ASTES

Advances in Science, Technology and Engineering Systems Journal
Vol. 6, No. 1, 66-77 (2021)
www.astesj.com

ASTES Journal
ISSN: 2415-6698

Modified Blockchain based Hardware Paradigm for Data Provenance in Academia

Devika K N*, Ramesh Bhakthavatchalu

Amrita School of Engineering, Department of Electronics and Communication, Amrita Vishwa Vidhyapeetham, Kollam, Kerala, 392025, India

ARTICLE INFO

Article history:
Received: 08 October, 2020
Accepted: 26 December, 2020
Online: 10 January, 2021

Keywords:
Blockchain
Data security
Cryptography
Immutability
Academic transcripts
FPGA
Xilinx

ABSTRACT

Educational organizations often need to distribute academic transcripts and certificates upon student's request since they are mandatory for admission into new scholarly programs including placement activities. Manual procedures involved with the transmission process of academic document is indeed a tedious task that results in substantial overhead. Thus the necessity for an autonomous electronic system for transfer of records among institutions is on the verge. This paper discuss and portray a hardware approach on the cryptographic elements of blockchain to impart data security and privacy that are found inadequate in its software counterpart.The novelty of this work relies on the design and implementation of a hardware equivalent structure for blockchain which could greatly alleviate the chances of various software attacks and security breach in existence. The solution proposed could cut down the waiting period of students to transmit their credentials and in addition provide a trustworthy verification platform to elude academic deceit. It can be integrated along with existing permission based blockchain framework to form a conjoined hardware-software architecture.

1 Introduction

Internet acquired it's admiration since 1990's, after which hard copy references and encyclopedias became ineffectual. During the initial times, internet was troublesome for the educators to adapt it into the academic domain. However, the field of education have progressed enormously over a short period of time. Online network had a great impact in the process of imparting knowledge and brought about a substantial revolution in the way people learn. Online learning platforms hold considerable amount of private documents and data related to students. These should be kept inaccessible to the third party user but at the same time should convey information to the concerned authorities to maintain data confidentiality. Currently India does not possess any law controlling data privacy or protection. Nevertheless, significant laws in India that serve data privacy are the Contract Act (India) 1872 and Information Technology Act, 2000. Presently, Blockchain comes out as the best solution to this scenario by forming an impregnable data repository and security from hacking. Cryptocurrency that turned out as the foremost noteworthy and the most inquiring wonders of the final century have Blockchain at its back end. Blockchain forms an ideal technology for storing and tracking scholarly documents. At present, all student credentials are stored as paper records or in a digital centralized directory which makes it accessible to third party.

Drawbacks of paper records include:

- Requires huge amount of storage space.
- Can easily be manipulated or misplaced by unauthorized individuals.
- Can be subjected to unexpected permanent destruction due to natural calamities like flood.
- Creation of paper records is itself a tedious task in terms of time span involved.
- There can be trust issues in relation to the accuracy and authenticity of data.

Centralized repositories that are considered as a reservoir of private data could be targeted by hackers leading to security breach.

*Corresponding Author: Devika K N, Research Scholar, Department of Electronics and Communication, Amrita Vishwa Vidhyapeetham, Kerala, India, Tel: +919744968667, Email: devikanandalal@gmail.com

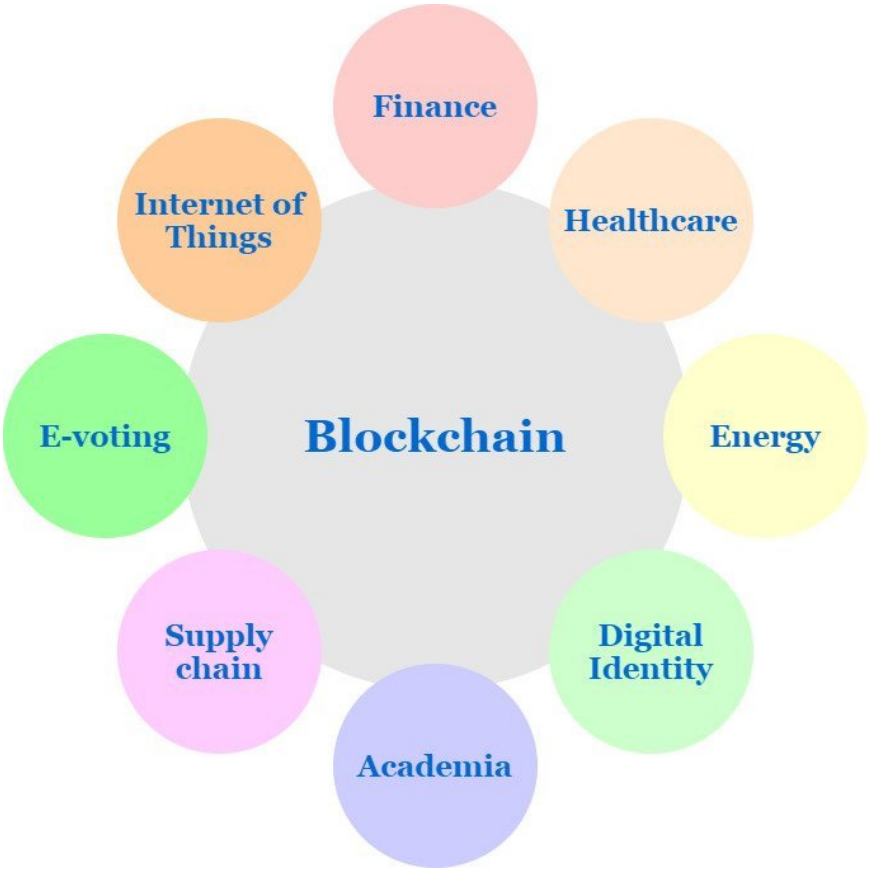

Figure 1: Applications of Blockchain technology

In a Blockchain, each participating entities called nodes are provided with a replica of the entire data communicated within the network. Thus it impedes the attempt to manipulate the contents imparting immutability. Data loss is prevented by avoiding centralization of information. In addition, it also provides the freedom to view information in public by any individual in case of Public Blockchain or only by the concerned participants for Private Blockchain. It prevents fraudulent individuals among teaching professionals who may provide fabricated certificates to highlight their experiences in academic field. Such untrustworthy officials questions the credibility of scholastic documents. Immutable property of the decentralized ledgers are utilized to guarantee the trustworthiness of the members involved through the submission of necessary credentials required.For placement purposes, it gives the freedom for the employers to directly access the records of students without involving colleges or universities. Presently, many universities around the globe have stepped into blockchain technology for tracing and screening academic transcripts.

Edublock is an innovative idea put forth by company called "Learning is earning" to collect the proof that a person have completed the required classes on his/her subject of study. This venture thus opens a wide range of opportunity to reform the sphere of education. All entities involved in the educational sector like students, professors, parents and other officials can be completely assured of the security provided by this emerging technology.

This paper provides a novel dimension to the world of blockchain by exploring the possibilities to design a dedicated hardware blockchain structure to securely store the academic information of students in Schools or Universities.

