Master Thesis

Master's in Network Forensics , 15 credits

Blockchain Technology

a new domain for Cyber Forensics

Digital Forensics, 15 credits

Halmstad 2018-10-12

Muhammad Ahsan Rasool , Hafiz Muhammad Shafiq

HALMSTAD UNIVERSITY

HÖGSKOLAN I HALMSTAD

Blockchain Technology

A new domain for Cyber Forensics

by

Muhammad Ahsan Rasool

Hafiz Muhammad Shafiq

Supervisor: Eric Järpe

A thesis submitted in fulfillment for the
degree of Master's in Network Forensics

in the
Department of Computer Science and Engineering
Halmstad University

October 2018

Declaration of Authorship

We, M. Hafiz Shafiq and M. Ahsan Rasool, declare that this thesis titled, 'BLOCHCHAIN- A new domain for cyber forensics' and the work presented in it are our own. We confirm that:

- This work was done wholly or mainly while in candidature for a Master's degree at this University.
- Where any part of this thesis has previously been submitted for a degree or any other qualification at this University or any other institution, this has been clearly stated.
- Where We have consulted the published work of others, this is always clearly attributed.
- Where we have quoted from the work of others, the source is always given. With the exception of such quotations, this thesis is entirely our own work.
- We have acknowledged all main sources of help.

Signed:

Date: 2018-10-12

"No doubt ! Smart Contracts are only as smart as their creators are"

Abstract

Traditional database with no prior security measures is becoming challenging in the era of data technology. Database storage on a central location with single point of failure and vulnerable to cyber attacks is getting exposed to big risk of being hacked with the evolution of powerful machines and modern hacking techniques. Since its commencement, the BlockChain technology has shown a promising performance for application buildup in diversed fields of life from cryptocurrency to smart contracts and decentralized applications. Although multiple studies on privacy, data confidentiality and security issues of BlockChain are performed but a systematic examination is still needs attention. In this thesis work we conduct a systematic study about the vulnerabilities of BlockChain system and review the security enhancement solutions that may point to a good future direction for further research into the area of BlockChain technology and its applications.

Smart contracts are self-executable objects hosted on the 2nd generation blockchain like Ethereum, carry billions of SEK worth of cryptocoins and cannot be updated once deployed. Smart contracts are generally considered secure objects but the systematic analysis of technology and source code exposes a new class of vulnerabilities which are more likely an ethical aspect of programming than the software coding errors. Besides the literature review we empower our results with a static code analysis especially with the perspective of cyber forensics.

Acknowledgements

We would like to express our extreme gratitude to our teachers of grade one school through Halmstad University, especially our programme director Olga Torstensson for her great support throughout the course.

We truly appreciate Stefan Axelsson and Urban Bilstrup for their thorough guidance for the topic selection, advice on academic research and direction to focus on a single point out of widespread technology spectrum.

We would like to thank Mr.Eric Järpe for his constructive feedback, motivating advice and valuable supervision.

We acknowledge the unconditional contribution of DAPPS developers community and Securify team to provide us support for code analysis.

And finally, we would also like to appreciate our families for their patience and unconditional support.

Contents

List of Figures

List of Tables

Abbreviations

DPOS	**D**elegated **P**roof **O**f **S**take
EVM	**E**thereum **V**irtual **M**achine
IDE	**I**ntegrated **D**evelopment **E**nvironment
IoT	**I**nternet **o**f **T**hings
PBFT	**P**ractical **B**yzantine **F**ault **T**olerance
PoA	**P**roof **O**f **A**uthority
PoB	**P**roof **O**f **B**andwidth
PoET	**P**roof **O**f **E**lapsed **T**ime
PoW	**P**roof **O**f **W**ork
PoS	**P**roof **O**f **S**take
SEK	**S**wedish **K**rona

Dedicated to all parents in the globe, who sacrifice their present to build the future of their children. Thank you for being our first teachers and guardian for entire life

Chapter 1

Introduction

Multitrillion industries are going to rely on a system which has never been tested for its complete scalability. Blockchain is a linked list(digital ledger) comprised of blocks connected and secured using cryptography where each block contains a cryptographic hash of the prior block in the chain, a time-stamp and the transaction data which forces these blocks to maintain integrity of existing data.

Decentralized nature of this chain provides secure, confidential and integral means to maintain the records without modification. Today this concept is used in various fields of life to keep maintaining the records and also considered as a hot topic of research for using blockchain framework in social networking, Internet of Things (IoT) and banking systems [1]. Cryptocurrency also known as virtual or digital currency is a creation of modern era in which cryptographic techniques are used to generate the basic unit.

Wherever the money is involve, risk for illegal financial gain is always there. Since cryptocurrency uses cyber channel for mining, trading and transaction therefore crime related to this domain comes in the category of cyber or digital crime and needs to be investigated using digital and cyber forensics techniques.

2009 with the advent of first blockchain (named as bitcoin blockchain) and first ever digital cryptograpic currency -BITCOIN , introduced by Satoshi Nakamoto (still an enigmatic figure) a new era of decentralized payment system is opened to shake the financial systems, trading and to provide an anonymous system of financial transactions.

July 2015 was presented the second generation of blockchain, most famous of them was named Etheruem, contains an application layer to develop distributed application(just like the cellphone or internet application we have in our cyber world) and smart contracts which are predicted to replace the traditional banking, mortgage, trading, real estate record, health sector, databases and web itself.

Today hundreds of different coins and token are available for trading, crowd funding for kick-start,fund raising and even for financial fraud.

Millions of open-source smart contracts are developed by the potential developers to server the technology and blockchain market, regardless of their quality, vulnerabilities, bugs and errors these contracts have reached to the height of hypes in blockchain and cryptocurrency community and here started the hackers to exploit vulnerabilities in the system and software and so far hundreds of millions SEK were lost by corporate sector and individuals in the result of cryptocurrency trading, initial coin offering(ICO), hacking attacks, leakage, fund locks and ransom-ware transactions.
Today banking sector and financial corporate are one of the major client who is adopting blockchain technology for immediate and incorruptible transactions on the other hand public blockchaines are getting more popularity because of no intermediary and cost effective solution with anonymity.
All together it leads to open the discussion of broader technical standardization, code analysis, auditing tools, new methods of forensic investigations, regulations and legislation in a global perspective

1.1 Keywords

Blockchain , Bitcoin , Ethereum , Ethereum Virtual Machine , Smart Contracts , vulnerabilities , Securify , Remix IDE , Solidity , Locked Funds , Initial Coin Offering , cryptocurrency , attacks , bytecode analysis , wallet , Public Key , Untested Code.

1.2 Topic Goals

This thesis is a systematic review of previously performed scientific research on Blockchain technology but with the perspective of cyber forensics. We have concentrated on technology vulnerabilities that may attract the hackers to exploit the system. The aim of research and analysis in this thesis is to provide comprehensive understanding of blockchain technology, dive deep to explore security challenges and risks in the existing technology and to propose and/or highlight the proposed possible solutions to minimize these risks.

1.3 Motivation

Blockchain as one of the fast growing technology, every day incidents, ransom-ware attacks, financial frauds supported by cryptocurrency and cyber attacks on smart contracts due to existing vulnerabilities was fair enough to provide motivation for this thesis work.

Oyente - an execution analysis tool was developed in 2016 [2] which focused on smart contract analysis in ethereum blockchain and presented a result with identification of potential vulnerabilities in aprox. 8,000 out of 19,366 smart contracts motivated as well to perform a short code analysis to investigate the forensic aspect.

1.4 Definition of research question

This thesis addresses two questions related to the application layer of blockchain 2.0 (2nd generation) and clearly specifies in the light of existing research, available grey literature and the experiment performed by the authors.

