

**Blockchain based Muslim Marriage Certification  
with the Supremacy of Web 3.0**

by

**Md. Al - Sajiduzzaman Akand**

ID: 191-15-2484

&

**Sarwar Azmain Reza**

ID: 191-15-2562

This report is presented in partial fulfillment of the requirements for the degree of Bachelor of Science in Computer Science and Engineering.

Supervised by

**Amatul Bushra Akhi**

Assistant Professor

Department of Computer Science and Engineering

Daffodil International University



**Daffodil International University**

Dhaka, Bangladesh

January 2022

## Approval

This project, titled **Blockchain-based Muslim Marriage Certification with the Supremacy of Web 3.0**, is submitted by **Md. Al-Sajiduzzaman Akand (191-15-2484)** and **Sarwar Azmain Reza (191-15-2562)** to the Department of Computer Science and Engineering, Daffodil International University, has been accepted as satisfactory for the partial fulfillment of the requirements for the degree of Bachelor of Science in Computer Science and Engineering and approved as to its style and contents. The presentation has been held on 1 February 2023.

### Board of Examiners

**Chairman**

---

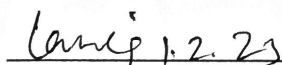
**Dr. Touhid Bhuiyan**  
**Professor and Head**  
 Department of Computer Science and Engineering  
 Faculty of Science & Information Technology  
 Daffodil International University



**Internal Examiner**

---

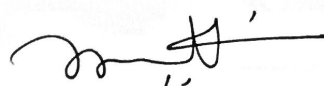
**Tania Khatun (TK)**  
**Assistant Professor**  
 Department of Computer Science and Engineering  
 Faculty of Science & Information Technology  
 Daffodil International University



**Internal Examiner**

---

**Ms. Lamia Rukhsara (LR)**  
**Senior Lecturer**  
 Department of Computer Science and Engineering  
 Faculty of Science & Information Technology  
 Daffodil International University



**External Examiner**

---

**Dr. Mohammad Shorif Uddin**  
**Professor**  
 Department of Computer Science and Engineering  
 Jahangirnagar University

## Declaration

We hereby declare that, we have done this project under the supervision of **Amatul Bushra Akhi**, Assistant Professor, Department of Computer Science and Engineering, Daffodil International University. We also declare that neither this project nor any part of this project has been submitted elsewhere for the award of any degree or diploma.

**Supervised by:**

*Amatul Bushra Akhi*  
01.02.23

---

**Amatul Bushra Akhi**  
Assistant Professor  
Department of Computer Science and Engineering  
Daffodil International University

**Submitted by:**

*Sajid*  
01.02.2023

---

**Md. Al - Sajiduzzaman Akand**  
ID: 19-15-2484  
Department of Computer Science and Engineering  
Daffodil International University

*Sarwar*  
01.02.23

---

**Sarwar Azmain Reza**  
ID: 19-15-2562  
Department of Computer Science and Engineering  
Daffodil International University

## Acknowledgment

First, we express our heartiest thanks and gratefulness to almighty God for His divine blessing making us possible to complete the final year project successfully.

We are grateful and wish our profound indebtedness to Supervisor **Amatul Bushra Akhi**, Assistant Professor, Department of Computer Science and Engineering, Daffodil International University, Dhaka, Bangladesh. Deep Knowledge & keen interest of our supervisor in Blockchain to carry out this project. His endless patience, scholarly guidance, continual encouragement, constant and energetic supervision, constructive criticism, valuable advice, reading many inferior drafts, and correcting them at all stages have made it possible to complete this project.

We want to express our heartiest gratitude to **Professor Dr. Touhid Bhuiya**, Professor & Head, Department of Computer Science and Engineering, for his kind help in finishing our project and to other faculty members and the staff of the Computer Science and Engineering Department of Daffodil International University.

We want to thank our entire course mate Daffodil International University, who participated in this discussion while completing the course work.

Finally, we must acknowledge with respect the constant support and patients of our parents.

## **Abstract**

Marriage is a momentous event in anyone's life. It is not just an ordinary relationship. This partnership is supported legally by a civil contract between a man and a woman. According to Islamic values, the Muslim community keeps records of their marriage contract called Nikah-Nama. Currently, the Bangladesh government records the NikahNama in a classic logbook. It is 2022, and this sector has not seen significant upgradation for decades. This system is highly inefficient, prone to impairment, and has fraud loopholes. Corrupt citizens use these loopholes to cheat life partners, cross the marriage limits and conduct an enormous number of offenses. This paper proposes an approach to revolutionize the entire marriage recording system of Bangladesh. It describes step-by-step procedures and the better way to implement a digital Muslim marriage data preservation system. Bleeding-edge technologies are prioritized in this work by keeping web 3.0 in mind to bring innovation to this segment. This paper reflects the minimal approach to the proper digitalization of this issue. The whole idea of this concept is highly scalable. This prototype implementation is ready for any community, group, religion, or Government with an affordable technical infrastructure. The demonstration version is developed according to the conventional marriage rules and guidelines of Bangladesh. Nevertheless, others can also adopt this software ecosystem with minor or further modifications.

## Table of Contents

### Contents

Board of Examiners	i
Declaration	ii
Acknowledgment	iii
Abstract	iv
<b>Chapter</b>	
<b>Chapter 1: Introduction</b>	1-3
1.1 Blockchain	1
1.2 Blockchain Data Structure	1
1.3 Methodology of Blockchain	1
1.4 Introduction to NikahNama	2
1.5 Drawbacks of the Traditional NikahNama System	2
1.6 Our Approach to These Issues	3
<b>Chapter 2: Related Works</b>	4-6
2.1 Blockchain Technology for Islamic Marriage Certificate	4
2.2 Blockchain and Identity Persistence	4
2.3 Blockchain for record-keeping and data verifying: proof of concept	4
2.4 Role of Blockchain and Smart Contracts in Transforming Social Contracts	5
2.5 Smart Marriage Contracts: The Future of Blockchain in Matrimonial Property Law?	5
2.6 Blockchain Technology for Data Management of Research Data	6
2.7 A study of blockchain technology on securing the personal health record	6
<b>Chapter 3: Existing Issues and Work Plan</b>	7
<b>Chapter 4: Methodology</b>	8-28
4.1 Block Formation	8
4.2 Proof of Work Concept	10
4.3 Blockchain Architecture	11
4.4 Digital Signature Mechanism	12
4.5 Backing Up the Blockchain	14
4.6 Distributed Blockchain Network	15
4.7 Peer to Peer Networking	15
4.8 Real Time Communication (WebRTC)	17
4.9 Disadvantages of Real Time Communication	18
4.10 Application Development	19
4.11 National Identity Verification	20
4.12 Structure of the Application	22
4.13 React	22
4.14 Create React App Library	23
4.15 React Router DOM	23

4.16 Firebase Authentication	24
4.17 Tailwind CSS	25
4.18 Node.js	25
4.19 Express.js	26
4.20 Progressive Web Application (PWA)	27
4.21 Blockchain Deployment	28
<b>5. Extended Work &amp; Future Plan</b>	<b>29</b>
<b>6. Conclusion</b>	<b>30</b>
<b>References</b>	<b>31-32</b>

## List of Figures

<b>Figure No</b>	<b>Name</b>	<b>Page</b>
1	Block Formation	8
2	Nikah-Nama Blockchain Architecture	9
3	Proof-of-Work Concept	11
4	Digital Signature Mechanism	12
5	Nikah-Nama Blockchain Prototype	13
6	Backup Management	14
7	Peer-to-Peer Networking Structure	16
8	Real-time Communication in Distributed Computing	17
9	Hierarchy-Based Distributed Computing.	18
10	Homepage of Nikah-Nama	19
11	Marriage Registration Form.	21
12	Demo Marriage Certificate	22



## **Chapter 1: Introduction**

### **1.1. Blockchain**

In this decade, Blockchain has been at the fore among the technologies that have created hype. Blockchain is a concept of storing data in a very secure technique. It has earned popularity because of its method of protecting data privacy and trust. By definition, Blockchain is a shared, immutable ledger that facilitates the process of recording transactions and tracking assets in a business network. An asset can be tangible (a house, car, cash, land) or intangible (intellectual property, patents, copyrights, branding). Therefore, virtually anything of value can be tracked and traded on a blockchain network, reducing risk and cutting costs for all involved. As a result, Government agencies and other security-enthusiastic companies are adopting this technology rapidly in diverse domains.

### **1.2. Blockchain Data Structure**

One can get an idea of the working methodology of Blockchain from its name. A block of a Blockchain contains specific data, and the system arranges the blocks sequentially in a chain-like data structure. Typically in the Blockchain concept, a block should keep at least three types of elements. They are – the primary data, the current block's hash, and the previous block's hash. To generate the hashes computer system uses a cryptographic algorithm like MD5, SHA-1, SHA-2, etcetera.

