Intelligent Control and Automation, 2022, 13, 39-53
https://www.scirp.org/journal/ica
ISSN Online: 2153-0661
ISSN Print: 2153-0653

Blockchain-Based Islamic Marriage Certification with the Supremacy of Web 3.0

Md. Al-Sajiduzzaman Akand, Sarwar Azmain Reza, Amatul Bushra Akhi

Department of Computer Science & Engineering, Daffodil International University, Dhaka, Bangladesh
Email: sajiduzzaman15-2484@diu.edu.bd, sarwar15-2562@diu.edu.bd, akhi.cse@diu.edu.bd

How to cite this paper: Akand, Md.A.-S., Reza, S.A. and Akhi, A.B. (2022) Blockchain-Based Islamic Marriage Certification with the Supremacy of Web 3.0. *Intelligent Control and Automation*, **13**, 39-53.
https://doi.org/10.4236/ica.2022.134004

Received: November 12, 2022
Accepted: November 27, 2022
Published: November 30, 2022

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 Nikah-Nama 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.

Keywords

Blockchain, Cryptography, Digital Signature, Distributed Computing, Data Encryption

1. Introduction

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. As a result, Government agencies and other security-enthusiastic companies are adopting this technology rapidly in diverse domains.

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.

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 that block's 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.

On the other hand, marriage data recording deserves this 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.

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. 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].

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.

1.1. Related Works

1.1.1. Blockchain Technology for Islamic Marriage Certificate

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. They built a user interface that takes information as required and stores it in the Smart Contract deployed inside the Blockchain system.

1.1.2. 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.

1.1.3. 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.

1.1.4. 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.

1.1.5. Smart Marriage Contracts: The Future of Blockchain in Matrimonial Property Law?

Ľ. 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.

1.1.6. 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 data management of research data and evaluates whether or not 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 immutabil-

ity, and time stamping features can improve research data quality.

1.1.7. Blockchain Technology for Data Management of Research Data

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.

1.2. 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 type of 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 tide of 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 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.

2. Methodology

Although Blockchain started to gain popularity in 2016, the concept was first in-

troduced 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.

The system of Nikah-Nama Blockchain is designed according to the architecture shown in **Figure 1**.

2.1. Block Formation

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

As shown in **Figure 2**, 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

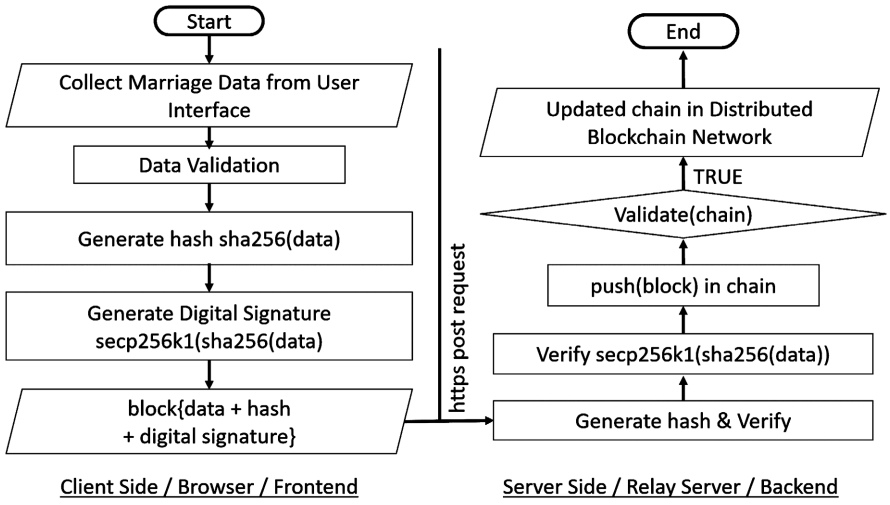

Figure 1. Nikah-nama blockchain architecture.

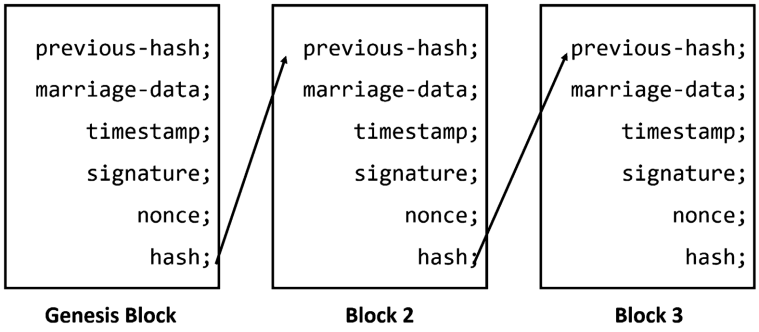

Figure 2. Blockchain formation.

