Scientific and Practical Cyber Security Journal (SPCSJ) 1(2):21-27
Scientific Cyber Security Association (SCSA), 2017 ISSN: 2587-4667

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

ABSTRACT

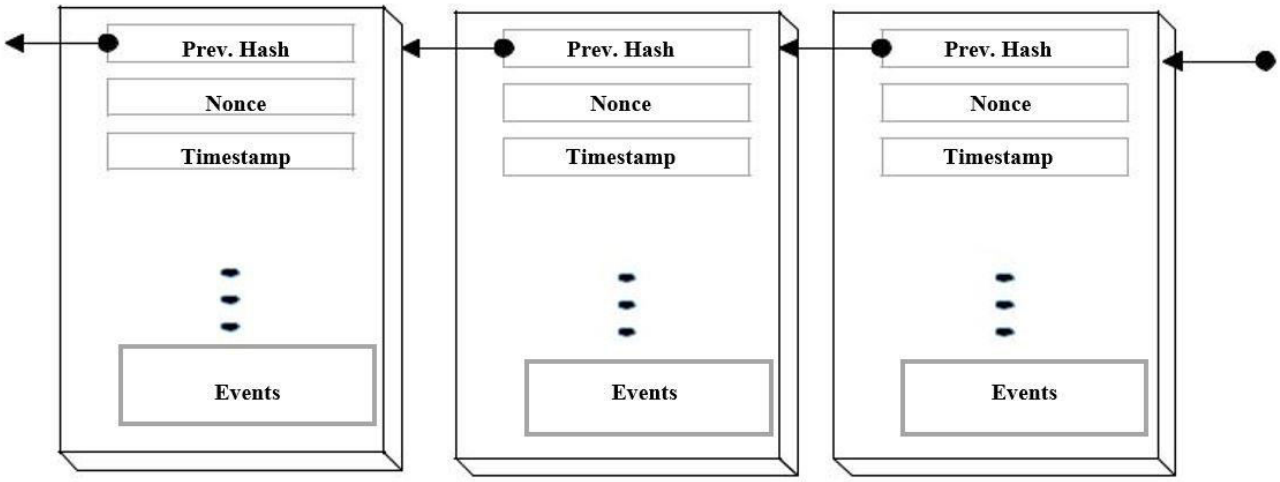
Digital evidence plays an important role in cyber crime investigation, as it is used to link persons with criminal activities. Thus it is of extreme importance to guarantee integrity, authenticity, and auditability of digital evidence as it moves along different levels of hierarchy in chain of custody during cyber crime investigation. Blockchain technology's capability of enabling comprehensive view of transactions (events/actions) back to origination provides enormous promise for the forensic community. In this research we proposed to use a blockchain that can be leveraged for forensic applications in particular bringing integrity and tamper resistance to digital forensics chain of custody.

KEYWORDS: Blockchain, Ethereum, Chain of Custody, Smart Contracts.

INTRODUCTION

In today's digital world, with rapid increase in cyber crimes, the importance of digital evidence is also growing for provenance of persons linkage with cyber crimes. Digital evidence comes with its own unique challenges related to chain of custody. Chain of custody can be defined as a process used to maintain and document the chronological history of han-dling digital evidence [1]. In digital forensics evidence passes through different levels of hierarchy i.e from first responder to higher authorities responsible for handling cyber crime investigation. During this passage of digital evidence there is always higher degree of integrity violation and repudiation. As a matter of fact, the need of the hour is to have a system that guarantees transparency, authenticity, security and auditability. Blockchain in its simplicity is a series of connected data structure called blocks, which contains or tracks everything that happens on some distributed systems on a peer to peer to network [2]. Each block is linked to and depends on previous block forming a chain, resulting in an append only system: a permanent and irreversible history that can be used as a real time audit trail by any participant to verify the accuracy of the records by simply reviewing data itself. Ethereum is a

blockchain with built-in Turing-complete programmming language, giving users power to write smart contracts, de-centralized applications where users define their own arbitary rules for



ownership, transaction formats and state transition functions [3]. Blockchain by design guarantees transparency, authenticity, security and auditability and thus making it best fit for maintaining and tracing chain of custody for forensic applications. The motivation behind using ethereum blockchain smart contracts is that they provide more power in terms of Turing-completeness, value-awareness, blockchain-awareness.

Fig. 1. Blockchain and state.

