# B.Sc. Project/Thesis Proposal

Bangladesh Army International

University of Science and technology (BAIUST) Date: 23/6/2019

|  |  |  |  |
| --- | --- | --- | --- |
| **Author:** | **Lamiya Zahan**  **Nelofa Akter**  **Fahmida Haque** | **Supervisor: Mamun Ahmed** |  |
| E-mail: | Lamiyazahan052@gmail.com | E- mamun@baiust.edu.bd |  |
|  |  | Phone: |  |
|  |  | Defense Planned: |  |
|  |  |  |  |

**Proposed Topic:**

**Securing the Forensic System for medical science using Ethereum Blockchain.**

**Topic Characteristics:**

**A Blockchain** originally block chain, is a growing list of [records](https://en.wikipedia.org/wiki/Record_(computer_science)), called blocks, that are linked using [cryptography](https://en.wikipedia.org/wiki/Cryptography). Each block contains a [cryptographic hash](https://en.wikipedia.org/wiki/Cryptographic_hash_function) of the previous block, a [timestamp](https://en.wikipedia.org/wiki/Trusted_timestamping), and transaction data. Blockchain was invented by a person (or group of people) using the name [Satoshi Nakamoto](https://en.wikipedia.org/wiki/Satoshi_Nakamoto) [14] in 2008 to serve as the public transaction [ledger](https://en.wikipedia.org/wiki/Ledger) of the [cryptocurrency](https://en.wikipedia.org/wiki/Cryptocurrency) [bitcoin](https://en.wikipedia.org/wiki/Bitcoin). Blockchains could be categorized into permissionless (or public), or permissioned (sometimes called private or consortium blockchain) [12]. Bitcoin and cryptocurrencies such as Ether [13] are permissionless systems which are open to public to join the network and maintain the transactions. By design, a blockchain is resistant to modification of the data. It is "an open, distributed ledger that can record transactions between two parties efficiently and in a verifiable and permanent way". For use as a [distributed ledger](https://en.wikipedia.org/wiki/Distributed_ledger), a blockchain is typically managed by a [peer-to-peer](https://en.wikipedia.org/wiki/Peer-to-peer) network collectively adhering to a [protocol](https://en.wikipedia.org/wiki/Protocol_(communication)) for inter-node communication and validating new blocks. It secures the transactions in a way that any record of transaction that occurred in the past can not be modiﬁed as the modiﬁcation changes the hash of several blocks and all the peers connected to that system does not support that modiﬁcation excluding the modiﬁer.

**Ethereum** is an [open source](https://en.wikipedia.org/wiki/Open-source_software), [public](https://en.wikipedia.org/wiki/Types_of_blockchain), [blockchain](https://en.wikipedia.org/wiki/Blockchain_(database))-based [distributed computing](https://en.wikipedia.org/wiki/Distributed_computing) platform and [operating system](https://en.wikipedia.org/wiki/Operating_system) featuring [smart contract](https://en.wikipedia.org/wiki/Smart_contract) (scripting) functionality. Ethereum is a cryptocurrency based system that is built on the Blockchain technology where the cryptocurrency is called ’Ether’. Ethereum has got many facilities over other Blockchain based cryptocurrency systems. The mining process of almost every cryptocurrency system consumes huge energy which is not bearable at all for most of the countries in the world. This mining also takes a lot of time to verify any transaction. Moreover, most of these systems are not open-source. Ethereum removes all these deﬁciencies, is open-source where developers from all around the world can use this system in diﬀerent aspects and therefore, is preferable over all other Blockchain based systems. This Ethereum protocol can be used to secure any virtual transactions as the blocks containing the transactions records are not alterable at any means. Ethereum was split into two separate blockchains – the new separate version became Ethereum (ETH) with the theft reversed, and the original continued as [Ethereum Classic](https://en.wikipedia.org/wiki/Ethereum_Classic) (ETC).

**Digital Forensics** is defined as a legally acceptable procedure to collect, examine, analyze and finally report the digital evidence. The ubiquitously deployed IoT devices, although constantly been the target for attack, also helps to facilitate the digital forensics procedure, especially during evidence collection period by providing a rich set of personal and environmental data sources and the high connectivity. However, as IoT devices are mostly configured with limited computational power and storage, the collected evidence need to be stored elsewhere apart from IoT devices for later analysis and reporting in an integrity-protected and authenticated way.

**Existing work:**

A Blockchain-based IoT Forensics Framework with Identity Privacy[1]. In this paper, leverage on the emerging blockchain technology they propose a new IoT forensic framewrork to record all the events in the life cycle of digital evidence instead of relying on the trust assumption on the devices, to ensure its integrity and traceability.

Brieﬂy speaking, blockchain, the technology underpinning Bitcoin [14], is a trusted and distributed ledger, in which users are able to record information, prove and transfer their ownership from one to another without a trusted third party intermediary.

