Cardiff University School of Computer Science and Informatics

CM2303 – One Semester Individual Project (40 Credits)

INITIAL PLAN

A standalone crypto currency seed analyser. (Suggested by South Wales Police)

Author: Andre Mansley

Supervisor: Michael Daley

Moderator: Stefano Zappala

Initial Plan Contents

Project Description and Background Information

Cryptocurrencies are decentralised digital currencies which use blockchain technology to cryptographically secure data and transactions. The first and most well-known cryptocurrency is Bitcoin which was created in 2009 [1] during the last economic recession by someone under the name 'Satoshi Nakamoto'. However, the real identity of this 'Satoshi Nakamoto' is still a mystery to this day.

Blockchain technology is the foundation of all cryptocurrencies. This is a distributed ledger of connected blocks which are cryptographically secured to ensure that transactions are immutable, secure, and anonymous (no personal identity or information is attached to a transaction) [2]. Blockchains run on a peer-to-peer network which relies on many computer's processing power to validate transactions sent across the Blockchain.

Each time a wallet is created for a cryptocurrency, a unique address is provided to that user. These addresses are known as wallet addresses which are comprised of a long string of numbers and letters that can be used to send and receive cryptocurrency. However, 1 wallet can only hold 1 type of cryptocurrency and therefore someone may hold multiple addresses for multiple different coins. Whilst creating a wallet, it will prompt the creator to note down a list of around 12 random English words known as recovery seeds which can be used to recover a wallet if they are unable to access it for any reason.

The project I am undertaking will analyse a recovery seed from a crypto wallet and will cross reference the Blockchain to output any wallet addresses that it has used as well as the amount of cryptocurrency that may present inside. The aim of this project will be to develop a standalone application that will enable the South Wales Police investigators to analyse a retrieved wallet recovery seed and to quickly and efficiently determine if the wallet possesses any cryptocurrency that can be recovered. [3]

There are other tools out there that have similar functionality to the proposed project I am developing. An example of these tools can be found on iancoleman.io [4]. This website derives blockchain address from using mnemonic words and wallet seeds. Whilst this is like the application I will develop; I will be developing an application that will take in a wallet seed which will find known addresses and then display how much cryptocurrency is being held within the wallets.

Aims and Objectives

The aims and objectives for the development of the Standalone Cryptocurrency seed analyser are detailed below:

Aim 1: An easy-to-use application

This aim will be to develop an application interface that will be easy to use and understand. The interface will enable the user to enter a wallet recovery seed and submit this recovery seed for instant analysis which will be done by algorithms that I will develop into the program.

Objectives:

a. Design a text box input that takes in a wallet recovery seed as a string
b. Design an 'Analyse' button that will start the analysing process of the entered recovery seed
c. Design an area of the application that will be used to output the returned results of the analysis

Aim 2: Analyse the entered recovery seed

This aim will be to analyse the recovery seed that the user has entered. The provided recovery seed will then be used to attempt a wallet recovery and fetch the associated address of the wallet.

Objectives:

a. Recover the wallet associated with the provided recovery key
b. Extract the wallet address (a long string of numbers and letters) that can then be used to cross reference the blockchain

Aim 3: Cross reference the blockchain

This aim will be to use the extracted wallet address and cross reference the blockchain to return and display the amount of cryptocurrency that is held within the wallet as well as list other known wallet addresses that it would use.

Objectives:

a. To output known addresses related to the entered recovery seed (returned and displayed as a text string)
b. To display the amount of cryptocurrency inside the wallet being analysed (returned as values in the format $0.00, and BTC format 0.00000000)
c. Retrieve and display the results within 5 seconds

Ethical

There are no ethical certifications / approval required for this project as no people will be involved and no personal data is gathered or stored that may reveal an individual’s identity. I will use addresses on the blockchain explorer to test the application as all information on the blockchain is publicly available to all without providing any identity of whom the wallet address belongs to. I will also create my own wallet for the purpose of testing the recovery seed analysis.

Time Plan:

Week / Dates	**Tasks / Milestones / Deliverables**
Week 1: 1st – 7th February	• Complete Initial Plan ○ Project Description ○ Aims and Objectives ○ Ethical ○ Time Plan **Deliverable:** Initial Plan
Week 2: 8th – 14th February	• Background Research into wallet seeds and Blockchain • Start main report ○ Project Introduction & Abstract • Supervisor Meeting
Week 3: 15th – 21st February	• Development of website UI interface • Main Report ○ Background Information **Milestone: Website UI Interface Completed**
Week 4: 22nd – 28th February	• Start developing some basic functionality of the seed analysis algorithm • Main Report: ○ Functional Requirements of the project • Supervisor Meeting
Week 5: 1st – 7th March	• Main Report: ○ Non-Functional Requirements of the project **Milestone: Seed analysis functionality Complete**
Week 6: 8th - 14th March	• Main Report: ○ System Design and Architecture • Start cross referencing the blockchain • Supervisor Meeting

Week 7: 15th – 21st March	• Core functionality of the cryptocurrency seed analyser mostly built (seed analyser + cross referencing) • Main Report: o Continue with System Design and Architecture
Week 8: 22nd – 28th March	• Functional web application. Seed analysis and blockchain referencing to be functional. • Main Report: o System Implementation • Supervisor Meeting • **Milestone: Functional web application**
Week 9 - 11: 29th March – 18th April	• **Easter Recess** – Catch up on any work if I have fallen behind in the previous weeks
Week 12: 19th – 25th April	• Testing of the Cryptocurrency seed analyser web application • Main Report: o Testing • Supervisor Meeting
Week 13: 26th April – 2nd May	• Make amendments to the application if required • Main Report: o Evaluation and reflection
Week 14: 3rd – 9th May	• Main Report: o Conclusion • Supervisor Meeting **Milestone: Complete the report**
Week 15: 10th – 16th May	• Read over report, make any small last edits if needed **Deliverables: Final Report, Web Application** **Milestone: Project Completed**

References:

[1] Zoë Bernard. 2018. *Everything you need to know about Bitcoin, its mysterious origins, and the many alleged identities of its creator*. Available at: **https://www.businessinsider.com/bitcoin-history-cryptocurrency-satoshi-nakamoto-2017-12?r=US&IR=T#in-2008-the-first-inklings-of-bitcoin-begin-to-circulate-the-web-1** [Accessed 03 February 2021].

[2] Euromoney. 2020. What is Blockchain. Euromoney. Available at: **https://www.euromoney.com/learning/blockchain-explained/what-is-blockchain** [Accessed 03 February 2021].

[3] Project Allocation & Tracking System (PATS). 2021. Available at: https://pats.cs.cf.ac.uk/ [Accessed: 03 February 2021].

[4] BIP39 - Mnemonic Code. 2021. Available at: https://iancoleman.io/bip39/ [Accessed: 06 February 2021].