Secure Web-Based System to Find Life Partner Based on Blockchain Technology under Islamic legislation

Ayman Alharbi†, Mawaddah AlHarbi†, Arwa AlMelibari†   and Haya AlAgil†

aarharbi@uqu.edu.sa   s43980131@st.uqu.edu.sa   s43980126@st.uqu.edu.sa   s43980121@st.uqu.edu.sa

† Umm Al-Qura University, Collage of Computer and Information Systems, Mecca KSA

Summary

Marriage is the foundation of society and family life. In our society, due to the difficulties that some people face when they are trying to find the appropriate life partner, because of the lack of finding the desired partner, the high cost of a third party finding the qualified person who usually does not meet the person's expectations. To the best of our knowledge, our proposed system is the first of its kind to act as a platform for those who wish to get married, by providing their information and the needed specifications with a high level of privacy, confidentiality, and the guarantee of the individual's honesty based on blockchain technology. Besides, the usage of the Advanced Encryption Standard (AES) algorithm secures users' images, which gives the user the trust to use the system and to support the authentication process. Images are processed by multiple image processing techniques to ensure that each image is accepted by both the Islamic and the public morals. The fact that this proposed system serves the community by its work.

Key words: Blockchain, Smart Contract, distributed ledger, AES.

1. Introduction

Righteous and Valid marriage is an essential matter in all aspects of life. It is a valuable step in the process of creating a loving family, and a healthy relationship that can sustain forever.

With respect to marriage in Islam, Legal relationship between a man and a woman is a marriage which is like a contract between two parties, that has different types of conditions must be met. Such Conditions required to initiate the contract: the presence of the guardian or representative (wali) of the woman, at least two non-discredited witnesses, and the dowry given to the woman from the man (mahr).

Considering the bride guardian's approval i.e. the father or representative (wali) of the woman. The groom and the bride must agree to marry with their own free will. The Valid marriage in Islam has a formal mandatory contract which usually be on a paper and might also be a verbal. This contract summarizes groom and bride rights and responsibilities.

Therefore, The Islamic marriage contract contains four basic signatures that considered to be the conditions of completing this contract. Which is groom's signature, the bride, the guardian of the bride, the first witness, and the second one.

Despite the sanctity of marriage association, the correlation process may permeate numerous manipulations and problems, for example, lack of credibility between the parties, or the presence of a third party that may leak some sensitive information of the parties involved in the association.

In Arab societies, some people act as a third party in the process of marriage, where there could be exploiting for the men's need for marriage so that they provide them higher fees for the provided services. The man usually lists the specifications of the desired bride, then the third party displays some samples for the man to choose the suitable one.

This third party may deceive the concerned parties, manipulate their information, or leak it for any purpose.

As a result, this may endanger the reputation of the parties involved in the marriage association. Hence the idea of employing a modern technology that regulates the selection process of a life partner resulting in higher privacy, secrecy, and confidentiality of the information of the parties concerned without the need for an intervention of a third-party.

More recently, distributed ledger technologies such as Blockchain and its endless possibilities have been used to record different sorts of data on a global scale in a decentralized form.

Blockchain technology stands out as a presented solution to this task of uniting life partners across the world.   It can be used as a unified system to create a decentralized and transparent global marriage registry portal which not only transforms the institution of marriage but also provides a high level of security by allowing the couple to specify the extra conditions as per their marriage contracts.

This paper is divided into seven sections as follows: Literature Review, Preliminaries, Proposed System, Research Framework, Challenges, System Considerations, Conclusion, And Future Work.

2. LITERATURE REVIEW

Many authors have proposed several different systems based on the blockchain technology to serve various aspects of life such as an electronic voting systems, a health care, an e-commerce, and an e-government, but there was not any research that serves the marriage by finding the suitable life partners using such technique.

In this section, Systems that are related to our proposed system will be presented.

There are Numerous authors who proposed different secured systems based on blockchain:

In [1] they proposed an electronic voting system based on blockchain, that utilizes smart contracts to provide secure and cost-efficient electing while insuring voters privacy, they are using an Ethereum private blockchain, that have a possibility to send hundreds of transactions per second onto the blockchain, the authors employ the blockchain to enhance the security of a nationwide election. In [2] The authors provide a theoretical research of a proposed E-government System based on the blockchain can solve interoperability issues between the government departments and raise the security and privacy of an individual's data.

