CRYPTOGRAPHIC HARDWARE FOR SECURE CRYPTOCURRENCY PAYMENTS OVER BLUETOOTH

A PROJECT REPORT

Submitted by

HASHIKA KALISETTY – RA1611004010820

AKANKSHA MATHUR– RA1611004010829

RITIKA BHATIA– RA1611004010840

PROJJAL GUPTA – RA1611004010860

Under the guidance of

MR. B. SRINATH

(Associate Professor, Department of Electronics and Communication)

in partial fulfilment for the award of the degree

of

BACHELOR OF TECHNOLOGY

in

Electronics and Communication Engineering

of

FACULTY OF ENGINEERING AND TECHNOLOGY

SRM
INSTITUTE OF SCIENCE & TECHNOLOGY
(Deemed to be University u/s 3 of UGC Act, 1956)

S.R.M. Nagar, Kattankulathur, Kancheepuram district

SRM INSTITUTE OF SCIENCE AND TECHNOLOGY

(University under Section 3 of UGC Act,1956)

BONAFIDE CERTIFICATE

Certified that this project report titled “**Cryptographic hardware for Secure cryptocurrency payments over bluetooth**’’ is the bonafide work of **HASHIKA KALISETTY [RA1611004010820], AKANKSHA MATHUR [RA1611004010829], RITIKA BHATIA [RA1611004010840], PROJJAL GUPTA [RA1611004010860]**, who carried out the project work under my supervision. Certified further, that to the best of my knowledge the work reported herein does not form any other project report or dissertation on the basis of which a degree or award was conferred on an earlier occasion on this or any other candidate.

SIGNATURE	SIGNATURE
Mr. B. Srinath	Dr. T. Rama Rao
PROJECT GUIDE	**HEAD OF DEPARTMENT**
Associate Professor	Dept. of Electronics and
Dept. of Electronics and	Communication Engineering
Communication Engineering	
Signature of internal examiner	Signature of external examiner

ABSTRACT

With the introduction of cryptocurrencies into the market, there has been a rapid influx in the adoption of said payment integrations and technology. However, multiple concerns regarding wallet safety and transactions integrity has severely compromised the rate of growth of this technology. Albeit safe, people with malicious intent tend to cause problems with selfish interests such as monetary gain. We propose to create a cryptographically secure hardware cold wallet on a microcontroller to make sure that the private key of the user is never sent over internet as raw data.

To understand how the hardware works, we have to understand the entire transaction procedure. We will be using Ethereum™ Blockchain as the main cryptocurrency platform. Each account comprises of a public key and a private key. The Public key is derived from the private key, and can be given to people. The private key, however, is the master password to an account, which needs to be safely guarded by the user. If a hacker gets hold of a private key, then he has full access rights to move all the funds to another account (Basically theft of cryptocurrency). This is getting more and more prevalent with centralised online wallet architecture solutions.

Our hardware will securely store the private key, and the data will be secured using multiple security standards. Communication over BLE with be a half-duplex solution and all data will be securely transmitted over RSA protocol to ensure utmost security. The hardware will not lose any data even during loss of power.

Another feature of the hardware is to allow offline transactions over BLE using said hardware-to-hardware interaction. However it will be validated only after it communicates with a computer (Offline-Online validation Barrier). We aim to design the most efficient device for the said tasks and can work towards enabling blockchain technology to the general people.

ACKNOWLEDGEMENTS

We would like to express our deepest gratitude to our guide Mr. B. Srinath, his valuable guidance, consistent encouragement, personal caring, timely help and providing us with an excellent atmosphere for doing research. All through the work, in spite of his busy schedule, he has extended cheerful and cordial support to us for completing this research work.

GROUP MEMBERS

1) Hashika Kalisetty	RA1611004010820
2) Akanksha Mathur	RA1611004010829
3) Ritika Bhatia	RA1611004010840
4) Projjal Gupta	RA1611004010860

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

BLE	Bluetooth Low-Energy
RSA	Rivest-Shamir-Aldeman
OLED	Organic Light Emitting Diode
ESP	Espressif Systems Product
AES	Advanced Encryption Standard
MCU	Microcontroller Unit
USART	Universal Synchronous/Asynchronous Reciever/Transmitter
I2C	Inter-Integrated Circuit
BMS	Battery Management System

CHAPTER 1
INTRODUCTION

Designing of a cryptographically secure hardware for secure cryptocurrency payments over Bluetooth could be a useful and inexpensive secure tool, which can reduce the chances of malicious data hacks with simple operation. The hardware will securely store the private key, and the data will be secured using multiple security standards. The system mainly consists of a ESP12 microcontroller, Bluetooth, OLED screen and an appropriate battery management system for a 1100 mAh Li-Po battery.

1.1 CRYPTOCURRENCY

Cryptocurrency is digital or virtual currency designed to work as a medium of exchange. A cryptocurrency (or crypto currency) is a digital asset designed to work as a medium of exchange that uses strong cryptography to secure financial transactions, v stores the public and private "keys" or "addresses" which can be used to receive or spend the cryptocurrency. With the private key, it is possible to write in the public ledger, effectively spending the associated cryptocurrency. With the public key, it is possible for others to send currency to the wallet.

Wallets can either be digital apps or be hardware based. They either store the private key with the user, or the private key is stored remotely and transactions are authorized by a third party.

Figure 1.1 Various Cryptocurrencies

Multi signature wallets require multiple parties to sign a transaction for any digital money can be spent. Multi signature wallets are designed to have increased security.

With a deterministic wallet a single key can be used to generate an entire tree of key pairs. This single key serves as the root of the tree. The generated mnemonic sentence or word seed is simply a more human-readable way of expressing the key used as the root, as it can be algorithmically converted into the root private key. Those words, in that order, will always generate exactly the same root key.