### **1.3. Methodology of Blockchain**

The data in the Blockchain becomes change resistant and immutable because of its chain of hash. A Blockchain is stored in a decentralized computer network. Here each machine entity of the network is called a node. Whenever a new node connects to the Blockchain network, it creates a copy of the whole or a portion of the Blockchain. If hackers try to forgery any block's data, it changes its hash. If the hash changes in any prospect, it declares the whole chain invalid. The affected node recovers the valid Blockchain by copying the data from unaffected nodes. Generating a cryptographic hash consumes an immense amount of time and power. In addition, pushing a valid block in the chain becomes more critical because of the hashing technique, and

manipulating block data over many nodes becomes a mammoth task. This feature makes it technically almost impossible to manipulate any data in the Blockchain approach.

#### **1.4. Introduction to NikahNama**

Marriage data recording deserves a high rank of security, privacy, and trust. Especially in a Muslim marriage, Nikah-Nama ensures the protection of the family and relationship. By definition, Nikah-Nama is the marriage contract signed by the bride and bridegroom in the eyewitness of two men or one man and two women [1]. The Government of the People's Republic of Bangladesh has been maintaining this record officially since 1974 [2]. Back then, the officials used to record marriages in their registration books in handwritten format. These officials are traditionally called Kazi. It takes roughly months or more to process a marriage certificate in handwritten format. This method of storing essential data is unduly fragile, easily exploitable, and highly impractical in the era of Virtual Reality. This procedure also opens the door for the fakers to mutate the necessary evidence of incidents and contracts. However, there remains a high-risk possibility of information breaches by fraud.

#### **1.5. Drawbacks of the Traditional NikahNama System**

Recently, a critical case came to light; it was filed against Tamima Sultana Tammi, who tied the knot with famous cricketer Nasir Hossain without divorcing the complaint [3]. As a result, concerned authorities had to go through challenging procedures to find out the reality and the actual date of the divorce. This case is just an example. Many similar allegations have been raised in every corner of the country. In most cases, looking out the marriage registration by going through page by page of the registry book is not practical at all, and this is a very time-consuming procedure that delays the court's judgment.

Nonetheless, the integrity of the evidence is not full-proof and trustful. For example, a few days ago, a tragic road accident occurred in Bangladesh's capital. Seven women appeared at the morgue to claim the dead body of a person who died in this incident [4]. None of them used to know that her husband had other wives. Another example is that recently, police got a marriage registry book with blank pages between the records.

After the investigation, police found out that a corrupted Kazi used to leave the pages blank so that he could register underage marriages in the future when the bride and bridegroom were mature after a few years [5].

### **1.6. Our Approach to These Issues**

In this circumstance, the digitalization of this sector has become a must to secure families, society, and the future. The traditional method of keeping matrimonial acknowledgment can be replaced with promising technologies. The information technology world is evolving at a swift speed daily. This work aims to solve these issues and achieve a sustainable technical architecture to be the legal backbone of social culture.

## Chapter 2: Related Works

### 2.1. Blockchain and Identity Persistence

First, N. Elysha Kamaruzaman et al. [6] proposed an application implemented on the Ethereum platform with Smart Contracts. The prime objective behind this paper is to develop a highly scalable application that stores marriage information as a Blockchain transaction. That can replace traditional paper-based Nikah-Nama, which has a significant risk of being forged.

The Smart Contract was written in solidity and deployed in Ethereum TESTNET. Authors used MetaMask to provide the capability to make Ethereum transactions through a regular website. In addition, they built a user interface that takes information as required and stores it in the Smart Contract deployed inside the Blockchain system.

### 2.2. Blockchain and Identity Persistence

A. Marthews and C. E. Tucker et al. [7] were concerned about the security and privacy of people's identities. According to the author, securing identity from exterior discovery and explication is significant. On the other hand, privacy covers a more substantial domain than securing a static identity. The authors make a chart of ways that people's numerous identities may be impacted and sabotaged by the evolution of public and unmodifiable ledgers of transactions and contractual undertakings. They proposed an identity model for the various use cases of Blockchain. They used the concept of "narrative identity" to locate the nature of the privacy violation involved more precisely. They also used examples of marriage, money laundering, and criminal justice records to examine some of the negative significances of Blockchain proceeding beyond dealing with movements of assets and physical goods to maintaining an authoritative, longitudinal record of people.

### 2.3. Blockchain for record-keeping and data verifying: proof of concept

R. Ghazali et al. [8] aimed to preserve marriage data using Blockchain and improve data sharing efficiency. That involves accessing data from the Blockchain and multiple users through proof of concept (POC). They presented a POC to design and develop

Muslim marriage data preservation using private Ethereum Blockchain for Malaysia. Their proposed POC has demonstrated that marriage data recording, sharing, and managing issues could be resolved by Blockchain implementation. However, there are some drawbacks to their POC. For example, a monitoring and auditing mechanism for data storage transaction logs is needed to ensure security, inspectability, and transparency.

#### **2.4. Role Of Blockchain And Smart Contracts In Transforming Social Contracts**

N. Asfour et al. [9] focused on two circumstances. These are - the significant similarities and distinctions between the innovative contract-based model and the traditional model in funding networks and marriage contracts and the anticipated advantages and drawbacks of the Smart Contract-based model over the classic model. First, the author designed two models built upon Blockchain and Smart Contract technology. The purpose of the models is to solve the existing problems, such as being inflexible and having so many parties involved in the network of existing traditional models. They developed two networks, a crowdfunding network, and a marriage contract network. Then, they compared two cases based on the modification in structure and functions of each party in the network.

#### **2.5. Smart Marriage Contracts: The Future Of Blockchain In Matrimonial Property Law?**

L. Sisák et al. [10] focus on Smart Marriage Contracts (SMC) using Blockchain in the matrimonial property law of contracts. First, they clarified SMC's origin, technical functionality, and legal nature. After that, they confront them with the national private law of three jurisdictions – Germany, Austria, and Slovakia. Finally, they focus on the possibilities of initiating SMC in these countries. They also ambitioned to make the reader aware of the topic at hand and suggest solutions to the fundamental problems of the Smart Marriage Contract.

## **2.6. Blockchain Technology for Data Management of Research Data**

R. Duchemin et al. [11] were concerned about the replication crisis of research data. They identified three reasons for the replication crisis - lack of data quality, indefinite methodology, and publication bias. Their analysis aims to identify how Blockchain technology can influence research data management and evaluates whether Blockchain technology can reduce the replication crisis. After their analysis, they concluded that Blockchain for scientific research data management could result in a higher rate of replicable studies.

The programmability characteristic of the Blockchain resolves the issue of indefinite methodology. Furthermore, the same programmability aspect can be used to address the publication bias. Using private keys and security, data immutability, and time stamping features can improve research data quality.

## **2.7. A study of blockchain technology on securing the personal health record**

This work is about a comprehensive survey of healthcare using Blockchain. R. Vidhyuth and T. Manoranjitham al. [12] gave an overview of Blockchain's healthcare application. Their survey shows that most Blockchain research focuses on electronic health records, and Blockchain has been applied to enhance medical service automation in several use cases. They described the most critical Blockchain analysis for the medical field and the techniques and applications of Blockchain.

### Chapter 3: Existing Issues and Work Plan

The existing governmental logbook-based marriage registration system needs to be upgraded as soon as possible. Digitalizing the entire system is the immediate solution to this issue to move toward paperless generation. The general approach can be developing an advanced web portal for registration with a traditional relational database management system (RDBMS).

However, the issue with this database management system is that the data can be altered, updated, or deleted. The power of altering data leaves a backdoor open for corruption. Administration power can be controlled, but corruption can spread to the highest hierarchy. In this situation, sensitive data like birth, death, vaccination, marriage, divorce, and other notary certification data must be immutable. As this governance division has not modernized for a long time, the idea should be visionary enough to keep it sustainable, feasible, scalable, and futuristic.

The upcoming Web 3.0 can probably be a standard solution at this stage. Blockchain is one of the optimum keys to the world of Web 3.0. Many researchers and experts suggest this technology for this niche e-governance, healthcare, digital currency, banking systems, supply chains, and other sectors. With this approach, previously, several developers have written Smart Contracts for Ethereum Blockchain to store marriage data as a transaction.

Ethereum is a public Blockchain network. However, according to the Data Privacy and Security Rules, 2019, and Cloud Computing Policy 2022 of Bangladesh, citizens' sensitive personal data should not be stored outside the geographical land area of Bangladesh [13]. Ethereum has an additional cost for mining and storing blocks in the network. The Bangladesh Government also does not legally allow cryptocurrencies like Bitcoin or Ether. So, using a public Blockchain is unsuitable according to this country's regulations.

