Document Information

Project name:	Paper Gap Wallet
Date:	28th Jan 2021
Author:	Team 12
Owner:	Jason Quinlan
Document code:	001
Version:	V0.03

Color legend:

Black - older than last week

Blue – updates since last week

Definition

Background:	By solving the Byzantine Generals Problem anonymous cryptographer Satoshi Nakamoto offered an alternative to the modern Central Banking system and economic problems created by the Keynesian monetary policy. Bitcoin blockchain first came online on 3rd January 2009 and it represents the first implementation of fully decentralized peer-to-peer currency protected by Proof Of Work cryptographic technology.
Main Goal:	Build a secure environment for Bitcoin Paper Wallet Generation
Desired Outcomes:	Have a fully functional, easy-to-use app, even for non-technical users
Constraints and Assumptions:	The "Paper Gap Wallet" app will be used by Bitcoin enthusiasts who have a need for a cold storage Paper Wallet. The main constraint is that the app needs to be simple enough that even non-technical users are able to use it securely
Interfaces:	Bitcoin network Other Cryptocurrencies will be added if time permits
Project Approach:	In-house project
Project Product Description:	An App, that creates a live, bootable USB Linux distribution (i.e. Linux distribution that can be booted from removable storage media (USB) instead of installed/booted from Hard Disk Drive) Once booted, the system will present a one-app system that is air-gapped (i.e. network security measure used by computer to ensure that a secure computer network is physically isolated from unsecured networks (public Internet/ unsecured LAN). The User is then welcomed by a start page of the wallet app that takes them through steps to generate wallet seed and public keys.

Project Objectives

	Target	**Tolerance**
Scope	Paper Gap Wallet Application	Some flexibility in final deliverable
Time	22nd March	No late submissions
Cost	n/a	n/a
Quality	Excellent	Nothing but the best
Risks	Security gaps	Community peer review
Benefits	Contributing to the community	n/a

Outline Business Case

Bitcoin is a cryptocurrency invented in 2008 by an unknown person or group of people using the name Satoshi Nakamoto. The currency began use in 2009 when its implementation was released as open-source software.
Bitcoin is a decentralized digital currency, without a central bank or single administrator, that can be sent from user to user on the peer-to-peer bitcoin network without the need for intermediaries. Transactions are verified by network nodes through cryptography and recorded in a public distributed ledger called a blockchain. Bitcoins are created as a reward for a process known as mining. Research produced by the University of Cambridge estimated that in 2017, there were 2.9 to 5.8 million unique users using a cryptocurrency wallet, most of them using bitcoin.
Our team is aiming to create a new Bitcoin wallet application for creating so-called Paper Cold storage wallets.
As we believe the project will benefit the Bitcoin community greatly by increasing the security of Bitcoin network users and their funds. Especially for new and non-technical users who wish to keep their Bitcoin in cold storage for long periods of time.
The major risk as always with the Cryptocurrency space is the possibility of losing the funds or funds being stolen by a malicious entity (hacker). Our team will try to combat this by keeping up with the latest security standards when developing our application and by keeping the code base as small as possible to reduce the attack surface.
Our app will be first of its kind due to its easy use and security, only one OS with the same purpose as our app exist but it is a lot bigger and much more complicated to use:. https://bitkey.io/

There is also an Mobile application called **Coinomi** which acts as a crypto wallet generator, but unlike our product it does not have the secure air-gapped environment feature that our application holds, and all confidential contents of the crypto wallets are stored on local memory of the device, our product on the other hand will have all contents stored on a removable storage medium (USB) which far exceeds the application in security.