The remaining of the paper is organized as follows: Section II deliberate about the background research done on the innovative technology. Section III analyzes the benefits of Hardware cryptography over software cryptography. In Section IV, the technology behind blockchain is highlighted. Section V explains the proposed hardware approach to blockchain architecture. Section VI displays the results after synthesis and simulation in Hardware programming language. Section VII concludes the paper along with its future scope.

2 Background Research

Experts believe that blockchain application is never limited to bitcoin but uncover solutions in divergent fields as in voting, medicare, supply chain, energy industry, identity management and so on [1]. Figure 1 portrays different sectors in which blockchain is gaining significance. The paper work [2] does a survey on the application of blockchain technology in various industrial sectors. It in turn analyze the scope, advantages and threats of integrating this technical knowledge in industry.

In healthcare [3],[4], blockchain finds use in managing patient's information and in tracking medicines. It can resolve drug forgery to a great extent as all the data communication within the decentralized ledger are transparent and immutable that leads to tamper resistant

data. Participants involved comprises of medical experts, patients, insurance agencies, researchers etc. It enables interoperability of timely renewed medical profile of patients and in addition provides data protection, identity maintenance and transparency. Blockchain provides a framework for integrating medical transcripts of all patients among multiple healthcare expertise. It also enables patients to share their health details to medical experts through this platform [5]. Another work [6] discusses the usability of blockchain in healthcare domain to implement Adoptive Leader Election Algorithm (ALEA) for maintaining parallelism in accessing files.

Through distributed ledgers, blockchain certifies and reserves each execution in logistics industry that permits reduction in human flaws, time lag and management costs. In energy industry, blockchain uncover its utility in micro grid technology for power trading [7]. Thus it eliminates the necessity of a centralized controller for decision making and payment management [8], [9]. Blockchain can be applied to promote e-agriculture systems among farmers to improve farming process and provide improved productivity, food safety and reduced risks [10]. In food industry, it enhances food quality and trust by preventing food adulteration and reducing wastage of food [11]. This peer to peer technology put forward novel ideas for gamers through better containment on top of virtual assets in online entertainment platforms [12]. Aura network is an online gaming dais that utilizes it to sustain decentralization in games [13] and to assist the virtual world. It enables online streaming music platforms such as "spotify" to have direct transactions with the customers [14].

Stock market shareholders are currently experiencing tiresome proceedings due to the involvement of mediators and regulatory process which thereby delays the time taken for confirming transactions. In finance, blockchain permits decentralized stock exchanges and financial settlements completely, thus relieving the requirement of a negotiator and gearing up clearances [15], [16]. In e-voting , the voters are able to view the total votes taken for count through the transparent ledger mechanism assuring trustworthy and secular voting system [17]. Decentralization process in blockchain facilitates a person to create digital ID for identity verification on every online proceedings without relying on biometric systems or password [18]. This emerging science aids the dealers and consumers to differentiate between fabricated and original goods, thus impart trust into sale of goods.

In [19], the author presented a novel approach of creating Digital Twins (DT) using blockchain for ensuring immutable, reliable transactions and data availability. Smart contracts are utilized to manage and trace all proceedings involved in Digital Twin creation. They are virtual 3D representation of any real world object. Main objective of DT is to enhance manufacturing process and industrial operations of a system before its actual formation. In [20], the author investigates the pros and cons of applying blockchain to enlarge Industry 4.0. Industry 4.0 model propose the usage of significant technologies such as Augmented Reality (AR), Industrial Internet of Things (IIoT) that helps in free communication among numerous devices all over the industry and online network. Intensive research is done related to this ingenious automation for its utilization in Industry 4.0. Since the latter comprises of different entities such as customers, suppliers, manufacturers, operators and other IIoT nodes there arise trust issues with regard to each other.

Blockchain provides an interactive trusted platform for various smart technical clients [21]–[23] does a relative analysis regarding blockchain trade-offs, classification, details its architecture and also explore the challenges and future scope of this technology. [24] suggests authentication scheme based on blockchain that support user obscurity, inter mutual authenticity and security for multiple server platforms. Unlike other analogous strategies, this proposal offer centralized registration and introduce user revocation as added feature.

In addition to the above mentioned areas, there are numerous other fields where blockchain turn out to be beneficial for instance research sector that include both academia and industry. In [25], the author explains a solution that includes web interface to register and transfer record with permissioned blockchain framework functioning as the back end for verification purpose. Main aim of Academic Transcripts is to display a formal report of students performance [26]. It may take several days to certain months for the transfer of academic documents with the widely accepted paper approach due to processing and transmission time involved. Along with considerable time taken and chances for spoilage, there prevails the threat for fraudulent documents by deceitful intermediaries. Processing of paper transcripts amounts to huge expense related to the manual effort, proceeding time, delivery and conveyance fees. There exists 3rd party services for online document verification thereby avoiding manual procedures. Blockchain contribute in maintaining distributed and permanent list of records by educational institutions to assure authenticity of transcripts. Another effective method in [27] is despite recording the entire transactions, hash of the document that contain the hash list of all scholarly certificates is recorded in the ledger to be checked out by the receiver. Smart contracts are used in [28] along with Ethereum blockchain for managing identity and certificates.

When the current researchers focused more on the application of blockchain in miscellaneous sectors, hardly any analysis has been accomplished with regard to the implementation of blockchain technology. The proposed hardware prototype detailed in this work introduces a new outlook to the realization of blockchain architecture. Higher levels of security is offered by hardware cryptographic elements over software components since the latter are more susceptible to security attacks.

3 Hardware cryptography v/s Software cryptography

With the surge in the use of smart gadgets and as the attacks against confidential data in business and government sectors are enlarging, data security is gaining predominance among IT users and programmers. Recent progress in technology set forth many solutions for the above problem and it is up to the user to choose whether the solution should be hardware based or software based.

3.1 Software encryption

Currently software encryptions are more popular than hardware based solutions since they are easy to handle, upgrade and renew. Software programs are portable and accessible for every operating systems and devices. However, these encryptions provide protection

as long as the operating system on which it runs have high grade of security. If OS have any security blemish, the whole encryption would be compromised [29]. When a software program is executed in parallel with other operations in the environment, confidential information could be leaked through side channel attacks. Thus open platforms can recover the data on secret keys. Hackers can easily compromise software encoding by duplication of encrypted records and through frequent attempts of parallel breaking in different systems. Since software need frequent up-gradation they are more vulnerable to security attacks. There are many recovery options available to access data in spite of its failure.

In software cryptography, threats posed by side-channel attacks goes unnoticed. Side channels is a perceivable change as a result of ciphering which an attacker can sense and utilize to his favour. Predominance of side channels and its sensibility factor have increased the risk of hacking due to new features like advanced processors introduced in the host computers. In [30], the author discussed how data could be retrieved based on recent attacks that exploits timing of CPU cache, branch algorithm logic and correlation function.