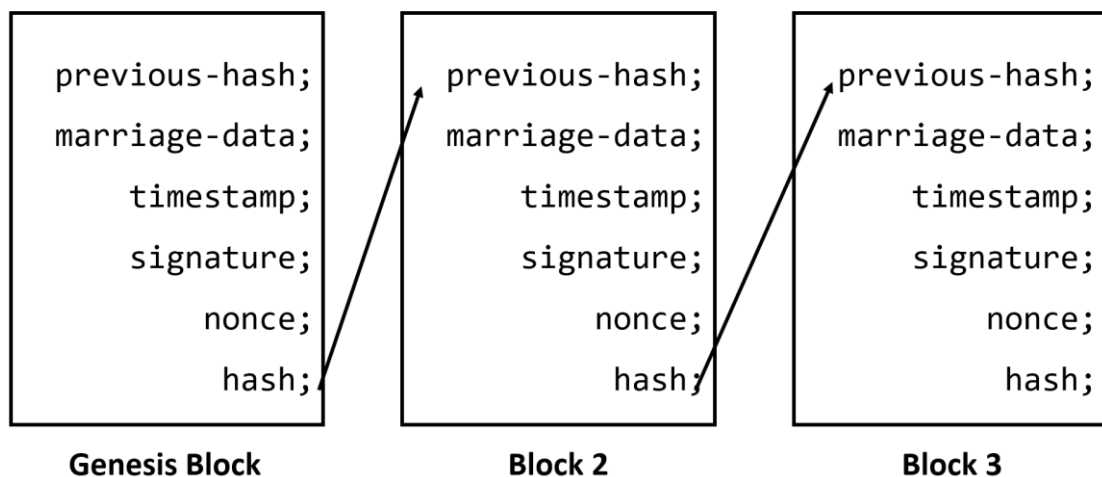
At this point, the plan is one step further to develop a private Blockchain network for this niche E-governance area. The goal is to design a nationally feasible application architecture with an affordable infrastructure.

## Chapter 4: Methodology

Although Blockchain started to gain popularity in 2016, the concept was first introduced by the research scientist Stuart Haber and W. Scott Stornetta in 1991 [14]. However, Satoshi Nakamoto discovered a revolutionary application of it in 2008 by developing Bitcoin [15]. Bitcoin is open source, and its design is public. Besides, many other open-source Blockchain networks have been developed this decade. These efforts are the inspiration to achieve the goal and design a straightforward Blockchain prototype.

### 4.1. Block Formation

Firstly, this is the basic design for the blocks and chain foundation-

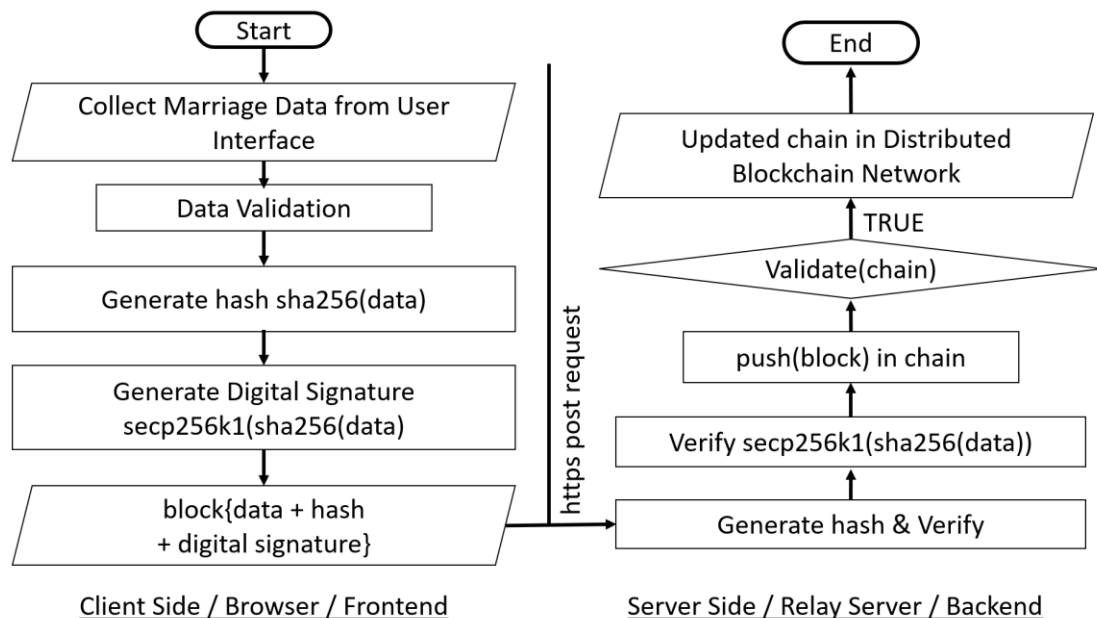


**Figure 1.** Block Formation.

According to the above figure, each block contains six types of information. Firstly, an object containing all necessary marriage data in a particular structure. Then, it stores the UNIX timestamp in the timestamp variable. The timestamp tracks time at the Unix Epoch on 1 January 1970 at UTC [16]. The millisecond format is used to keep the accuracy higher as needed. In the block, the timestamp represents the block creation time.



After that, the system generates a hash using the SHA-2 algorithm. SHA-2 is a set of cryptographic hash functions developed by the United States National Security Agency and first released in 2001. SHA-2 offers better protection against collisions. This means that the same input data will always have different hash values. SHA-2 uses 64 to 80 rounds of cryptographic operations and is commonly used for validating and signing digital security certificates and documents. Unfortunately, the previous generation, SHA-1 or MD5, is vulnerable to powerful computers. So, SHA-256 is used, which generates a unique hash of 64 characters. Bitcoin also uses the same algorithm for hashing [17]. SHA-512 ensures the system is more secure but takes up more space.



**Figure 2.** Nikah-Nama Blockchain Architecture.

The system of Nikah-Nama Blockchain is designed according to the architecture shown in figure 2.

It passes stringified marriage data object + timestamp + nonce through the hash function to generate a hash. Here, the nonce in Blockchain is an arbitrary number to manipulate the actual hash of data. The hash must be manipulated to implement the proof-of-work (PoW) concept [18]. To prevent the rapid insertion of blocks in the Blockchain network, the client has to perform a complex mathematical calculation or work to prove the block is valid. This mechanism is known as proof-of-work (PoW).

Usually, this calculation takes massive electrical power and consumes time. The more time it takes, the harder it becomes to manipulate a Blockchain network for hackers. If a hacker pushes an invalid block in the chain, the network gets enough scope to recover a valid chain before adding a new block because of its proof-of-work mechanism. However, modern Blockchains are being developed with other innovative methods like proof-of-stack to save valuable resources and energy like electricity. Generating the target hash is also called Blockchain mining.

#### **4.2. Proof of Work Concept**

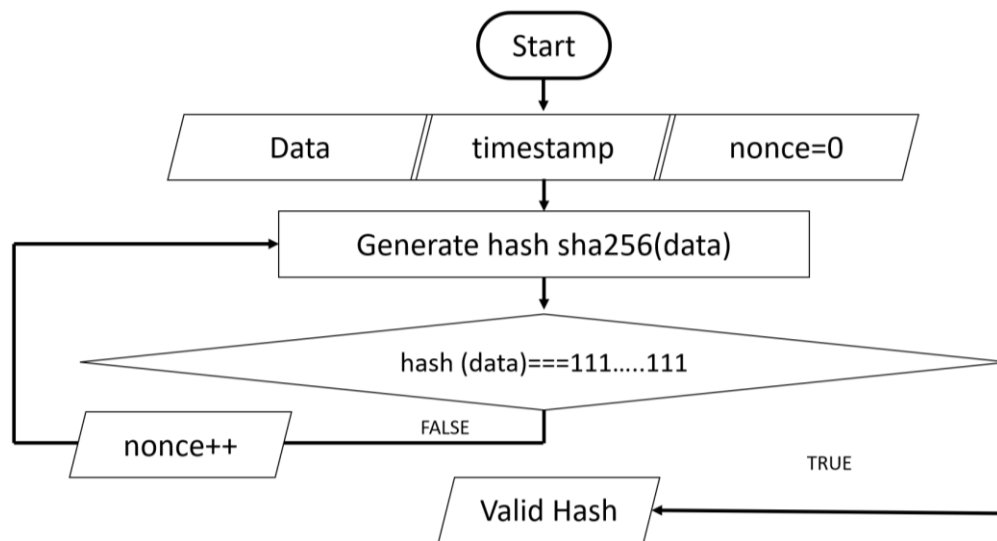
In a blockchain, the proof of work concept is used to create new blocks and add them to the blockchain. The process of creating a new block involves solving a complex computational problem, known as a "proof of work problem." The process of solving this problem is known as "mining."

When a miner successfully solves the proof of work problem, they are able to create a new block and add it to the blockchain. This process is crucial for maintaining the integrity and security of the blockchain.

One of the main benefits of the proof of work concept is that it helps to prevent fraud and tampering on the blockchain. Since creating a new block requires a significant amount of computational power and resources, it is expensive and time-consuming to do so. This makes it difficult for any one individual or group to dominate the process of creating new blocks and altering the blockchain.

