Money Saving With Time Locked Wallet

Zewei Wu
zwu@oxy.edu
Occidental College

1 Abstract

This research paper is a Occidental College Computer Science Comprehensive Project Proposal regarding my personal project: Time-Locked Wallet. The paper contains seven components, including: Introduction, problem context, technical background, methods, evaluation, ethical consideration, and software documentation. The paper will begin with an introduction of my project, then I will tackle down some of the technical aspects of the project. At the end I will present some ethical considerations regarding this project.

2 Introduction

For this project, I have chosen to build a Time-Locked digital Wallet on smart contract. This wallet will provide the feasibility in college-context and provide insights of students' saving habits and the tendency of practicing cryptocurrency assets.

3 Problem Context

3.1 Importance of Savings

Money management skills are vital life skills, especially for young people, because wealth development is not solely based on an individual's capacity to work hard, but also on aspects such as his or her ability to grasp how money works and implement its management principles. Savings are the backbone of personal financial success, so they are an important part of a person's financial management abilities. Savings entails not just putting money away for future use, but also keeping anything of economic worth. That is to say, saving creates security reassurance for the unknowns of the future.[**Loibl**]

Savings habits play a significant role in daily financial decisions. Research has shown that there is an increasing association between savings and growth. Saving on a regular basis is critical for financial independence and security. Greater savings has been proven to be an important component of fiscal development. To attain personal financial independence in an era of uncertain financial economies, one must ensure and implement smart financial management techniques, of which savings are critically important. As the world is predominantly plagued by ever-increasing rates of unemployment, savings have become vital in the lives of college students who aspire to acquire personal financial independence.[5] As the market continues to evolve with new consumer products, financial literacy in the area of saving is essential.

Even though habit creation is a difficult task, when establishing a saving habit, it can enhance a person's perception and intention to save. When a habit is fully developed, it can also have an positive impact on a person's consumption and savings. Savings is based on one's previous savings as well as a combination of current income changes and the "discounted value of future income changes." The habit of saving is, therefore, extremely important. As optimal financial leverage not only promotes a sound and stable economic life, but it is also critical in ensuring and assuring a better lifestyle in areas such as healthy living, quality health care, education, and better access to basic social amenities.[**Alessie**] Savings is an important element of life because it is required in almost every aspect of life, and the ability to develop the habit will help you achieve financial success.

3.2 Why time-locked wallet?

It is easy for some students, who are still in their early stage of extravagant college lifestyle, to ignore the importance of money savings. Without having any prior knowledge on investing. The effects on time-locked wallets could be equivalent to that of a traditional piggy bank, but in the form of smart contract. Students could use this medium as a savings account but will have no access to the assets before the timer expires. With the ongoing trending attention of smart contract, this could be a great opportunity for students to practice saving and making transaction with cryptocurrency before it becomes a universal trading method.

4 Technical Background

4.1 What is Blockchain

Before we dive into the topic of smart contract, we need to first have a little background on the topic of blockchain. Blockchain technology is used in cryptocurrencies. A distributed and secure database or ledger is referred to as a blockchain. dApps are the applications that conduct transactions and run the blockchain. Transactions are stored in blocks on the blockchain and subsequently validated by other users. If all of the verifiers agree on a transaction, the block is closed and encrypted, and a new block is created containing information from the preceding block. The information in each subsequent block "chains" the blocks together, giving the blockchain its name. There is no method to edit a blockchain since information in prior blocks cannot be modified without impacting subsequent blocks. The secure nature of a blockchain is provided by this notion, as well as other security mechanisms. The blockchain's novelty is that it ensures the fidelity and security of a data record while also generating trust without the requirement for a trusted third party.[3]

4.2 What is Smart Contracts

Smart contracts are essentially programs that run when certain criteria are satisfied and are maintained on a blockchain. They're usually used to automate the execution of an agreement so that all parties can be certain of the conclusion right away, without the need for any intermediaries or time waste. They can also automate a workflow, starting the following step when certain circumstances are satisfied.