3.1.1 Software security threats

Inefficiency of software to provide the required security is dependent on the following factors:

1. Limitation in security posed by OS
   Software security module are not standalone units. Therefore they rely on operating system of host computer for its functioning. Despite the complete security of the program, if OS is subjected to some defects such as memory leakage or trojan insertion then the whole system gets compromised. Safety of cryptographic software is directly related to OS security.

2. Random Access of Memory
   Another drawback of software implementation is the lack of dedicated memory. They entrust memory of host system to store private information. Sharing of system's memory with other operations concurrently will provide access to the contents inside memory for other applications thus confidentiality and privacy is threatened.

3. Code Integrity Issue
   Software codes stored in memory can easily be modified by a hacker through random access of cache. This could lead to impairment or data leakage. No system can detect software tampering thereby leaving integrity of codes at stake. No machines has been designed till date to identify or prevent manipulation of codes inside software. This increases the security concerns of software encryptions to a great extend.

4. Susceptibility to Reverse Engineering
   In Software domain it is much easier for an intruder to identify the functionality of a module by means of examining the instructions given in the code. This could jeopardize the design architecture before an attacker backing reverse engineering.

3.2 Hardware encryption

Most viable solution to protect drives that contains huge amounts of information in the fields of education, healthcare and finance are through hardware based encryptions. The contents within such devices will be protected even if these drives is taken and used in other systems owing to the effectiveness of hardware encryption keys. No encryption/decryption keys are stored inside systems memory and therefore less vulnerable to key attacks.

The recent surge in demand for power reduction in devices have motivated researchers to think about application specific hardware structures over generic processors. Computationally expensive and power hungry algorithms can be implemented using hardware methodology so as to match up with the present operational speed requisites. Application Specific Integrated Circuits (ASIC) showcase better efficiency in terms of speed, size and power but demands a huge non-recurring costs for prototyping. In these circumstances Field Programmable Gate Devices (FPGA) have superiority wherein they incorporate both hardware and programming on a single platform with low cost of application and reconfigurability in design. FPGA prototypes are designed using hardware description languages such as verilog or VHDL (Very Large Scale Integration Hardware Description Language) [31].

In hardware encryption, a customized processor handles the entire process of encryption, decryption and access to protect data [32]–[34]. Additional components are not required for encryption process as the device comprises of the required utilities. When a password is provided, processor employs random number generator to create encryption keys. It doesn't require additional software setup. Since the encryption solely runs on the dedicated hardware there is no forms of communication with the OS of the system. So the performance remains unaffected and is found to be much superior than software based solutions. Thus the hardware is basically protected from corruption, malicious software attacks and reverse engineering.

4 Blockchain Technology

Blockchain is an enlarging series of connected records called blocks secured through cryptographic algorithms. As per Gartner's prediction in 2017, market value of blockchain will emerge to about $176 billion by 2025 and can reach up to $3.1 trillion next to 2030. This emerging science can benefit different sectors and thus make possible a remarkable revolution form "Internet of Data" to "Internet of Value" and create a decentralized economic platform. Key features of this technology comprises of Decentralization, Data Authenticity, Transparency and Immutability [35].

The term "transactions" in this context refers to data framework that enables exchange of data or information of value among clients. Many such transactions are added up to form one block. Each block is linked with the other over one-way secure algorithms called hash functions [36]. Cryptographic hash forms the linking thread between current block and its predecessor.

It enables a group of members within a network to share and store information related to transactions or events. Transactional records can be examined by the participants but none can alter or manipulate any of the validated data proceedings. This impart

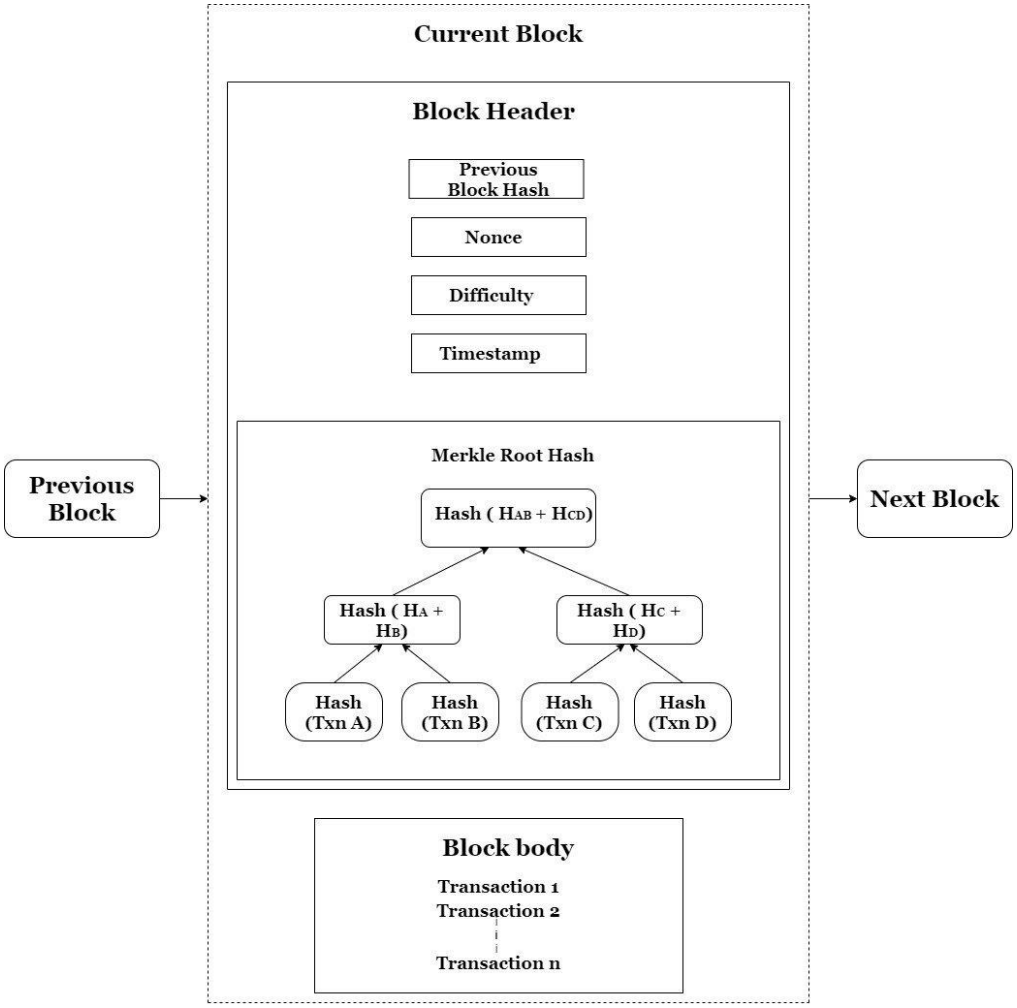

Figure 2: Typical Blockchain Architecture

blockchain with immutability in regard to all events undergone in the network. Thus the shareholders even if not known to each other can trust themselves, arrive at an agreement, record them and form connected transactions in the form of chain. This technology can grant digital identities similar to passports or license for performing financial and other confidential tasks. Every transactions are approved by all individuals in the network before its linkage to the chain based on predefined criteria, thereby avoiding any possibility of repudiation. Figure 2 represents the typical Blockchain architecture.