It uses cryptography to secure and verify transactions as well as to control the creation of new units of a particular cryptocurrency. We aim to create hardware device with 0.96" OLED screen and requires the user to manually verify and sign every transaction. The use of this hardware aims to eliminate human error and reduces receptivity to malicious attacks.

1.2 LITERATURE SURVEY

Results of a feasibility study about Bluetooth Low Energy (BLE) based wireless sensors show a huge scope of use of BLE as a mode of communication in data spectrum. However, some problems regarding data integrity are yet to be verified as non-threatening.

A novel triple algorithm based on RSA (Rivest-Shamir-Adleman), AES (Advanced Encryption Standard), and TwoFish in order to further improve the security of bluetooth that is currently using only 128-bit AES for encryption in its latest versions (Bluetooth 4.0 - 5.0). On a microcontroller based system, low size key AES can be implemented with almost nil effect to data security strength.

Estimation of the power consumption of Bluetooth Low Energy modules being used with continuous data transmission modes reveals that Low Energy feature only uses 5% of regular bluetooth data transmission in similar test cases

Use of a hardware token for the authorization of transactions and protect the Bitcoin private keys is possible if the private key of each multi-sig wallet is masked by a layer of hardware abstraction.

CHAPTER 2

DESIGN METHODOLOGIES

2.1 SYSTEM ANALYSIS

Proposed system is based around a microcontroller, with onboard flash memory, so that it can store private and public keys. The system requires the use of a Bluetooth module which can support low energy protocol, and can be interfaced with the central MCU via USART or I2C protocol for ease of development. The system requires push buttons for user input, OLED screen for display and an appropriate BMS

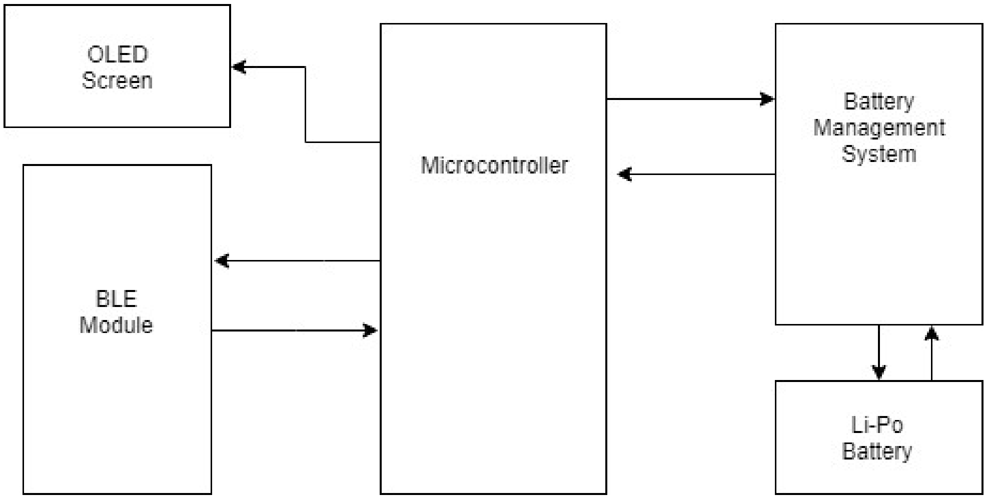


Figure 2.1 Block Diagram

The system should be programmable and should have additional features to allow debugging and testing of the above hardware design. It should be able to run USART protocol and implement a functional finite state machine on the MCU.

2.2 DESIGN PRINCIPLES

Proposed model contains three parts – Command Acquisition and State Control, State based hardware control (for screen control and button polling), and cryptographic data handler.

1) The command acquisition and state control section deals with receiving and parsing command inputs made to the system via a mobile phone using BLE, and based on the command received, progress the state machine accordingly.
2) State based hardware control reads the state value, and accordingly sets the OLED screen output to said state. It also enables sleep mode and enables interrupts whenever required for button polling or waiting for user input.
3) The cryptographic data handler is a purely software side feature which completely deals with maintenance of data integrity. This means that it takes care of the initial handshake, implement Speck cipher based AES encryption, generation of a pseudo-random number, encrypt command responses and decrypt incoming data or commands as and when required.

The criteria that determines key performance and parameters in the proposed system are as follows:

- Watchdog Timer Reset Count
- Power Consumption during operation
- Charging vs Discharging time
- CPU frequency

If these criterias are met correctly, the system will function as expected and will maximise the flow of work, while minimising any possible errors in the system.

2.2.1 ESP12 MCU

Proposed model will be based around the ESP12 microcontroller. The ESP12 is a low powered – high performance microcontroller built around Xtensa Tensilica Core. It is a single core device which runs at a base 80 MHz frequency and has a wide reange of developer support available. The following features are the most useful features that are being integrated into the model :

1) Hardware runs at base 80 MHz. With further tweaking, it can pushed upto 160 MHz frequency.
2) Complete disabling of on-board wifi reduces 80% of the power requirements.
3) Compact footprint is a bonus when designing handheld electronics
4) 14+ GPIO pins for interfacing all peripherals
5) Availability of I2C, USART, SPI, SPIFFS and Crypto protocols on board.
6) Arduino hardware abstraction library support to ease the process of debugging, testing and development overall.
7) Deep sleep power <10uA, Power down leakage current < 5uA.
8) Standby power consumption of < 1.0mW (DTIM3)
9) OTA update support

2.2.2 HM-10 Bluetooth Low Energy

Proposed model uses the HM-10 BLE module to facilitate communication between the phone and the hardware. HM10 is based around the CC2540 BLE chip developed by Texas Instruments as a part of their development hardware series. The module communicates at 2.4Ghz (Bluetooth standard) and can work at lower baud rates. It also consumes 235uA on battery backup, which is significantly low and has an open-space long range of 100m (line of sight). It works fully using UART and support full AT command set for configuration.