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. SHA-256 belongs to the SHA-2 hash algorithm family, which is the most popular one. Bitcoin also uses the same algorithm for hashing [17]. SHA-512 ensures the system is more secure but takes up more space.

The system 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.

As shown 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

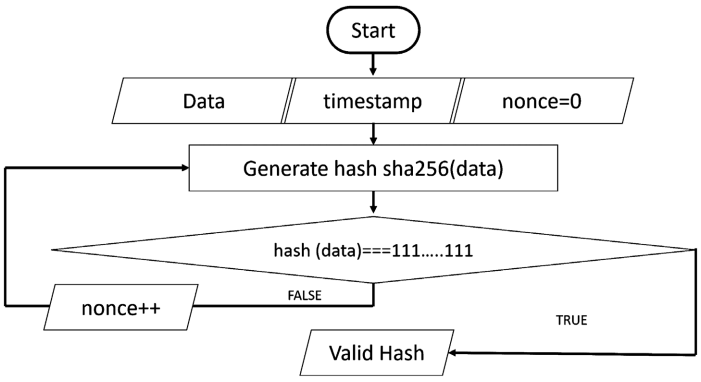

Figure 3. Proof-of-work concept.

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.

2.2. Blockchain Architechture

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.

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.

As shown in **Figure 5**, 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 is generated again and verifies 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.

2.3. Backing Up the Blockchain

The Blockchain is built on runtime and stored in the machine's Random Access

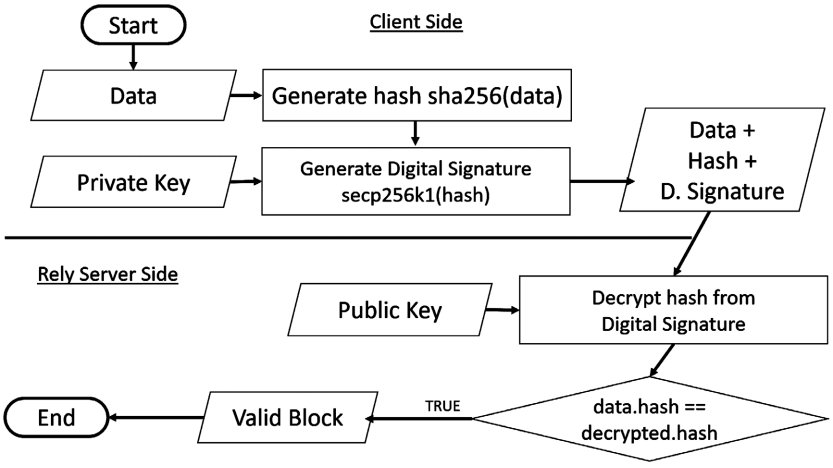

Figure 4. Digital signature mechanism.

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.

As shown in Figure 6, 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,

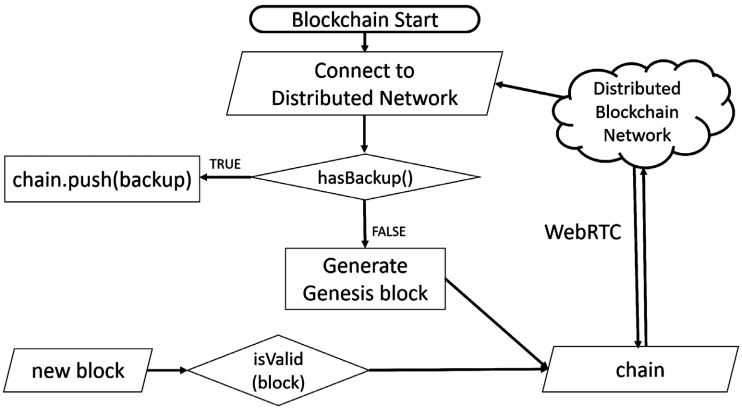

Figure 5. Nikah-nama blockchain prototype.

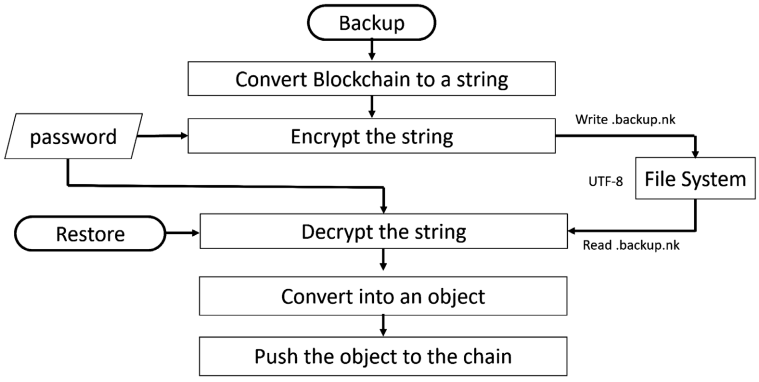

Figure 6. Backup management.

which prevents Blockchain forgery.