4.1 Fundamentals of Blockchain

1. Block
   Block forms the principle constituent of the blockchain. Structure of a block consist of following elements:

   - Block Header
     It comprises of metadata related to block that includes hash of the previous block, difficulty, merkle root hash, nonce and timestamp. Merkle hash constitute the hash value of all transactions recorded in that particular block.
   - Block body
     It consist of all the transactions included in the block.

2. Hash functions
   Hashing is the technique to transform random sized input data to output of fixed size. Message Digest 5 (MD5) is extensively used for generating hash values of 128 bit length [37].

Table 1: Performance comparison of different hash algorithms

Hash function	Speed of operation	Security level	Hash size
SHA-1	Medium	High	160
SHA-3	Slower than SHA-1	High	256
SHA-256	Slower than SHA-1	Highest	256
MD5	Fastest	Lowest	128
SHA-512	Slower than SHA-256	Highest	512

The limitations of MD5 algorithm to create unique hash functions lead to the development of Secure Hash Algorithms(SHA).

At present various set of algorithms have been designed which includes SHA-1, SHA-2, SHA-3 and latest being SHA-256 and SHA-512. The execution time required by the above mentioned algorithms are furnished in [38] which gives an insight into the frequency of operation needed by each of the hashing methods. Most popular hash functions in usage is SHA-256 on account of its trade-off with respect to level of security and the bit length as shown in Table 1.

SHA-256 are one way hash functions that produce untampered 256 bit hash value [39], [40]. The string created after encrypting the block of information is irreversible. They are highly collision resistant since even a one-bit change in input reflects significant change in the output bits. Currently bitcoin utilizes SHA-256 for hashing blocks of data.

3. Consensus Algorithms
Consensus procedure in blockchain assures data consistency and enable all peers to reach on to common agreement in block creation[41]–[45]. In such a way reliability is attained and also empower trust among participants in a decentralized network. There exists different categories of consensus mechanisms as mentioned below:

   - Proof of Work
   In Proof of Work(PoW) consensus process, a complex numerical puzzle needs to be solved by the participating node to mine the adjoining block. A good deal of computational power need to be spend by the mining node to find the solution to the puzzle. PoW is adopted by bitcoin for block formation.
   - Proof of Stake
   In comparison to PoW, the holder with maximum share is given top priority for block creation in Proof of Stake (PoS). As the blocks get added the concerned shareholders get more assets as reward. This incentive provided encourages participation in PoS. Ethereum is found to utilize PoS to achieve consensus.
   - Proof of Burn
   In Proof of Burn coins are burned by sending them to a random address, which will be nominated by the network. Through this burning process, the clients gain the authority to mine the blocks based on arbitrary selection procedure. More the coins are burned, greater is the probability to select the concerned node as miner. But as in PoW, the resources are wasted unnecessarily.
   - Practical Byzantine Fault Tolerance
   The ability to arrive at an agreement between two communicating nodes in a decentralized network in the existence of malicious nodes is referred to as Byzantine Fault Tolerance. In Practical Byzantine Fault Tolerance (PBFT), the primary node is selected in a round robin fashion. This nodes creates the block upon receiving the request and broadcast it to all other nodes present in the network. Primary node reach to a decision based on majority voting so that data authenticity and integrity is assured. Each request is processed on getting support from two-third of the votes from the network. Thus this consensus process function efficiently on the criteria that only one-third of the nodes are malicious in nature.New improved version of PBFT called Tendermint blockchain algorithm is proposed in [46].
   Apart from the above discussed algorithms there are many other proofs such as Proof of Capacity, Proof of Space, Proof of Elapsed Time and so on. These consensus algorithms give an insight about their mode of execution and they are often used by experts in bitcoin. Blockchain application still may vary based on its utilization in other fields and the agreement process discussed in this section need to be modified related to the type of application.

4.2 Features of Blockchain

The Blockchain framework provide the following attributes that prove it to be a successfull platform for online data transfer [47], [48].

1. Data Integrity
   The decentralized connected network of blockchain guides students and teachers to apply, transfer and authenticate records. Entire process is automated, user friendly and openly accessible.

2. Data security
   Transparent ledger mechanism render safe and secure methods to transit, store and validate transcripts. Data is disclosed only to the destined receiver.

3. Flexibility
   Blockchain network is able to hold increasing number of colleges, institutions, students and documents. They are able to manage conversions and enhancements to record at the same time and thus maintains reliability.

4. Immutability
   The information once uploaded in the database can never be modified or updated. As a owner and also as a recipient of data, the participants can be confident on the provenance of the information.

5 Proposed Model for Hardware Blockchain

This research work discuss the hardware approach to blockchain architecture in order to safeguard and authenticate academic information in educational institutions. But the current blockchain structure has to be modified due to following limitations:

1. This work considers all subject marks attained by students on semester basis as the Academic record.The marks scored could be stored only after generating the block. So block needs to be created before storing the transactions.

2. Ownership of a particular block belongs to a single authority. Further, it is imperative to create block without introducing

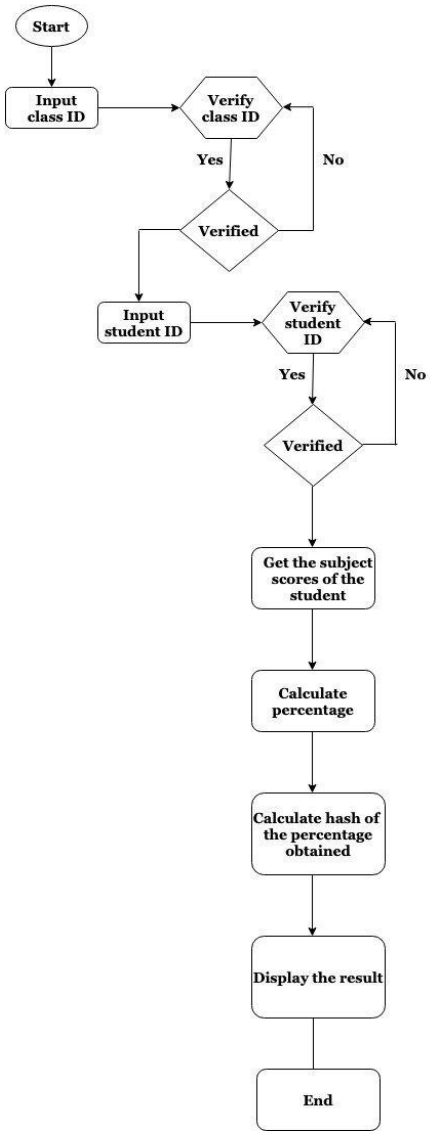

Figure 3: Flowchart of different operations performed within a single block

any computational complexity. Therefore consensus algorithms such as Proof of Work, Proof of Stake, or Proof of Burn are not significant in this context.