The concept of "Smart Contract" was introduced in 1994 by Nick Szabo as "a computerized transaction protocol that executes the terms of a contract".[8] To reduce the need for trusted intermediaries between transacting parties and the incidence of malicious or accidental exceptions, Szabo proposed converting contractual provisions into code and embedding them into property that may self-enforce them.[7]

Smart contracts are scripts stored on the blockchain in the context of blockchain. They're similar to stored procedures in relation to database management systems in terms of functionality. They have a distinct address because they are part of the chain. Smart contract is triggered when sending a transaction. It then operates independently and automatically on every node in the network in a prescribed manner. This means that every node in a smart contract enabled blockchain is running a virtual machine, and the blockchain network acts as a distributed virtual machine.

Smart contracts are self-contained actors whose actions are totally predictable. They may be trusted to advance any on-chain logic that can be represented as a function of on-chain data inputs, as long as the data they need to manage is within their grasp. To fulfill its principal purpose, a smart contract sends an address to another smart contract. The address is stored in the contract's internal database's mutable section. The contract also includes a list of members, whose addresses are used to vote on the company's actions. A rule can be placed in the contract that states that if a majority of the voters vote one way, the contract will change its behavior and call the address that obtained the majority of the votes to perform its main purpose.

Here is a simple example to help you understand the basics of the statements above. Let's say Bobby is trading digital assets Ethereum. Bobby deploys a smart contract defined as "deposit" that allows Bobby to deposit x amount of Ethereum into the contract. Then he deploys another smart contract as "withdraw" that permits him to withdraw all of his digital assets that the contract holds. These "functions" are encrypted in a way that only user "Bobby" can call upon. If Bobby sends an amount of assets to that smart contract's address, using the "deposit" and sends 3 units of ethereum to the contract, this transaction is permanently recorded on the blockchain. If someone else owes Bobby some amount of Ethereum, then the contract checks the signature to make sure the withdrawal is initiated by the contract's owner, and transfers all of its deposits back to Bobby.

Smart contracts actions are totally predictable based on their autonomous actors characteristics . They may be trusted to advance any on-chain logic that can be represented as a function of on-chain data inputs, as long as the data they need to manage is within their grasp. To fulfill its principal purpose, a smart contract sends an address to another smart contract. The address is stored in the contract's internal database's mutable section. The contract also includes a list of members, whose addresses are used to vote on the company's actions. A rule can be placed in the contract that states that if a majority of the voters vote one way, the contract will change its behavior and call the address that obtained the majority of the votes to perform its main purpose.

4.3 Framework

1. Ethereum
2. Truffle Framework

For the project, it will be built on the Ethereum Blockchain, which is a decentralized, open-source blockchain with smart contract functionality. With the use of Truffle framework, the provided resources within the framework should make the time-locked wallet doable.

4.3.1 Ethereum

Ethereum is a decentralized blockchain technology that creates a peer-to-peer network for securely executing and verifying smart contract code. Participants can transact with one another without relying on a trusted central authority. Participants have full ownership and visibility of transaction data since transaction records are immutable, verifiable, and securely distributed across the network. User-created Ethereum accounts are used to send and receive transactions. As a cost of processing transactions on the network, a sender must sign transactions and spend Ether, Ethereum's native coin.[**Eth**]

Using the native Solidity scripting language and the Ethereum Virtual Machine, Ethereum provides an extraordinarily flexible platform on which to create decentralized apps. Decentralized application developers that use Ethereum to create smart contracts benefit from the robust ecosystem of developer tools and well-established best practices that have accompanied the protocol's maturation. This maturity is reflected in the quality of the user experience provided by Ethereum applications, with wallets such as MetaMask, Argent, Rainbow, and others providing straightforward interfaces for interacting with the Ethereum blockchain and smart contracts placed there. Because of Ethereum's massive user base, developers are more likely to put their applications on the network, cementing Ethereum's position as the principal platform for decentralized applications like DeFi and NFTs. The Ethereum 2.0 protocol, which is currently in development and backwards compatible, will enable a more scalable network on which to construct decentralized applications that require higher transaction throughput in the future.[**Eth**]

4.3.2 Truffle Framework

The Truffle framework is a popular development environment for Ethereum dApp development, with a large community of users. Furthermore, its goal is to make smart contract development more basic and accessible.