2.2.3 128x64 OLED Screen

Proposed model uses the SSD1306 driver based 128x 64 OLED screen as the primary data display for the user. The main features and positive points are :

1) Low power consumption: 0.04W during normal operation
2) High contrast, thus supporting clear display with no need of backlight
3) PCB size: 2.8 x 3.2cm. (Low size, More compact design)

2.2.4 TP4056 Charging Board

The BMS uses TP4056 IC based charging board to connect battery to the system. The IC provides four main features which makes it suitable for the system:

1) Over-Charge Protection
2) Over-Discharge Protection
3) Surge-Current/Over-Current Protection
4) Short-Circuit Load Drop Protection

CHAPTER 3

ALGORITHM FOLLOWED

3.1 DESIGN FLOW

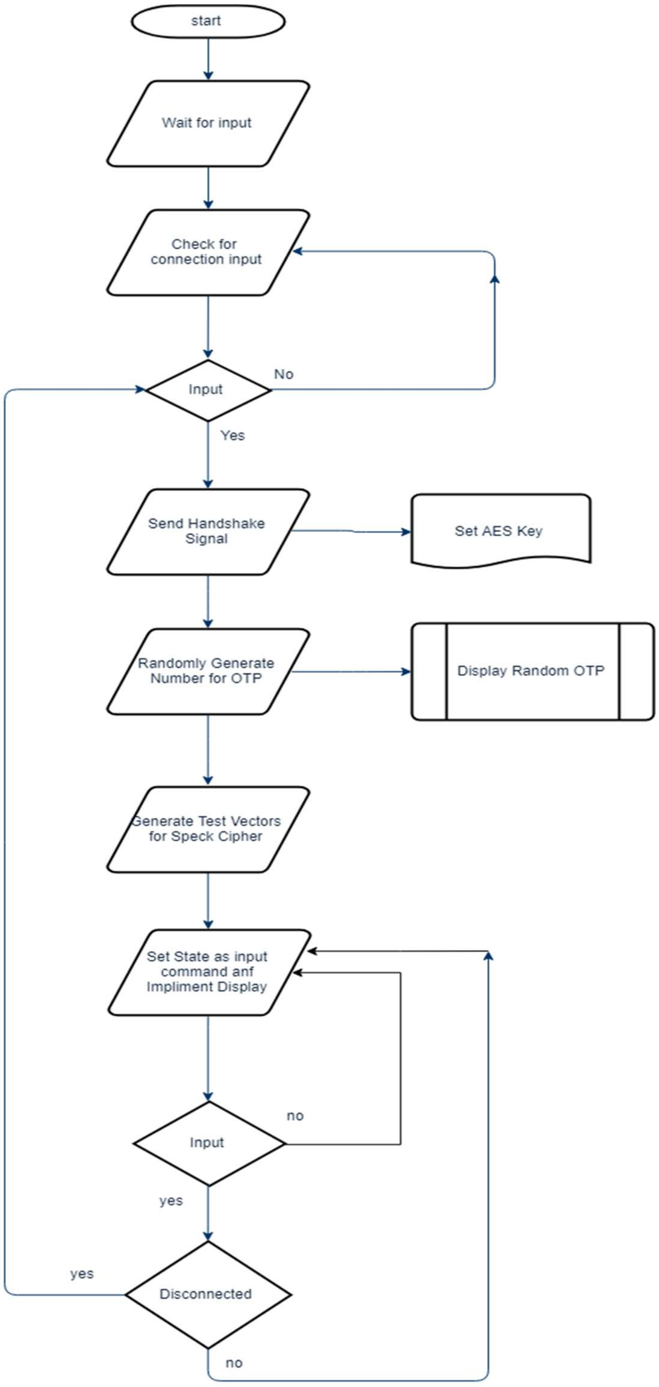

start
Wait for input
Check for connection input
Input
No
Yes
Send Handshake Signal
Set AES Key
Randomly Generate Number for OTP
Display Random OTP
Generate Test Vectors for Speck Cipher
Set State as input command anf Impliment Display
no
Input
yes
yes
Disconnected
no

Figure 3.1 Flow Chart

3.2 CRYPTOGRAPHIC ALGORITHM

Speck is a family of lightweight block ciphers publicly released by national security agency (NSA) in June 2013. Speck is an add–rotate–xor (ARX) cipher. Speck has been optimized for performance in software implementations, while its sister algorithm, Simon has been optimized for hardware implementations.

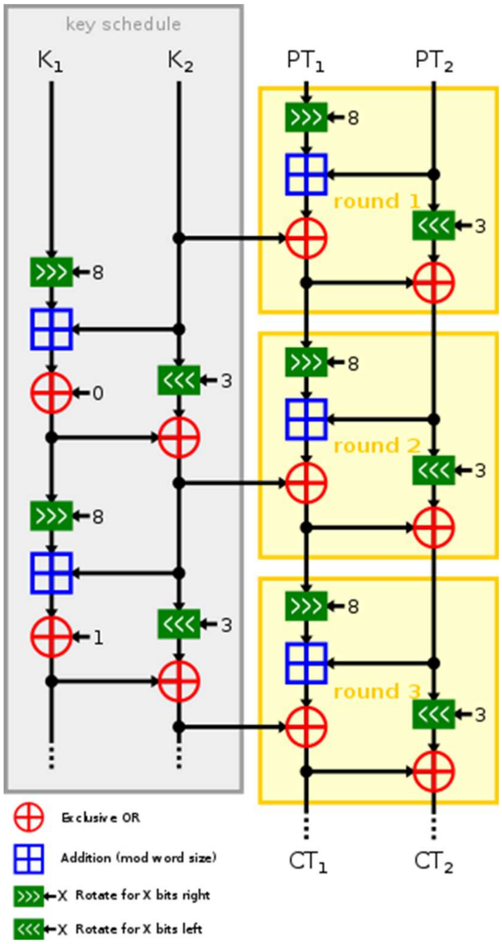
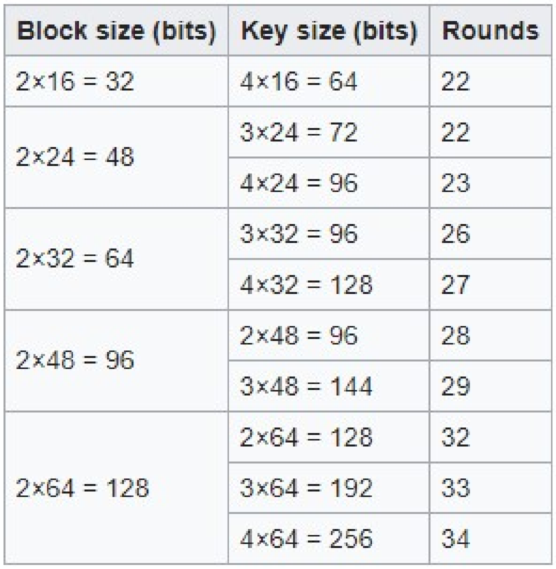