3. The proposed framework does data transmission only when the concerned students or teachers need to view and display their academic progress. Hence unlike the proofs detailed in the previous section that recursively repeat their execution, this system utilizes minimum resources saving energy, time and cost.

4. The suggested prototype assumes classroom as the block and the percentage of marks attained by each student that belongs to that class will act as a new ”transaction”. Typical consensus process are efficient for long transactions thereupon not acceptable for this application.

5. The officials authorized to enter the students credentials in the block repository are expected to do the same after thorough content analysis and verification to prevent any typos or errors since the block contents once added remains immutable.

In view of the above limitations a different approach is introduced in the implemented design. The proposed hardware concepts are detailed here:

5.1 Formation of Block

In Academia data could be recorded in the corresponding blocks only after its creation. Each block represents a class room. Class teacher and the students of the respective classes are assumed to be the authorized members of a block. Every class room is allotted with a unique identification number called Class ID. Each student in a class is provided with student registration number known as Student ID. Its is presumed that the class ID, student ID, and the subject marks attained by every students are stored in a dedicated memory within the concerned block. In this architecture every block in the chain consists of Block ID, Block Header, Previous Block

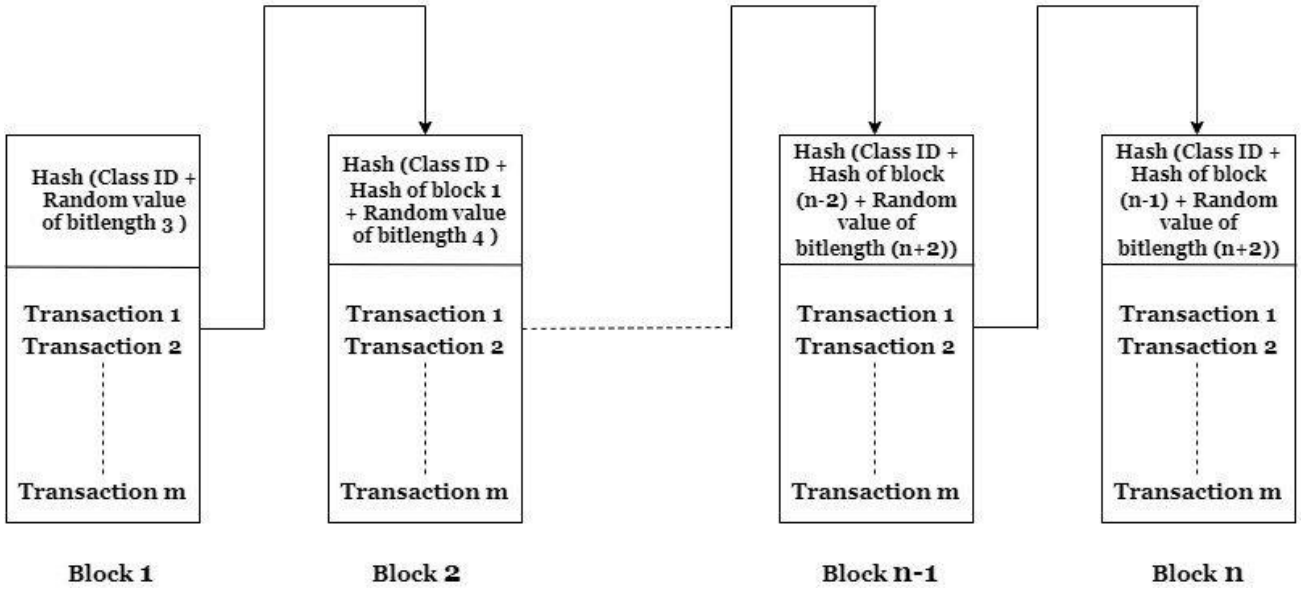

Figure 4: Block Formation in the blockchain

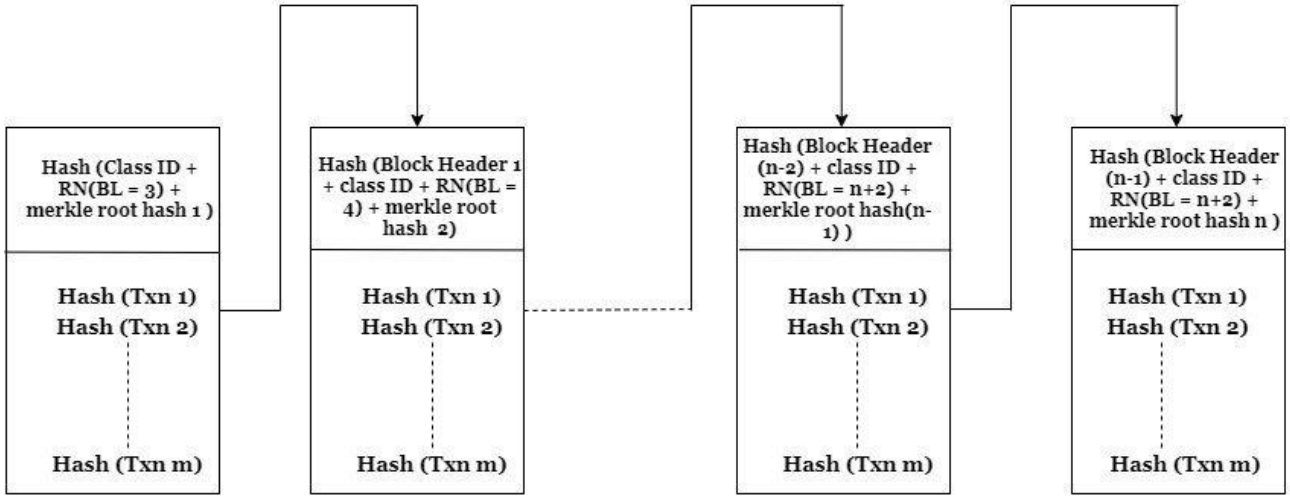

Figure 5: Block Securing Strategy

Hash and Merkle Root Hash. Figure 3 illustrates the flowchart of the different operations executed within a block.

1. Block ID creation
   Block ID refers to the unique number created for Block identification. It contains a random number that is generated by applying SHA-256 hashing algorithm on Class ID value. The Class advisor can enter the Class ID as the input and if it matches with the identification value assigned for the class, block ID will be created else the access is denied. Except the first block every other block have additional parameter called Block Header in the Block ID. Block ID formulas are as follows:

$$Block\_1\_ID = hash(ClassID + RN(BL = 3)) \quad (1)$$

$$Block\_n\_ID = hash(ClassID + Block\_n-1\_Header + RN(BL = n+2)) \quad (2)$$

   RN stands for Random Number
   BL stands for Bit Length

2. Block body
   After the generation of Block ID, in the next phase the student can enter his/her Student ID. The student ID is verified with the original value already stored in the memory of block and if it is matched, the subject marks for the respective student is accessed and percentage is computed. Hash algorithm is applied to the unique value obtained after concatenating Student ID with the percentage scored. This results in a unique hash value which is displayed along with the percentage value as outputs.