**Working hypotheses:**

In a medical forensic department, every piece of evidence would be properly identified, collected, preserved, analyzed and finally admitted to the proper authority. But in reality, transparency is not maintained in most of the cases and the justice is not prevailed for the sufferers. Assembling, evaluating, storing evidence is not secured enough. There are also some issues involved in forensic analysis:

1. Forensic science lacks specific and true analysis. Any act of fraud in the case of analysis lead to a disastrous situation where the victim gets deprived from justice. Forensic analysis can be deterred via powerful influences (political or financial factors).
2. The evidence cannot be accessible at all times.
3. Maintaining privacy and secrecy of the information gathered across forensic analysis is relatively difficult

Blockchain based Digital Forensics refers to the process of collecting, analyzing, storing and presenting digital evidence within devices in a legally binding manner. The goals of the proposed thesis are as follows :

1. Creating a Blockchain based Medical Forensic System. There will be no involvement of third parties. Instead, the overall medical forensic system will be handled by ‘Smart Contract’, a protocol which will consist all the terms and regulations of the medical forensic system.
2. In Blockchain based Digital Forensics system , maintaining privacy and secrecy of the information gathered across forensic analysis is relatively easy.
3. Only authorized persons or department can access to the evidence at all times.
4. No intruder can decrypt and modify the forensic data because all the data are encrypted using powerful and much secure SHA-256 algorithm and even if that person decrypts the data and try to modify them, it will never be possible as Consensus Algorithm does not allow to do so.

**Methodology:**

Throughout the development of the proposed DAPP, the following steps will be used:

1. Creating a Javascript Project Directory as the code for testing, compiling and deploying to the test network will be written in Javascript.

2. Creating a Local Test Network as the proposed Decentralized Application will be deployed and tested there.

3. Getting Ethers from a website which provides these crypto-currency free of cost.

4. Writing Smart Contracts for the proposed systems.

5. Creating test modules to test whether these smart contracts are functioning properly

6. Creating a deployment module to deploy these smart contracts in the Blockchain.

7. Creating a compile module to compile each of the smart contracts available in the project directory.

**Possible Outcome:**

1.Data will be secured because data cann’t be decrypted from blockchain by third parties.

2.Minimizing middle man.

3. Maintaining privacy and secrecy of the information will be relatively easy.

4.When the evidence is stored once, these can’t be modified.

**Outline:**

**Doctor**

**Blockchain Platform**

**Evidence Analysis**

**Victim**

examine

Collecting sample

Trigger the evidence analysis

Submit evidence

If evidence is sufficient

Analysis result

acknowledgement

Acknowledgement & ask for additional evidence

if evidence is insufficient

& victim has additional

evidence

Submit additional evidence

Trigger the evidence analysis

Analysis result

**Figure: Sequence diagram for evidence collection**

**References / Bibliography:**

# [1] BIFF: A Blockchain-based IoT Forensics Framework with Identity Privacy, Duc-Phong Le, Huasong Meng, Le Su, Sze Ling Yeo, Vrizlynn Thing, Cyber Security & Intelligence, Institute for Infocomm Research (I2R), A\*STAR, {ledp, menghs, lsu, slyeo, vriz}@i2r.a-star.edu.sg

**[2]** A Certified Digital Signature Conference Paper · August 1989 DOI: 10.1007/0-387-34805-0\_21 · Source: DBLP

**[3]** ETHEREUM: A SECURE DECENTRALISED GENERALISED TRANSACTION LEDGER EIP-150 REVISION (1e18248 - 2017-04-12) DR. GAVIN WOOD FOUNDER, ETHEREUM & ETHCORE GAVIN@ETHCORE.IO

**[4]** Digital Forensic Research: Current State-of-the-Art Sriram Raghavan Queensland University of Technology Brisbane, Queensland 4000, AUSTRALIA [s.raghavan@qut.edu.au](mailto:s.raghavan@qut.edu.au)

**[5]** Digital Forensics Research: The Next 10 Years By Simson Garfinkel From the proceedings of The Digital Forensic Research Conference DFRWS 2010 USA Portland, OR (Aug 2nd - 4th)

**[6]** Blockchain technology, bitcoin, and Ethereum: A brief overview Conference Paper · March 2018 DOI: 10.1109/INFOTEH.2018.83455.

**[7]** Blockchain Solutions for Forensic Evidence Preservation in IoT Environments Preprint · March 2019

**[8]** FIF-IoT: A Forensic Investigation Framework for IoT Using a Public Digital Ledger Mahmud Hossain, Yasser Karim, and Ragib Hasan {mahmud, yasser, ragib}@uab.edu Dept. of Computer Science, University of Alabama at Birmingham, USA

**[9]**Data Protection with Ethereum Blockchain Duarte Teles Dissertation to obtain the Master’s Degree in Informatics Engineering, specialization in Computer Systems

**[10]** An Overview of Ethereum & Its Comparison with Bitcoin Article · February 2018

**[11]** FORENSIC-CHAIN: ETHEREUM BLOCKCHAIN BASED DIGITAL FORENSICS CHAIN OF CUSTODY Auqib Hamid Lone, Roohie Naaz Mir Department of Computer Science and Engineering NIT Srinagar, Jammu and Kashmir 190006

**[12]** V. Grewal-Carr and S. Marshall, “Blockchain: Enigma. Paradox. . Opportunity,” Deloitte, UK, Tech. Rep., 2016.

**[13]** G. Wood, “Ethereum: A Secure Decentralised Generalised Transaction Ledger,” Ethereum & ETHCore, Tech. Rep., 2016.

**[14]** S. Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System,” Tech. Rep., 2008.