Some Key Terms:

Mnemonic/Bitcoin Seed: Is a 24 word list that stores all of the info needed for a user to recover their wallet. Each wallet has a seed.
Wallet: A software program which stores cryptocurrency/Bitcoin keys.
Cold Wallet: it cannot be compromised as it is not connected to the Internet. It stores the user's address and private key and works in conjunction with compatible software in the computer.
Paper Wallet: a physical source (e.g barcode on paper, with private/public addresses etc) that acts as the key to the safe that stores your bitcoin
Public Address: unique identifier serving as a virtual location where the currency can be sent.
Public Key: corresponds to private key, and compressed into a public address that is shared in blockchain.
Blockchain = records info in a way that is hard to hack/change as every ledger has all records.
Private Key: allows users to access their cryptocurrency and is proof they own the public key.

High Level Requirements:

- Python3.6 Bitcoin libraries
  - our team will use existing well established and tested Bitcoin libraries to create an secure and robust Paper Wallet generator
- Kivy Python Front-End framework
  - our team will use Kivy framework to create simple and clean GUI
- TinyCore Linux distribution
  - our team will use extended and modified TinyCore Linux distro to create an air gapped and secure environment

Milestones of Key Deliverables

Milestones	**Finish Date**
Idea Brainstorming And Planning	31. Jan 2021
Terminal Seed Generator App	07. Feb 2021
Front End For Generator App	07. Feb 2021

Linux Distro Build	14. Feb 2021
Seed Generator App GUI	14. Feb 2021
Project Beta Release	21. Feb 2021