In [3] the authors provide the solution of privacy concern of the medical data by taking advantage of using blockchain technology such as a hash chain with the features of verifiability, privacy, decentralization, and immutability, blockchain technology guarantees the secured storage of personal medical data. [4] The rises of smart contract in different areas ranging from finances, E-voting - healthcare, energy, to life sciences. The smart contract became one of the most desirable technologies because of the high level of privacy that is provided to transactions. In [5] the authors proposed a system to manage the package delivery based on the blockchain infrastructure. The proposed system has an ability to control the problems of the current centralized System such as verification and Manipulation of data. They found that Using the blockchain technology has benefits, it enhances security, data integrity, and verifies both users and data.

Through research and exploration, we found that there are not any academic studies to facilitate marriage using blockchain, so we took the lead to propose our secure web-based system to Find Life Partner Based on Blockchain Technology.

In the west, many social networks help users to create relationships such as Tinder.com and Match.com those sites designed to assist single people to seek for relationships and love. but our site has a different goal, we target people who seek honesty relationships for marriage applying Islamic laws, so we choose to build this site based on blockchain and some Images processing techniques to guarantee that.

3. PRELIMINARIES

3.1 Blockchain and Marriage

Blockchain is mainly intended to exchange assets securel without any middlemen. The chain grows with verified information. Every new transaction creates a new block and each block has its attached hash value which makes the blocks immutable.

In the blockchain, decentralized distributed databases are used to keep consistency of stored transactions.

Some technologists call the blockchain as the essential technological building block which could revolutionize big data, healthcare, marriage, currency and other things.

Marriage via Blockchain is not an idea that emerged today, where readings in the topic tells that the first couple to get married based on the blockchain was David Mondrus serial entrepreneur, Bitnation advisor and Joyce Bayo took place on the 5th of Oct 2014 at Disney World, Bitcoin Conference, Florida. Their marriage oath was *"Life is not eternal, and death can separate us but blockchain is forever"*. They engraved their wedding on the bitcoin blockchain.

Susane Tarkowski Tempelhof got married to James Fennel Tempelhof on Blockchain in 2016.

This technology can make the process of finding the life partner easier and hassle free as well. Anyone can register marriage on a global public ledger without the need for a middleman.

3.2 Blockchain Technology

The blockchain is an open and distributed peer to peer mechanism used as data storage, it is defined as a storage technique designed to protect the transactions by keeping the record that occurred between parties in a constant and verifiable method [8].

blockchain technology is a peer-to-peer process without an intermediate agency to validate the transaction [11], it designed in a way that enhances security, this design allows the records to be stored on different interconnected computers. Therefore, the storage of data is not required with third parties.

Although blockchain technology has been created as the cryptographic foundation of bitcoin virtual currency, the power of blockchain is not restricted to a financial field. it involves other fields of applications such as E-voting, healthcare, and new digital identity [11].

As a result of used Blockchain technology, business activities can be achieved in an inexpensive and fast method. Moreover, the stability of blockchains also assures the distributed trust since it is nearly impossible to manipulate with any transactions stored in blockchains and all the historical transactions are auditable and traceable [12].

Based on blockchain restrictions there are two different types of the blockchain (public and private). A public blockchain is less restricted; it can be readable and writable for all users of

the networks. This type is widespread for cryptocurrencies such as bitcoin, Ethereum.

As for A private blockchain is more restricted, it determines who can read or react with the blockchain. The blockchain provides many services such as cryptocurrencies as well as it provides a platform for building distributed and immutable smart contracts.

3.3 Ethereum Blockchain

Since the 1990s the Trend towards the idea of smart contracts, but the blockchain has been transformed the concept of smart contracts to reality especially by Ethereum blockchain [13].

Ethereum applications have the ability to store several information in the network of blockchain, just like that it provides a public distributed ledger for transactions.

Simply, Ethereum is a platform used for involving information across the globe which cannot be manipulated or modified.

It enables the user to develop, build and deploy decentralized applications such as smart contracts.