In addition, the proof of work concept helps to ensure that the blockchain is decentralized and not controlled by any single entity. Since anyone can participate in the mining process, there is no single point of control or failure in the system.

Overall, the proof of work concept is a key component of the blockchain technology, helping to ensure its security, integrity, and decentralization.



**Figure 3.** Proof-of-Work Concept.

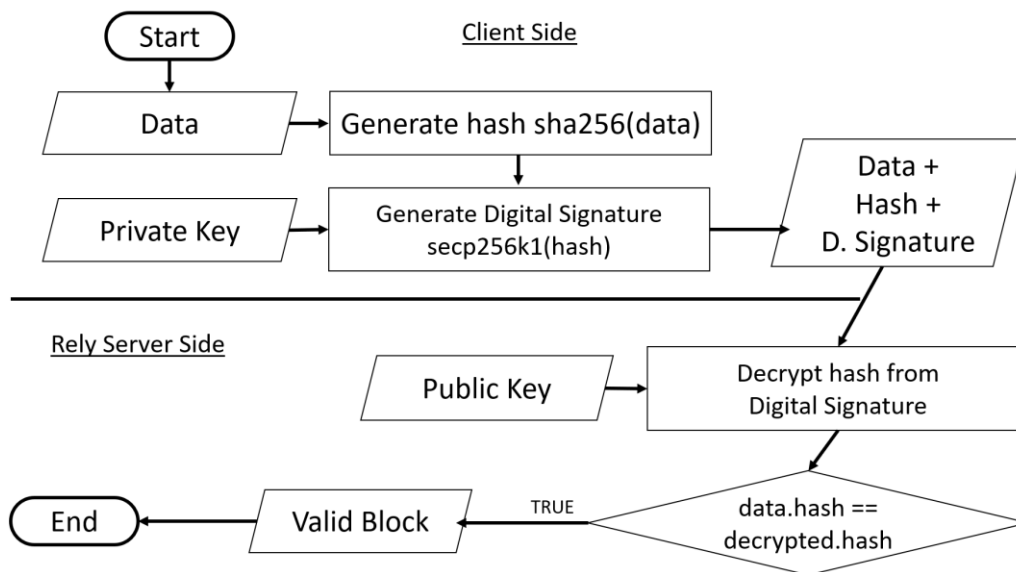
In figure 3, the system first generates a hash with the nonce value of 0. Then it keeps increasing until it finds a hash that starts and ends with three consecutive 1. Here, the more rules are applied, the more difficulty increases. Bitcoin adjusts the difficulty level according to the mining machine's capability. The target is to make it much more difficult to mine a block, which should take up to 10 minutes. Bitcoin accepts a finite number of consecutive 0 at the beginning of the hash as the target value [19].

After that, the system automatically adds the previous block's hash to the current block. A valid block should always point to another valid block's hash. Actual chain relation is established through the chain of hash; if anyone tries to change any single value of block-protected data, the hash changes. As a result, the whole chain is declared invalid. To manipulate a single block, hackers have to manipulate all consecutive blocks of the chain, which is nearly impossible.

### 4.3. Blockchain Architecture

All blocks point to the previous block, but the first block. The first block is automatically system-generated and points to no block called the genesis block. The genesis block includes metaphorical information about the Nikah of Adam and Eve (peace be upon them), the first couple on earth. New blocks are added later on the chain.

#### 4.4. Digital Signature Mechanism



**Figure 4.** Digital Signature Mechanism.

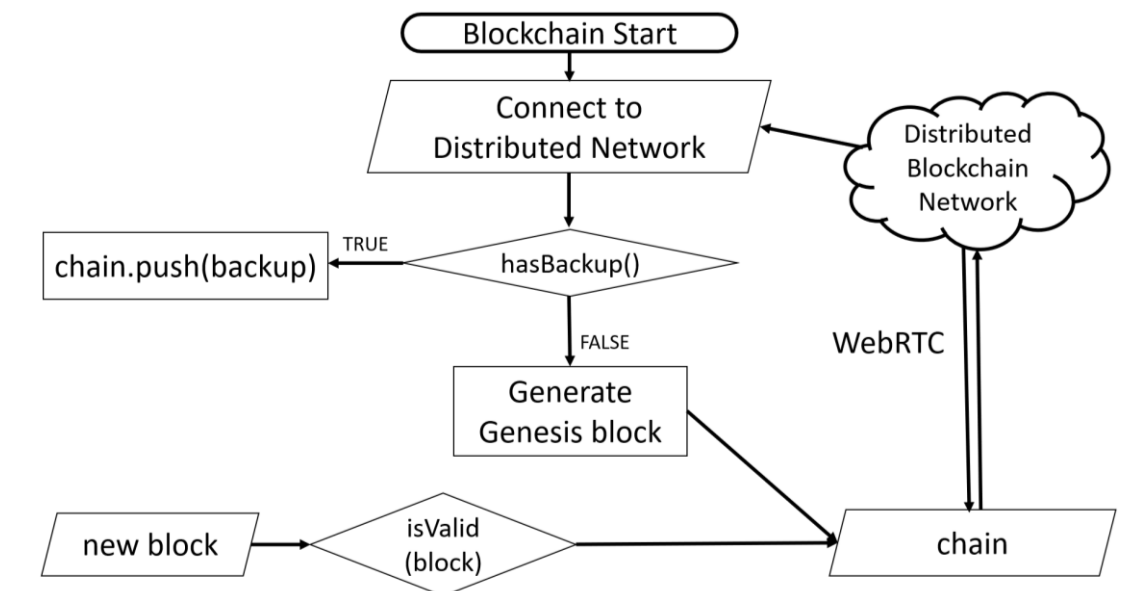
A digital signature is a mechanism used in blockchain technology to ensure the authenticity and integrity of a digital message or document. It uses cryptography to provide a secure and tamper-evident way to verify the identity of the sender and the authenticity of the message.

In a blockchain, each transaction is digitally signed by the sender using their private key. The private key is a secret piece of information known only to the owner of the key, and it is used to generate a digital signature. The digital signature is then attached to the transaction and broadcasted to the network.

The network verifies the authenticity of the digital signature using the sender's public key, which is publicly available and can be used to verify the signature. If the signature is valid, the network can be confident that the transaction was indeed sent by the owner of the private key and that the transaction has not been tampered with during transmission.

Digital signatures are an essential part of the blockchain system and play a crucial role in ensuring the security and integrity of the network. They allow the network to trust the authenticity of transactions and prevent fraud or tampering.

Now, it is time to ensure the integrity of the block. The system uses the secp256k1 for generating digital signatures to verify if the generated blocks come from the right source. Secp256k1 is the name of the elliptic curve used by Bitcoin to implement its public key cryptography. As shown in figure 4, the system passes the current block's hash through the secp256k1 function with a private key stored in the system's client software. This key must be kept in the environment variable. It prevents the key from being compromised by any party.

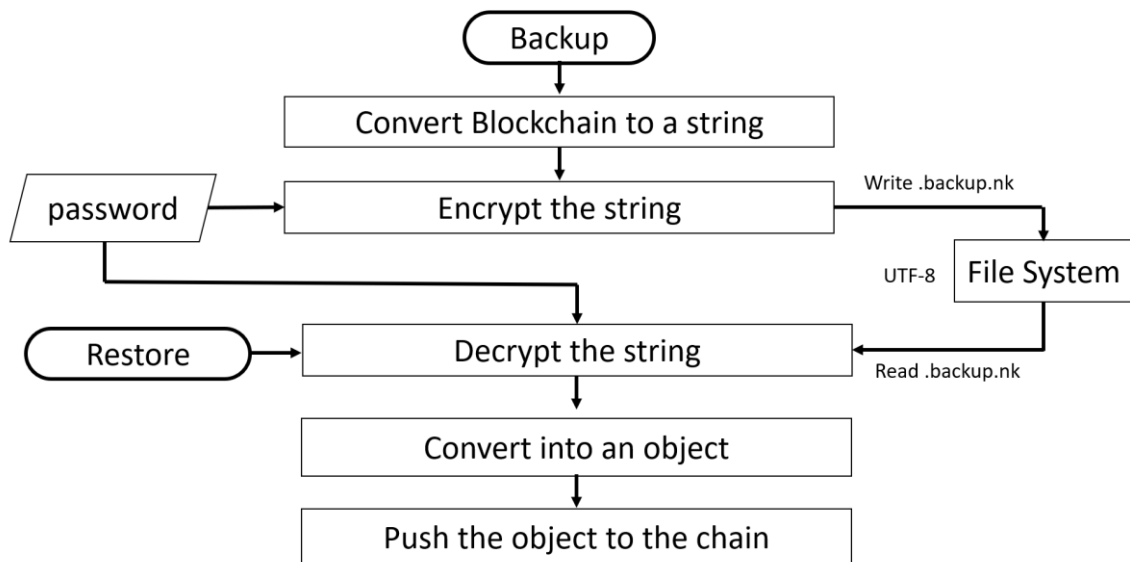


**Figure 5.** Nikah-Nama Blockchain Prototype.

After that, all these components are packed in a block and sent to a server using a secure HTTPS POST request protocol. On the server side, the hash of the data was generated again and verified whether it is valid. Then the system decrypts the digital signature with the same algorithm with the public key of that pair. If the contained hash and the decrypted hash match, the block is pushed to the chain of the node. Then an advanced verification algorithm checks whether the whole chain is valid. If the chain is valid, it spreads through the distributed Blockchain network.