- **Research Question 1**. Information security risks of smart contracts
  - **Sub-Question 1**:What are the information security risks of smart contracts?
  - **Sub-Question 2**: How can they be reduced?
- **Research Question 2**. Smart contracts- A matter of trust
  - **Sub-Question 1**: Can open source smart contract be trusted without code analysis?
  - **Sub-Question 2**: What preventive measure needs to be considered before using them ?

1.5 Existing Research

We have gone through the most relevant research work in the domain of Distributed Ledger, BlockChain, Cryptocurrency and other applications, no doubt blockchain technology is, one of the hottest topic of present time. Dozens of researches available, which unveil the technology, feature and possibilities for future usability of blockchain but when analyzed critically, unluckily we could not find enough deep information that may satisfy the question of cyber security.
Since bitcoin is assumed as the first application therefore major portion of available research and literature as well deals with the financial aspect of blockchain. Although the supporters see all positives in blockchain technology and its application, but the reality shows many negative aspects not according to the general perception. Blockchain does fulfill the criteria of CIA (confidentiality, integrity and availability) in some way, but

with the modern tools, hacking techniques and huge computation power there are several parameter needs to be taken into consideration like private and public key security, end point vulnerabilities, security upon scalability.
If we have a look only on bitcoin blockchain there is no mechanism to track the real and original value of assets it has, therefore it is impossible to estimate the worth of losses due to security breaches and hacking attacks, and when it comes to altcoin (all cryptocurrencies except bitcoin) the statistics will be mind blowing. Several organization, Government sector and corporate are attracted by the vendors and developers of blockchain products; therefore at present, with the appreciation of the positive side it is needed most to pay attention on the security weaknesses to establish preventive measures for the future.

1.6 Thesis Structure

Thesis starts with the introduction of topic, applied research methods, key concepts, tools and rest of the report is organized as follow, chapter two describes the theoretical background of the topic and review of available literature. Chapter 3 comprises of blockchain overview. Chapter 4 describes the forensic aspect of blockchain and cryptocurrency mining, ransom-ware and malware and also presents the evaluation of the examination. Chapter 5 presents the results, and Chapter 6 shows the direction for future work, discuss the answers the research questions, our contribution and also concludes the thesis.

1.7 Hypothesis

- Blockchain is an error free infrastructure for implementation of distributed application.
- Smart Contracts are secure but still there are risks which cannot be ignored.
- Majority of open-source software are free but not secure to be implemented
- cryptocurrency financial frauds, nowhere to report

1.8 Method

In this thesis work we used several different techniques to cover the topic from all dimensions, techniques are following:-

- Scientific literature review / relevant research papers.
- Grey Literature.
- Online search (news, blogs and other web-based material).
- Survey of victims (web discussion forums).
- Static code analysis.
- Systematic examination of security risks in existing literature.

1.8.1 Source of Literature

The review draws on multiple authentic databases covering the most important IS journals and conferences. The selected databases were INSPEC, Scopus, Web of Science (WoS), DBLP and and Google Scholar (GS).

1.8.2 Search criteria

Based on combinations of the search terms blockchain, ethereum, smart contracts security and vulnerabilities, we conducted a title/ abstract/ keyword search. This resulted in an initial set of 27 smart contract as well as 627 blockchain-related articles.

1.8.3 Literature selection

The retrieved papers were analyzed based on title, abstract, and keywords. The two main selection criteria were the match to the previously introduced concepts of blockchain technology and the smart contracts

An article was excluded if not addressed by means of valid methodology in a reasonable depth i.e., a framework or model, literature review, experiment, case study, code analysis, simulation or empirical approach)

29 articles were considered for further review and analysis. This first selection step resulted in a list of 16 smart contracts and 13 blockchain technology-related articles. To extend the coverage of the review and analysis these were included for a forward and backward search (Google Scholar) .

By narrowing down the selection this resulted in 22 articles. Literature selection was focused on articles for last 5 years of publications.

1.8.4 Static code analysis

Code analysis was performed to support the results extracts from the literature analysis. Securify is the tool selected on the parameters of its broader error and bug detection range, highly rated in overall analysis tool ranking in the reviews by blockchain developer community forums. Our data set was comprised of 257 open-source contracts which were randomly selected from the reputable database sources for the experiment and a static code analysis was performed with the perspective of intentional buggy codes and other vulnerabilities.

1.8.5 Ethics

Besides the scientific papers, a lot of material was extracted from gray literature, blogs and forum.
Open source codes are procured from GITHUB (one of the renowned database for smart contracts and other distributed applications)

Chapter 2

Theoretical background and the review of available literature

Perhaps the first article was written on blockchain and bitcoin in 2008 and few hundred publications in form of short papers and booklets till 2011 and later a drastic increase in literature is seen after 2012. Publications on bitcoin are almost double than its underlying technology, while the other application could not get attention of researchers and authors even the last couple of years [3] most of the publications focused on business and financial aspect of cryptocurrencies and a large number of the blockchain based publications were confused with bitcoin in the start. Latest literature is more specific to technical topics especially on blockchain. Still needs more deeper studies of technology rather than overviews.
We have selected 22 papers based on title and abstract description relevant to our topic, reviewed them and presenting the extract following:-

2.1 Blockchain services and application

Since the introduction of blockchain technology 2008 and its revolutionary application like Bitcoin and other cryptocurrencies, researchers and experts are now preparing to build over supply chain, commercial application, business models and market structures and many projects are on their way from prototype phase to deployments. Hundreds of successful applications are already deployed and available for the user on internet. Web 3 standard is introduced MIST as a web3 browser as well launched by the decentralized application programmers and blockchain community.

2.1.1 Cryptocurrency

one of largely deployed application on blockchain technology. Today hundreds of different coins available in the commercial market to support different projects from humanitarian and charity to development of new technologies and financial institutional infrastructures. We will discuss details with the flow of thesis, for now we can have a look on RIPPLE a gateway to replace the traditional banking transaction system by speeding up the transaction time to few seconds and reducing the transfer cost.

Beside that there are many coins came into being with great ideas and investment opportunities but died after a small lap of time, such coins require more attention to investigate whether they are dead because of technical issues or they were made to get illegal financial gains and here it strengthens our hypothesis that cryptocurrency financial frauds, nowhere to report, who will launch investigation? how to investigate ? will become a global question.

2.1.2 Internet of Things (IoT)

Current IoT ecosystems rely on client server paradigm, so regardless of distance and geographical locations connectivity between IoT devices will have to establish through internet exclusively. This model serves good for small scale IoT networks as today and may cause scalability issues with the growth of networks and devices. This network model comprises on centralized cloud, huge data and server farms and other attached network equipment and finally everything added up to cost and running expenses, imagine if the IoT devices grow several 100 times and the same way network resources as well consequently the cost will increase substantially. New challenges will rise in form of cloud bottleneck and machine-2-machine communication will become a difficult task when it comes to the point of diversity of vendors equipment and their supporting clouds infrastructure. [4] A peer to peer decentralize approach will be the solution of afore mentioned issues, it will provide comparatively faster communication, prevention from failure of entire network in case of failed node and most of all is the security as IOT system security is much more bigger issue than securing just data. [4] On the other hand dealing with big data may limitise the implementation of IoT

2.1.3 Land registration and Record keeping

Besides the cryptocurrency usage of blockchain technology is already tested in the recordkeeping and it has given very appreciating results. Some of the ongoing tests are following:-

During the spring, Lantmteriet has been involved in a project together with the companies Kairos Future, ChromaWay and Telia. The purpose has been to take a closer look at the blockchain technology and what it may mean if used in connection with the real estate transfer process.
The reason that we are looking at this technology is that it is very safe while it can support processes in several ways and offers transparency.[5] Later Lantmteriet has launched the test in 2017 named as the land registry in blockchain Testbed and look forward for the results and scope [5]
A pilot project for the registration of land transfer record has been launched in august 2017 by the local authorities at municipality of Pelotas in Brazil named as blockchain Land Registry tech Gets Test in Brazil[6]

2.2 Challenges and Limitations

On contrary to benefits of the blockchain there are many limitation needs to consider while addressing the technology in details. One of the major challenge for the present time is the dramatic increase in the computational cost of mining, when continuously too many blocks are submitted, therefore due to increase in computational difficulty, increase cost directly[7]. other limitations are mentioned following:-

- Wasted resources
- Usability
- Long term preservation challenges
- Throughput
- Latency
- Size and bandwidth
- security breaches
- scalability

2.3 Major research topics

Blockchain security is the major research topic directly addressed in our selected scientific publications and the second most important discussion is about the technology related challenges and limitations.