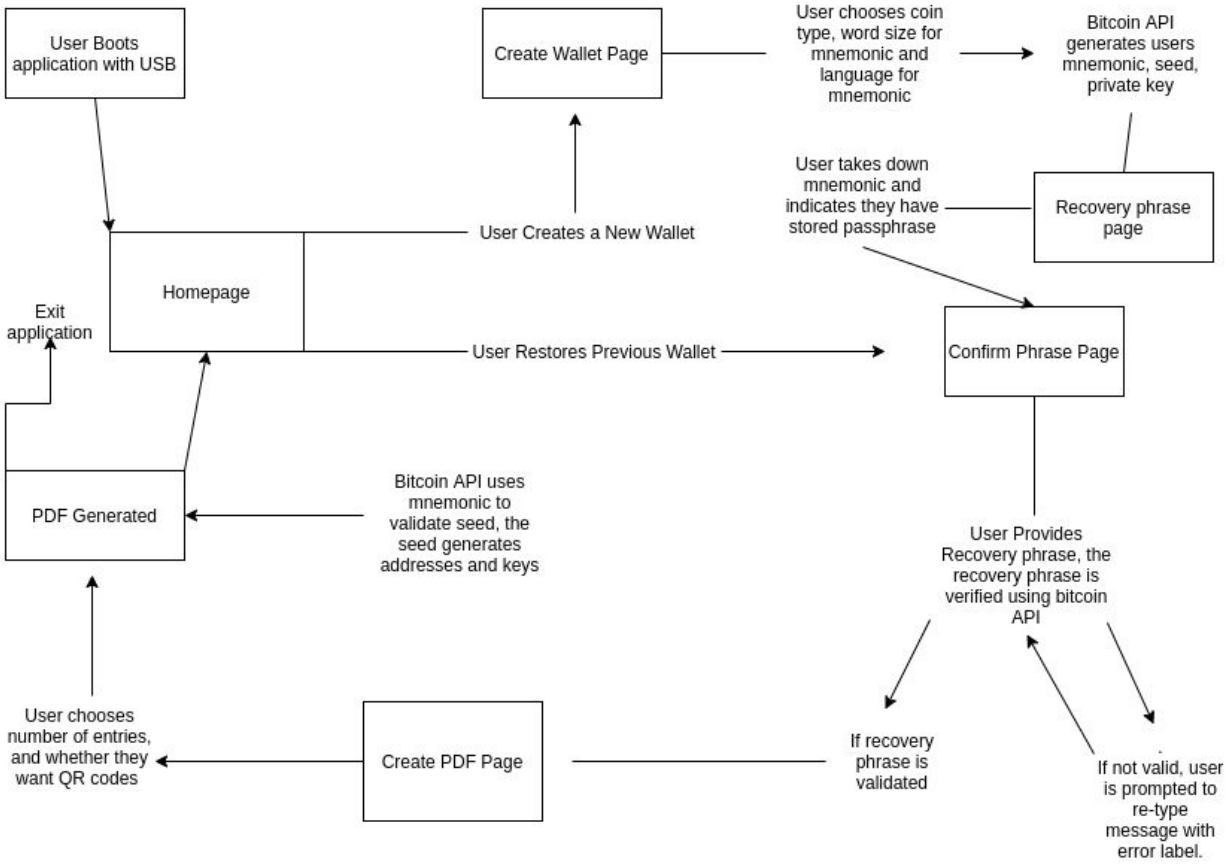
External Resources

Linux From Scratch: http://linuxfromscratch.org/lfs/view/stable/index.html
Linux From Scratch Live CD Tutorial: https://youtu.be/A9pmmKx0iAU
Tiny Core Linux: http://tinycorelinux.net/welcome.html
Python3 Bitcoin Library: https://github.com/primal100/pybitcointools
Gantt Chart: https://app.agantty.com/#/gantt

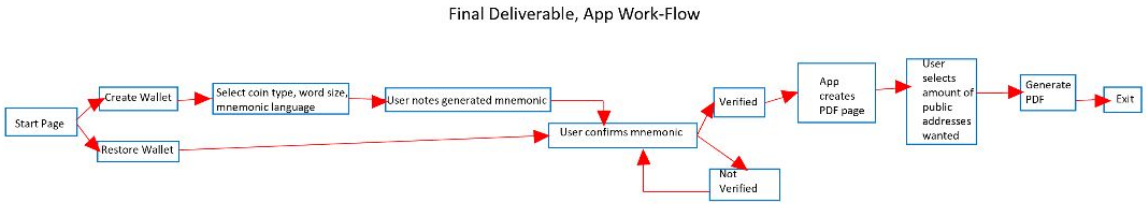
Notes (MoSCoW)

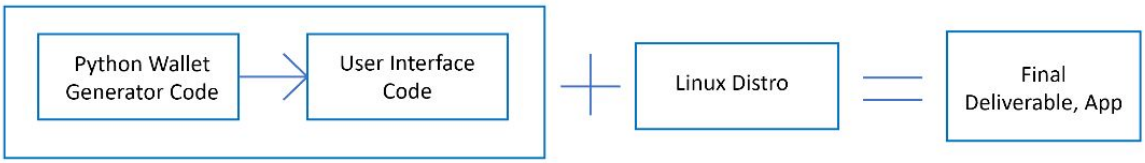
Must Have	- Secure wallet generation for bitcoin - A fully functional Simplistic User interface for breaking down wallet creation/restoration process - A fully air-gapped distro as the environment for our app - Suitable/up to date encryption for wallet restoration/storage
Should Have	- A fully Responsive UI - A suitably sized project (within 2gb)
Could Have	- The availability to create wallets in other crypto currencies e.g ethereum, bitcoin cash, dogecoin.
Won't Have/Would Want	- Wallet creation for further kinds of crypto currencies

Application Architecture



Application Work-Flow





Key Stakeholders

Major Stakeholder	**Notes**
Jason Quinlan	Project Owner
Janine Dunlea	Project Stakeholder
Robert O'Brien	Project Stakeholder
John Furlong	Project Stakeholder
Oliver Cunnington	Project Stakeholder
Ozzak Matic	Project Stakeholder

Project Management Team

Appointee	**Role**	**Description**
Ozzak Matic	Master Of The Universe	Linux development and project management
Oliver Cunnington	Technomancer	Linux development and Linux distro integration
Robert O'Brien	Grand Byte-Wizard	FrontEnd development and integration using Kivy python framework.
John Furlong	PyLord	Python development and blockchain operations in charge of back end wallet generation.

Janine Dunlea	Code Empress	Python development and blockchain operations in charge of back end wallet generation.

Gantt Chart