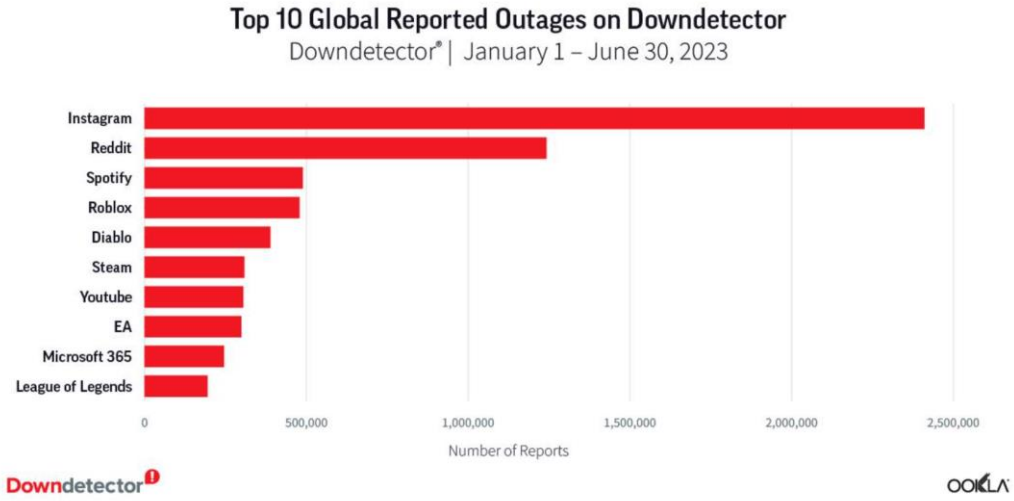
Nearly two decades of blockchain research and experiments have converged to the same performance scalability challenge: how to deliver database-like transaction processing performance while keeping the blockchain reliability and security benefits. Traditional databases rely on data partitioning (vertical or horizontal) to gain high performance. However, higher performance can only be delivered with negative impacts on service reliability, availability, and security. This was the well-known database scaling dilemma [1]. Applying data partition in blockchain protocol adds a new dimension to the database scaling dilemma. Blockchain scalability is now a trilemma [2]. Unless there is a provable infinitely scalable storage protocol design, the currently proposed data “sharding” [3] and multi-chain solutions [4-7] can only “kick the can down the road”.

Different nomenclatures were created to identify the scalability of a service infrastructure. For sustainable transaction processing in general, the service infrastructure scalability requirements are very simple: how to deliver incrementally better performance, reliability and security as the network expands. There should be no single-point failures (remember the AOA sensor for Boeing 737 Max’s MCAS deadly accidents?) For Open-Source projects, tamper resistance is also required.

There are at least three well-known impossibilities for traditional database transaction processing. These include the “danger of transaction replication” [8], “the impossibility of implementing reliable communication in the face of crashes” [9], and the “CAP Theorem” [10]. The blockchain experiments seem to break all these impossibilities [11]. The blockchain successes inspired new applications, including NFT (non-fungible tokens) and DeFi (decentralized finance) applications. However, broad applications of blockchain technology still require, in addition to the complete program/data decoupling, a truly performance scalable solution that is also tamper resistant and energy efficient.

As mentioned earlier, it is still also not clear if all applications should be decentralized and approved by anonymous users. Many applications still require centralized authentication, such as KYC (know your customer) for fraud prevention and for regulatory compliance in financial services [12-13].

Meanwhile, existing infrastructures have become increasingly more vulnerable. In the first three months of 2024, there are multiple USA nation-wide infrastructure outages. These include AT&T network that is responsible for running the FirstNet (first responder network authority), February 29 UnitedHealthCare was hit with a ransomware attack that stopped nation-wide insurance payment processing; in January, PA court system suffered DDoS attack causing prolonged outage, and March 5, 2024 Comcast network observed a sudden congestion without network re-routing activities. Some speculated that the recent solar flares may have contributed to these outages. In contrast, the global Bitcoin network was completely unaffected.