2.3.1 Trends of security incidents

with an increased use of cryptocurrency for transactions, payments and trading, risk factors and losses increased drastically. Because of illegal financial gain activists not only individual but the mining pools and trading platform like exchanges suffered with hacking attacks, scams and distributed denial-of-service attacks [8].
The most common scams investigated for last couple of years are Ponzi scams, fake wallets, mining scams and even fraudulent trading platforms and the financial losses were in millions. Survey performed on different forums shows that approx. 13000 bitcoin users became victim of scam and shared a loss of USD11 million in one year September 2013-September 2014 [9].
Lim et al. presents the analysis of security breaches in cryptocurrency describing all possible threats including private account hacking with Trojan horses, virus from advertisements and DDoS attacks. They have proposed solution with hardware wallets and authentication devices.[9]
Vasek et al. [8] presents a study of DDoS attacks on trading exchanges 41% followed by the cryptocurrency mining pools 38 %. Paper concludes that over 60% of DDoS attack victims were large mining pools and 17 % small pools although majority of these pools use anti DDoS protection but it is yet unclear whether they had protection on the time of attack or not. Papers we have gone through focus 88 percent on bitcoin and other cryptocurrencies and only 12 % research was focused on other applications.

2.4 Key concepts and tools

In order to understand the blockchain technology, smart contracts and their application some of the key concepts and building blocks are very important to be grasped.

2.4.1 Hash

A hash is 32-byte(256 bit) and almost-unique string of letters and numbers forms in the result of the application of hashing function, By applying algorithm on a simple data and perform the conversion.
Example can give a better explanation: [10]
SHA256 + Hello World = a591a6d40bf420404a011733cfb7b190d62c65bf0bcda32b57b277d9ad9f146e
SHA256 + Hello Worl = 12fec4c65dd4455c48aff8977a7cd8ccb97539ad4cd7c37f13cf71ba8bee9a98
Even a slight change in data will make the resulting value of hash entirely different.

2.4.2 Block

A container and a building block of blockchain. The common attributes of a block is an index (number of the block in the chain), transaction data, time-stamp, nonce and hash of previous block.

Any change in the contents, the hash will be changed and the block will become invalid.

Nonce is an input to the hashing algorithm, not possible to predict and it is considered as proof of work by the machine creating the hash.

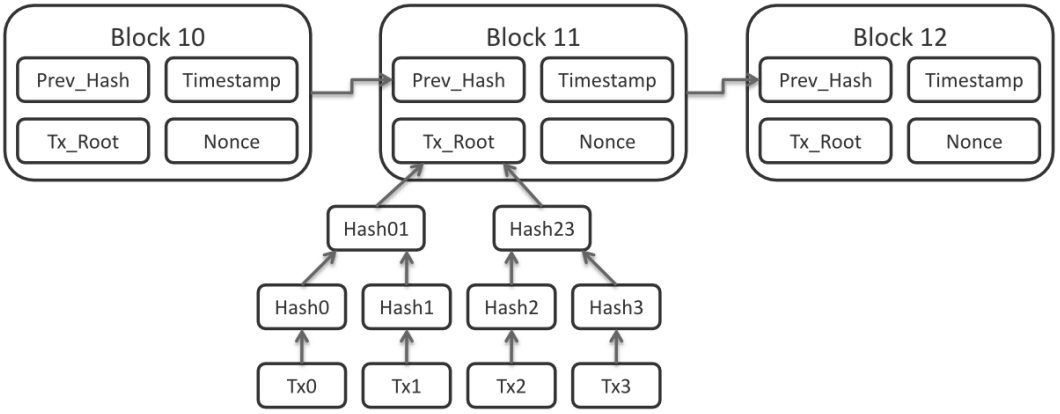

FIGURE 2.1: Blocks in a chain
[11]

2.4.3 Wallet

Wallet is an open-source, user-side interface(software). Just like a traditional bank account number, every Wallet has an address and the public key denotes that address.

Wallet as a client side software allows user to interact directly with the blockchain while remaining in full control of his / her keys & funds, using private key the proof of ownership.

Private key is the most sensitive part of wallet and the owner is responsible for his / her own security to keep the key unexposed and hidden from hackers. In a simple explanation wallet is a container to keep the assets like cryptocoins.

2.4.4 Remix

Remix is a powerful, open source integrated development environment (IDE) uses to write smart contracts in solidity development language. The tool (IDE) can be used

on local computer or browser based, written in Javascript. The most common features are writing, debugging, testing and deploying the smart contract over the virtual machine. Remix IDE and its feature and a full documented support is available at remix.ethereum.org.

2.4.5 Solidity

Solidity is a high level language, designed to target the on various blockchain platforms especially Ethereum Virtual Machine(EVM) with the basic objective for implementing smart contracts over EVM, therefore it is known as contract-oriented language. Solidity was developed by Gavin Wood, Christian Reitwiessner, Alex Beregszaszi, Liana Husikyan, Yoichi Hirai and several former Ethereum core contributors and influenced by C++, Python and JavaScript and it supports inheritance, libraries and complex user-defined types.

Contracts can be created for different application like voting, crowdfunding, blind auctions, multi-signature wallets and many others.

Chapter 3

Blockchain Overview

Blockchain is new class of information technology based on the combination of cryptography and distributed computing, which exist for a number of decades. The cryptographic secured chain of blocks was described by Stuart Haber and Scott Stornetta in 1991 and later worked on the decentralized digital currency by using similar technology was done by Nick Szabo in 1998.
Financial crisis of 2007 - 2008 AKA. global financial crisis hit the world financial market and because of that incident an experiment was launched by Satoshi Nakamoto (still an enigmatic figure) with the solution of decentralized payment network and in the result, he came up with the first blockchain named as bitcoin[12].

3.1 Fundamental trust mechanism

Unlike in centralized systems where some administrator manages database and makes the decision of file storage and update, in decentralized systems Fundamental trust mechanism also known as consensus mechanism is used to make the nods agree upon storage of data. There are many consensus mechanisms in existing blockchain technology but four of them are considered major in use [13].

3.1.1 Proof of Work (PoW)

To prove the credibility of data in blocks PoW mechanism uses the method to solve the puzzle. When a node wants to create a block it must resolve a puzzle. Upon resolving the puzzle successfully a new block is created and broadcasted to other nodes to achieve the consensus [13].

- Probability of mining a block directly depends on the work done by miner.
- Consumes more energy than other Mechanism like POS
- can cause a 51% attack if overall computational power is achived

The contents of a block may vary in different chains.

