PPP Project: Blockchain and Scaling Enterprise Networks

Brian Arturo Cuevas Fuentes, Ashton Curry and Connor Kreis

University of Alaska Anchorage

CSCE 365: Computer Networks

Pradeeban Kathiravelu

Sep 14, 2023

Abstract

The purpose of this paper is to give insight into the history of Blockchain technology, to then explain the basic functionality of the systema and visualize how it is applied nowadays in scaling distributed networks .

Keywords: Computer Science, Blockchain, Python, Cryptocurrency, Distributed Networks

Introduction

Most people have heard about cryptocurrencies, and the most popular of its kind, Bitcoin (Statista). However, a lot of people confuse Bitcoin with blockchain, when in reality Bitcoin is a virtual currency and blockchain is the system behind what makes Bitcoin safe and possible. We will explore the history of blockchain, how blockchain works on the theoretical level, and how blockchain is used today. We will also design and implement our own blockchain application that attempts to solve the issue of scaling enterprise networks in a Wide Area Network (WAN). The goal is to allow multiple organizations to securely exchange data over a shared network that all entities can trust.

History of Blockchain

The system has its origin in 2008 when Satoshi Nakamoto made the concept of "Distributed Blockchain" a reality by publishing his paper "A Peer-to-Peer Electronic Cash System" (Marr). However, Nakamoto didn't come with the idea by himself as Blockchain technology started to develop as early as 1991 by different researchers, but failed to become used (GeeksforGeeks). It wasn't until 2004, when Cryptographic activist Hal Finney introduced the system of "Reusable Proof of Work" to shake the history of Blockchain and Cryptography. This new system solved the "Double Spending problem by introducing by keeping the ownership of tokens registered on a trusted server" (GeeksforGeeks). Despite this, Nakamoto took the idea of "Secured Chain of Blocks" from Merkle Tree research in 1992, which led to the innovation of Blockchain.

One proof that the system is secure became news in 2009, when an IT worker from the United Kingdom named James Howels mined bitcoin from 2009 to 2013, but sold most parts of his laptop and only kept the drive to keep on working on Bitcoin later. Unfortunately, he trashed the drive some time after, leaving around $127 million behind that still remains unclaimed on Bitcoin's database (GeeksforGeeks).

In 2013, an initial contributor of the Bitcoin codebase, Vitalik Buterin, noticed the limitations in the system and pushed for a more malleable blockchain. Due to the resistance from the Bitcoin community, Buterin pursued the development of a second public blockchain and Ethereum, ending in him being the Co-Founder of it. In 2014, entrepreneurs realized the impact of the technology and they decided to start investing in it, leading to the immense growth in popularity (Marr). By 2015, Ethereum Frontier Network was launched leading developers to the creation of smart contracts and dApps (GeeksforGeeks); digital applications that run on a blockchain network of computers.

How Blockchain Works

At its core, blockchain is a publicly available ledger that is completely resistant to tampering. This tamper resistance is due to the nature of SHA-256 encryption and how it relates to a blockchain. When a new block is added to the blockchain, the contents of the block are then run through a SHA-256 cryptographic hash function that returns an almost certainly unique 256-bit number that is then included on the block's header as a form of identification. This is the part that makes the ledger unalterable, since even minorly changing a single value on the ledger will drastically alter the outcome of the cryptologic hash. (Handschuh, 2014) This key attribute of cryptologic hashing is how trust in the contents of the blockchain is formed, since the trust does not need to be placed in the individuals who created the block who are complete strangers to you, but rather the trust is placed in the highly secure process that creates the blocks in the first place.

Since new blocks on the blockchain are mined from the previous block's header, a long list of blocks can be traced back to the genesis of the blockchain itself with an extremely high level of confidence in the authenticity of each block's contents. Whenever new transactions are to be included in the blockchain, they are simply added to a new block that points to the previous block in the chain, and so on. A "transaction" in this context is essentially any new update to the state of the network. In the case of cryptocurrencies, this would be cash payments to other users on the network, however a transaction can really be anything the network defines them as. This could include additions of new users on the network, changes to the nodes on the network, etc.