#### 4.5. Backing Up the Blockchain

The Blockchain is built on runtime and stored in the machine's Random Access Memory (RAM). RAM is a volatile memory. So, the entire Blockchain gets lost if any node shuts down or gets restarted. For this reason, Blockchain is stored in a distributed cloud computing network so that nodes can restore the chain from cloud backup. The number of nodes is limited as it is planned to be operated in a private network environment. If hackers manage to shut all the nodes simultaneously, the whole network gets destroyed. To prevent this, designing a secure backup system is a requirement.



**Figure 6.** Backup Management.

Here, two functionality is developed- backup and restore. First, to make a Blockchain backup, the chain needs to be converted into a string. Then the string is encrypted using a password stored in the runtime environment variable. Finally, this encrypted string writes in a custom hidden file format named .backup.nk (hidden file). Here, the custom file extension .nk stands for Nikah. Then this file is stored in the secondary non-volatile storage of the machine using the File System API of the operating system.

Restoring process is the inverse of the backup process. Firstly, the system reads the target .backup.nk file and gets the encrypted string. After decrypting the string, the output needs to be converted into an object again and pushed to the chain. Here encrypting the data is essential unless hackers can get access to alter backup files to change the data of the Blockchain system. If hackers change the backup file string, it decrypts meaningless data when the data is encrypted, which prevents Blockchain forgery.

#### **4.6. Distributed Blockchain Network**

Distributed cloud computing comes into play to decrease the vulnerability of a Blockchain. Here every node fully or partially copies the Blockchain data. If any node gets hacked or becomes invalid, other nodes support it to recover the data as soon as possible. Many Blockchain uses a consensus algorithm to decide whether a block is valid.

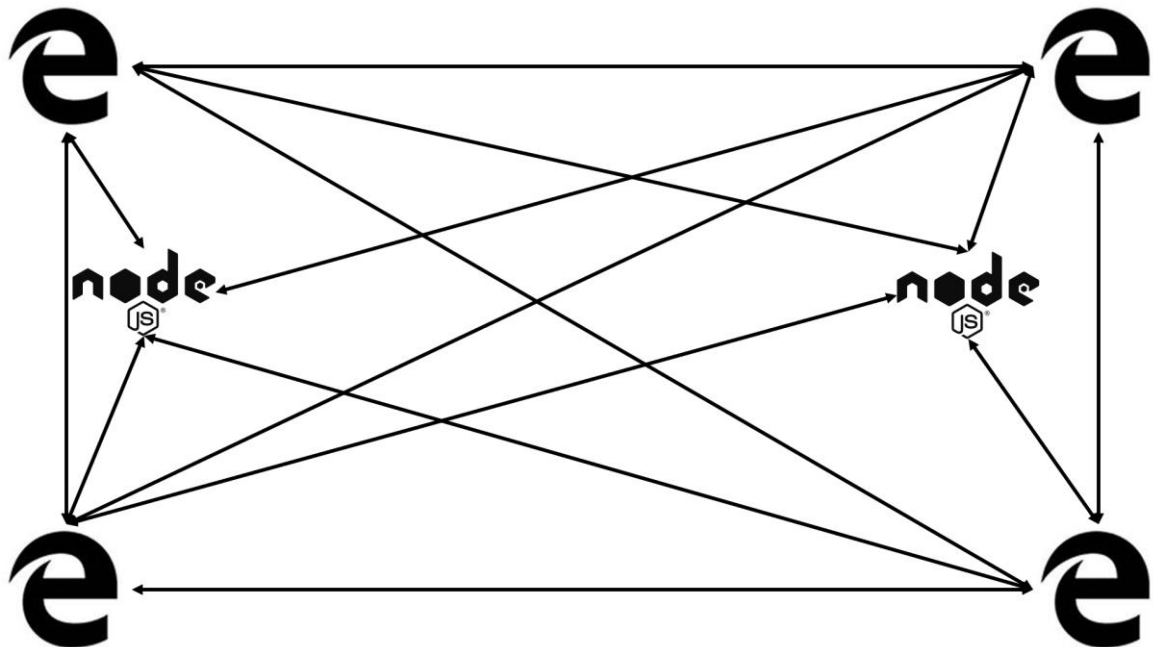
#### **4.7. Peer to Peer Networking**

Peer-to-peer (P2P) networking is a decentralized type of networking in which individual computers or devices are connected to each other directly, without the need for a central server or other intermediaries. In a P2P network, each device functions as both a client and a server, allowing users to share resources and exchange data with one another directly.

One of the main advantages of P2P networking is that it can be more resilient and efficient than traditional client-server networks. Because there is no central server or other single point of failure, P2P networks can continue to operate even if some of the devices within the network go offline. Additionally, P2P networks can be more efficient because the workload is distributed among all of the devices in the network, rather than being concentrated on a single server.

P2P networks are commonly used for a variety of applications, including file sharing, video streaming, and online gaming. Some well-known examples of P2P networks include BitTorrent, which is used for file sharing, and Skype, which is a popular P2P communication tool.

Overall, P2P networking is a powerful and flexible approach to networking that allows devices to connect and share resources directly, without the need for a central server or other intermediaries.



**Figure 7.** Peer-to-Peer Networking Structure.

In this Blockchain, three types of distributed networks are designed. The first one is a peer-to-peer networking system. In this network, no machine is a client or server. Every node is equally connected to all other nodes. Every node contains a partial or complete copy of the Blockchain. Bitcoin uses a peer-to-peer network for transactions.

In figure 7, 'e' represents the browser-type nodes, and the 'node.js' icon refers to relay server-type nodes. Here, every node is connected to other nodes. The advantage of this infrastructure is that it is very cost-efficient. Therefore, there is no hassle of managing a dedicated server. In addition, a few relay servers can be deployed to increase the system's reliability.

On the contrary, the disadvantages are that the data becomes inaccessible if any nodes go to sleep. Also, there is no central authority; everyone has the same power level.



Finally, connecting many nodes drops the performance [20]. This idea makes the networking idea seem inappropriate in this situation.

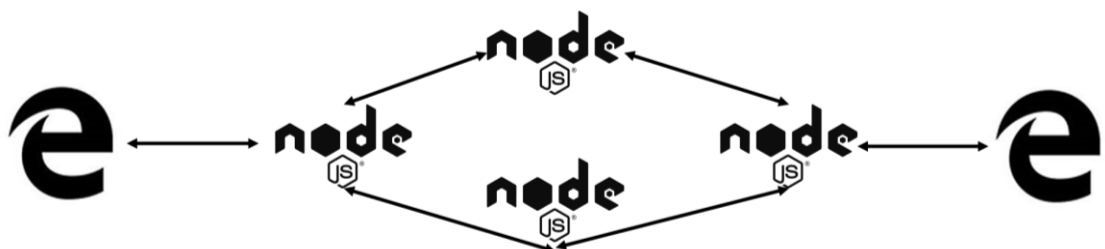
#### 4.8. Real Time Communication (WebRTC)

Real-time communication is the exchange of information between devices in real-time. In web technology, this is often accomplished using WebRTC (Web Real-Time Communication) and WebSocket.

WebRTC is a set of open-source technologies that allow web browsers to communicate directly with each other without the need for an intermediate server. This enables peer-to-peer (P2P) communication, such as video and audio calls, file sharing, and live streaming. WebRTC uses a combination of JavaScript APIs and HTML5 technologies, such as the HTML5 canvas element, to enable real-time communication in the browser.

WebSocket is a protocol that allows for full-duplex communication over a single TCP connection. It allows a web server and a client (such as a web browser) to communicate with each other in real-time, enabling the exchange of data in both directions. WebSocket is often used in conjunction with WebRTC to provide a secure, reliable connection for real-time communication.

Both WebRTC and WebSocket are important technologies for enabling real-time communication in web applications. They provide a way for web browsers to communicate with each other directly, enabling a wide range of real-time communication applications, such as video conferencing, online gaming, and live streaming.