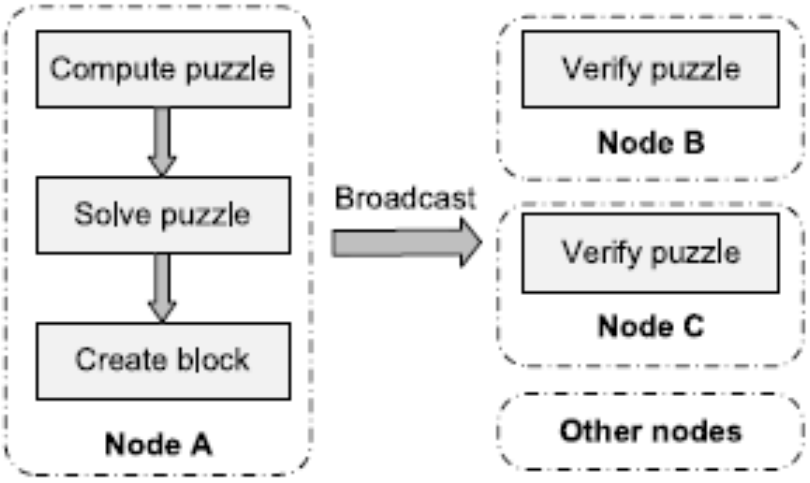

FIGURE 3.1: PoW consensus Mechanism
[13]

3.1.2 Proof of Stake

To prove the credibility of data in a POS mechanism, a node should have enough stake in the assets to validate the block.

- Stake holder validates by using its share in assets(coins)
- Less power consumption
- To attack the network need to own majority of assets (coin)

The two most popular blockchains systems, BITCOIN and ETHEREUM uses Power of Work(PoW) and in future planning to use a hybred mechanism which will comprise on a merged functinality of POW and POS consensus mechanism while many other systems use Proof of Bandwidth (PoB)[14], Proof of elapsed Time(PoET)[15], Proof of Authority (PoA) [16] , Practical Byzantine Fault Tolerance (PBFT) and Delegated Proof of Stake (PDoS) as well.

3.2 Block propagation and synchronization

Despite the fact that blockchain technology is fast growing and has a great capability to play a vital role to construct the future inter-network systems, many challenges like capability to handle large data, latency and synchronization exist when it comes to address the capability of high frequency transactions of block.[13] Bitcoin block size is limited to 1 Megabyte only and it requires 10 minutes to be mined with the computational power of a miner. Bitcoin network is incapable to deal with high frequency transactions due to restricted rate of transaction which is 7 trans/sec. The larger the blocks are the requirements of storage space increases and it leads to slower propagation in the network Synchronization of blocks over the network became challenging with security measures because miners can hide their mined blocks for the sake of high revenue. [13]

3.3 Ethereum Next generation BlockChain

Over the last couple of years developers stared using blockchain technology to build a variety of applications. Ethereum has become one of the pioneers to facilitate programmers and developers to create their decentralized application (Dapps) taking the advantage of decentralized network. A decentralized application serves some specific purpose to its user without relying on third party ownership or existence and without any centralized intermediary. BitTorrent for a file sharing and cryptocurrency like Bitcoin are the earliest example of decentralized application. The primary development idea was taken from BitTorrent as peer to peer network and Bitcoin blockchain to create the general platform of Ethereum and make it available for developers to use as underpinning technology for variety of applications for any purpose. In other words an Ethereum blockchain can be described as a blockchain with a feature of built-in programming language or it can be call as a globally executed virtual machine based on consensus mechanism for transaction confirmation.

3.4 Ethereum Virtual Machines

EVM is a decentralized computation, data storage and communication protocol, used as a sandbox while remaining completely isolated from the network, operating system, file system and other resources of the host machine

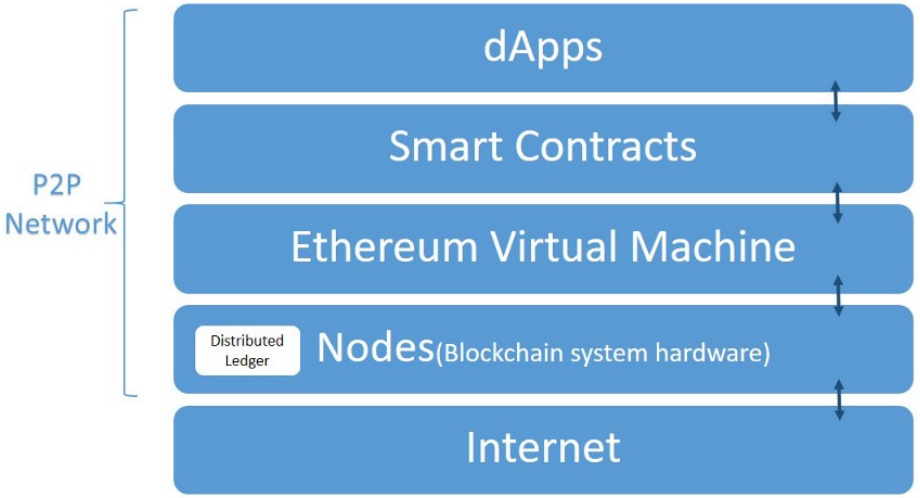

FIGURE 3.2: Ethereum Layer model
[17]

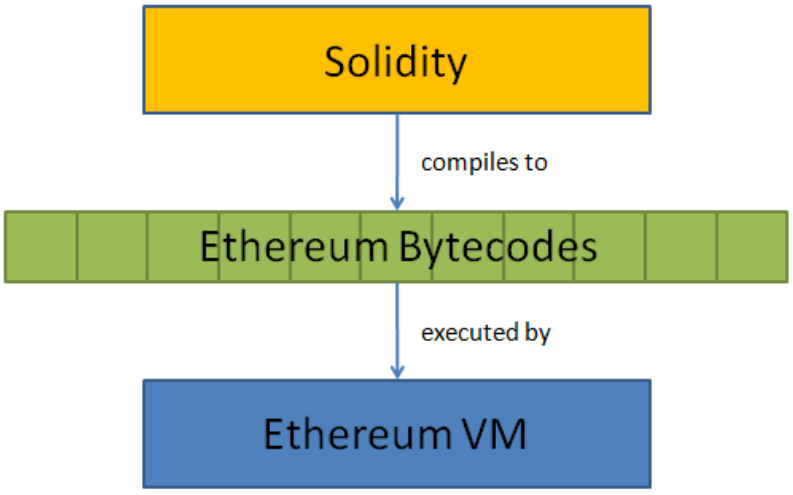

FIGURE 3.3: Bytecode over EVM
[11]

3.5 Ether

Ether is the crypto-fuel (cryptocurrency)introduced by the Ethereum developers to use for the services of Ethereum Network [18]. The consumer of Ether are the developers who are willing to develop Distributed applications(Dapp) and also the users who intends to access these Dapps and interact with smart contracts while using Ethereum blockchain. 60 millions Ether were created to support the development of Etheruem platform and 20% of that will go to the contributors and remaining to the Ethereum Foundation.

5 Ether is rewarded to the miners for the creation of every block which were reduced to 0,625 after Bayzantium update implementation. the price of Ether in coin market is 517 USD [19] at the time this report was written.

3.6 Smart Contracts

Unlike the legal agreements, as expressed by names, Smart contracts are piece of software which are designed and implemented in many high-level programming languages depending on the platform but Ethereum smart contracts are usually developed in the most prominent language Solidity [20] and the programs is compiled into EVM bytecode to run over Virtual machine.
Smart contracts provide the support not only for cryptocurrency exchange between users, but to exchange other assets like property, insurance, share, contents or any thing which carries some value [21]. Smart Contracts behave like self-executing and self-operating programs when running on EVM, upon meeting the specific requirement a smart contract and trigger itself to execute without any interruption, delay, down-time and third party control, exactly as the sequence of instruction are given.

3.6.1 Dapp

A decentralized application can have a front end code just like any applications and a user interface written in any language and has ability to call the backend code which is running on blockchain platform. Majority of the smart contracts interact with traditionally developed web application front end to facilitate them with contract functionality, and when a Dapp user sends a transaction, the contract function invokes and executes as programmed, these functions can be financial, gambling, gaming or any other possibly programmed.

3.6.2 Execution fee

The user who invokes the function is liable to pay the execution fee to and this fee is distributed among all the miners who consume their computational power to support execution of the function over the network.[22] This execution fee in term of Ethereum is defined as "gas" and is limits up by the transaction which invoke the function, the more gas price is to pay the more miners are willing to work. Overall execution fee depends on number of instruction in the executed contract.

