Journal of Database Systems (1) 2021 01-10 Submitted 11/20; Published 11/20

Summary of the Lecture Presentation on Blockchain Data Management With Specific Reference to Byzantine Consensus

Joshua Ryan Steenson joshua.ryan.steenson@gmail.com
Michael Anthony Marler michael.marler2@student.montana.edu
Samuel Caekaert samdcaek@gmail.com

Editor: Joshua Ryan Steenson, Michael Anthony Marler, Samuel Caekaert

References

K. Orlando. Non-Fungible Guide of Ars Technica to NFTs, 2021. URL https://arstechnica.com/gaming/2021/03/ars-technicas-non-fungible-guide-to-nfts/.

A. Silberschatz, H. F. Korth, and S. Sudarshan. *Database System Concepts, Seventh Edition.* McGraw Hill, 2020.

A blockchain is defined to be a data structure that functions as a linked list of blocks of data, thereby comprising a log of updates for a given set of data. A blockchain can either be considered public such that anyone can be granted access to maintain it or permissioned such that only a permissioning authority authorizes access to maintain it (Silberschatz et al. (2020)). The pointers of the blockchain include not only the identifier of the next older block, but also a hash of that older block (Silberschatz et al. (2020)). Beginning from the genesis block created by the creator of the blockchain, whenever a block is added to the blockchain, both the pointer and the hash of the previous block are included when the blockchain undergoes an insertion operation, thereby rendering any block in the blockchain, along with its successor, affected by any and all changes in the blockchain. The property of tamper resistance is also the result of the mathematical properties of the hash functions that enable this level of interdependence in the blockchain operations. At a very fundamental level, there are two types of attacks that have the potential to maliciously affect the nodes in a blockchain. Whereas a Sybil attack overwhelms the majority of the nodes present in the blockchain in a computational capacity, the malicious variant of forking adds new blocks to blocks in the blockchain other than the most recent blocks (Silberschatz et al. (2020)).

Byzantine consensus, which is a form of consensus intended to ascertain the correct state of the blockchain, determines whether a given block can be added to the chain depending on the extent to which a node is considered to be malicious, doing so with a great capacity for tolerance of the potentially malicious nodes that are the result of a Sybil attack. Proof of work and proof of stake are also consensus algorithms that utilize mathematical problems to ascertain that the correct block is added to the chain and selects the next node based on the currency value utilized by the nodes of the blockchain, respectively (Silberschatz et al. (2020)). Blockchains are decentralized with limited central authority for both variants, resistant to tampering, irrefutable, and anonymous (Silberschatz et al. (2020)).

Byzantine consensus is predicated on its tolerance for potentially malicious nodes, proof of work utilizes cryptographic hash functions to determine whether a node is considered to be appropriate, essentially subjecting a given node to work, and with proof of stake, the probability of mining new blocks scales relative to the currency stake of each node in the chain (Silberschatz et al. (2020)). For managing data in a blockchain, a valid transfer of data requires that the transaction is syntactically well formed, a valid transfer of data requires a signature by the user submitting that valid transfer of data so that it can be verified, and the transaction for a valid transfer of data must not have already been spent, so to speak (Silberschatz et al. (2020)).

- Postchain utilizes a consensus algorithm based on Byzantine fault tolerance. Because it is also a database model that is relational and based on SQL, the documentation for Postchain permits many features that are key to a relational database model and a database model based on the blockchain data structure (Silberschatz et al. (2020)).

- Another database model that is considered to be based on the blockchain is known as BigChainDB, which is a document store non-relational database model that utilizes MongoDB. While it utilizes a different consensus algorithm, it appears to support many of the features, if not all of the features, of the blockchain (Silberschatz et al. (2020)).

- For a blockchain database, the advantages are decentralization, immutability and transparency, while the disadvantages are resource consumption, scalability, and size (Silberschatz et al. (2020)).

One of the most interesting practical application of blockchains is the utilization of non-fungible tokens, which are built on the ERC-71 standard (Orlando (2021)). With the capacity to represent any digital object, a non-fungible token **(NFT)** is an indivisible smart contract (analogous to an atomic unit) with an associated blockchain digital ledger to certify whoever owns a distinct NFT (Orlando (2021)).