ABIGAIL H. SHRIVER
SELF-TRACKING CRYPTOCURRENCY

December 10, 2016

OVERVIEW

1. Project Background and Description

In a modern world where digital transactions are increasing in popularity by the year, the demand for new innovative cryptocurrencies is high. In 2015, the percentage of smartphones users engaged in mobile banking increased to 53% and mobile payments to 24%. Among these users there is a higher share of young adults who have utilized their phones for digital transactions, demonstrating the popularity and customer base for generations to come in innovating and developing forms of cryptocurrency. Furthermore, of smartphone users reporting they did not engage in utilizing digital transactions through their mobile devices, 73% claimed security concerns as being the main prohibiting factor.

For these reasons, via a secure, user friendly platform, the Self-Tracking Cryptocurrency project seeks to revolutionize digital transactions for individuals and organizations across the world. The Self-Tracking Cryptocurrency project will have two main distinguishing functionalities. First, it will allow the spender to specify and restrict how funds can be used. The system will then automatically verify and approve the use of funds based on the spenders specified restrictions. Second, the cryptocurrency will track transactions and send notifications to the spender and other necessary personnel verifying funds were used appropriately.

Furthermore, the cryptocurrency will implement and enhance current security practices, to address users' security concerns, which are currently deterring them from fully taking advantage of digital transactions. The currency will ensure to implement necessary precautionary measures to prevent social engineering attacks, data breaches, outside infiltration and other common security threats.

The proposed project will address two innovative challenges that will distinguish Self-Tracking Cryptocurrency from current cryptocurrencies. First, the ability to track how funds are being spent over several transactions. Second, the ability for a spender to restrict how funds will be used, and receive notifications that funds were used as specified. The development of algorithms to address these two functionalities will create a system that increases the security of digital transactions for businesses, individuals and organizations.

The proposed system would mark the beginning to a new way in which spenders will have assurance that their funds are utilized in ways they have specified and restricted. Large businesses would be able to automate the allocation of funds from the top although way down to sub-departments, while providing automatic notifications and feedback up the hierarchy that funds have been spent appropriately. Furthermore, government agencies would be able allocate welfare funds and then verify recipients are utilizing funds appropriately. Lastly, nonprofits would be able to allow donors to specify how they desire their donations to be spent, potentially facilitating an increased interest in donating. The adaptability of the cryptocurrency will address several pressing current needs of individuals and organizations.

2. Project Scope and Affected Parties

Self-tracking cryptocurrency will create a unique ability for users to track and restrict digital transactions. This will allow businesses, organizations and individuals across the world to facilitate secure transactions with ease. By specifically designing an interface for two user types, the payee and the receiver, the system will efficiently give the functionality of tracking the transactions of the cryptocurrency, while

also giving the payee the functionality to restrict how the funds will be used. Once the receiver has utilized the funds, the payee will be sent a notification confirming funds were spent appropriately. The restriction, tracking and verification functionalities of the cryptocurrency are the distinguishing factors that set this currency apart from systems that already exist.

With Self-Tracking Cryptocurrency, large scale businesses will be provided a system to automate budgeting process. From the top down finance directors, can allocate and restrict funds to appropriate departments for use on approved vendors and products. Using this system departments will be able to spend their funds without having to go through an approval process, as the system will automatically approve purchases based on how the director restricted the funds. Furthermore, upon the spending of the funds the director will be sent a notification verifying that the funds were spent appropriately. Additionally, large businesses will be able to create budgets for sub-departments or sub-budgets within a department. Tracking how the funds are being spent and sending notification to the head of the sub-department, as well as anyone deemed necessary in the overall hierarchy of the company.

Self-Tracking Cryptocurrency can also be used by government departments to provide funds for those receiving welfare from the government or for other specific government funded programs. Departments would be able to specify and restrict specific vendors and approved products. This would automate the reimbursement, spending and approval process, reducing the resources and time necessary for the departments disbursing funds as well as the recipient of their funds.