Chapter 4

Forensic aspect of blockchain

Blockchain technology as an implementation of peer to peer computing model contains more security comparatively but lacks in a central control over the system, not having a single point of failure like client server model it becomes harder to penetrate the system and destroy the data it self or its integrity or confidentiality as data is in encrypted form when as far as applications are concerned there is no privacy generally as applications are visible.

4.1 51% Attack

the design of blockchain mechanism is based on the assumption that honest nodes with large computational power control the network. Here it comes the risk of 51% attack if the collective computational power of bad or attacker nodes becomes more than the honest nodes. Beikverdi et al.[23] presents arguments that market based centralized mining pools with huge computational power can increase the risk of 51% attack although the designed blockchain is decentralized. Their study shows a continuous increase in the centralization factor of Bitcoin from 2011 (0.26) to 2014 (0.33).

4.2 Authentication and cryptography issues

In cryptocurrency one of the major authentication element is the private key. Several authentication incidents we reported in the past few years. One of the well-known case is MT.Gox, where Mt.Gox storage was attacked by hackers and the information was stolen where private keys of clients were stored and this incident lead to the study for

strengthen the authentication issues. Boj et al. [24] in the case of Mt.Gox, states the ECC (elliptic curve cryptography) does not meet the requirement of randomness.

4.3 Distributed Denial of Service attack

The mining pool that provide computational power to mine the blocks are frequently targeted by the distributed denial of service() attacks. Majority of mining pool providers do not have anti DDoS attack protection. Besides the mining pools the trading platforms (cryptocurrency exchanges) are always stand one first place for DDoS attacks. [25]

4.4 Data integrity issues

Data integrity is an important part of communication and same with the blockchain environment. It is necessary that data has not been tempered during the transmission and verification process. In case of cryptocurrency transaction can meet an interception, modification and rebroadcast if there occurs a malleability attack and causing the issuer to believe that transaction is lost or not confirmed by the service providers [26]. Decker & Wattenhoffer studied that the signature being transferred in a transaction, that proves the ownership do not provide guarantee for signature integrity itself [26].

4.5 Endpoint Vulnerabilities

End point in the blockchain is the point where humans and blockchains meet, more simply the end point is a computer which is used by any individual or organization to access the blockchain services, and this is infact one of the most important point to be considered when deal with the security of blockchain. Regardless of blockchain based service whether it is a financial institution, public or community organization or a financial transaction in form of cryptocurrency exchange the area of blockchain remains in between the sender and the receiver computers with the information therefore the time while data is processes on any of both ends is most vulnerable in its nature because it deals with the credentials and the shared ledger. This is the weakest point where credential are exposed due to weakness of users and the limitations of blockchain.

4.6 Vendor Risks

Blockchain has no value without the building blocks of distributed ledger, the transaction in, out and balance.The more communities and organization adopting the blockchain the more application developed by 3rd-party will be deployed with the passage of time within the blockchain ecosystem. The requirement of more modern application, functionality and programs brought more 3rd-party vendors to develop the different software for different point of execution like:-

- Client software(Wallet)
- Payment processing modules
- Smart contracts
- Blockchain payment platforms
- Integration platforms
- cryptocurrency exchanges
- Dapps for Ecommerce

Organization who wish to deploy 3rd-party developed solutions should aware of the severe risk of malware, buggy codes and codes with intentional fraud functionality like exposing credential and important data to the unauthorized persons.

4.7 Public and Private Key Security

To get connected and access the blockchain a user requires to be authenticated by the combination of both public and private key. These keys work like the user-name and password by behaviour but different in structure as these comprise of the cryptic strings made of numbers and characters with a sufficient length that makes it almost impossible to guess them by humans and the computers as well.
The combination of private and public keys is an ultimate strength of the blockchain as without a right combination no hacker can access the data ever and simultaneously is the drawback or weakness of the technology as the only thing hackers need is these keys, and the game will be out of control even for a legitimate users.
Malware, Trojan,social engineering techniques, key loggers or other malicious software are used to get these keys by hackers instead of wasting time on guess, therefore, weak points of computers and mobile phones are always targeted.

4.8 Untested platform at Full Scale

Many industries may not have much concern with this unknown and unproven vulnerability of blockchain, what will happen at a full scale, perhaps they do not want to think about this issue before time. Architecture of distributed ledger is inherently scaleable but may be very complex to maintain since it was never tested for its functionality at full scale.

4.9 Lack of Standards and Regulation

Decentralized cryptocurrencies have rapidly gained popularity, and are often quoted as a next generation of financial technology based on decentralized infrastructure of blockchain, The terms blockchain and miners are therefore often used interchangeably. Hence the requirements to introduce new technical and legal standards can not be eliminated to overcome the security issues.[27] Different from from other financial institutions and wealth issuing organizations cryptocurrencies usually do not owned by any proper institution therefore it has feature of no regulation by any region, countries or companies.[9]

4.10 Vulnerabilities of Smart Contracts

The mechanism of BlockChain as an underlying technology is secure with some limitations and weaknesses, vulnerabilities in smart contracts exist due to codes which generate these contracts, and these may be intentional by developers or the poor code structure. In June 2016, over 500 million SEK were made off by anonymous hackers by exploiting bugs in smart contract code. In July 2017 a very well-known Ethereum wallet was compromised when another bug was exploited in the code and estimated damages were reported over 300 million SEK.[28]
With the inception of cryptocurrecy transfer facility to anonymous accounts the attraction for hackers is becoming more charming to invest their time and resources to find loopholes and vulnerabilities in the smart contracts and no matter how they attack to procure an extremely lucrative incentive if they get successful.

Chapter 5

Results

In the light of selected literature, a review and analysis of existing research publications and available gray literature was performed and further more we have analyzed the procured code statically. results extracted from the review and analysis and from the performed experiment is described following in two different sections respectively.

5.1 Literature Review

Here are some findings for the overall literature available in different databases over blockchain technology, its financial aspects and applications. First publications which may fall in the topic of blockchain can be considered in the start of 2008 and in next three years researchers continue focusing on the publications more related to crypto currency and these were around 400 white papers and research articles were available in the databases till 2011 and later a drastic increase in literature can be seen after the year 2012.
Although bitcoin is a part of blockchain system and a considered as a product(application) but publications on bitcoin alone are more than double of its underlying core technology. Research papers regardless of their nature if were written for the bitcoin as a cryptocurrency or the bitcoin blockchain, most of these focused on business and financial aspect of cryptocurrencies.
Blockchain based publications were confused with bitcoin(as a crypto currency) in the start while latest literature is more specific to technical side, especially on blockchain and discusses the application, core structure, possibilities and future expectations.

Although many researcher touch the security issues but still needs more depth studies of technology rather than overviews.