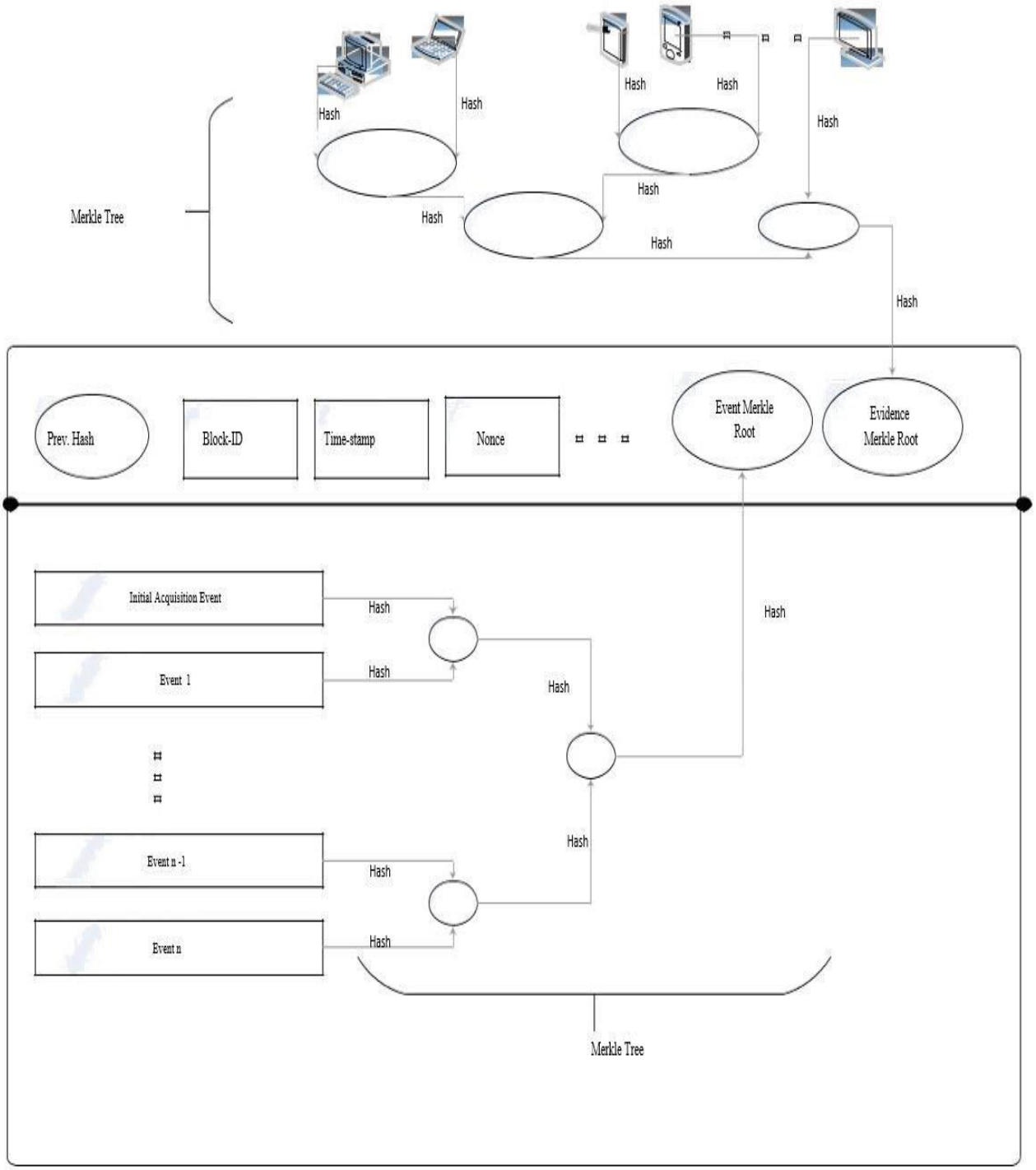
PROPOSED FORENSIC-CHAIN MODEL

Forensic-Chain is a blockchain based solution for maintain-ing and tracing digital forensics chain of custody. Blockchain is a data structure that allows to create a digital ledger for recording and storing transactions (events/records) shared by all participating parties over a distributed network of computers. Blockchain makes use of cryptography for protecting the process of recording and storing transactions (events/records) that happen within the network, creating unimpeachable audit trail.

In relation to chain of custody, the blockchain's capability specifically in combination with cryptographic hashing and encryption could potentially create documentation pertaining to access to evidence that is tamper- proof [4], [5] . The evidence that is to be preserved is first encrypted securely and have a blockchain capability added on.The encrypted data would be accessible only to desired party on the blockchain but would simultaneously record the time,date and possibly user-ID of the accessing party and add it to the unalterable record in blockchain all done automatically through smart contract The blockchain itself can be read via a special function in a way that is similar to how the bitcoin blockchain can be decoded. This functionality of blockchain allows courts

and associated personnel the ability to examine historical chain of custody without accessing data itself.

