Decentralized Time Clocking System

CS4991 Capstone Report, 2024

Alexander Johnson
Computer Science
The University of Virginia
School of Engineering and Applied Science
Charlottesville, Virginia USA
alexjohnson0123@gmail.com

ABSTRACT
Possible implementations for blockchain based decentralized systems have been underexplored. I propose a decentralized time clock system that does not need to rely on a third-party as most time clock systems do. Instead, it uses the Ethereum blockchain to securely track and store data. The system can be accessed via a website or mobile app by employers to view hours and pay wages, and by employees to clock in and out, as well as receive their wages. The goal of this system is to create a more direct relationship between the employer and employee, increasing access and reliability over traditional payroll systems. Future work would require an encryption system, as well as new decentralized systems in other fields.

1. INTRODUCTION

To understand the workings of this proposed system, we must first understand what a centralized vs decentralized system is. A centralized system is the traditional framework that digital systems run on in the internet age. The system is managed by a third party who is in charge of the physical hardware the system runs on, as well as all of the data stored in the system. This third party has all of the control; users must conform with the rules that the third party sets up.

For example, consider a centralized time clock system. We'll call it, "Clockr." To interface with the Clockr system, the employee opens the Clockr app and clocks in. The request is sent to Clockr servers and then entered into the Clockr database. In order to get paid, it is up to Clockr to interface with the user's bank to make sure money gets transferred from the employer's account to the employee.

The whole system is reliant on this third party, "Clockr" in this example, which is fine as long as Clockr is reliable and trustworthy. However, corporations are not infallible and tend to serve the needs of the shareholder over the user. What if Clockr decides to double their fees? What if they decide to stop accepting a certain currency? What if their services or data are the target of a cyberattack? Assume the system works as intended, the weak point becomes the party in charge of the system. The benefit of a decentralized system is to remove that third party, allowing the system to function directly with the users.

2. RELATED WORKS

Stackpole (2023) overviews the concept of web3, which some call the "next phase" of the internet. What this next phase entails is blockchain integration. While "web2" uses javascript integration to enable things like interactive web pages and games, web3 enables another slew of new features. These features involve "decentralized apps" that live or store data on the blockchain instead

of a traditional web server or database. For example, the web3 streaming service sound.xyz uses the blockchain features of web3 to provide a more fair way to convert user listens into payment for the artists.

While there are many promises about what web3 could be and what it could achieve, the practical use is still uncertain. The proposed system aims to explore the use of web3 and blockchain applications in order to develop our understanding of the technology.

According to Mason (2019), the advent of decentralized systems reflect changes in our world, and the unique advantages that these systems offer may be essential to the function of our world in the future. As we have become more globalized, our laws and systems have started to stretch thin. The idea is that the world runs on "trust"—trust that currency can be exchanged for goods, that contracts will be respected, that banks will return money when asked, and a long list of other things. What if we could replace "legal trust," with "programmable trust"? The blockchain provides for a means of trust that runs not by contract backed by force, but trust that runs on code, backed by cryptographic algorithm.

3. PROPOSED DESIGN

This system would run as a "smart contract" on the Ethereum blockchain. First, a quick overview of "blockchain." A blockchain is a decentralized data structure. Traditionally, this data structure keeps track of the transfer of crypto currency. Every transaction is recorded, and kept forever in the blockchain. Instead of being maintained by dedicated servers, it is maintained by users around the world who are incentivized by "mining" rewards. The idea is that by pooling the world's computing power into maintaining the security of the system, no single attacker can attack the system, and if an attacker was powerful enough to attack the system, it would be more profitable for them to mine normally and collect the cryptocurrency reward for doing so.

The system is set up with cryptographic algorithms so that the contents of each "block" in the blockchain is dependent on every block that has come before it. To make a change in a block would require changing every block afterwards; and figuring out what these changes would have to be would require an impossible amount of computing power. Therefore, when a transaction is recorded into the blockchain, it effectively becomes unchangeable. Within minutes of entering the transaction, it is recorded globally, and within an hour, unless the entire system fails, it becomes impossible to change, forever.

While the Ethereum blockchain is a decentralized system mainly used for the transfer of Ethereum cryptocurrency, it is capable of much more. The Ethereum blockchain can store not only cryptocurrency transactions, but also programs. The program's code is stored on the blockchain, along with all of its data. Each time the program's data is changed, it is recorded on the blockchain just as it records cryptocurrency transactions. Additionally, these "smart contract" programs can hold, receive and pay cryptocurrency to other Ethereum accounts.

This means that it is a possible feature for the proposed system to directly pay employers in cryptocurrency, if cryptocurrency is adopted to the point that wages are paid directly though the blockchain, though this system can be implemented with traditional banking services, as well.

The design of the system consists of a smart contract running on the Ethereum blockchain, and local applications that interact with the smart contract. Employees run an application on a local device such as a phone, and once at the physical time clock, they are able to acquire a time-sensitive cryptographic signature from the time clock (through means such as nfc scanner or qr code) and use that to verify their "clock in." Their mobile application will then send this clock-in to the smart contract on blockchain. Once minted to the blockchain, the "clock-ins" and "clock-outs" are irreversible, and stored forever. As long as the Ethereum blockchain is maintained; the employee will have concrete, public and unchangeable records of their work. The employers will be able to use their own employer-specific application that will check the hours worked by each employee, and payout the labor using either traditional banking or directly using cryptocurrency. In a cryptocurrency implementation, the account employees use to log their hours will be the same account that receives the Ethereum cryptocurrency.

4. ANTICIPATED RESULTS

This proposed system is not meant to be a finalized transformation of the time clocking system; rather, it is an exploration into one of many applications of blockchain technologies. This exploration will deepen understanding of the interaction of individuals and organizations with the blockchain and the challenges that arise therein. This means that the user-based results are uncertain. A trial run of this system would be invaluable in gauging the practicality of the system. It would be important to collect user satisfaction with aspects of the system such as speed, convenience, reliability and ease of use.

However, in regards to the security of the system, the expectation is high. This does not mean that it is guaranteed to be flawless, as user error in the development of the smart contract program can easily lead to security holes, resulting in the loss of money, or the modification of records. But if the program is meticulously developed and tested with a mindset of security, I expect it to be strong, practically unbreakable.

5. CONCLUSION

By outlining a decentralized timeclock system, I have demonstrated a possible use case for blockchain technology. This system aims to leverage the unique qualities of the blockchain in order to provide a service in a way that sidesteps traditional third party providers. In doing so, it works towards a goal of understanding the abilities and the limits of blockchain technology. The development and testing of this proposed system would serve to provide an example for future blockchain implementations to build off of, and to inform of the general usefulness of the technology itself.

6. FUTURE WORK

Future work will involve further investigation into blockchain technology implementations. That will include iteration over the proposed system. An importation addition would be an encryption system. Since blockchain data is public, any practical implementation would require a way for the information to only be readable by privileged parties. Encrypting the data would ensure data privacy while keeping the data easily accessible by users.

Additionally, and perhaps more importantly, future work should be done that views this system as an example for other possible uses. There are many opportunities in new areas in which the technology may be useful. The more legitimate uses a blockchain system can support, the more

justified the widespread use of the system will become.

REFERENCES

Mason, M., Spoke, M., & Centre for International Governance. (2019). Programmable Trust: A Practical Approach to Governance in the Digital Age. http://www.jstor.org/stable/resrep26129.17

Stackpole, T. (2023, January 10). What is web3?. Harvard Business Review. https://hbr.org/2022/05/what-is-web3