3. Block Header
   Block header contains Merkle root hash of all transactions and Block ID. Block ID corresponds to the 256-bit hash value that distinguishes and identifies the block. Merkle root hash is obtained by hashing the sum of hashes of all the transactions conducted within the block. The "transactions" in this context refers to the percentage calculated for each student. Block Header is calculated based on the given equations:

$$Block\_1\_Header = hash(Block\_1\_ID + Merkle\_hash\_1) \quad (3)$$

$$Block\_n\_Header = hash(Block\_n - 1\_ID + Merkle\_hash\_n) \quad (4)$$

4. Nonce and Difficulty
   First block is developed based on the unique class ID allocated to each class and a three bit random number. Hashing algorithm SHA-256 is imposed on these parameters to generate the hash for the block. Random Number is created by hashing the class ID and considering the last three bits from the LSB of the resultant hash. For the succeeding blocks, previous block hash, unique class ID and the random number are utilized. With the increase in the number of blocks, the bit size of the random number is also incremented. Random value assigned for hash generation determines the Nonce and difficulty. In this blockchain, block formation is confined only with the teachers who is entrusted with the class ID. Figure 4 shows how the blocks are formed within the blockchain.

5.2 Interconnection of Blocks

For ensuring additional security to the blocks created the following concept is applied:

- Block ID is the principle component that interlinks each block.
- Block Header of the current block consists of Block ID and merkle hash root of the commenced block. Every individual transactions that happened within a block are hashed separately using SHA-256 hash algorithm. These hash values are added on each time and once the entire transactions gets completed the resultant hash value is hashed once again to get the merkle root hash of the block.
- The block ID of the current block includes Class ID and random number that belongs to present block but block header of the previous block. Preceding block header contains block ID and merkle root hash of the previous block.
- Thus all the contents within each block gets interconnected with the other as the length of the chain increase.
- Therefore Nth block ID could be created only if the complete data is consistent from the first block to the preceding block with regard to data integrity and provenance.
- Interconnection of blocks thus assure added security since the contents within the block cannot be updated or manipulated as the hash values computed through SHA-256 are NP hard to find a solution. Figure 5 demonstrates the method adopted for securing blocks.

The main objective of blockchain hardware platform for storing academic database is to gain trust of the entities involved that includes students, teachers, parents, other higher officials who needs to validate the transcripts whenever required without the help of an external third party. Data security is ensured through block formation, block interconnection and hashing of contents. Other authorized educational organizations can access the blockchain database through creation of unique ID number followed by its verification by the authority in-charge (class advisors).

6 Synthesis and Simulation Results

The proposed hardware prototype for blockchain is designed in Hardware programming language Verilog. The functionality has been verified using Modelsim Simulator tool. The design is synthesized in Virtex 7 FPGA using Xilinx ISE design suite software tool.

The architecture designed can be programmed to include any number of blocks within the chain of blocks and is also flexible with respect to the number of transactions per block. As part of the research work, a miniature model of blockchain is considered that contains four blocks in the chain. Each block represents a class that comprises of 50 students. Four subjects pertaining to the current semester is stored within the blocks for estimating the Academic grade in percentage.

6.1 Simulation Results

Figure 6. displays the simulation results after percentage estimation for a particular student in Block 1. Inputs given were as follows:
Class ID = 20171
Student ID = 17002
Outputs obtained were :
Percentage = 82
Hash output of percentage for the student with ID 17002
= db3eee73beca217620ec21c37c0c07ccb0b65eddc1c9d9
a4382f7cd931696c7e
Block ID = d9bae266e5eb6914800a1894b8a5567290d63
efe7df89536892dafe4beb921a2
Block Header = df8c153e6682c3cb6c3330e804c3a44c983
246886ad888bc05832e57f177aaea
Merkle root hash = f3e886b34a03f33bf98d449f57d8cd562
fb1fb6f58f6c66ce3e985ee727900e5

6.2 Synthesis Results

The framework was designed to exist as different modules, synthesized separately and later integrated to form the entire architecture. The structure contained standalone modules for Block ID creation,

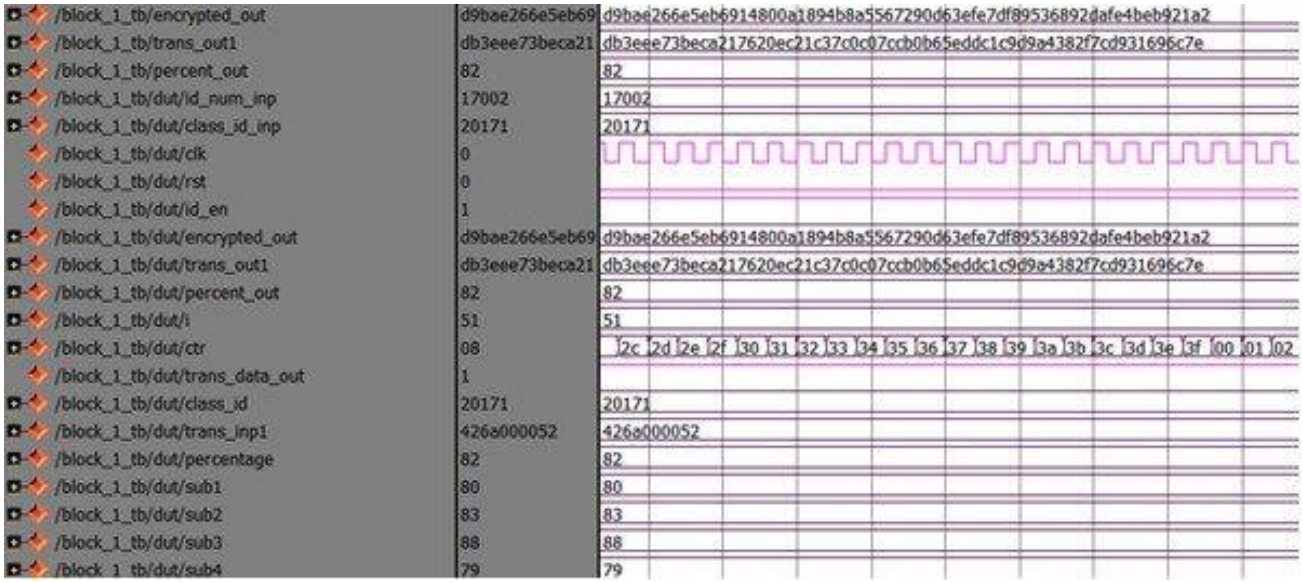

Figure 6: Simulation result after percentage estimation in block 1

Merkle hash computation, Block header creation and a Block module that includes the design for percentage computation. Table 2 shows the performance parameter summary for different design modules in the blockchain paradigm. In the table LUT-FF stands for Look Up Table and Flipflop pairs and IOB is the abbreviated form of Input-output buffers utilized by the design modules.

The entire system comprising of all the modules designed, functioned at an operational frequency of 95.138MHz. All modules were synthesized in xc7v1500t-2flg1761 device belonging to Virtex-7 FPGA family.