Actual implementation is as follows: The blockchain's first entry i.e genesis block com-prises of



initial hash of the data such as time,date and location of initial acquisition as shown in figure 2.

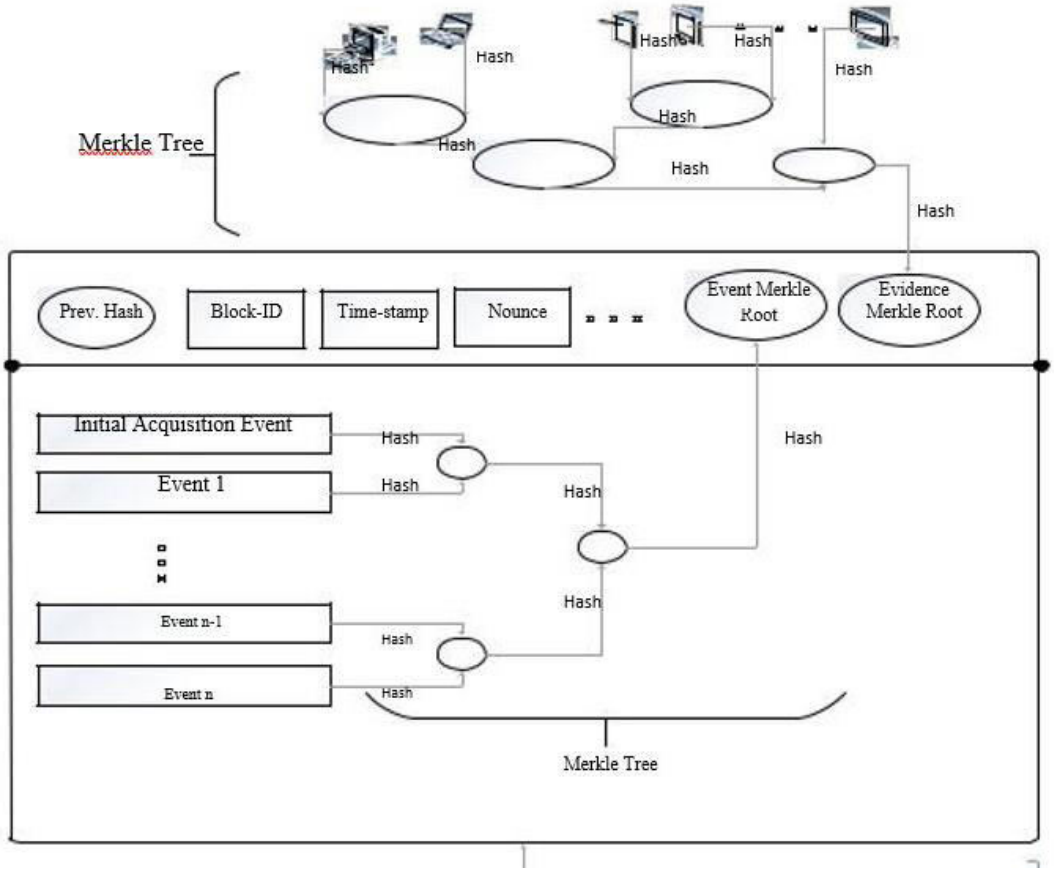
Fig. 2. Genesis Block of Forensic Chain Model

1. Subsequent accesses made possible only via a special program (like the one used to read a bitcoin blockchain), will add additaional blockchain entries each time access or transfer of evidence occurs. In simpler terms during subsequent accesses of evidence a new, non-repudiable, irreversible, cryptographically secure block gets added to blockchain based chain of custody every time a bit of critical information is touched as shown in figure 3.

2. Automated access tracking through smart contract will help in detection when copies of evidence are being made and record them in the blockchain, but authorized copies or other types of housekeeping or record keeping activities would be specially entered into the chain of custody of blockchain.