2.4. 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.

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.

As shown 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. 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.

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. As shown in Figure 8, 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. If a new block is pushed to the chain, it is broadcasted over the network.

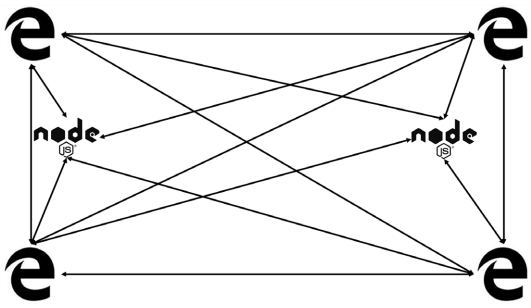

Figure 7. Peer-to-peer networking.

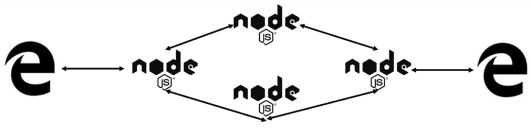

Figure 8. Real-time communication in distributed computing.

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]. 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.

The architecture shown in **Figure 9**, after mining a block, the system 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.

2.5. 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.

When a user opens the application, the homepage will be displayed, as shown in **Figure 10**. Users will be able to navigate to interrelated options.

Initially, as shown in **Figure 11**, an application form collects necessary information about marriage according to the Muslim Marriage and Divorce (Registration) Rules 2009, Bangladesh [22]. The system uses an Application Programming Interface (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.

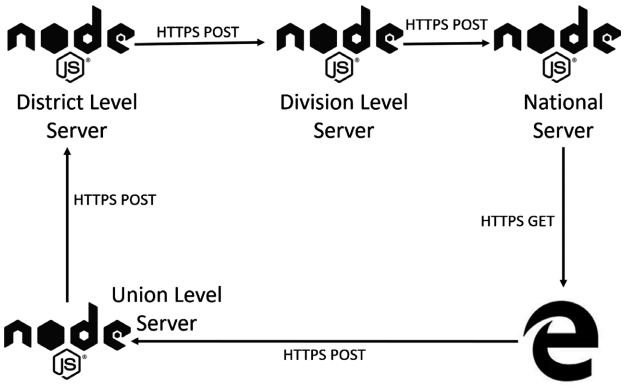

Figure 9. Hierarchy-based distributed computing.

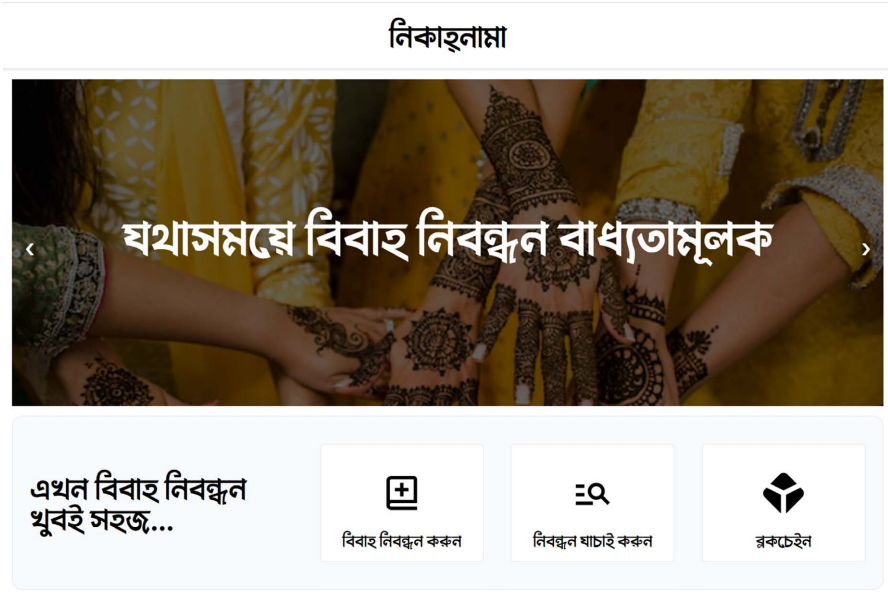

Figure 10. Homepage of Nikah-Nama.

Figure 11. Marriage registration form.

After completing a successful registration, couples can instantly download and print their marriage certificate, as shown in Figure 12. 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.