The reasons for choosing public blockchains such as Ethereum can be summarized as follows [13]:

1- it helpful for managing the automatic payments that are we need in (mahr) transformation from the groom to the bride.

2- Ethereum provide secure trust between the parties.

useful for managing automatic payments with existing crypto-currencies or when there is a need to secure trust between the parties.

3.4 Smart Contract

Smart contracts are similar to conventionally written contracts, it can be defined as programmable contracts that can be executed automatically when their Conditions are met, it can be used as a direct Legal agreement between the parties without an intervention of a third party.

The smart contract protects the involved parties by ensuring that the clearance of terms of the agreement, and the expected penalties the agreed will not happen. The contract is trustable because it is visible to all blockchain users ، which facilitates the verification process.

The smart contract provides security of transactions, avoids conflict and protects the party's possessions, furthermore, enhances the efficiency, reduces the risks and saves the cost.

The smart contract contains various codes and functions for decision making, and then the cryptocurrencies are sent to others.

Since the smart contract is implemented within the blockchain so, it possesses its properties, such as:

Immutability: It can never be modified by anyone.

Distribution: any attempting to tamper the contract will inform all participants to the contract, then they will mark it as an invalid contract.

4. PROPOSED SYSTEM

At this time, there are many websites that concern this issue but missing privacy, credibility, and honesty. Exploiting the needs of the person, profiteering, and misuse of the personal information of their customers. Based on the previously mentioned points, we propose a Secure web-based System to find a life partner based on Blockchain technology, this system provides a contribution to the international Muslim community.

The usage of blockchain keeps users' information private and guarantees the individuals honesty. In addition, the usage of different image processing techniques to support the authentication and guarantee that the entered images are accepted by Islamic and public morals.

Our system aims to provide a high level of privacy, trust, security and safe information sharing for the user. This effective technology ensures many important properties for the user such as anonymity, privacy protection and non-repudiation that makes it an attractive alternative to existing systems.

The system aims to build a new concept which serves the community in a very safe, within the limits of Islamic Laws. To ensure confidentiality within the system to gain the customer trust for all parties involved. The system satisfies customers' needs by applying a high level of security using the technology of blockchain, such technology keeps the secrecy of the information, as a result, unauthorized access is prevented. In addition to preventing information manipulation.

The system consists of five phases:

- *phase 1: registration and Authentication*

our proposed System allows various users to register [bride, groom, witness، guardian] each user must register with his essential correct information such as [real name, national ID, phone number] in this stage we propose to connect the system with e-governance System such as [Absher] in Saudi Arabia to Authenticate the user information this stage will guarantee the user's honesty. Furthermore, guarantees the accuracy of information about the guardian in terms of relationship type between him and the bride. The witness must be male, Muslim, wise, adult, fair. Both bride and groom must register with their essential information also and in this stage, the system will guarantee the confidentiality of the information, also the bride must indicate to her guardian profile.

In addition, the groom must deposit to his account the amount of the dowry as a cryptocurrency in the system to ensure his honesty.

At this stage, the system allows users to fill their profiles information among three privacy levels as followed:

1- ***first level:*** is a piece of public information such as (username, gender, nationality, age, his specifications, partner's specifications), this level of information is available to be viewed by anyone who visits the user profile.

2- second level: it is a more private information such as (a brief description of more private information, and a personal picture)
this type of information is available to the user after requesting connection, and only appears upon approval.

3- The last level of the information contains contact information such as [the full name, mobile number, and location]. This type of information is the critical and private information, due to the fact that this level appears upon acceptance by both partners for the two previous levels.

Phase 2: System recommendations of matched profiles based on profiles comparison.
System offers matched profiles, which allows the user to go through the provided profiles and send a connection request in case the required specifications are met. The request is sent to the second party as an invitation to visit the first party's profile.

Phase 3: After initial approval, the parties are able to share their personal information such as their shading images, in this stage, we proposed a combination of two algorithms:

The benefits of this combination are keeping the images valid in accordance with Islamic law and free from moral transgressions, which we will discuss in detail the processes applied on images in the section[V].