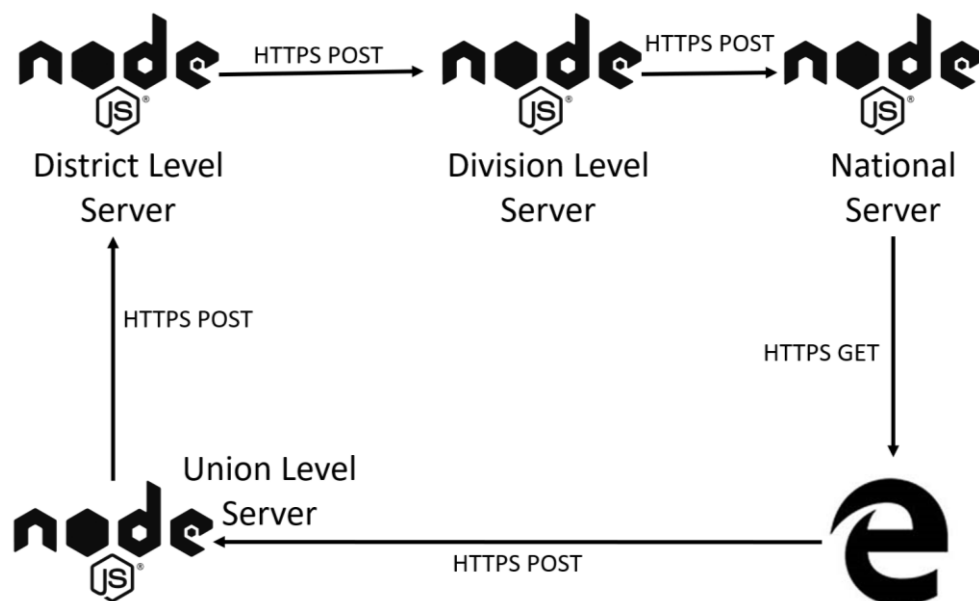
**Figure 8.** Real-time Communication in Distributed Computing.

The next idea behind distributed computing lies in WebSocket, a full-duplex communication channel over TCP/IP protocol. WebRTC (Web Real-time Communication) via application programming interface is introduced by an open-source project to take this one step further. With this technology, backend servers connect and keep the connections alive with each other to listen if any nodes get any changes in the chain. A new block is broadcasted over the network if it is pushed to the chain.

#### 4.9. Disadvantages of Real Time Communication

The disadvantage of this infrastructure is- that real-time communication is a resource-hungry process. Keeping the connection alive back and forth is a tedious task [21]. Moreover, it might not be scalable for a significant level at an affordable operational cost. So, there requires a more efficient solution in this regard.

Then comes the good old HTTPS with a hierarchy structure. The administration infrastructure of Bangladesh is designed on five levels- divisions, districts, sub-districts, unions, and villages. The Government has successfully enhanced high-speed internet connectivity and IT services up to the union level. So, this distributed server design can match Government administrations.



**Figure 9.** Hierarchy-Based Distributed Computing.

In this architecture, after mining a block, it pushes into the nearest union-level Nikah-Nama Blockchain server. That server pushes the block to the upper level. This way, blocks reach the national data center and store copies in local servers concurrently. In this concept, the whole infrastructure can be maintained with low costs efficiently. Connections between servers can be established on demand. Clients requesting data from the network are delivered from the national server.

#### 4.10. Application Development

Developing a scalable application for digital marriage registration is the primary vision of this paper. The client-side and backend of the application have to be designed independently. The data is served from the backend through the secured REST API. So, the client user interfaces can be built with cross-platform support such as Android, Windows, iOS, etcetera. The primary focus is Web UI because it is accessible from the most popular operating systems.

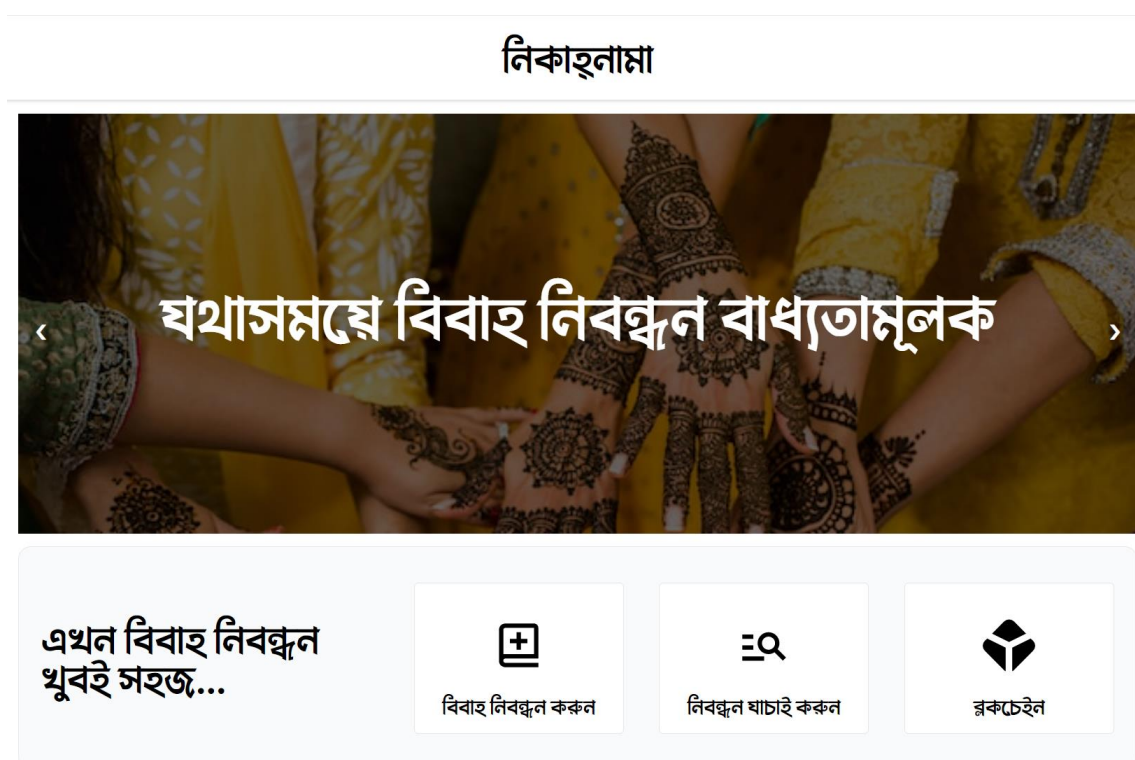


Figure 10. Homepage of Nikah-Nama.

When a user opens the application the homepage will be displayed as shown in the figure 10. The users will be able to navigate through the interrelated options.

Initially, an application form collects necessary information about marriage according to the Muslim Marriage and Divorce (Registration) Rules 2009, Bangladesh [22]. Then, the system uses API to retrieve data from the NID server to verify the identity of every party (bride, bridegroom, witnesses, and Kazi). After submitting this form, the system lets the register mine the hash for adding a block in the proposed Blockchain.

#### **4.11. National Identity Verification**

The Bangladesh National Identity Card, or NID, is a document issued by the government of Bangladesh to its citizens. It is issued by the National Identity Registration Wing of the Bangladesh Election Commission and is used as a form of identification and proof of citizenship. The NID includes personal information about the cardholder, such as their name, photograph, and signature. It is a very important document in Bangladesh and is used for a wide range of purposes, including voting in elections, opening bank accounts, and obtaining government services.

The NID is a crucial document for Bangladeshis, as it allows them to participate in various activities and transactions that require identification. For example, it is necessary to present an NID when voting in elections, as it serves as proof of identity and citizenship. The NID is also often required when opening a bank account, as banks use it to verify the identity of their customers. Additionally, the NID is used to access various government services, such as obtaining a passport or driver's license.

In summary, the Bangladesh National Identity Card is a government-issued identification document that is used by citizens of Bangladesh as proof of identity and citizenship. It is an important document that is used for a variety of purposes, including voting, opening bank accounts, and obtaining government services.

**ডিজিটাল নিকাহনামা**

[বিধি ২৪ (১) (ক) দুফর্ম]  
মুসলিম বিবাহ ও অলাক (নিবন্ধন) বিধিমালা, ২০১৯ এর বিধি ২৪ (১) (ক) অনুযায়ী বিবাহ ফর্ম

বরের জাতীয় পরিচয়পত্রের নম্বর	বরের জন্মতারিখ	ঘাটাইকরণ
৪৬৫৮৫৩৬৩৬৪	০১/০২/২০০০	
বরের নাম	বরের পিতার নাম	বরের মাতার নাম
সারওয়ার আজমাইন রেজা	মোহাম্মদ দেলোয়ার হোসেন	লাজনীন ফেরদাউস
বরের ঠিকানা		
ঢাকা	কিশোরগঞ্জ	কটিয়াদী
	আচমিতা	৯
পূর্ববর্তী ধাপ	পরবর্তী ধাপ	

**Figure 11.** Marriage Registration Form.

After completing a successful registration, couples can instantly download and print their marriage certificate. The certificate contains a QR code. Any entity can verify the authenticity of the certification without any hassle just by scanning it from any device. The Blockchain network verifies the certification by checking whether a specific block exists in the network or not. Couples can also confirm marriage validation to entities like police, guesthouses, or any other by sharing minimum marriage information without exposing potentially sensitive personal data.