Table 2: Performance analysis of various blocks in the blockchain in Xilinx Virtex 7 FPGA

Design Modules	#Registers	#LUT-FF pairs	#IOBs	Speed (Mhz)
Merkle_hash_1	5804	4631	276	95.138
Block_1	6296	5528	569	95.235
Block_1_header	12269	9877	276	95.142
Merkle_hash_2	5807	4617	276	95.138
Block_2	18746	15369	571	95.132
Block_2_header	24678	19789	276	95.142
Merkle_hash_3	5804	4623	276	95.138
Block_3	31119	25442	571	95.138
Block_3_header	37046	29900	276	95.145
Merkle_hash_4	5804	4638	276	95.137
Block_4	43546	35356	571	95.138
Block_4_header	49471	39738	276	95.138

7 Conclusion and Future Scope

Credibility and authenticity of academic records are prerequisites to the reputation of academia and graduates. Unreliability of paper records and centralized electronic storage system demands the requirement of a distributed transparent platform to enable data sharing and communication. This scenario reveals the importance of Blockchain that offers a vital platform to implement an open access framework and attain interoperability. However the software elements in this technology are subjected to serious security threats that seems to put a downfall on the level of security provided by them in comparison to the hardware equivalents. This research work suggests a hardware approach that unfolds a new dimension to the architectural perspective of blockchain and helps the online experts that rely on this technology to overcome many vulnerabilities and challenges of an autonomous software application. In addition to Academic record maintenance, the proposed paradigm can be extended to higher levels that covers multiple domains and universities. Thus as an element of future work, the design find its application in University Management Scheme and Online Academic Systems so as to receive the complete details of the student performance.

Conflict of Interest The authors declare no conflict of interest.

References

[1] J. Wan, J. Li, M. Imran, D. Li and Fazal-e-Amin, "A Blockchain-Based Solution for Enhancing Security and Privacy in Smart Factory," IEEE Transactions on Industrial Informatics, **15**(6), 3652–3660, 2019, doi:10.1109/TII.2019.2894573.

[2] J. Al-Jaroodi and N. Mohamed, "Blockchain in Industries: A Survey," IEEE Access, **7**, 36500–36515, 2019, doi:10.1109/ACCESS.2019.2903554.

[3] Shan Jiang, Jiannong Cao, Hanqing Wu, Yanni Yang, Mingyu Ma, Jianfei He, "BlocHIE: a BLOCkchain-based platform for Healthcare Information Exchange," in 2018 IEEE International Conference on Smart Computing, 49–56, 2018, doi:10.1109/SMARTCOMP.2018.00073.

[4] Thomas McGhin, Kim-Kwang Raymond Choo, Charles Zhechao Liu and Debiao He, "Blockchain in healthcare applications: Research challenges and opportunities," Journal of Network and Computer Applications, **135**, 62–75, 2019, doi:10.1016/j.jnca.2019.02.027.

[5] C. C. Agbo, Q. H. Mahmoud, and J. M. Eklund, "Blockchain technology in healthcare: A systematic review," Healthcare, **7**(2), 56, 2019, doi:10.3390/healthcare7020056.

[6] B. Assiri, "Leader Election and Blockchain Algorithm in Cloud Environment for E-Health," in 2019 2nd International Conference on new Trends in Computing Sciences (ICTCS), 2019, doi:10.1109/ICTCS.2019.8923099.

[7] A. Cohn, T. West, and C. Parker, "Smart after all: Blockchain, smart contracts, parametric insurance, and smart energy grids," in Georgetown Law Technology Review, 273–304, 2017.

[8] E. Münsing, J. Mather, and S. Moura, "Blockchains for decentralized optimization of energy resources in microgrid networks," in 2017 IEEE Conference on Control Technology and Applications (CCTA), 2164–2171, 2017.

[9] M. Mylrea and S. N. G. Gourisetti, "Blockchain for smart grid resilience: Exchanging distributed energy at speed, scale and security," in 2017 Resilience Week (RWS), 18–23, 2017, doi:{10.1109/RWEEK.2017.8088642}.

[10] Y. Lin, Joy R. Petway, Johnathen Anthony, Hussnain Mukhtar, Shih-Wei Liao, Cheng-Fu Chou and Yi-Fong Ho, "Blockchain: The evolutionary next step for ICT e-agriculture," Environments, **4**, 50, 2017, doi:10.3390/environments4030050.

[11] F. Yiannas, "A new era of food transparency powered by blockchain," Innovations: Technology, Governance, Globalization, **12**(1-2), 46–56, 2018, doi:10.1162/inov -a -00266.

[12] CIOReview. (2019)., "How Can Blockchain Technology Revamp Gaming Industry," 2019.

[13] G. Schillinger, Z. Huang, and S. Snyder, "The infrastructure for games of the future," 2018.

[14] C. Sitonio and A. Nucciarelli, "The Impact of Blockchain on the Music Industry," in 29th European Regional Conference of the International Telecommunications Society (ITS), 1–14, 2018.

[15] L. Lee, "New kids on the blockchain: How bitcoin's technology could reinvent the stock market," Hastings Business Law Journal, **12**, 81, 2015, doi:10.2139/ssrn.2656501.

[16] P. Poonpakdee, Jarotwan Koiwanit, Chumpol Yuangyai and Watchara Chatwiriya, "Applying Epidemic Algorithm for Financial Service based on Blockchain Technology," in 2018 International Conference on Engineering, Applied Sciences, and Technology (ICEAST), 1–4, 2018, doi:10.1109/ICEAST.2018.8434512.

[17] B. Shahzad and J. Crowcroft, "Trustworthy Electronic Voting Using Adjusted Blockchain Technology," IEEE Access, **7**, 24477–24488, 2019, doi:10.1109/ACCESS.2019.2895670.

[18] O. Jacobovitz, Blockchain for identity management, Ph.D. thesis, 2016.

[19] H.R. Hasan, Khaled Salah, Raja Jayaraman, Mohammed Omar, Ibrar Yaqoob, Saša Pesic, Todd Taylor, Dragan Boscovic, "A Blockchain-Based Approach for the Creation of Digital Twins," IEEE Access, **8**, 34113–34126, 2020, doi:10.1109/ACCESS.2020.2974810.

[20] T.M. Fernández-Carames, Paula Fraga-Lamas, "A Review on the Applica-tion of Blockchain to the Next Generation of Cybersecure Industry 4.0 Smart Factories," IEEE Access, **7**, 45201–45218, 2019, doi:10.1109/ACCESS.2019.2908780.

[21] S. Wang, L. Ouyang, Y. Yuan, X. Ni, X. Han and F. Wang, "Blockchain-Enabled Smart Contracts: Architecture, Applications, and Future Trends," IEEE Transactions on Systems, Man, and Cybernetics: Systems, **49**(11), 2266–2277, 2019, doi:10.1109/TSMC.2019.2895123.