Phase 4: If the parties accept each other, they can share their last level of information such as their contact info.
In our proposed system, the smart contract will be issued after conditions are met, i.e. it must have approval from five accounts [groom - the bride - guardian - and two different witnesses] then accept to release the cryptocurrencies from man wallet to woman wallet considered as dowry and the smart contract will be issued as a Marriage certificate.

4.1 The Interaction Between Users in Blockchain

In peer-to-peer network, the blockchain is a public, distributed and decentralized ledger technology. It stores and verifies data in linked block structure.
The free communication between the blockchain nodes is responsible for the peer-to-peer network, where the linked nodes are geographically scattered, but evenly concurrent in the application.
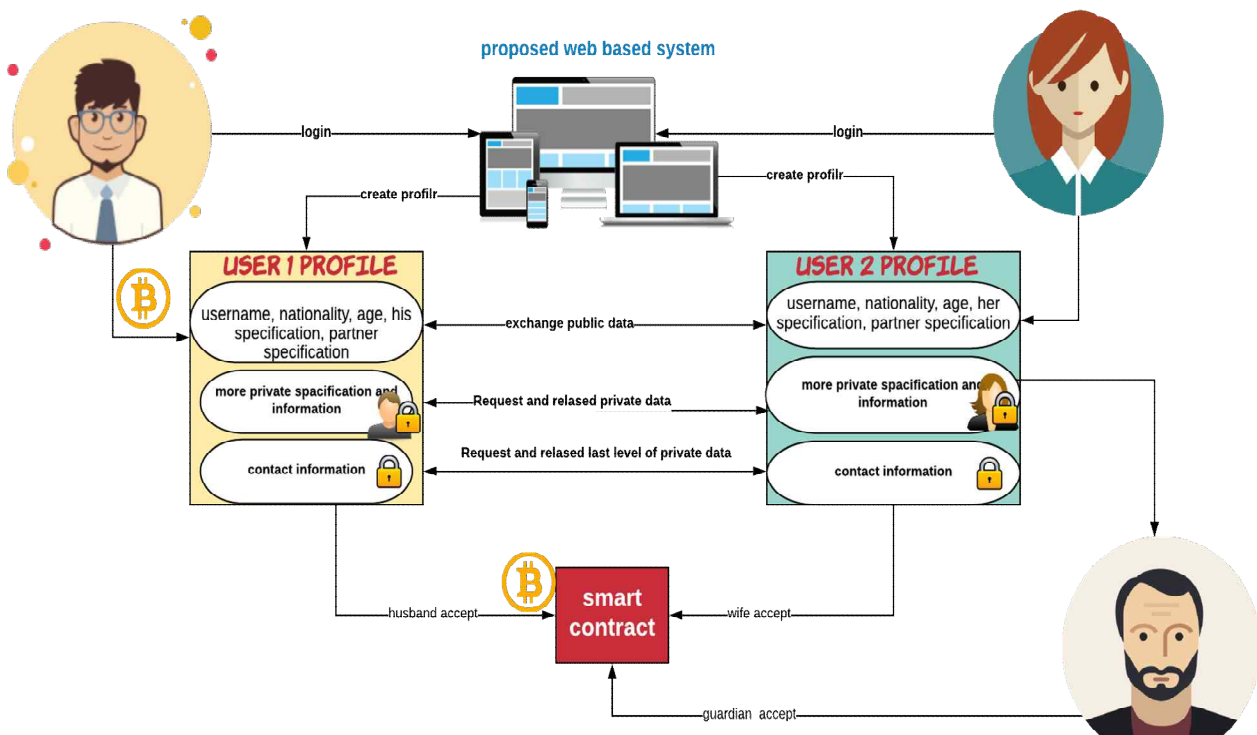

Figure 1: proposed system overview

1. The first one is used to detect the human face using skin color and Golden Ratio.
2. The second algorithm is A SELECTIVE ENCRYPTION OF HUMAN SKIN IN JPEG IMAGES we will use this algorithm for shading the users' images.

In Blockchain applications the users can interact directly with each other via application program interfaces (APIs) which are provided by the application of blockchain technology.