5 Prior Work

Recent years, the volume of the DeFi market has been growing rapidly. The value of funds that are stored in DeFi smart contracts has reached 10 billion USD in 2021. The study speculates that the growth of these smart contracts assets reflects on DeFi becoming more relevant in the broader context, which can have acute interests to financial institutions and policy makers.[3] However, the article targeted individuals who have an economics or legal background. With this project, it will be focusing on the likelihood of students using smart contracts to store cryptocurrencies assets.

6 Methods

After the wallet platform is built, students will be able to store cryptocurrency for a fixed period of time. Firstly, a survey will be conducted to measure individuals' prior knowledge on smart contracts, prior experience with cryptocurrencies and money savings. Afterwards I will then have a showcase on what the project is about. I will be inquiring about 200 students. The wallet will then be presented to those who show interest in the topic and wish to perform transactions and store assets on the platform. Hopefully I can get more than 30 students to participate in this project. Once the project starts, I will be monitoring the backend to see the amount of assets and time periods the participants set in the wallet. given the time constraint the maximum amount time the participants can lock will be two months. Once every participant has used the wallet and made transactions, time expired on every wallet, another survey will be conducted. This survey will inquire information such as: how this project impacts your perspective on money savings; how likely you will practice cryptocurrency trading/saving in the future etc. Then, all data and tendencies will be presented.

7 Evaluation

8 Ethical Considerations

8.1 DeFi

The current state of decentralized finance related research encompasses a wide range of ethical challenges and situations, as well as a diversified user base. With the continued development of Bitcoin technology and its widespread adoption, it is feasible that this technology may become a global financial transaction mechanism. However, there are still a lot of unsolved questions. These decentralized peer-to-peer transactions raise numerous privacy and ethical concerns. Furthermore, the future of some cryptocurrencies has remained dubious.[6]

Blockchain's immutability Concerning the Blockchain's immutability, an important ethical point must be posed. From an operational standpoint, blockchain is, of course, a fantastic breakthrough. To have a limitless number of immutable transaction records, as well as a large amount of data to support each Ledger entry. Amazing and incomprehensible at the moment. The idea behind the "immutable model" is that having a better collection of "real-time data" will result in better forecasting of bitcoin trends. The removal of ambiguity in the Micro could lead to errors in the Macro. Is technology capable of truly bridging the valuation, accounting, and ledger gaps? Alternatively, the grand

concept of Blockchain may be destined to be used solely for the distribution of information.

Necessity of governance In DeFi, there is a "decentralization illusion," because the necessity for governance necessitates some level of centralisation, and structural characteristics of the system result in power concentration. DeFi's flaws could jeopardize financial stability if it becomes widely used. Due to excessive leverage, liquidity mismatches, built-in interconnection, and a lack of shock absorbers like banks, these can be severe. Existing governance processes in DeFi would serve as natural reference points for authorities when dealing with issues such as financial stability, investor protection, and illegal activities. Various sorts of intermediation support the cryptocurrency markets. DeFi, in theory, can be used to supplement traditional financial activity. However, it currently has few real-world applications and is primarily used for speculation and arbitrage among several crypto assets. Given its self-contained character, DeFi-driven disruptions in the broader financial system and actual economy appear to be restricted for the time being. Concentration can enable collusion and hinder the viability of blockchains. It raises the possibility that a few major validators will gather enough authority to manipulate the blockchain for financial advantage.