Figure 3.2 Speck Cipher Flow

CIPHER DESCRIPTION

Speck supports a variety of block and key sizes. A block is always two words, but the words may be 16, 24, 32, 48 or 64 bits in size. The corresponding key is 2, 3 or 4 words. The round function consists of two rotations, adding the right word to the left word, xoring the key into the left word, then and xoring the left word to the right word. The number of rounds depends on the parameters selected



Block size (bits)	Key size (bits)	Rounds
2×16 = 32	4×16 = 64	22
2×24 = 48	3×24 = 72	22
	4×24 = 96	23
2×32 = 64	3×32 = 96	26
	4×32 = 128	27
2×48 = 96	2×48 = 96	28
	3×48 = 144	29
2×64 = 128	2×64 = 128	32
	3×64 = 192	33
	4×64 = 256	34

Table 3.1 Speck Cipher Block Sizes

PERFORMANCE

According to ECRYPT's stream cipher benchmarks (eBASC), Speck is one of the fastest ciphers available, both for long as well as short messages. Some median performances for long messages (128-bit, 128-block size version) are: 1.99 cycles per byte (cpb) on an AMD Ryzen 7 1700; 1.27 cpb on an Intel Core i5-6600; 15.96 cpb on a Broadcom BCM2836 Cortex A7. For example, on the ARMv7 platform, Speck is about 3 times faster than AES.

When implemented on 8-bit AVR microcontroller, Speck encryption with 64-bit blocks and 128-bit key consumes 192 bytes of Flash, temporary variables consume 112 bytes of RAM, and takes 164 cycles to encrypt each byte in the block.

SECURITY

Cryptanalysis

Speck, though a "lightweight" cipher, is designed to have the full security possible for each block and key size, against standard chosen-plaintext (CPA) and chosen-ciphertext (CCA) attacks. As of 2018, no successful attack on full-round Speck of any variant is known.

Due to interest in Simon and Speck, about 70 cryptanalysis papers have been published on them. The best published attacks on Speck in the standard attack model (CPA/CCA with unknown key) are differential cryptanalysis attacks. Speck has been criticized for having too small a security margin, i.e. too few rounds between the best attacks and the full cipher.

Speck includes a round counter in the key schedule. This was included to block slide and rotational cryptanalysis attacks. Certain weak key classes make it through slightly more rounds than the best differential distinguishers. However, this type of cryptanalysis assumes the related-key or even the known-key attack models. Speck was not designed to resist known-key distinguishing attacks (which do not directly compromise the confidentiality of ciphers)

NSA cryptanalysis found the algorithms to have no weaknesses, and security commensurate with their key lengths. The NSA has approved Simon128/256 and Speck128/256 for use in U.S. National Security Systems.

Side-channel attacks

Being an ARX cipher, Speck does not use S-boxes or other lookup tables; it is therefore naturally immune to cache-timing attacks. This contrasts with ciphers that use lookup tables such as AES, which have been shown to be vulnerable to such attacks. However, like most block ciphers (including AES) Speck is vulnerable to power analysis attacks unless hardware countermeasures are taken.

Block and key sizes

Although the Speck family of ciphers includes variants with the same block and key sizes as AES (Speck128/128, Speck128/192, and Speck128/256), it also includes variants with block size as low as 32 bits and key size as low as 64 bits. These small block and key sizes are insecure for general use, as they can allow birthday attacks and brute-force attacks, regardless of the formal security of the cipher. These block and key sizes were included for highly resource-constrained devices where nothing better is possible, or where only very small amounts of data are ever encrypted, e.g. in RFID protocols. Only the variant with a 128-bit block size and 256-bit key size is approved for use in U.S. National Security Systems.

STANDARDIZATION EFFORTS AND CONTROVERSIES

Initial attempts to standardise Simon and Speck failed to meet International Organization for Standardization super-majority required by the process and the ciphers were not adopted. As of October 2018, the Simon and Speck ciphers have been standardized by ISO as a part of the RFID air interface standard, International Standard ISO/29167-21 (for Simon) and International Standard ISO/29167-22 (for Speck), making them available for use by commercial entities.

CHAPTER 4

ELECTRONICS HARDWARE DESIGN

4.1 Hardware

- ARDUINO IDE is an Integrated Development Environment which can be used to write Embedded C code (ESP-IDF SDK inbuilt Support) and can abstract with the hardware at bitwise level if required.
- Using ARDUINO IDE, a functional program was written. It allows the use of external libraries to enable Crypto support and natively call all hardware protocols.
- Circuit Designing was done through EAGLE CAD, which is an Autodesk owned PCB Computer Aided Design Tool.
- Eagle CAD supports footprint builder tools, using which footprints were designed for the ESP12 MCU.
- Initial Circuit was designed using resistors, peripherals and switches, and appropriately connecting them to power and ground lines.
- Voltage Regulator block was designed with coupling capacitors to maintain a certain voltage and protect against voltage spikes
- Boot Modes were set using ESP pinouts and fuse bits
- ESP-IDF Monitor was used to monitor how system responded to different test inputs.
- Code was written and uploaded as per above algorithm using Speck cipher as cryptographic standard.