4.2 PROPOSED SYSTEM REQUIREMENTS

There are four main requirements in our proposed system we represent it in the following points:

- **Verification:** The system must verify the seriousness of the man and his real desire to marry by checking his cryptocurrency amount that is available in his account, it must contain the dowry.
- **Privacy:** our proposed system has three levels of data: the first type of data is public to all, the second and third are private, the users are responsible for releasing their data to who concern.
- **Accuracy:** the users' information must be unchangeable [cannot be modified]
- **Convenience:** our proposed system must be convenient to the Islamic religion. To keep images secrecy, the image encryption algorithm will be applied to shade 30% of each image.

5.RESEARCH FRAMEWORK

Our research focuses on proposing a secure web-based System to find life partners based on Blockchain Technology. It investigates the foundation of an efficient global marriage system based on a permanent, publicly distributed ledger that verifies transactions, records events and is resistant to the modification of data. The system provides and manages three levels of information, the first level is public to all authorized users. The second level is naturally private, and it will be revealed to the involved parties whenever they initially accept each other. Finally, the third level is extremely private, and it will be revealed if and only if the involved parties have already met in person and accept the agreement and then the smart contract will be created.

In order to seek solutions to many security issues, Blockchain Technology will be used.
In particular, our system will be developed using an open source blockchain platform (Ethereum technology). Ethereum runs smart contract applications by a high level of secures with no possibility of downtime, censorship, fraud, or third-party interference, it runs smart contract applications exactly as programmed.
Users' privacy is considered as one of the most important things. Whenever the user uploads his/her image, the system applies AES encryption algorithm in Output Feedback (OFB) mode of operation to ensure the security of the original image.

The proposed system is going to be implemented as a web-based application that serves as a front-end application to enable users to use it in an easy way. In particular, our system will be developed using an Ethereum development environment based on JavaScript (EthereumJS-lib) to build a secure web-based system.

5.1 Images processing techniques

1- step 1: Face Detection Technique:
Face Detection is used to extract the face from uploaded images. This is a crucial step to avoid manipulation, abusive

materials (nudity) which supports the reliability of the system.
Based on [9], a robust model will be used for defining a human face in colored images. As well as the color histogram will be used by that model for human skin in HSV (hue, saturation, value) space, connectivity analysis, the golden ratio and edge information.

The model consists of three main phases:

- **Phase1:** identifying each pixel if it is skin or non-skin pixel. This was done by calculating H and S values of HSV which showed skin color falls in a very small area instead of whole HS space. Finally, they utilized threshold values between 0 and 1 to differentiate if the selected pixel is skin or non-skin region. Using edge information which uses Sobel operator to find the edges in an image at the lowest level with smooth direction edge to enhance the result and reduce fault percentage of non-skin pixels, this improves the performance of the skin color approach and detecting skin pixels.
- **Phase2:** classifying different skin areas by using connectivity analysis. Using skin color to detect whether the pixel is a skin or non-skin pixel, but it does not identify if the pixel is face or not.
to solve that the skin pixels are gathered and grouped in different categories to gain meaningful information like hands, neck and face. the combinations geometrically of pixels that are near to each other will decided whether the grouped pixels belong to the same region or not, then we have to decide if this region is a face or not.

- **Phase3:** Based on the study results of [9] these phases able to ignore all skin pixels with a non-face area. Width to the height ratio of the human face comes in a range of golden ratio ($(1+\sqrt5)\,/2$). The results of the model located all faces that come in this range, as well as it doesn't pick out any part as a face which is out of that selected scale.

We propose to use the previous technique with its phases Because the model was tested using various and large numbers of images captured using a variety of backgrounds and in different lighting conditions. this model also applied to non-face pixels of different parts of the human body like hand and foot for ensuring results. In [9] They used Matlab10 for implementation but in this study, we suggest using C or C++ to comply with our framework and to require less time for detection compared with the MATLAB.

2- step 2: The image shading technique

After we have discovered the face and cropped the image, we suggest adding some image processing techniques (shading) by encrypting the image resulting from previous operations. based on [6] The given image by the user (male or female) is shading according to the secrecy of information. In users' state to achieve their confidentiality, it is important to cipher the digital images. the original plaintext image is converted into another meaningful plaintext image using Image camouflage, by applying a specific rule, that reduces

3. This layer Serves as the first point of Interacting with a user, and it is responsible for the validation of the provided information by users if it follows the rules and policies of system specifications or not.