## নিকাহনামা

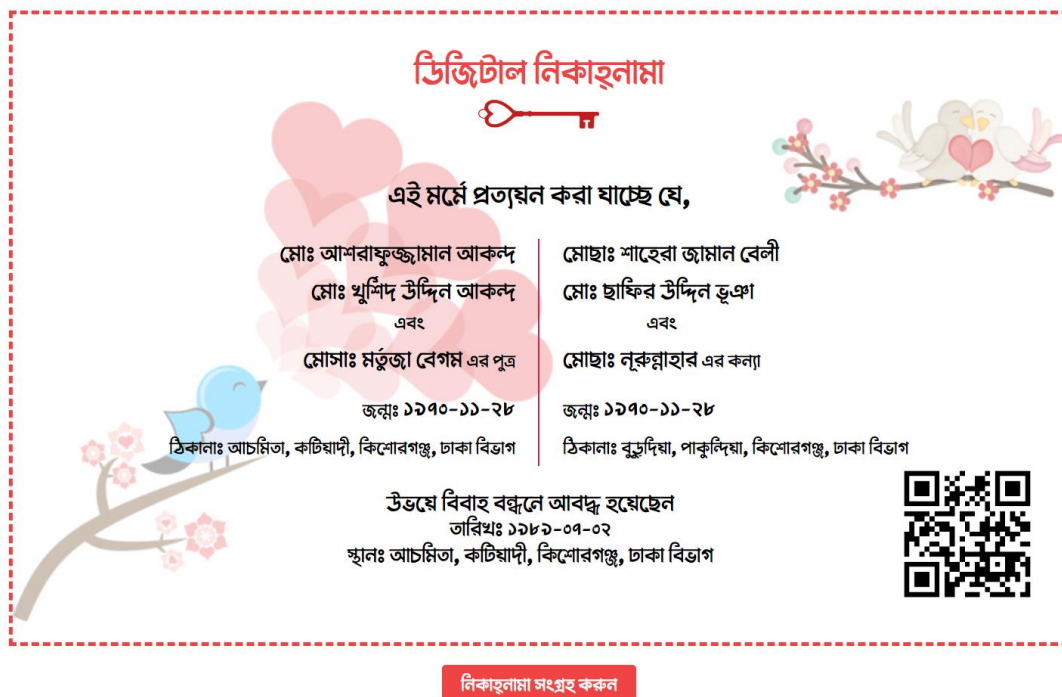


Figure 12. Demo Marriage Certificate

### 4.12. Structure of the Application

Here, the whole system is separated into three sections. They are - the frontend, backend, and the Blockchain.

### 4.13. React

React is a JavaScript library for building user interfaces. It was developed by Facebook, and is often used for building single-page applications and mobile applications.

React allows developers to create reusable UI components, which can significantly improve the developer experience when building complex user interfaces. It also uses a virtual DOM (a lightweight in-memory representation of the actual DOM), which can improve app performance by reducing the amount of DOM manipulation required.

React follows a declarative programming paradigm, meaning that developers describe the desired state of the UI and React takes care of updating the actual DOM to match.

This can make it easier to understand and reason about an application's UI, as the developer only needs to worry about the state of the app, rather than the details of how that state is reflected in the DOM.

With these benefits of React we have chosen this library to develop the client-side of our project.

#### **4.14. Create React App Library**

For the front end, create-react-app is used to build the user interface base. It is a JavaScript library to develop the front end using react.js with minimum effort. It is a comfortable environment to learn React and the best way to start creating new single-page apps in React. Create React App is a tool developed by Facebook that allows users to easily create and set up a React application with no configuration required. To use it, you need to have Node.js and npm installed on your computer.

To create a new React app using Create React App, run the command `npx create-react-app my-app` in your terminal. This will create a new directory called "my-app" with the required files and dependencies to run a React application.

To start the development server, navigate to the new directory and run the following command: `npm start`. This will start the development server and open a new browser window with your React application. You can then start building your application by modifying the files in the "src" directory.

Create React App is a great tool for getting started with React, and it can also be used to build and deploy production-ready applications.

Our application has a very simple interface structure; this library is a perfect fit for this project.

#### **4.15. React Router DOM**

React Router is a library that makes it easy to add routing to a React application. It allows you to define your application's routes declaratively, mapping them to the components that should be rendered when the route is active.

The 'react-router-dom' package provides specific components and hooks for use in browser-based React apps. These include the <BrowserRouter> component, which creates a router object and makes it available to the rest of the app via the context API. The <Link> component is used to create links between routes, and the <Route> component is used to render a specific component when the current URL matches the specified path. The 'useHistory' hook provides access to the history object, which can be used to navigate between routes programmatically.

Overall, React Router is a powerful tool for adding navigation and routing functionality to a React app. It makes it easy to define and manage routes, and provides a variety of features for rendering content based on the current URL and navigating between routes.

We used React Router DOM to implement multiple routes to easily navigate through the interface.

#### **4.16. Firebase Authentication**

Firebase Authentication is a service that allows developers to authenticate users with email and password accounts, phone numbers, and popular third-party identity providers like Google, Facebook, and Twitter. It provides a secure and convenient way for users to sign in to an application, and helps to prevent unauthorized access to protected resources.

One of the main benefits of using Firebase Authentication is that it handles much of the heavy lifting involved in authentication, such as securely storing passwords and handling password reset flows. It also provides a number of pre-built UI components that can be easily integrated into an application, allowing developers to quickly and easily add authentication functionality to their apps.

In addition to traditional email and password authentication, Firebase Authentication also supports federated authentication, which allows users to sign in with a third-party identity provider such as Google, Facebook, or Twitter. This can be especially useful for applications with a large number of users, as it allows them to use an existing account to sign in, rather than creating a new account specifically for the app.



Overall, Firebase Authentication is a powerful and easy-to-use service that can help developers add robust authentication functionality to their applications with minimal effort.

Firebase is used to implement the authentication system with email and password and sign in with google in the project.

#### **4.17. Tailwind CSS**

Tailwind CSS is a CSS framework that makes it easy for developers to create custom user interfaces. It does this by providing a set of low-level utility classes that can be combined to create complex styles. This is different from traditional CSS frameworks, which usually provide a set of pre-designed components that you can use in your application.

One of the benefits of using Tailwind CSS is that it gives you more control over the individual elements of your HTML. This means you can create custom designs that better fit the specific needs of your application, rather than being limited to the design of pre-built components.

Utility-first CSS frameworks like Tailwind CSS can also save you time and effort. They provide a set of ready-made styles that you can use right away, rather than having to write your own CSS from scratch or try to customize the styles of a traditional CSS framework.

Tailwind CSS is used to ensure reasonable customization at the design level. Finally, as a web-based project, JavaScript is utilized to write all the logic to make things functional.

#### **4.18. Node.js**

Node.js is a runtime environment for JavaScript that allows developers to run JavaScript on the server side, outside of a web browser. It is built on the Chrome JavaScript runtime and allows developers to create server-side applications with JavaScript.

One of the main benefits of using Node.js is its ability to handle a large number of concurrent connections with high performance. It uses an event-driven, non-blocking I/O model which makes it lightweight and efficient. This makes it well-suited for real-time applications that require a lot of data streaming, such as chat apps and online games.

Node.js also has a large and active community, with a wealth of third-party packages available through the Node Package Manager (NPM). This makes it easy for developers to find and reuse code, as well as share their own packages with others.

Overall, Node.js is a popular choice for building web applications and APIs due to its performance, versatility, and strong developer community.

From the backend aspect, the cross-platform and open-source JavaScript runtime environment Node.js is in action.

#### **4.19. Express.js**

In addition, another open-source server framework, Express.js, is used to build APIs to communicate with the Blockchain.

Express.js is a fast, minimalist web framework for Node.js. It is designed to simplify the process of building scalable web applications by providing a robust set of features for routing, middleware, and handling requests and responses.

One of the key benefits of using Express.js is that it allows developers to build APIs quickly and easily. It includes a number of built-in middleware functions that make it easy to parse incoming request data, handle file uploads, and serve static files. It also supports the use of third-party middleware, allowing developers to extend the functionality of their application with minimal effort.

Another advantage of Express.js is that it is highly flexible and customizable. It is designed to be used as a standalone web framework, or as a layer in a larger application stack. It can be paired with popular libraries like MongoDB and Socket.io to build powerful full-stack web applications.

Express.js is a popular choice for building web applications due to its simplicity, performance, and flexibility. Its comprehensive feature set and robust ecosystem of plugins and middleware make it a powerful tool for building scalable, high-performance web applications.

This is why we have chosen Express.js to build the Application Programming Interface (API) to communicate with the Blockchain.

#### **4.20. Progressive Web Application (PWA)**

Progressive Web Application (PWA) is a type of application software that is built using web technologies and can be run on various devices, including smartphones, tablets, and desktop computers. The main goal of a PWA is to provide a native app-like experience to users, but without the need to download and install an app from an app store.