While DeFi is still in its infancy, it provides services that are similar to those given by traditional finance and has some of the same flaws. The fundamental mechanisms that give birth to these vulnerabilities — leverage, liquidity mismatches, and their interaction via profit-seeking and risk-management techniques – are all well-known in the established financial system. However, several aspects of DeFi may make them particularly disruptive. We'll start with the role of leverage and run-risk in stablecoins due to liquidity mismatches in this section, then go on to spillover channels to traditional intermediaries.

Money laundering The DeFi ecosystem is continuously evolving, despite its tremendous growth. It is now focused mostly for crypto asset speculation, investment, and arbitrage, rather than real-economy use cases. DeFi is vulnerable to criminal activities and market manipulation due to the insufficient application of anti-money laundering and transaction anonymity. Overall, DeFi's core premise – lowering the rents paid to centralized middlemen – does not appear to have been accomplished.[**Fletcher**] History has shown that the early development of novel technologies is typically accompanied by bubbles and a loss of market integrity, despite the fact that it produces inventions that could be useful to a wider audience in the future. DeFi might still play a key role in the financial system with advancements to blockchain scalability, large-scale tokenization of traditional assets, and, most critically, appropriate regulation to maintain protections and boost confidence.

8.2 Environmental Consideration

Expansion of crypto The explosive growth of cryptocurrencies has been astounding. The global cryptocurrency market was worth 793 million dollars in 2019. According to market research conducted by de Vries, it is now predicted to reach over 5.2 billion dollars by 2026. The global use of cryptocurrencies increased by more than 880 percent in just one year, from July 2020 to June 2021. However, environmentalists are concerned about the growing popularity of cryptocurrencies, because the digital "mining" of it produces a significant carbon footprint due to the massive amount of energy required.

Carbon Emission The amount of energy used by blockchain computation is a significant factor to consider. According to a February 2021 CNBC article, the carbon footprint of Bitcoin, the world's largest cryptocurrency, is equivalent to that of New Zealand, based on data from the Bitcoin Energy Consumption Index from Digiconomist, an online tool created by data scientist Alex de Vries. Both emit nearly 37 megatons of carbon dioxide into the atmosphere every year.[1] This energy-intensive procedure is enabled through "mining," a process in which computer problems are solved in order to authenticate transactions between users, which are subsequently added to the blockchain.[10] According to Digiconomist, the carbon footprint of a single Ethereum transaction was 102.38 kg of CO2, which is "equivalent to the carbon footprint of 226,910 VISA transactions or 17,063 hours of watching YouTube." Meanwhile, a single Ethereum transaction consumes nearly the same amount of electricity as an ordinary US household consumes in 8.09 days, according to the website.[4]

Combined with the fact that major corporations such as ATT, Home Depot, Microsoft, Starbucks, and Whole Foods have begun to accept bitcoin payments, might pave the way for widespread adoption. However, if the bulls are correct and the price of a single Bitcoin finally reaches 500,000 usd, it will emit more CO2 into the sky than countries like Brazil and Mexico.[9]

NFTs The art industry has also been jolted by digital assets, with digital artworks making headlines for the high amounts they've been selling for on the market through the use of nonfungible tokens , NFTs, a sort of guarantee backed by the Ethereum blockchain. According to an article on Hyperallergic, the works are made by a procedure known as proof-of-work, which confirms its unique identity. While this is an improvement over the traditional art market

in terms of preserving the value of the original work, it is extremely harmful to the environment.

Limited supply Another important feature of most cryptocurrencies is that there is a finite supply. As more cryptocurrencies are mined, the complicated math problems required for transactions get more difficult to solve, requiring more energy.[2] The system is set up in such a way that each digital token created has its own unique cryptographic reference to the blockchain, which ensures its security. The problem of energy use over time is aggravated by mining incentives. When a miner solves the complex hashing process required to create bitcoin, they are rewarded with a little amount of the cryptocurrency.

9 Timeline

Timeline	Performing Task
May-August	Build Smart Contract
September	Final testing stage
October-November	Start Survey and experiment with sample groups
December	Finished research and present findings

10 Reference

references