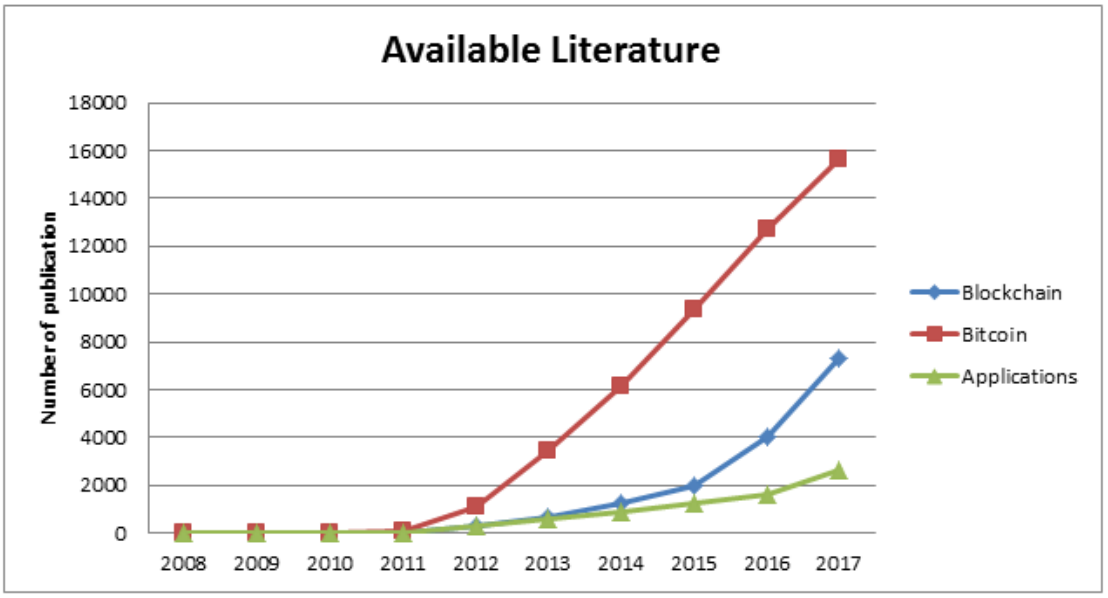

FIGURE 5.1: Research papers and publications on blockchain and its application Based on publications from IEEE Xplorer, ACM, Springer, Ebsco and ScienceDirect [3]

5.1.1 Untested Code

One of the biggest concern about Ethereum smart contracts is that it is hard for an average user to check and analyze that if there is no hidden bug or secret piece of code that facilitates the developer of the smart contract to run away with some assets, although this is theoretically and practically possible to go through the code for verification if it does the same job it is made for.

above mentioned criterion may apply to widely used distributed applications and as well as customized ones.

Hundreds of thousands smart contracts are used today by different applications and number of these codes increasing gradually with the passage of time.

Unfortunately, traditional tools for code analysis often fails while analyzing the application specially the smart contracts, they successfully modify or undo the official terms of contracts and create more difficulties when it reach investigation and prosecution in the court of law [29].

Many frameworks and tool are in the phase of development to find bugs in source codes and many other tools are already designed to write secure smart contracts [27]

We have gone through dozens of real life source codes available on github as open source smart contracts and the results were found surprising.

```
...
Player[] public persons;

uint public payoutCursor_Id_ = 0;
uint public balance = 0;

address public owner;

uint public payoutCursor_Id=0;
...
while (balance > persons[payoutCursor_Id_].deposit / 100 * 115) {
  uint MultipliedPayout = persons[payoutCursor_Id_].deposit / 100 * 115;
  persons[payoutCursor_Id].etherAddress.send(MultipliedPayout);

  balance -= MultipliedPayout;
  payoutCursor_Id_++;
}
```

FIGURE 5.2: Code chunk with bug

Below is the chunk of code written in solidity language for a gambling application where it was featured to double your Ether in a dice game

5.1.2 Reentrancy

With the recent hacker attack The Dao hack [], reentrancy became a well known vulnerability of smart contracts, where hackers exploited this weakness and became successful to steal over 3,6 million ether(valued 60 million USD at the time of attack). [22] Simple explanation of this vulnerability is when in Ethereum an attacker's contract calls the withdraw function of victim contract function which is responsible to send Ether(upon purchase or other activity) and callee's in our case is Attacker's fallback function calls for withdraw for multiple time unless the balance gets zero.

```
pragma solidity ^0.4.8;

contract Victim {

    uint public payableToAttacker;

    function Victim() {
```

```
        payableToAttacker =11;
    }

    function withdraw() {
        if (!msg.sender.call.value(payableToAttacker)()) revert();
        payableToAttacker = 0;
    }

    // deposit some funds for testing
    function deposit() payable {}

    function getBalance() public constant returns(uint) { return this.balance; }
}

contract Attacker {

    Victim v;
    uint public count;

    event LogFallback(uint count, uint balance);

    function Attacker(address victim) payable {
        v = Victim(victim);
    }

    function attack() {
        v.withdraw();
    }

    function () payable {
        count++;
        LogFallback(count, this.balance);
        // crude stop before we run out of gas
        if(count < 20) v.withdraw();
    }

    function getBalance() public constant returns(uint) { return this.balance; }

}
```

5.1.3 Immutable bug

Smart contracts are immutable in their nature, means once implemented on blockchain can never be alters for the set of instruction programmed in them.[22] This feature of contract code makes it execute exactly as it decided to, but on the other hand it has a big advantage that there is no possibility to patch a code while deployed, if it contained a bug and executes it has to be terminated by the owner. There are few tools already introduced to alter the set of rules but they are fail in case of smart contracts [30]

5.1.4 Ether lost in transfer

The public key or the wallet address is a hashed sequence of 160 bits and should have an association to any user contract or to the recipient wallet, if not associated or the address is incomplete it is called an orphan address and if the sender by mistake or some other reasons pointed to such address the ether will lost forever and there s no mechanism to sort it out whether an address is valid or orphan. this vulnerability is called as leakage as well. [22]

Beside the above mentioned vulnerabilities there is a huge number that was not really addressed in the research papers available in grey literature.[22]

- Transactions may affect Ether Receiver
- Transactions May Affects Ether Amount
- Reentrancy Gas-dependent
- Reentrancy with constant gas
- Reentrancy method call
- Unchecked Transaction Data Length
- Unhandled Exception
- Use of Origin instruction
- Missing Input Validation
- Locked Ether
- Use of untrusted Inputs

- Strict balance equity
- Byte array
- Transfer forwards all gas
- DoS by external contract
- Token API violation
- Costly loop
- Integer division
- Malicious libraries
- Compiler version not fixed
- Private modifier
- Redundant fallback function
- send instead of transfer
- Style guide violation
- Tx.origin usage
- Unchecked external call
- Unchecked math
- Unsafe type inference
- Implicit visibility level
- Callstack depth attack
- Transaction ordering dependency
- Assertion failure
- Inline assembly
- Low level calls
- Blockhash usage
- Constant functions
- Similar variable names

- Timestamp-dependency

Some of vulnerabilities are mentioned in different literature with different names but identical in nature with the above mentioned vulnerabilities and these are exposed ones while everyday there are new discoveries.

5.2 Code Analysis

The research conducted with an automated tool and later published as research paper[31] was a point of motivation to perform a code analysis of open-source smart contracts therefore we have downloaded 257 contracts code randomly.
The objective of performing this analysis was to support our hypothesis that smart contract are not really secure and to highlight the forensics aspect therefore the selection criteria was to procure the contracts

- lower download rate
- less number of review
- deal with gaming
- deal with gambling

5.2.1 Search for fingerprints

For every identified vulnerability category we have examined through the code with the help of Securify and tried to find without reading the code and functions in depth. smart contracts are available for every field of life but most vulnerable contracts are gambling based and dice gaming related.

5.2.2 Static Code analysis

Common tools used for the code analysis are usually debug the broken links, find missing variables, this manual code analysis was performed in the guidance of best practice and recommendations by consensys [32]. Result of the analysis reflects in the table below.

Vulnerabilities mentioned as a "common by tool " are the already discovered weakness and holes and mostly covered in the research publications and as well arranges in the list shown afore and was captured by the tool Securify, while hard coded public keys

Description	number	Classification
Total number of analyzed contracts	257	Common by tool
Exposed to external hackers	31	Forensic aspect
Hard coded public keys in the code	10	Forensic aspect manually scanned
fund locker	8	Forensic aspect
other vulnerabilities	15	Common by tool

TABLE 5.1: Reflection of code analysis

in the code may have a strong argument of intentional fraud, leakage and on the same parameters fund locker can be a bug in the source code or programmed specifically for illegal financial gain either by the developers or the owner of the smart contract.