Second layer: this layer is responsible for image encryption and shading.

Third layer: we can say that this layer is a core layer in the proposed system architecture layers, it is responsible for system transaction and control the role management. It is also responsible for mapping to the blockchain transaction.
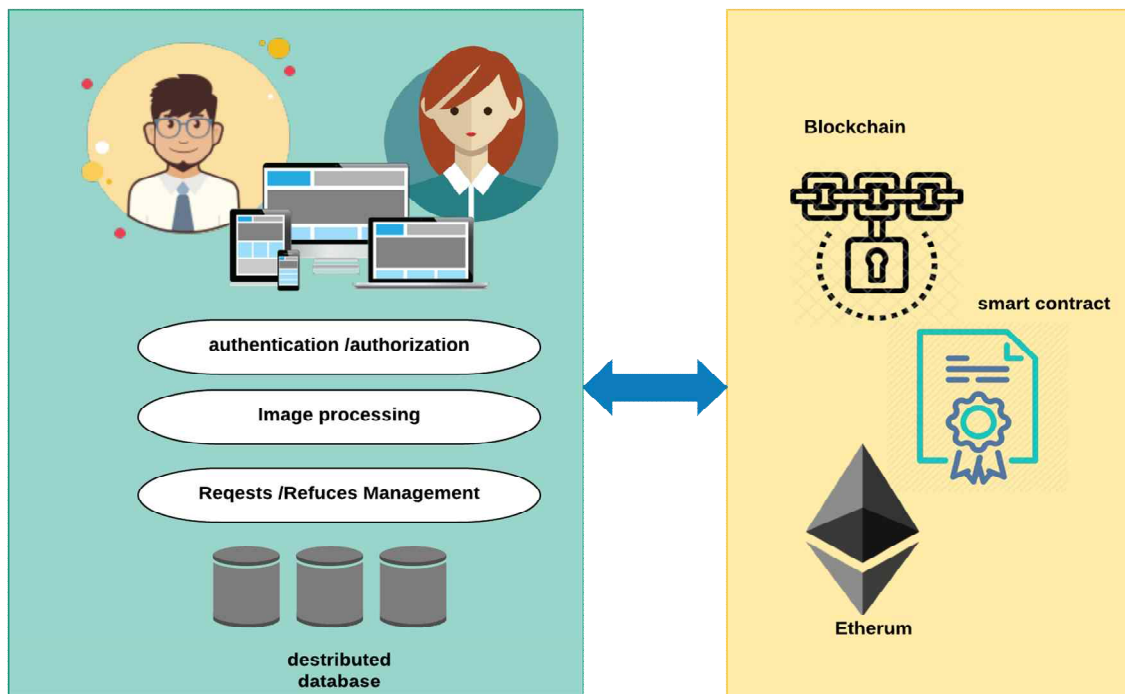

Figure 2: System framework

the attackers' uncertainty and ensures the privacy of the original image using Selective encryption of JPEG images by using the Advanced Encryption Standard (AES) cipher in Output Feedback mode of operation (OFB). Through the resulting image, the partner can know a little of the partner's other features and the color of his skin.

5.2 Architecture Detailed Description of proposed System

We design our proposed system as layered architecture; the architecture is divided into multiple layers as presented in figure 1.

First layer: Graphical User Interface and front-end security layer, this layer responsible for:
1. Interacting with registers users.
2. Authentication and authorization of the user's information and their wallet.

6   Challenges
1. **Social Challenges**: A new and innovative idea in our Arab and Islamic world, we tried to adapt it with the Islamic Law and customs.
2. **Religious challenges:** For example, the consent of the guardian to the marriage is important to be considered.
3. **Ethical Challenges:** Ensure that people do not manipulate information, such as attaching a photograph that is not real, or providing false information.

7   System Consideration
- Each one must insert his/her real information, If not there will be a punishment as Financial sanction.