One of the key features of a PWA is that it can be accessed through a web browser, just like any other website. This means that users can simply visit the URL of the PWA and start using it, without the need to go through any additional installation process. This can be particularly convenient for users who don't have access to an app store, or who don't want to clutter their device with too many apps.

Another important characteristic of PWAs is that they are designed to work offline or with low-quality internet connections. This is achieved through the use of caching and other techniques that allow the PWA to store a copy of its content on the user's device. This way, the PWA can still be used even when the device is not connected to the internet, or when the connection is slow or unstable.

Overall, PWAs offer a convenient and seamless way for users to access and use web-based apps on a variety of devices. They combine the best features of native apps and traditional websites, making them a popular choice for developers and businesses looking to reach and engage with their users in the digital world.

We generated a PWA of our system so that it can be accessed with any device with any operating system. It will give native experience without developing native applications for different platforms.

#### **4.21. Blockchain Deployment**

The pilot Blockchain can be hosted on a remote node at the Blockchain part. Later, any number of new nodes can be connected with that node. First, a secure HTTPS connection is established over the internet by completing the authentication process. After that, the new node is instantly decrypted from the latest state of the Blockchain. Every individual block of the Blockchain contains a single Nikah-Nama. The Blockchain architecture is developed according to the discussed workflow.

## Chapter 5: Extended Work & Future Plan

In this project, there is much room for work and future updates. This system is also scalable to related work fields.

Anil Narasipuram married Shruti Nair in the first Blockchain wedding in India [23]. Nowadays, the metaverse allows couples to marry and own the NFT-based marriage certificate. It immortalizes their love on the Blockchain forever. The system can be customized to offer couples to hold their Nikah-Nama as a Non-Fungible Token (NFT). This NFT can be showcased in the metaverse world.

We are also willing to crack down on severe social issues and generate digitally verifiable marriage certificates. However, from a commercial perspective, it is an untapped market in Bangladesh. Couples can also demand a hard copy of their Nikah-Nama beautifully designed custom templates in different sizes and forms. The creation will be delivered to their doorstep.

## **Chapter 7: Conclusion**

This paper discusses an experimental blockchain prototype that maintains the immutability of marriage data. It is expected to have lackings and potential bugs at any level. Although having these drawbacks, the model of the system can be implemented nationally and globally. The Bangladesh government can expertly develop this infrastructure to keep digital marriage records inside the border. These data are intended to be stored in a decentralized private network. Citizens will be able to access their marriage information securely anytime. This system will reduce the annoyance and exertion of processing the paperwork and verifying the legal records of marriage. This system will help to reduce social misconduct like marriage without informing present wives, marriage without divorce, marrying with a disguised identity, etcetera, which happens often. Bangladesh will be able to ensure the social security of its citizens and save valuable work time by avoiding primitive methods and adapting to emerging technologies.

## References

- [1] Counsels Law Partners, "MARRIAGE & DIVORCE IN BANGLADESH: EVERYTHING YOU NEED TO KNOW," counselslaw.com (CLP), 16-Oct-2019. [Online]. Available: <https://www.counselslaw.com/marriage-divorce-in-bangladesh-everything-you-need-to-know/>. [Accessed: 29-Sep-2022].
- [2] "The Muslim Marriages and Divorces (Registration) Act, 1974," Gov.bd. [Online]. Available: <http://bdlaws.minlaw.gov.bd/act-details-476.html>. [Accessed: 29-Sep-2022].
- [3] Staff Correspondent, "Trial against cricketer Nasir, 'wife' Tammi begins," daily-bangladesh.com, 09-Feb-2022. [Online]. Available: <https://m.daily-bangladesh.com/english/Trial-against-cricketer-Nasir-wife-Tammi-begins/69310>. [Accessed: 29-Sep-2022].
- [4] "Seven women claim to be Rubel's wife, wait at morgue," The Daily Observer. [Online]. Available: <https://www.observerbd.com/details.php?id=379420>. [Accessed: 29-Sep-2022].
- [5] Channel, "অপ্রাপ্তবয়স্ক মেয়ের বিয়ের গাড়ি আটকে হতবাক প্রশাসন | Cox's Bazar News | Channel 24," 10-Sep-2022. [Online]. Available: <https://www.youtube.com/watch?v=WfwMXupMHGc>. [Accessed: 29-Sep-2022].
- [6] N. Elysha Kamaruzaman et al., "Blockchain technology for an Islamic marriage certificate," Int. j. eng. technol., vol. 7, no. 4.11, p. 193, 2018.
- [7] A. Marthews and C. E. Tucker, "Blockchain and identity persistence," SSRN Electron. J., 2019.
- [8] R. Ghazali et al., "Blockchain for record-keeping and data verifying: proof of concept," Multimed. Tools Appl., 2021.
- [9] N. Asfour, "Role of blockchain and smart contracts in transforming social contracts," İbn Haldun Üniversitesi, Lisansüstü Eğitim Enstitüsü, 2019.
- [10] E. Sisák, "Smart marriage contracts: The future of blockchain in matrimonial property law?," Zb. Pravnog fak. Sveučilišta u Rijeci, vol. 42, no. 3, pp. 657–676, 2021.
- [11] R. Duchemin, "Blockchain technology for data management of research data: A systematic review and proposed research design," 2018
- [12] R. Vidhyuth and T. Manoranjitham, "A study of blockchain technology on securing the personal health record," Palarch.nl. [Online]. Available: <https://archives.palarch.nl/index.php/jae/article/download/4714/4660/9024>. [Accessed: 05-Sep-2022].

- [13] "Bangladesh - Data Protection Overview," DataGuidance, 19-Jul-2022. [Online]. Available: <https://www.dataguidance.com/notes/bangladesh-data-protection-overview>. [Accessed: 29-Sep-2022].
- [14] "History of Blockchain," www.javatpoint.com. [Online]. Available: <https://www.javatpoint.com/history-of-blockchain>. [Accessed: 29-Sep-2022].
- [15] J. Ducreé, "Satoshi Nakamoto and the Origins of Bitcoin -- The Profile of a 1-in-a-Billion Genius," 2022.
- [16] "Unix Time Stamp - Epoch Converter," Unixtimestamp.com. [Online]. Available: <https://www.unixtimestamp.com/>. [Accessed: 29-Sep-2022].
- [17] Patrick, "What Is SHA-256 And How Is It Related to Bitcoin?," Mycryptopedia, 24-Apr-2022. [Online]. Available: <https://www.mycryptopedia.com/sha-256-related-bitcoin/>. [Accessed: 29-Sep-2022].
- [18] "Blockchain Proof of Work - Javatpoint," www.javatpoint.com. [Online]. Available: <https://www.javatpoint.com/blockchain-proof-of-work>. [Accessed: 29-Sep-2022].
- [19] C. Faife, "Bitcoin Hash Functions Explained," CoinDesk, 19-Feb-2017. [Online]. Available: <https://www.coindesk.com/markets/2017/02/19/bitcoin-hash-functions-explained/>. [Accessed: 29-Sep-2022].
- [20] 'Peer-to-Peer Network: advantages and disadvantages,' Teach-ict.com. [Online]. Available: [https://www.teach-ict.com/gcse\\_new/networks/peer\\_peer/miniweb/pg5.htm](https://www.teach-ict.com/gcse_new/networks/peer_peer/miniweb/pg5.htm). [Accessed: 19-Dec-2022].
- [21] Marco, "Opportunities and Drawbacks of WebRTC," Marco, 25-Sep-2014.
- [22] "মুসলিম বিবাহ ও তালাক (নিবন্ধন) বিধিমালা, ২০০৯ (সংশোধন ২০১১)," দলিল সেবা, 10-Apr-2011. [Online]. Available: <https://dolil.com/gazettes/muslim-marriage-and-divorce-registration-rules-2009-amendment-2011/>. [Accessed: 05-Sep-2022].
- [23] M. Khanna, "How India's first couple got married on the blockchain: This is how they did it," India Times, 08-Feb-2022. [Online]. Available: <https://www.indiatimes.com/technology/news/india-first-couple-marriage-on-blockchain-561474.html>. [Accessed: 05-Sep-2022].



ORIGINALITY REPORT

6%

SIMILARITY INDEX

5%

INTERNET SOURCES

2%

PUBLICATIONS

3%

STUDENT PAPERS

PRIMARY SOURCES

1	Submitted to King Abdulaziz University Student Paper	2%
2	link.springer.com Internet Source	1%
3	hrcak.srce.hr Internet Source	1%
4	Syed Akhter Hossain, Lora Annanya Biswas, Md Iqbal Hossain. "Analysis of Bangla-2-Braille machine translator", 2014 17th International Conference on Computer and Information Technology (ICCIT), 2014 Publication	1%
5	acikerisim.ihu.edu.tr Internet Source	1%
6	Nor Elysha Kamaruzaman, Ihsan Mohd Yassin, Azlee Zabidi, Fadhlan Hafizhelmi Kamaru Zaman et al. "Blockchain Technology for Islamic Marriage Certificate", International Journal of Engineering & Technology, 2018 Publication	1%