Here, the whole system is separated into three sections. They are the frontend, backend, and the Blockchain. 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. A utility-first CSS framework named Tailwind

Figure 12. Demo marriage certificate.

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

From the backend aspect, the cross-platform and open-source JavaScript runtime environment Node.js is in action. Another open-source server framework, Express.js, is used to build APIs to communicate with the Blockchain.

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. 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.

3. 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. 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.

4. 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.

Conflicts of Interest

The authors declare no conflicts of interest regarding the publication of this paper.

References

[1] Counsels Law Partners (2019) Marriage & Divorce in Bangladesh: Everything You Need to Know. https://www.counselslaw.com/marriage-divorce-in-bangladesh-everything-you-need-to-know

[2] The Muslim Marriages and Divorces (Registration) Act, 1974. Gov.bd. http://bdlaws.minlaw.gov.bd/act-details-476.html

[3] Staff Correspondent (2022) Trial against Cricketer Nasir, "Wife" Tammi Begins. https://m.daily-bangladesh.com/english/Trial-against-cricketer-Nasir-wife-Tammi-begins/69310

[4] Seven Women Claim to Be Rubel's Wife, Wait at Morgue. *The Daily Observer*. https://www.observerbd.com/details.php?id=379420

[5] Channel (2022, September 10) Administrations Left Speechless after Detaining Wedding Car of a Minor Girl|Cox's Bazar News|Channel 24. https://www.youtube.com/watch?v=WfwMXupMHGc

[6] Kamaruzaman, N.E., *et al.* (2018) Blockchain Technology for an Islamic Marriage Certificate. *International Journal of Engineering & Technology*, **7**, 193. https://doi.org/10.14419/ijet.v7i4.11.20802

[7] Marthews, A. and Tucker, C.E. (2019) Blockchain and Identity Persistence. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3316088

[8] Ghazali, R., *et al.* (2021) Blockchain for Record-Keeping and Data Verifying: Proof of Concept. *Multimedia Tools and Applications*, **81**, 36587-36605. https://doi.org/10.1007/s11042-021-11336-7

[9] Asfour, N. (2019) Role of Blockchain and Smart Contracts in Transforming Social

Contracts. İbn Haldun Üniversitesi, Lisansüstü Eğitim Enstitüsü.

[10] Sisák, Ľ. (2021) Smart Marriage Contracts: The Future of Blockchain in Matrimonial Property Law? *Zbornik Pravnog fakulteta Sveučilišta u Rijeci*, **42**, 657-676. https://doi.org/10.30925/zpfsr.42.3.4

[11] Duchemin, R. (2018) Blockchain Technology for Data Management of Research Data: A Systematic Review and Proposed Research Design.

[12] Vidhyuth, R. and Manoranjitham, T. (2020) A Study of Blockchain Technology on Securing the Personal Health Record. *Palarch's Journal of Archaeology of Egypt/Egyptology*, **17**, 12272-12283. https://archives.palarch.nl/index.php/jae/article/download/4714/4660/9024

[13] Bangladesh—Data Protection Overview. DataGuidance, 19-July-2022. https://www.dataguidance.com/notes/bangladesh-data-protection-overview

[14] History of Blockchain. https://www.javatpoint.com/history-of-blockchain

[15] Ducrée, J. (2022) Satoshi Nakamoto and the Origins of Bitcoin—The Profile of a 1-in-a-Billion Genius.

[16] Unix Time Stamp—Epoch Converter. https://www.unixtimestamp.com

[17] Patrick. What Is SHA-256 and How Is It Related to Bitcoin? https://www.mycryptopedia.com/sha-256-related-bitcoin

[18] Blockchain Proof of Work. https://www.javatpoint.com/blockchain-proof-of-work

[19] Faife, C. (2017, February 19) Bitcoin Hash Functions Explained. https://www.coindesk.com/markets/2017/02/19/bitcoin-hash-functions-explained

[20] Computer Science Learning for School Students. https://www.teach-ict.com/gcse_new/networks/peer_peer/miniweb/pg5.htm

[21] Marco. Opportunities and Drawbacks of WebRTC. Marco, 25-Sep.-2014.

[22] The People's Republic of Bangladesh, 'Muslim Marriage and Divorce (Registration) Rules, 2009', Aug. 2009. https://dolil.com/gazettes/muslim-marriage-and-divorce-registration-rules-2009-amendment-2011

[23] Khanna, M. (2022, February 8) How India's First Couple Got Married on the Blockchain: This Is How They Did It. *India Times*. https://www.indiatimes.com/technology/news/india-first-couple-marriage-on-blockchain-561474.html