A. Forensic-Chain in Action

Forensic-Chain is initiated or triggered by First Responder,taking hash of digital evidence and recording them securely on blockchain through smart contract. Other details like location, time, and date etc. of crime scene also gets recorded on blockchain. During the course of digital forensics investi-gation any evidence transfer gets automatically recorded on the blockchain through smart contract, recording details like address to whom evidence is transferred to, current state of evidence, permission level, date and time etc. Further any subsequent access to digital evidence also gets recorded securely on the blockchain by smart contracts triggered by corresponding rensic



investigator. Consequently, a chain of trust gets established by recording every action about digital

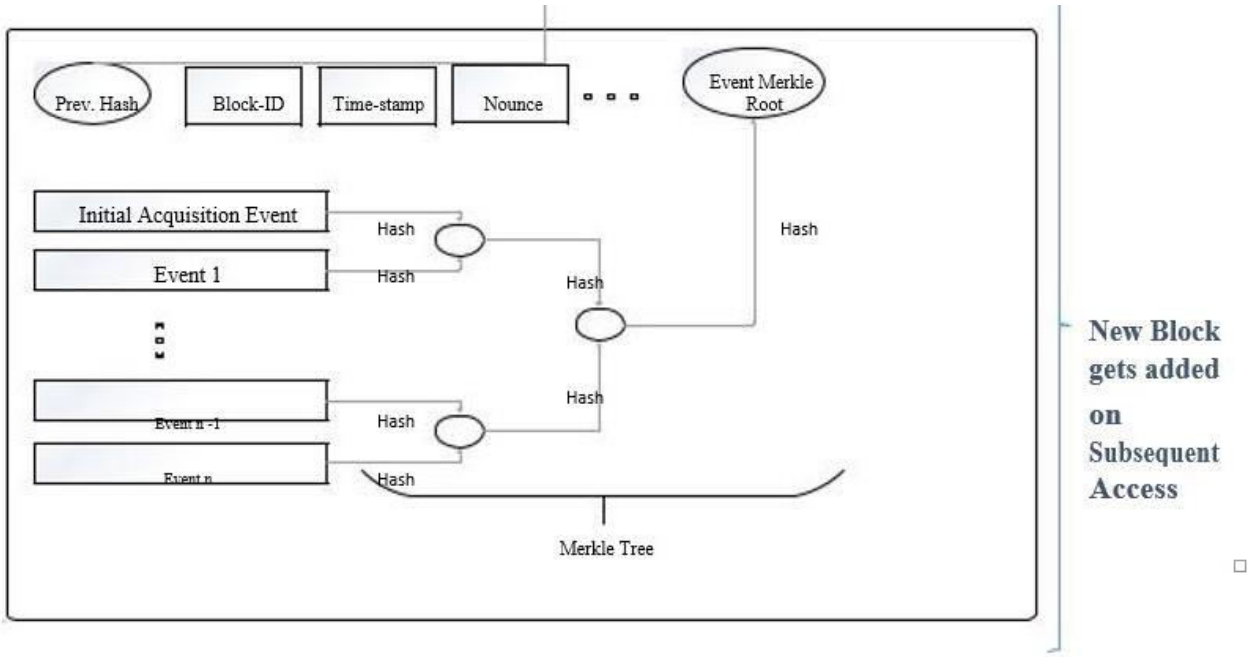


Fig. 3. Forensic-Chain on Subsequent Accesses

evidence, since it originally entered the process in question as shown in figure 4.

B. Benefits of Proposed Model

Forensic-Chain: Blockchain based digital forensics chain of custody has great potential to bring substantial benefits to forensic applications, by maintaining integrity, transparency