Chapter 6

Dissertation Conclusions

6.1 Discussion

Blockchain technology is comparatively secure infrastructure in its nature but when it comes the application layer of this model it exposes bunch of vulnerabilities and challenges to resolve them. Having a careful overview and analysis of the previous literature, these issues were tackled using different approaches by different researchers.
Unfortunately out of hundreds of articles and research papers on these topics, majority covers only financial aspect of the domain. Only few of them chosen the track to perform the code analysis by using an automated code auditing tool.
All the research papers selected for final analysis discuss the general weaknesses and address the issue of buggy code written by smart contract developers, they have pointed out a lot of coding errors that may expose to hackers to invite them for an attack as well as the vulnerabilities of solidity language which may lead to make the code buggy.

6.1.1 Answer to research question 1

The first part of the research question one " what are the security risks of smart contracts?" is very well answered in the selected research papers with the details of vulnerabilities on all the ends including blockchain architecture, smart contract technology and as well as issue with the built-in functions.The highlighted vulnerabilities are including reentrancy, fallback function call, wrong fund transfer, leakage, fund freeze etc.
One very deeply performed bytecode code analysis by a research group and later published as a research paper[31] unveils the results of their experiment highlighting the large number of(3.5%) of buggy code and categorized them in three classes

- Prodigal contracts - smart contracts that when attacked send funds to the wrong Ethereum address.
- Suicidal contracts - smart contracts that handover control to a hacker and can be killed by someone else and not just the owner.
- Greedy contracts - smart contracts that freezes the funds forever.

Answering the second part of first research question "how to reduce the risks? " we have composed our proposals

- Follow standard guidance from Ethereum Foundation
- Use approved Ethereum scripting programming language like solidity
- Update knowledge with latest attacks, vulnerabilities and bugs
- Stay active with community forums and social networks managed by blockchain and Ethereum developers community.
- Avoid being the victim of social engineering on these forums
- Write as many test cases as possible
- Needs to treat carefully if the smart contract directly deals with any cryptocurrency
- Withdraw, Winner, Payment function supposed to be handle with recommended coding patterns and avoid fancy coding.

6.1.2 Answer to research question 2

Very important aspect which has been ignored in almost all the studies and research performed so far(or at-least we did not come across a single research paper solely focused on this topic) is the Ethical Aspect. A partial answer to sub-question 1 of Research Question 2 "can open-source smart contract be trusted without code analysis?" can be found in the same research paper [31] which mentions about fund-lock and transfer the funds to other wallet addresses by mistake, our static code analysis support them fully with the same result but we came across to an other opinion that the objective of intentional financial gain can not be ignored in this matter.
Hard coded wallet address, transfer of funds to other contracts, fund lock and leakage motivates to see on the other side of coin that these errors can be a way beyond coding bugs and can touch the boundary of cyber crime instead.
We have composed a list of proposals to answer the last part of second question and these are following:-

- Code should be procured from a physical / responsible sources
- Static code analysis can be an answer
- Verify the false alarm rate of auditing tools before using for code analysis
- Run as many test to find hard coded address and jump in functions
- Code standardization needs to be improved for general guidance

Coding error and bug is an essential part of programming not only because of the programmer, they can be due to compiler , programming language or framework. these errors and bugs are discovered and fixed in the past, exist in the present and will remain in the future as well and we can not avoid them but our findings force us to think in a broader vision.
Overall crux of the code analysis performed by us showed up with the results of 10 out of 257 randomly selected smart contracts with hard coded address which may indicate the intentional fraud or sever mistake at developer side and such attempts can be an alarm for forensics and cyber security.

6.2 Our contribution

To achieve the goal of this thesis, our work consisted of two phases.

- To perform the thorough analysis and explore vulnerabilities of smart contracts which are mentioned and explained in the existing literature which we have found in gray literature more than the published research papers.
- To investigate the ethical aspect of the smart contracts and unveil developer made exploits by performing static code analysis and our contribution can be seen in the reflection of results table 5.1 in chapter 5.

The main contribution of this thesis is to highlight the vulnerabilities of smart contracts which fall in the area of security and forensics and also to address ethical aspect of coding and development in blockchain based distributed applications through literature review and code analysis.

6.3 Conclusion

The goal for this thesis has been to prove that the open source smart contracts are not as secure as they are propagated on electronic media, internet and discussion forums. Since the advent of blockchain technology bitcoin became the pioneer in cryprocurrency and bitcoin-blockchain stands first as an infrastructure but a relatively new blockchain based platform Ethereum proved to be game changer with its application layer functionality to develop distributed applications and smart contracts.
Smart contracts are self-executable and immutable piece of software which do not allowed to be altered once deployed over the system. Provide fast and unstoppable execution but could remain vulnerable and hackers target if the buggy/incomplete and vulnerable code was deployed once.
Hype within blockchain community that smart contracts are ultimate secure was at its peeks unless the DAO attack opened a new discussion for smart contracts security and brought a point of attention for the researchers. The purpose of this thesis was to highlight the vulnerabilities which smart contracts contain and was also to indicate the element of cyber crime and to its related forensics aspect in form of intentional frauds with buggy software development.
We have conducted a systematic analysis on existing research on blockchain and smart contracts and to support the extracted results presented by [31] we have analyzed solidity based open-source smart contracts procured randomly from well-known and authentic

sources online.

Our research shows that in contrary to hypes smart contracts have serious vulnerabilities and bugs while on the other hand our experiment indicates the existence of ethical issues from the developer side with or without intentional fraud attempts, since both comes in the domain of cyber crime and forensics.

World Economic Forum predicts that 85% of global technology will be based on blockchain by 2025[33] , therefore serious security measures, standardization, legislation and regulation are needed to be introduced to face the cyber security challenges and no doubt it is not an issue of single technology, community, authority or organization but it contains global concerns.

6.4 Future Directions

In the light of literature study and code analysis this thesis proposes several potential points which require more studies and experiments as a future work.
More attention of researcher is required in this fast growing field for a deeper scientific research and publications as the existing authentic research material is just like a tip of iceberg as compare to grey literature around.
Blockchain with programmable smart contracts like Ethereum needs more automated, stable code analysis tools with a broader range of error caption and larger test dataset to perform artificial intelligence based decision not only on variable assignment level but also with the function calls and validation.
Standards in the result of best practices will be a good addition to implement while updating the version of the platform, development language, IDE to program the smart contracts and Dapps.
Besides technology, legislation for such crimes and frauds(mentioned as the ethical issues), regulations and standardization require more attention from law and policy implementing authorities to control the ethical issues of decentralized open-source applications specially for smart contracts since these application may carry millions of SEK assets and are an attractive target for the hackers and cyber criminals.

Appendix A

An Appendix

FIGURE A.1: interface of Securify
[34]

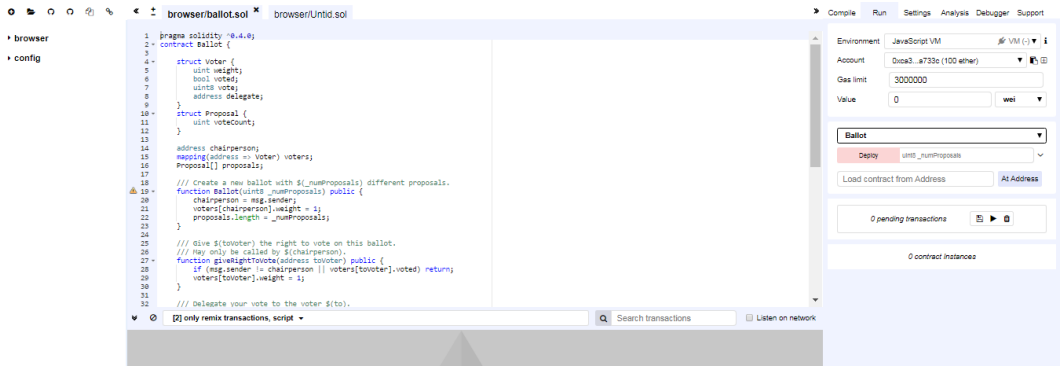

FIGURE A.2: interface of remix IDE
[35]

Bibliography

[1] EconoTime. blockchain based currency. URL http://www.econotimes.com/Tunisia-To-Replace-eDinar-With-Blockchain-Based-Currency-140836. last visited 21/02/2018 12:22.