- At the Registration Stage, System Will never accept any Male unless he has the required balance of bitcoins in his wallet.
- System will reject same gender communication i.e. Male to Male, Female to Female
- Personal images that are inserted to the system will go through two basic stages:
  - *First stage* is the Face Detection stage. Face will be detected then other non-face skin areas will be cut.
  - *Second stage* is Shading the image by applying the AES encryption algorithm in Output Feedback (OFB) mode of operation.

8   CONCLUSION AND FUTURE WORK

This research solved a social issue by providing a secure system for finding a life partner based on blockchain technology under Islamic legislation. Blockchain technology is used to link the users together and give them an appropriate environment under controls of Islamic rules and limits, the users can interact directly with each other via API. An AES cipher is used as the main method applied to the user's image to ensure the privacy of a user's personal information. In fact, before applying AES the image is processed to detect a face using skin color and Golden Ratio. By this way we proposed a comfortable environment to start honest relationship While maintaining privacy and security. We suggest that this environment operates under the shadow of governments by linking it to their ministry of interior to more authentication.

Our future work is focusing on the development stage and discussing the results.

References

[1]   G. K. H. M. H. G. H. Friðrik Þ. Hjálmarsson, "Blockchain-Based E-Voting System," in *2018 IEEE 11th International Conference on Cloud Computing*, San Francisco, CA, USA, 2018.

[2]   L. Y. C. ,. C. Noe Elisa ،"A framework of blockchain-based secure and privacy-preserving E-government system،" Wireless networks ،pp. 1-11 ،12- 1- 2018.

[3]   Y. C. e. al ،"Blockchain-Based Medical Records Secure Storage and Medical Service Framework،" Journal of Medical Systems ،vol 43 ،no.1, pp. 1-9**1** ،- 2019.

[4]   JD. Macrinici ،"Smart contract applications within blockchain technology: A systematic mapping study،" Telematics and informatics ،vol. 35 ، no .8 ,pp. 2337-2354**12** ، 1 2018.

[5]   S. Ngamsuriyaroj, T. Likittheerameth, A. Kahutson and T. Pathummasut, "Package Delivery System Based on Blockchain Infrastructure," in 2018 Seventh ICT International Student Project Conference (ICT-ISPC), Student Project Conference (ICT-ISPC), 2018 Seventh ICT International, Jul, 2018;.

[6]   W. P. a. A. B. J.M. Rodriguesa, "SELECTIVE ENCRYPTION OF HUMAN SKIN IN JPEG IMAGES," in 2006 international conference on image processing, image processing,2006 IEEE international conference, 2006.

[7]   N. Kshetri and J. Voas, "Blockchain-Enabled E-Voting," vol. 35, no. 4, pp. 95-99, 2018

[8]   A. Mohsin et al., "Blockchain authentication of network applications: Taxonomy, classification, capabilities, open challenges, motivations, recommendations and future directions", Computer Standards & Interfaces, vol. 64, pp. 41-60, 2019. Available: 10.1016/j.csi.2018.12.002.

[9]   Faizan Ullah, Dilawar Shah, Sabir Shah, Abdus Salam, and Shujaat Ali, "A Novel Approach for Human Face Detection in Color Images Using Skin Color and Golden Ratio," journal of Applied Environmental and Biological Sciences, 2017.

[10] Rahmadika, S. and Rhee, K. (2018). Blockchain technology for providing an architecture model of decentralized personal health information. International Journal of Engineering Business Management, 10, p.184797901879058.

[11] Schinckus, C. (2020) 'The good, the bad and the ugly: An overview of the sustainability of blockchain technology', Energy Research & Social Science, 69. doi: 10.1016/j.erss.2020.101614.

[12] Zheng, Z. et al. (2020) 'An overview on smart contracts: Challenges, advances and platforms', Future Generation Computer Systems, 105, pp. 475–491. doi: 10.1016/j.future.2019.12.019.

[13] Aleksieva, V., Valchanov, H. and Huliyan, A. (2019) 'Application of Smart Contracts based on Ethereum Blockchain for the Purpose of Insurance Services', *2019 International Conference on Biomedical Innovations and Applications (BIA), Biomedical Innovations and Applications (BIA), 2019 International Conference on*, pp. 1–4. doi: 10.1109/BIA48344.2019.8967468.