4.1.1 SCHEMATIC DESIGN

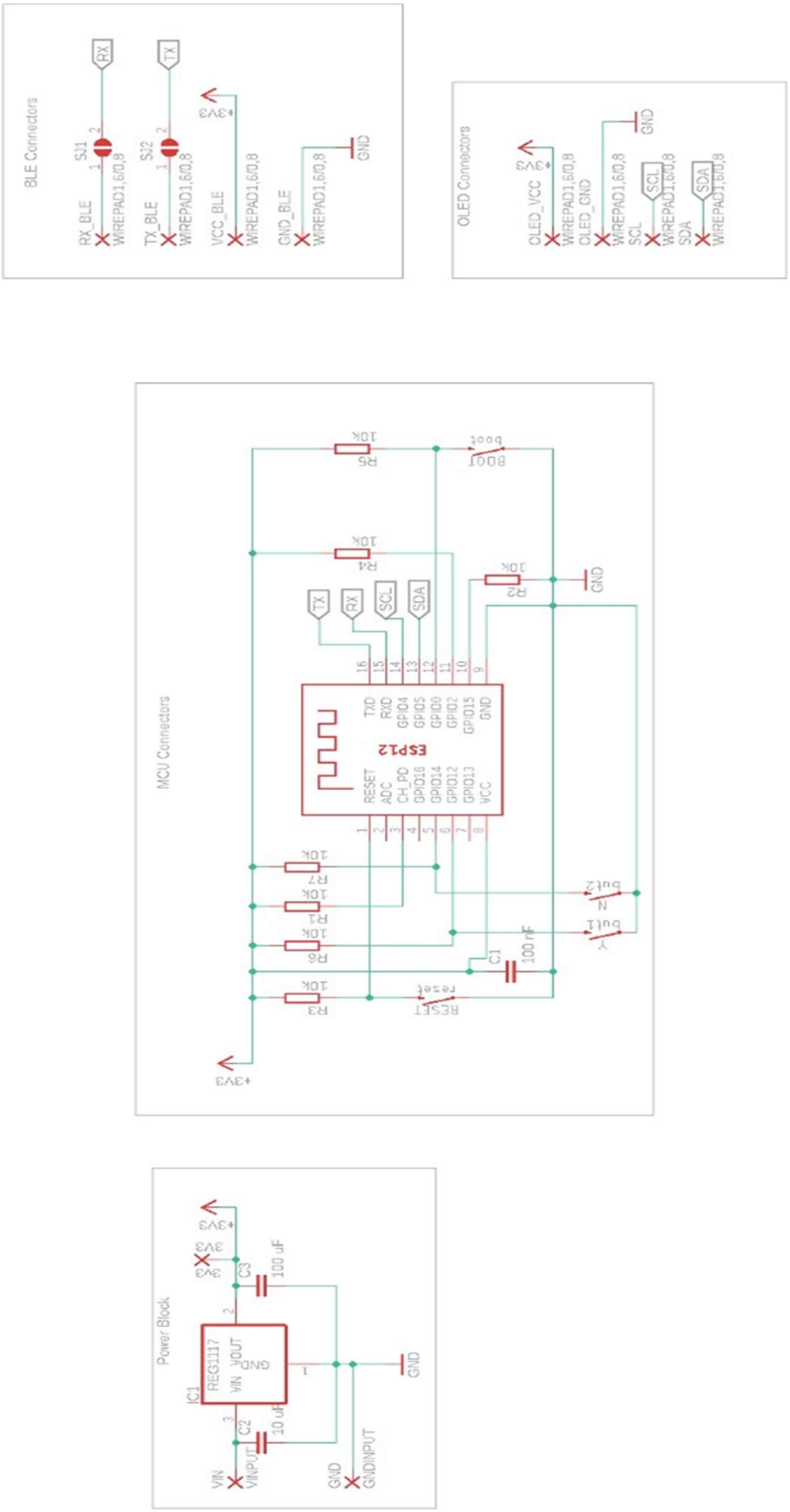


Figure 4.1 Circuit Schematic

4.2 PCB DESIGN

PCB footprint was laid out and designed using Eagle CAD circuit layout software. The wire width was decided as 0.3mm wide to allow safe flow of current upto 300 mA at a time.