Blockchain & Functionality

As mentioned by the Institute of Electrical and Electronic Engineers (IEEE), Satoshi Nakamoto created a blockchain to solve trust issues with distributed systems which are systems containing legal information. More specifically, by creating timestamps in node blocks (a software data structure) that will form part of a ledger that register data of a transaction. (Di Pierro)

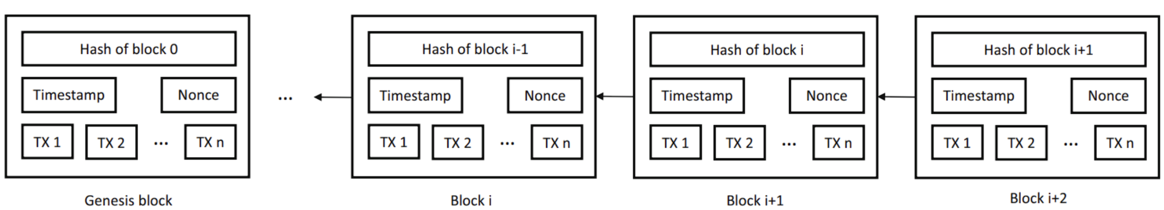

Fig. 1 Basic Blockchain Structure (Nofer)

Blockchain, Enterprise & Networks

The usefulness of blockchain across the enterprise has little to do with the financial implementations but instead with the more exclusive, private blockchains. As mentioned above, transactions on a blockchain can be more than just the cash transactions we normally associate with blockchains, and can instead be any update to the network in general. Helebrandt, et al. showed just that in 2018. In this case, blockchain technology was utilized to help monitor nodes across the enterprise network. Essentially, an administrator on the network would submit an update to a node, add it to the ledger, and add it to the blockchain. Once that update to the chain is received by the node or nodes affected by the update, the node then proceeds to update based on the administrator's specifications, and confirmation is then added to the ledger.

The process described above can be advantageous for networks of increasing size. As the size of a network increases, the complexity of maintaining that network also increases. This process serves as a way to effectively communicate needed updates to the network and allows errors in the process to be easily spotted. For instance, if a confirmation transaction is never recorded by the affected node, then it's safe to assume that the update never went through, making it very easy to pinpoint the exact nodes which are out of date and potential security risks. It also serves as a very detailed log of all of the updates across the network, making it very easy to troubleshoot exactly when a problem may have occurred and easily identify the troublesome changes or updates and quickly address the issues. The added level of security on top is the inalterability of a blockchain's ledger, making it easy to spot any inconsistencies in the network's transactions.

The utility of blockchain can even be seen across different enterprises. In 2020, Yang et. al. demonstrated the practical usefulness of blockchain in a very unexpected business: construction. By using blockchain technology, they were able to leverage the security advantage of an immutable ledger by logging transactions across all steps in the construction process. This had the effect of improving the transparency of business transactions and made all transactions traceable. This can help improve project supervision and reduce potential waste by being able to easily audit all transactions and quickly note any inconsistencies. This can further improve efficiency in the long run by being able to study trends easily due to the transparent nature of blockchain. Additionally, due to the immutable nature of a blockchain's ledger, it insulates itself from any fraudulent tampering.

While blockchain technology can be very useful and advantageous in certain scenarios, it certainly has its fair share of issues that prevent it from becoming a dominating technology across all enterprises today. One such issue that is faced by public blockchains as seen in the cryptocurrency world is scalability. Bitcoin, for instance, can handle very few transactions when compared to well established banking and credit agencies with generous estimates being as high as 27 transactions per second (Georgiadis, 2019). This speed penalty is mostly related to the public nature of these blockchains, however, and private implementations avoid many of the penalties incurred by their public counterparts. With a limited number of users that are permitted access to the blockchain, transaction throughput becomes a much smaller concern and the security and traceability advantages can be more effectively leveraged to scale the overall network.

TODO FOR CONNOR: EXPLAIN THE DIFFERENCE BETWEEN PUBLIC AND PRIVATE BLOCKCHAINS (consortium blockchains too)

Implementation of Blockchain in Python

There have been many demonstrations of blockchain technology applications in the real world. Anything on a network requiring transactions can have blockchain applied to it. Supply chain transparency (Glgor et al., 2022), Internet of Vehicles (IoV) distributed network architecture (Jiang et al., 2019), and decentralized storage (Shawn et al., 2016) are just a few applications of blockchain technologies. Each of these blockchain architectures look to solve the same problem: finding a decentralized, secure, and transparent way to exchange data and store the transactions. The particular problem we wish to solve is that of communications between two enterprise networks on a WAN. Both enterprises want to transact data with each other, and with other users on the WAN. The problem of transparent, secure and efficient data transfers is an issue for all involved.

Implementing blockchain technology will be our solution to this problem, as it has been to the various other applications mentioned in the literature. With this technology, each participant on the network will have a copy of the ledger, with secure transactions that are immutable and verifiable.

Solution Architecture

The solution architecture for this problem will follow a six step process that we will use to develop and implement for our program. As this is a course for computer networks and the time to develop a live solution is limited, we will create a simplified real world scenario within a controlled environment where the principles of blockchain technology can be effectively demonstrated and analyzed. Here are the six steps to our implementation:

1. **Define the Networks**

We will set up two separate networks that will represent our enterprises. We will host them on separate laptops to represent two separate entities. Each network will consist of multiple clients, processes and systems to simulate a real enterprise system. For the sake of simplicity, we will name our Enterprises “Enterprise A” and “Enterprise B”.