Furthermore, nonprofits can use Self-Tracking Cryptocurrency to increase donations from benefactors, through the ability for benefactors to restrict funds the utilization of their donations. The capability to restrict the utilization of funds will increase a donor's confidence that funds are utilized appropriately. The confidence the system provides will mitigate the deterring factor of donations being used for administrative expenses not related to the objectives of an organization, currently deterring benefactors from donating to organizations.

Self-Tracking Cryptocurrency will have an adaptable and customizable interface creating a diverse customer base. The product will be useful for consumers in both the private and public sector, as well as, a client bases ranging from individuals to large scale companies. The product takes the necessary steps to innovate current cryptocurrency technology to create a system that automates the everyday process of verifying funds are utilized appropriately, as desired by spenders or investors. Furthermore, the system will increase the efficiency of businesses and organizations looking to track and restrict the use of funds.

3. High-Level Requirements

Major Components	Function Requirements	Non-Functional Requirements	Classes/ Interfaces/ Software Modules
Database	• Keep track of users • Add user • Modify user • Keep track of currencies and transactions • Modify a currency • Queried to trace path of transaction	• Easily modified • Easily expanded in the case of additional users • Backed up in the case of corruption • Easily accessible, only to verified users • Access control to change or manipulate the database	• Talk with database to send and receive information from users and the execution of transactions • Use MySQL to implement database
Front-End	• Accept user requests • User login • User Account Creation • Accept modification to established transactions • Produce log of logged in user's past, and open currencies	• Intuitive UI for both technical and non-technical audience • Allow several requests to be made without downgrading the speed or functionality of the service	• Use Play to design the front-end and integrate the front-end with the back-end
Security	• Isolation of data to prevent data breaches	• Symmetric encryption to protect the data of the users	• Use the java security library and the methods included to implement several of

			the different security measures pertaining to the program
Tracking System	• Keep a record of the path currency goes through	• Maintain anonymity unless explicitly defined not to	• Tree class • Randomly generated id class
Notification System	• Send a notification to designated personnel once a transaction has been approved and executed	• Send an email or text message to user • Allow the designated personnel to be defined and modified	• JavaMail library

4. High-Level Timeline/Schedule

September 2016: Beginning of Research and Design

- Conduct Market Research: Research cryptocurrencies and e-currencies already on the market
- Outline the components of the project
- Determine the audience and main objects of the project
- Develop the user interface on paper
- Start user interface tutorial
- Finalize the design diagrams of the project along
- Finalize the proposal

October 2016: Design Phase

- Determine dependency diagram
- Continue market research
- Design the algorithm for implementing the restriction functionality
- Implement the technical tree restriction algorithm
- Design the restrictions of access for users of the system
- Begin the implementation of the user class based on restrictions
- Research on commercial impact and societal impact
- Complete commercial and societal impact write up

November 2016: Transaction Implementation

- Develop the passing of transactions from one machine to another
- Ensure that currency is updating properly and conducting a check on the restrictions and users
- Research security library in java

December 2016: Implementation Integration -- Database and Transactions

- Integrate the transactions with a database
- Develop a tree demonstrating how transactions are occurring
- Implement the ability for currencies to be split and distributed to several users

January 2017: Transaction Development

- Implement the ability for the transactions to be sent and received from a server
- Ensure that security measures are put in place preserve anonymity
- Begin the development of a marketing strategy

February 2017: Mutable Restriction Tree Implementation

- Conduct research on existing notification systems
- Integrate notification with the backend components

- Determine the process that allows users to modify restrictions that were not predefined

March 2017: User Interface Implementation and Testing

- Design and develop the user interface
- Integrate the user interface with the back-end component of the project
- Determine necessary product checks to ensure that the product is ready for market

April 2017: Final Implementation

- Integrate all components
- Finish development of any component that need further enhancement
- Extensive troubleshooting and testing
- Final presentation
- Finish packaging for market