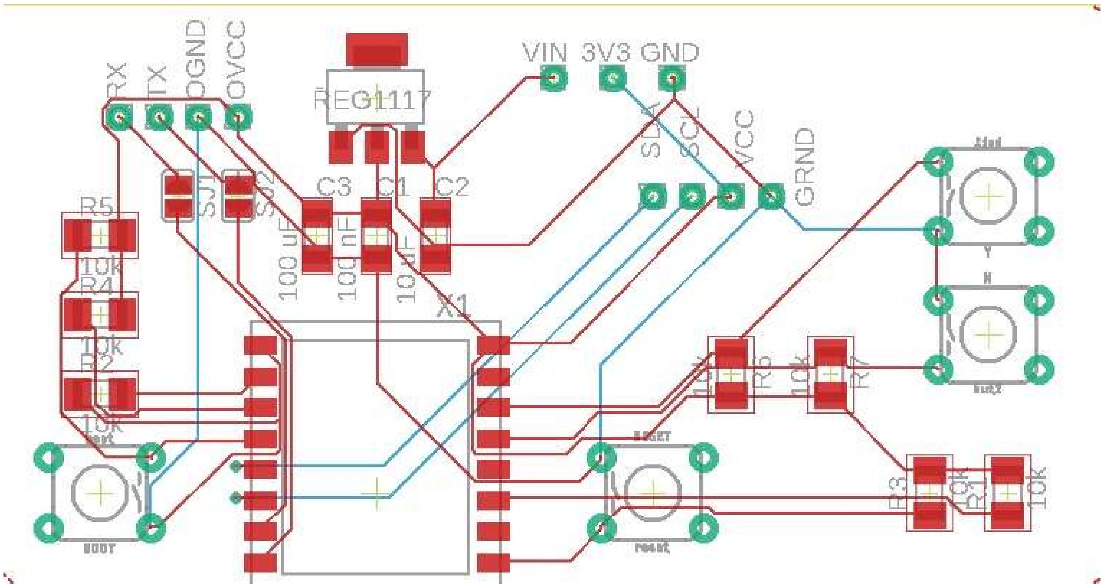


Figure 4.2 Circuit Layout

Based on the above layout, PCBs were manufactured with HSPA-Lead base and SMD components were procured to finish the hardware.

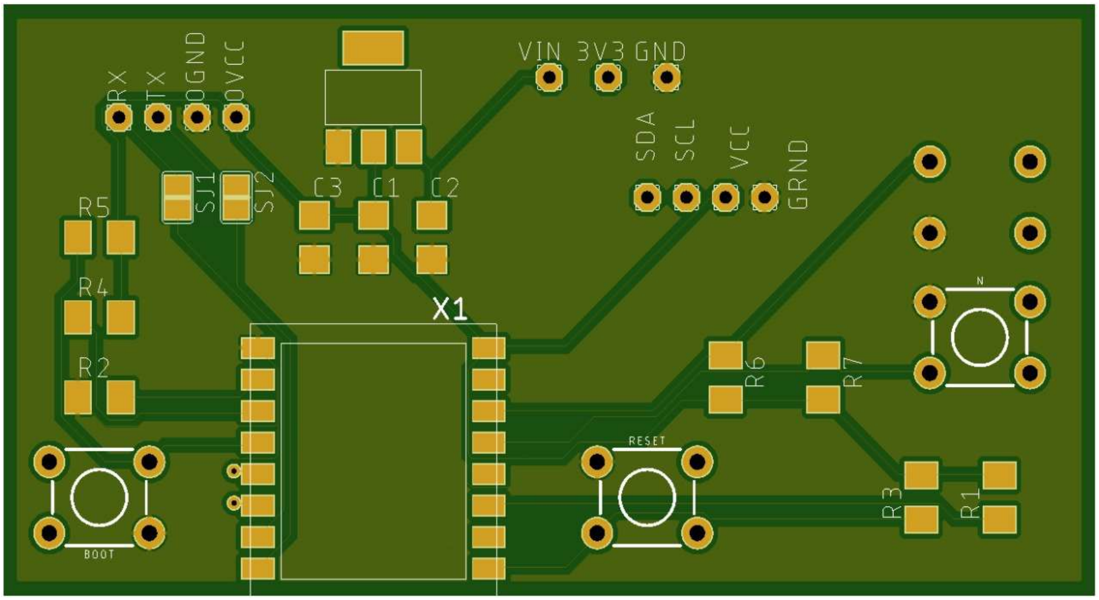


Figure 4.3 PCB Gerber View

4.3 FINAL PCB - POST FABRICATION AND SOLDERING

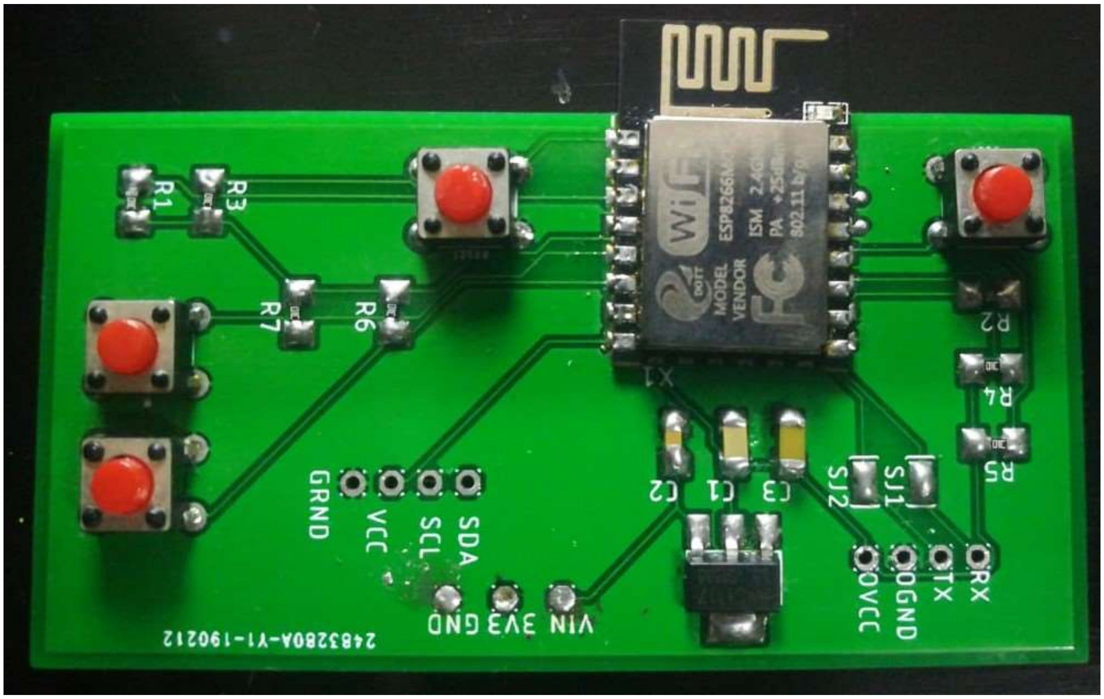


Figure 4.4 PCB Final Version

1. BOM was procured from electronics shops and 1206 footprint size was selected for the ease of hand soldering.
2. Button functions were tested and confirmed working.
3. Point to point voltage difference was tested ad working of regulator was confirmed.
4. Continuity test was performed on each and every pad of the manufactured PCB pre- and post-soldering of components.
5. Flux residue was cleaned out using IPA solution, and barebone testing was performed by setting board to boot-flash mode.