[2] Chu D.-H. Olickel H. Saxena P.- Hobor A. Luu, L. Making smart contracts smarter. *ACM SIGSAC Conference on Computer and Communications Security*, page 254269, 2016.

[3] Ebscohost. electronic liberary. URL http://eds.a.ebscohost.com.ezproxy.bib.hh.se/eds/resultsadvanced?vid=27&sid=ef8a1190-59b5-46cc-b5aa-fa079bf5c0db\spacefactor\@m{}sessionmgr101&bquery=blockchain. last visited 13/2/2018 15:43.

[4] Datafloq. Securing internet of things in blockchain. URL https://datafloq.com/read/securing-internet-of-things-iot-with-blockchain/2228. last visited 11/2/2018 11:41.

[5] Consensys. sweden launches blockchain solution for land registry, . URL https://consensys.github.io/smart-contract-best-practices/recommendations/. last visited 18/4/2018 18:48.

[6] Researchgate. Estate transaction recording in the blockchain in brazil. URL https://www.researchgate.net/publication/322665512_Title_and_code_Real_Estate_Transaction_Recording_in_the_Blockchain_in_Brazil_RCPLAC-01-Case_Study_1_Document_Control_Version_history_Version_Date_By_Version_notes. last visited 18/4/2018 19:38.

[7] Delignat-Lavaud-A. Fournet C. Gollamudi A.-Gonthier G. Kobeissi N. Rastogi A. Sibut-Pinote T. Swamy N. Zanella-Beguelin S Bhargavan, K. Formal verification of smart contracts. *In Proceedings of the 2016 ACM Workshop on Programming Languages and Analysis for Security-PLAS16*, page 91 96, 2016.

[8] Moore T. Theres Vasek M. No free lunch, even using bitcoin: Tracking the popularity and profits of virtual currency scams. *Springer Berlin Heidelberg*, pages 44–61, 2015. URL http://dx.doi.org/10.1007/978-3-662-47854-7_4.

[9] Lee JG Lee JP Nam-Gung H Lee JK. Lim IK, Kim YH. The analysis and countermeasures on security breach of bitcoin. *Computational Science and Its Applications ICCSA*, pages 720–732, 2014. URL http://dx.doi.org/10.1007/978-3-319-09147-1_52.

[10] Anders. Hash sha256 calculator. URL https://anders.com/blockchain/hash.html. last visited 29/4/2018 16:18.

[11] Science Direct. A survey on the security of blockchain systems. URL https://www.sciencedirect.com/science/article/pii/S0167739X17318332?via%3Dihub. last visited 02/03/2018 22:14.

[12] Nakamoto S. Bitcoin: A peer-to-peer electronic cash system. URL https://bitcoin.org/bitcoin.pdf. last visited 10/2/2018 10:13.

[13] H.-N. Dai H. Wang Z. Zheng, S. Xie. Blockchain challenges and opportunities. *A survey, Internat. J. Web Grid Serv*, 2016.

[14] miles richardson bryan ford, mainak ghosh. A torpath to torcoin: Proof-of-bandwidth altcoins for compensating relays. *U.S. Naval Research Laboratory, Washington, DC rob.g.jansen@nrl.navy.mil*, 2016.

[15] Intel, proof of elapsed time (poet), 2017, . URL https://sawtooth.hyperledger.org/docs/core/releases/latest/architecture/poet.html. last visited 03/03/2018 20:08.

[16] Proof of authority chain, . URL https://github.com/paritytech/parity/wiki/Proof-of-Authority-Chains. last visited 03/03/2018 18:12.

[17] EVM. Ethereum virtual machine. URL https://coin5s.com/content/blockchain-demystified-ethereum-virtual-machine. last visited 17/4/2018 21:20.

[18] Cedrec Fournet Anitha Gollamudi Georges G-Nadim Kobeissi Natalia Kulatova Aseem Rastogi Thomas S.P Nikhil S.Santiago Zannella B K Bhagrawan, Antoine.DL. Formal verification of smart contracts. pages 91–96, 2016.

[19] Coinmarketcap. Ether prices. URL https://coinmarketcap.com/currencies/ethereum/. last visited 1/3/2018 11:53.

[20] b Josef Urbana Chad E. Browna Ond, rej Kuncar. Formal verification of smart contracts. pages 1–3, 2016.

[21] Jae Hyung Lee. Dappguard : Active monitoring and defense for solidity smart contracts. 2017.

[22] Massimo Bartoletti Nicola Atzei and Tiziana Cimoli. A survey of attacks on ethereum smart contracts. 2016.

[23] Song J. Beikverdi A. Trend of centralization in bitcoins distributed network. in: Software engineering, artificial intelligence, networking and parallel/distributed computing (snpd). *IEEE/ACIS International Conference*, page 16, 2015.

[24] ELENA KARAFILOSKI BOJANA KOTESKA and ANASTAS MISHEV. Blockchain implementation quality challenges: A literature review. 2014.

[25] Moore T. Vasek M, Thornton M. Tempirical analysis of denial-of-service attacks in the bitcoin ecosystem. *Financial Cryptography and Data Security, Springer Berlin Heidelberg*, pages 57–71, 2014. URL http://dx.doi.org/10.1007/978-3-662-44774-1_5.

[26] Wattenhofer R. Decker C. Bitcoin transaction malleability and mtgox. in: Kutyowski m, vaidya j, editors. computer securityesorics 2014. *Springer International Publishing*, pages 313–326, 2014. URL http://dx.doi.org/10.1007/978-3-319-11212-1_18.

[27] Ahmed E. Kosba, Andrew Miller, Elaine Shi, Zikai Wen, and Charalampos Papamanthou. Hawk: The blockchain model of cryptography and privacy-preserving smart contracts. *2016 IEEE Symposium on Security and Privacy (SP)*, pages 839–858, 2015.

[28] Csoonline. How smart are smart contract. URL https://www.csoonline.com/article/3236054/network-security/just-how-smart-are-smart-contracts.html. last visited 08/04/2018 09:21.

[29] A Marino, B. Juels. Setting standards for altering and undoing smart contracts. *In International Symposium on Rules and Rule Markup Languages for the Semantic Web, Springer.*, page 151166, 2016.

[30] Ari Juels Bill Marino. Setting standards for altering and undoing smart contracts. page 151166, 2016.

[31] Kolluri Aashish Sergey Ilya Saxena Prateek Hobor-Aquinas. Nikolic, Ivica. Finding the greedy, prodigal, and suicidal contracts at scale. *14 March*, pages 1–15, 2018.

[32] Consensys. Recommendations for sc security in solidity, . URL https://consensys.github.io/smart-contract-best-practices/recommendations/. last visited 18/4/2018 18:28.

[33] White paper. World economic forum. URL https://www.weforum.org/whitepapers/blockchain-beyond-the-hype. last visited 28/4/2018 12:28.

[34] Chain security. securify. URL https://securify.chainsecurity.com. last visited 21/04/2018 12:22.

[35] Remix. Remix ide documentation. URL https://remix.readthedocs.io/en/latest/. last visited 21/4/2018 15:18.

Muhammad Ahsan Rasool
Bachelor's in computer engineering
National Technical university of
Ukraine

Hafiz Muhammad Shafiq
Bachelor's in computer science,
Preston university, Pakistan

PO Box 823, SE-301 18 Halmstad
Phone: +35 46 16 71 00
E-mail: registrator@hh.se
www.hh.se