[22] A.A. Monrat, Olov Schelén and Karl Andersson, "A Survey of Blockchain From the Perspectives of Applications, Challenges, and Opportunities," IEEE Access, **7**, 117134–117151, 2019, doi:10.1109/ACCESS.2019.2936094.

[23] T. Ali Syed, A. Alzahrani, S. Jan, M. S. Siddiqui, A. Nadeem and T. Alghamdi, "A Comparative Analysis of Blockchain Architecture and its Applications: Problems and Recommendations," IEEE Access, **7**, 176838–176869, 2019, doi:{10.1109/ACCESS.2019.2957660}.

[24] L. Xiong, F. Li, S. Zeng, T. Peng and Z. Liu, "A Blockchain-Based Privacy-Awareness Authentication Scheme With Efficient Revocation for Multi-Server Architectures," IEEE Access, **7**, 125840–125853, 2019, doi:10.1109/ACCESS.2019.2939368.

[25] A. Badr, L. Rafferty, Q. H. Mahmoud, K. Elgazzar and P. C. K. Hung, "A Permissioned Blockchain-Based System for Verification of Academic Records," in 2019 10th IFIP International Conference on New Technologies, Mobility and Security (NTMS), 1–5, 2019, doi:{10.1109/NTMS.2019.8763831}.

[26] Mona Al-Maharri, Hesham Al-Ammal, Lamya Aljasmi, "Usability of the Academic Transcript," in 2018 International Conference on Innovation and Intelligence for Informatics, Computing, and Technologies (3ICT), 1–7, 2019, doi:10.1109/3ICT.2018.8855746.

[27] "Academic Certificates on the Blockchain," 2018.

[28] S. Kolvenbach, R. Ruland, W. Gräther and W. Prinz, "Blockchain 4 Education," in Proceedings of 16th European Conference on Computer-Supported Cooperative Work-Panels, Posters and Demos, 2018, doi:10.18420/ecscw2018_p7.

[29] Nicolas Sklavos, Katerina Touliou, Costas Efstathiou, "Exploiting cryptographic architectures over hardware vs. software implementations: advantages and trade-offs," in Proceedings of the 5th WSEAS International Conference on Applications of Electrical Engineering, 2006.

[30] N. Lawson, "Side-Channel Attacks on Cryptographic Software," IEEE Security & Privacy, **7**(6), 65–68, 2009, doi:10.1109/MSP.2009.165.

[31] Samir Palnitkar, Verilog HDL: A Guide to Digital Design and Synthesis, Prentice Hall PTR, One Lake Street, Upper Saddle River, United States of America, 2003.

[32] Midhun Sasikumar, K.N. Sreehari, Ramesh Bhakthavatchalu, "Systolic Array Implementation of Mix Column and Inverse Mix Column of AES," in 2019 International Conference on Communication and Signal Processing (ICCSP), 0730–0734, 2019, doi:10.1109/ICCSP.2019.8697927.

[33] N.H.N. Sai Kiran, Ramesh Bhakthavatchalu, "Implementing delay based physically unclonable functions on FPGA," in 2016 International Conference on Advanced Communication Control and Computing Technologies (ICACCCT), 137–140, 2016, doi:10.1109/ICACCCT.2016.7831616.

[34] M. Anil Kumar, Ramesh Bhakthavatchalu, "FPGA based delay PUF implementation for security applications," in 2017 International Conference on Technological Advancements in Power and Energy (TAP Energy), 1–6, 2017, doi:10.1109/TAPENERGY.2017.8397339.

[35] I. Lin and Tzu-Chun Liao, "A Survey of Blockchain Security Issues and Challenges," International Journal of Network Security, **19**(5), 653–659, 2017, doi:10.6633/IJNS.201709.19(5).01.

[36] K. Devika and Ramesh Bhakthavatchalu, "Parameterizable FPGA Implementation of SHA-256 using Blockchain Concept," in 2019 International Conference on Communication and Signal Processing (ICCSP), 0370–0374, 2019, doi:{10.1109/ICCSP.2019.8698069}.

[37] K.N. Sreehari, Ramesh Bhakthavatchalu, "Implementation of hybrid cryptosystem using DES and MD5," in 2018 3rd International Conference on Communication and Electronics Systems (ICCES), 52–55, 2018, doi:10.1109/CESYS.2018.8724111.

[38] R. Purohit, Upendra Mishra, Abhay Bansal, "Design and Analysis of a New Hash Algorithm with Key Integration," International Journal of Computer Applications, **81**(1), 33–38, 2013, doi:10.5120/13978-1974.

[39] L. Bai, Shuguo Li, "VLSI Implementation of High-speed SHA-256," in 2009 IEEE 8th International Conference on ASIC, 131–134, 2019, doi:10.1109/ASICON.2009.5351591.

[40] N.C. Iyer and Sagarika Mandal, "Implementation of SHA-256 algorithm in FPGA based processor," International Journal of Advanced Research in Electronics and Communication Engineering (IJARECE), **4**, 334–344, 2015.

[41] N.S.Tinu, "A Survey on Blockchain Technology- Taxonomy, Consensus Al-gorithms and Applications," International Journal of Computer Sciences and Engineering, **6**, 691–696, 2018.

[42] Sol Jeon, Inshil Doh, Kijoon Chae, "RMBC: Randomized Mesh Blockchain Using DBFT Consensus Algorithm," in 2018 International Conference on Information Networking (ICOIN), 712–717, 2018, doi:10.1109/ICOIN.2018.8343211.

[43] L. M. Bach, B. Mihaljevic, M. Zagar, "Comparative Analysis of Blockchain Consensus Algorithms," in 2018 41st International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO), 1545–1550, 2018, doi:10.23919/MIPRO.2018.8400278.

[44] Zibin Zheng, Shaoan Xie, Hongning Dai, Xiangping Chen, Huaimin Wang, "An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends," in 2017 IEEE International Congress on Big Data (BigData Congress), 557–564, 2017, doi:10.1109/BigDataCongress.2017.85.

[45] Du Mingxiao, Ma Xiaofeng, Zhang Zhe, Wang Xiangwei, Chen Qijun, "A Review on Consensus Algorithm of Blockchain," in 2017 IEEE International Conference on Systems, Man, and Cybernetics (SMC), 2567–2572, 2017, doi:10.1109/SMC.2017.8123011.

[46] Basem Assiri, Wazir Zada Khan, "Fair and trustworthy: Lock-free enhanced tendermint blockchain algorithm," TELKOMNIKA Telecommunication, Computing, Electronics and Control, **18**(4), 2224–2234, 2020, doi:10.12928/telkomnika.v18i4.15701.

[47] M. Jirgensons and J. Kapenieks, "Blockchain and the Future of Digital Learning Credential Assessment and Management," Journal of Teacher Education for Sustainability, **20**, 145–156, 2018, doi:10.2478/jtes-2018-0009.

[48] M. Sharples and J. Domingue, "The Blockchain and Kudos: A Distributed System for Educational Record, Reputation and Reward," in 11th European Conference on Technology Enhanced Learning, 2016, doi:10.1007/978-3-319-45153-4_48.