CHAPTER 5

DESIGN OF UI AND EXTERNAL ENCLOSURE

5.1 MOBILE UI DESIGN

The aim of building the proposed model is to facilitate the ease of use of cryptocurrencies in the modern digital era, while putting extra emphasis on security aspects and data integrity. So naturally, the mobile application built to communicate with the hardware has to be functional, but easy to use.

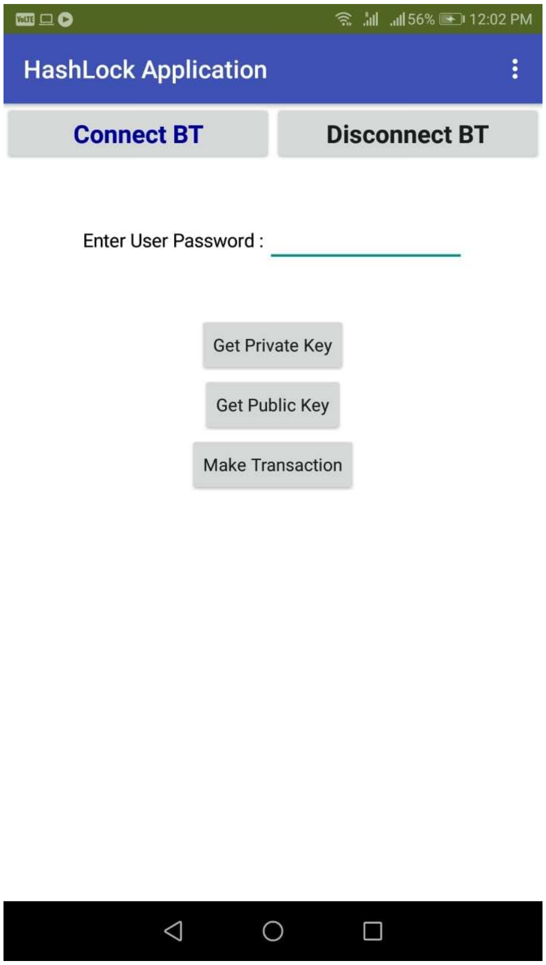


Figure 5.1 HashLock Android Application

5.2 OLED UI DESIGN

The OLED screen fitted on the proposed hardware is aimed towards regular use, and the screen UI is kept simplistic to not oversaturate the screen. The following are screenshots of the OLED UI in working state:

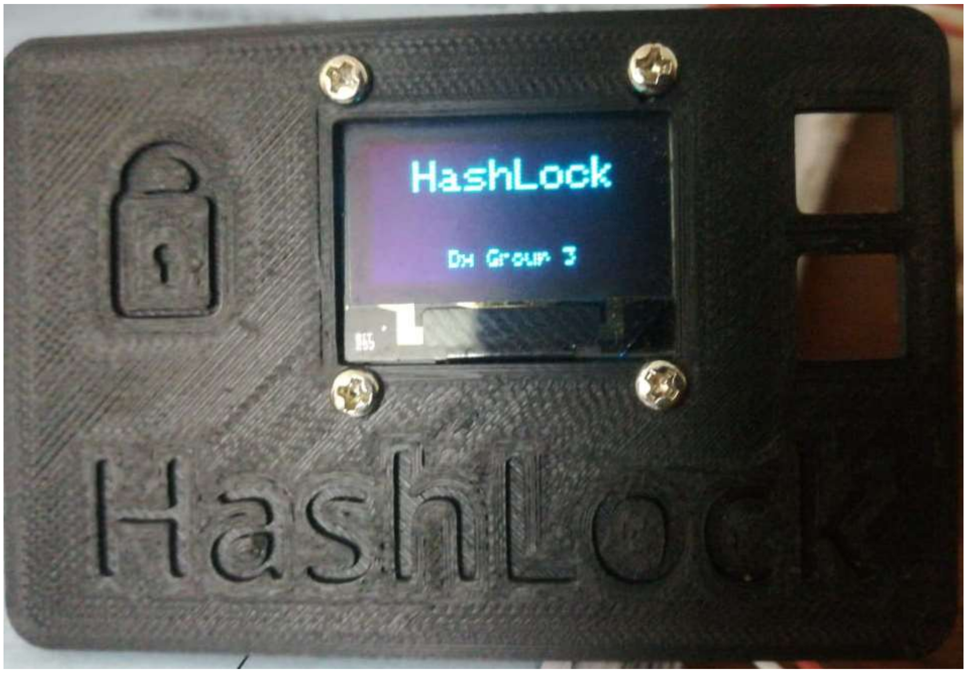


Figure 5.2 Splash Screen

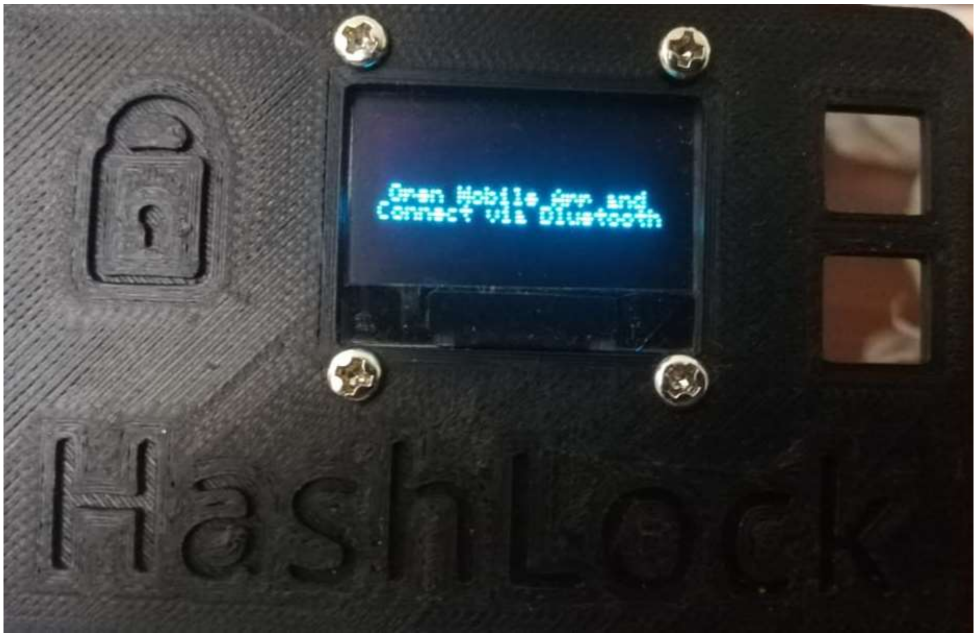


Figure 5.3 Connect Request Screen

5.3 ENCLOSURE DESIGN

To maximise utility, the hardware was encased in ABS based plastic casing with HashLock branding. As a product, the model will be self-sustained piece of technology which can benefit the current and future cryptocurrency users.

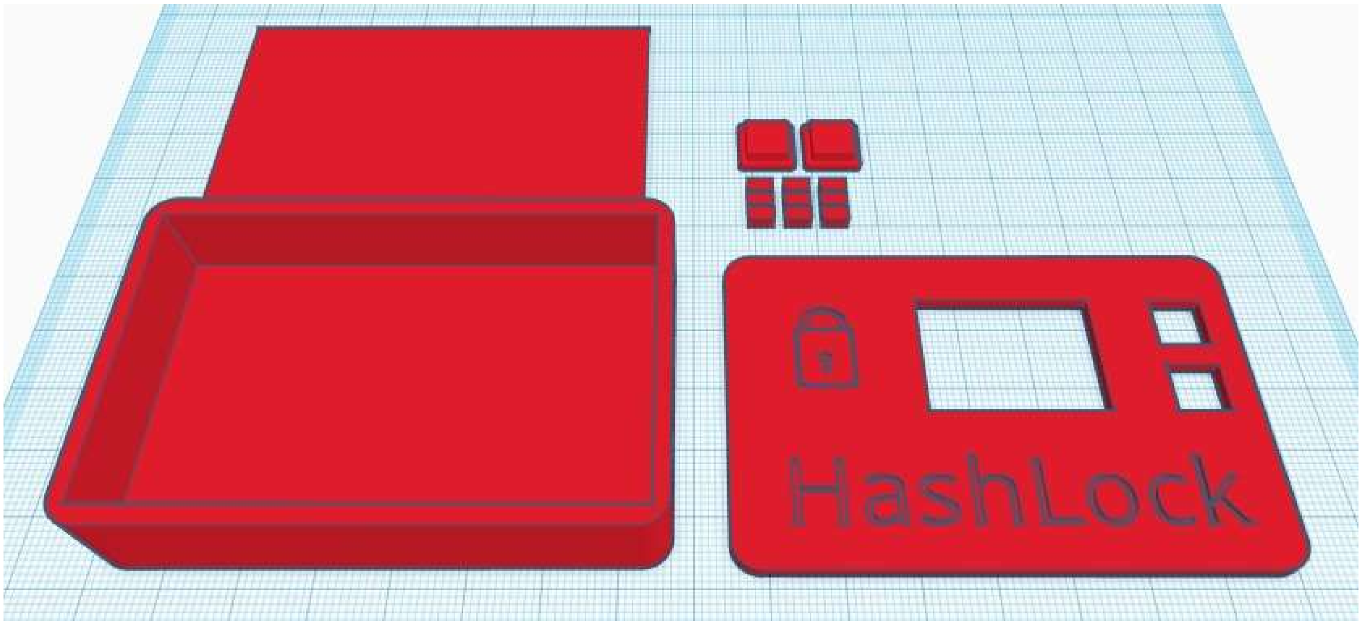


Figure 5.4 3D STL File Slanted View of Enclosure

The hardware casing was measured thoroughly to minimise the wasted space, and was tested using digital callipers. The box was designed specifically to look trendy, and be highly usable and affordable at the same time.

The case was finally printed using Ultimaker 3 (3D Printer) with 100% infill density and Black ABS filament. The net weight of the final print was 34gm with overhangs.

CHAPTER 6

RESULT

Hashlock was functionally tested, as well as structurally and electrically tested at various stages, and was tested in realtime post-build to make cryptocurrency transactions over Rinkeby Testnet for Ethereum Blockchain. The resultant model gave a model battery drain time of ~12 hours after heavy testing procedures. Drop tests revealed no structural faults and ensured safety and reliability of the model.

CHAPTER 7

REFERENCE

- E.Macksensen, M.Lai and T.M.Wendt, “Bluetooth Low Energy(BLE) based wireless sensors”,SENSORS,2012 IEEE,Taipei,2012,pp.1-4.

- R,Tei,H.Yamazawa and T.shimizu, “BLE power consumption estimation and its applications to smart manufacturing”, 2015 Annual Conference of the society of Instrument and Control Engineers of Japan (SICE),Hangzhou,2015,pp.148-153.

- Marwan Ali Albahar, Olayemi Plawumi, Keijo Haataja and PEKKA Toivanen, “Novel Hybrid Encryption Algorithm based on AES,RSA and Two fish for bluetooth encryption”.

- BamertT,Decker c., Wattenhofer R,Welten s.(2014) “BlueWallet: The Secure Bitcoin Wallet” Mauw S., Jensen C.D.(eds) Security and trust management. STM 2014. Lecture Notes in Computer Science, Vol 8743, springer, cham.