The strength of blockchain technology is also impacting financial policies. The U.S. financial regulatory conditions improved in favor for accepting cryptocurrency as ETF (electronic trading funds) [14], it indicates a window of opportunity for the blockchain technologies to become accepted by mainstream transaction processing industry. We hope to see more of these new technological developments in 2024.

Peer-to-peer or decentralized computing has caught the public's imagination. As the blockchain protocols differ fundamentally from the traditional web services and transaction processing methods, web3.0 was proposed to name these efforts. At the beginning of 2024, it is still not clear if all future applications should be decentralized. Although the blockchain immutability, transaction transparency and tamper-proof encryption provide great measures for data privacy, integrity and security, the centralized authentication for fraud prevention still seems unavoidable in many applications before the technologies could be widely adopted. To date, progress has been slow. We encourage submissions focusing on the

foundational blockchain challenges. The 2024 IEEE BCTB will be publishing the latest blockchain technology developments in industry, academic and government agencies.

References

1. M. Allen, "Relational Databases are Not Designed to Scale," Data Platform Blogs, Retrieved 2024: https://www.progress.com/blogs/relational-databases-scale
2. N. Crooks, "What is the Blockchain Trilemma?" The BLOCK News, Retrieved 2024: https://www.theblock.co/learn/249536/what-is-the-blockchain-trilemma
3. Consensys, "The Ethereum 2.0 Beacon Chain is Here. Now What?," https://consensys.net/blog/blockchain-explained/the-ethereum-2-0-beacon-chain-is-here-now-what/ , Retrieved 2024.
4. Cosmos.network, "Build on the Interchain," https://cosmos.network/ , Retrieved 2023.
5. Polkadot.network, "The multichain vision for Web3," https://polkadot.network/ , Retrieved 2024.
6. Tendermint.com, "Powerful & Secure Software for the Decentralized Future," https://tendermint.com/ , Retrieved 2024.
7. Polkadot.network, "Parachains' Protocol Overview," https://wiki.polkadot.network/docs/learn-parachains-protocol , Retrieved 2024.
8. J. Gray, P. Helland, P. O'Neil, D. Shasha, "The Dangers of Replication and A Solution," ACM SIGMOD Record, v25,2, June 1996.
9. A. Fekete, N. Lynch, Y. Mansour, and J. Spinelli, "The Impossibility of Implementing Reliable Communication in the Face of Crashes," JACM, Vol 40, No. 5, November 1993.
10. S. Gilbert, N. Lynch, "Brewer's Conjecture and the Feasibility of Consistent, Available and Partition-Tolerant Web," Laboratory for Computer Science, MIT, MA 02139, 2001.
11. Satoshi Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," https://bitcoin.org/bitcoin.pdf , 2008.
12. Dow Jones, "Risk and Compliance Glossary," Retrieved 2024: https://www.dowjones.com/professional/risk/glossary/know-your-customer/
13. Investopedia, "Distributed Ledger Technology(DLT): Definition and How It Works," Retrieved 2024: https://www.investopedia.com/terms/d/distributed-ledger-technology-dlt.asp
14. L. Lumley, "Much Anticipated, the US SEC approves bitcoin ETFs," The Banker.com, Retrieved 2024: https://www.thebanker.com/Much-anticipated-the-US-SEC-approves-bitcoin-ETFs-1705393382#:~:text=In%20a%20move%20widely%20anticipated,moment%20for%20the%20crypto%20industry.
15. Raphael Satter, Christopher Bing and Patrick Wingrove, "Healthcare providers hit by frozen payments in ransomware outage," REUTERS, retrieved 3/25/2024: https://www.reuters.com/technology/cybersecurity/healthcare-providers-hit-by-frozen-payments-ransomware-outage-2024-02-29/
16. Jonathan Greig, "DDoS attack on Pennsylvania …", retrieved 3/25/2024: https://therecord.media/ddos-attack-knocks-pennsylvania-court-system-services-offline