2. Set Up Blockchain Infrastructure

Our design will utilize the Ethereum platform for our blockchain. The choice to use Ethereum, which is a public focused blockchain, was that other platforms like Hyperledger are tailored more for professionals in industry rather than the community. It is also well documented and easier to produce with. Theoretically we would only need a single node from each network to participate in the blockchain, but there will be multiple nodes set up for each network.

3. Implement Smart Contracts

The next step is to develop and deploy the smart contracts for the system. These will govern the transactions/data exchanges that occur between Enterprise A and and Enterprise B. The data that will be exchanged is messages composed of strings between the simulated nodes/users.

4. Develop API for Integration

The creation of an API will allow us to interact with the blockchain by sending and receiving message strings that will trigger smart contracts. We will create a simple user registration, which allows users to connect and chat through a chat session. They will be able to message each other with the blockchain technology which will create smart contracts and transactions on the blockchain. For the sake of simplicity, we won’t consider real-time updates, security, or privacy. We will also have minimal error handling, as we are demonstrating the technology and not using real users on the system.

5. Frontend Interface

The frontend will be a simple interface showcasing how users within each network may view or input data for the chats. It will show how the blockchain ledger is updated and allows users to track or verify message transactions on the blockchain.

6. Demonstrate Interoperability

Our two networks will be able to establish simple chat communications across our public blockchain network using Ethereum. Our scenario will involve users connecting and sending messages over the chat system to display data exchanges that are verified securely and transparent on the blockchain.

References

Di Pierro, Massimo. “What Is the Blockchain?” *Computing in Science and Engineering*, vol. 19, no. 5, AIP Publishing, Jan. 2017, pp. 92–95. https://doi.org/10.1109/mcse.2017.3421554.

GeeksforGeeks. “History of Blockchain.” *GeeksforGeeks*, 6 Oct. 2023, www.geeksforgeeks.org/history-of-blockchain. Accessed 8 Oct. 2023.

Helebrandt, Pavol, et al. “Blockchain Adoption for Monitoring and Management of Enterprise Networks.” *IEEE Xplore*, Nov. 2018, https://doi.org/10.1109/iemcon.2018.8614960.

Nofer, M., Gomber, P., Hinz, O., & Schiereck, D. (2017). Blockchain. Business & Information Systems Engineering, 59(3), 183-187. https://doi.org/10.1007/s12599-017-0467-3

Marr, Bernard. “A Very Brief History of Blockchain Technology Everyone Should Read.” *Forbes*, 16 Feb. 2018, www.forbes.com/sites/bernardmarr/2018/02/16/a-very-brief-history-of-blockchain-technology-everyone-should-read/?sh=5bc41b9e7bc4.

Sherman, Alan T., et al. “On the Origins and Variations of Blockchain Technologies.” *IEEE Security & Privacy*, vol. 17, no. 1, Institute of Electrical and Electronics Engineers, Jan. 2019, pp. 72–77. https://doi.org/10.1109/msec.2019.2893730.

Statista. “The 21 Most Popular Cryptocurrencies in the U.S. 2021-2023.” *Statista*, 29 Aug. 2023, www.statista.com/statistics/1238481/crypto-ownership-usa-type.

Gilbert, H., Handschuh, H. (2004). Security Analysis of SHA-256 and Sisters. In: Matsui, M., Zuccherato, R.J. (eds) Selected Areas in Cryptography. SAC 2003. Lecture Notes in Computer Science, vol 3006. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-540-24654-1_13

Nakamoto, Satoshi (2008) Bitcoin: A Peer-to-Peer Electronic Cash System. Bitcoin.org

Yang, Rebecca, et al. "Public and private blockchain in construction business process and information integration." *Automation in construction* 118 (2020): 103276.

Georgiadis, Evangelos. “How many transactions per second can bitcoin really handle ? Theoretically.” *IACR Cryptol. ePrint Arch.* 2019 (2019): 416.

Gligor, D. M., Davis-Sramek, B., Tan, A., Vitale, A., Russo, I., Golgeci, I., & Wan, X. (2022). Utilizing blockchain technology for supply chain transparency: A resource orchestration perspective. *Journal of Business Logistics, 43*(1), 140-159. doi:10.1111/jbl.12287

T. Jiang, H. Fang and H. Wang Jiang, T., Fang, H., & Wang, H (2019). Blockchain-Based Internet of Vehicles: Distributed Network Architecture and Performance Analysis. *IEEE Internet of Things Journal*, 6(3), 4640-4649. doi: 10.1109/JIOT.2018.2874398.

Shawn, W., Tome, B., Josh, B., & Vitalik, B. (2016). Storj: A peer-to-peer cloud storage network.