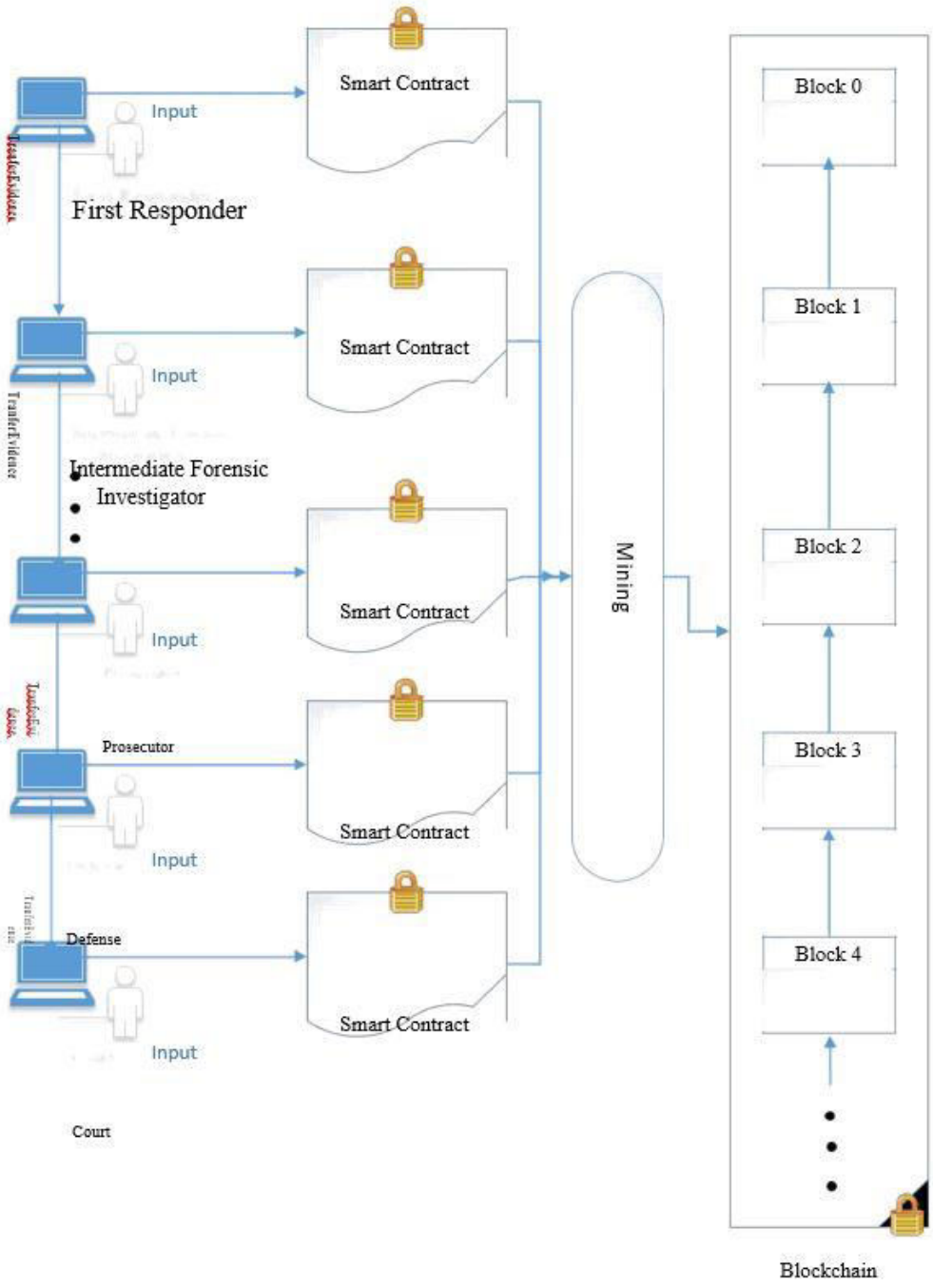


Fig. 4. Forensic-Chain in Action

authenticity, security and auditability of digital evidence to achieve the desired end. Some of the benefits are summarized below:

- Collecting, preserving and validating evidence can be strengthened with the help of Forensic-Chain.
- The provenance of any event or action can be traced back to where it originally entered the process in question.
- Forensic-Chain also helps in improving transactional efficiency and cost reduction of certain kind of transac-tions due to increased transparency resulting eliminat-ing the requirement of trusted third party for validation of certain claims or evidence transfer and consensus based Proof of Trust, resulting increased trust among communicating parties.
- Reduction of fraud due to increased transparency of the audit trail.
- Forensic-Chain allows organizations to embed veri-fication for the event or action within the evidence
- Record itself, thereby enabling an established and ongoing evidence which is both accessible verifiable.

CONCLUSION

Blockchain by design enforces integrity, transparency, au-thenticity, security and auditability thus making it possibly the best choice for maintaining and tracing forensic chain of custody. Blockchain helps in friction reduction through increased trust and thus brings the real promise for foren-sic community. The future work aims at developing complete Ethereum based smart digital forensic chain of custody using smart contracts.

REFERENCES

1. G. Giova, “Improving chain of custody in forensic investigation of electronic digital systems,” International Journal of Computer Science and Network Security, vol. 11, no. 1, pp. 1–9, 2011.

2. S. Nakamoto, “Bitcoin: A peer-to-peer electronic cash system,” 2008.

3. V. Buterin et al., “Ethereum white paper,” 2013.

4. C. Liu, “How the blockchain could transform the process of documenting electronic chain of custody.” [Online]. Available: https://venturaerm.com/Blog/9.html

5. K. Zatyko, “Improving cyber forensics cybersecurity through block chain technology with truth based systems,” International Symposium on Forensic Science Error Management, July-23-2015