International Journal of Engineering & Technology, 7 (4.11) (2018) 193-197

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper



Blockchain Technology for Islamic Marriage Certificate

Nor Elysha Kamaruzaman[1], Ihsan Mohd Yassin[1]*, Azlee Zabidi[1], Fadhlan Hafizhelmi Kamaru Zaman[1], Zairi Ismael Rizman[2], Rahimi Baharom[1], Norfishah Abdul Wahab[1]

[1]Faculty of Electrical Engineering, University of Technology MARA (UiTM), 40450 Shah Alam, Selangor, Malaysia
[2]Faculty of Electrical Engineering, University of Technology MARA, 23000 Dungun, Terengganu, Malaysia
**Corresponding author E-mail: ihsan.yassin@gmail.com*

Abstract

In recent years, an individual under the pseudonym of Satoshi Nakamoto devised a revolutionary technology called blockchain as the engine behind the first decentralized virtual currency called Bitcoin. A radical concept departing from government-centric controlled currencies, Bitcoin has emerged as a disruptive technology with the power to revolutionize business and its processes. Advantages of the blockchain include decentralized control, immutability, elimination of central authority and solution of concurrency problems in traditional databases. Leveraging on the advantages of blockchain technology defined above, this paper discusses the potential application of blockchain technology for storage of Islamic marriage certificates. Marriage certificates are documents issued to couples to legally recognize their marriage. Due to its paper-based nature, there is significant risk for them to be forged or frauded. These issues can be addressed effective using blockchain. The proposed application was implemented using smart contracts on a simulated Ethereum platform. A smart contract is designed to execute automatically under certain predefined conditions. The use of smart contracts eliminate manipulation by a single party. In addition, the immutable concept of blockchain ensures that data integrity is always preserved, greatly reducing the risk of fraud.

Keywords: *blockchain technology; Islamic marriage certificate; Ethereum; smart contract.*

1. Introduction

The name blockchain is derived from how data is stored. Data is stored in a sequence (chain) of blocks. In addition to the data stored in each block, it also contains a cryptographic hash of the previous block. Any changes made to any of the data in previous blocks causes the cryptographic hash to change, indicating that the block has been modified in some way. This chain of data and cryptographic hashes result in the technology being very resistant to changes – hence its immutable property. Additionally, copies of the blockchain is broadcasted and copied over participating nodes. This ensures transparency and integrity as the blockchain is public and available for inspection by anyone wishing to check its contents. The combination of these two properties means that any attempted changes can be easily verified and traced to the fraudulent node(s) [2]. The need for transparency and immutability in a wide variety of sectors means that blockchain technology has many application potentials. The most notable application using this technology is Bitcoin, the first decentralized digital asset created by person(s) known as Satoshi Nakamoto.

A valid Islamic marriage simply requires a groom, a bride, a wali (person responsible for the bride) and two witnesses to the marriage [1]. However, the current legislation in Malaysia and many other countries require that the marriage be recorded and documented.

An Islamic marriage certificate is defined as a formal agreement that outlines the rights and responsibilities of the groom and bride in marriage proceedings. The certificate is important for the newlyweds to obtain to legally recognize their marriage in Malaysia.

Currently, two methods can be used by the Muslims in Malaysia to register their marriage. The first method involves completing an online registration in the Islamic Marriage Management website. However, the method is currently available to couples residing in certain parts of Malaysia. Alternatively, applicants can visit the Islamic Religious Department in their respective states to register their marriage manually. This second method requires applicants to bring their government-issued identity cards, the wali and witnesses to the office together with a small processing fee. The processing time is approximately one month, and the certificate is typically written and documented in hardcopy or digital form exposing them to risk of fraud, tampering and loss [3].

In this paper, we demonstrate that such issues could be resolved by implementing a new and promising technology known as blockchain. The implementation of blockchain technology can create a superior system in terms of data integrity and transparency. The implementation is realized by using a smart contract which is another useful and promising feature of the technology.

2. Literature Review

2.1. Blockchain Technology

Blockchain technology is an online distribution ledger that records every single transaction made and it allows data or to be tracked all over the internet, so it cannot be modified or counterfeited. The technology does not require the involvement of any third party, meaning that it is decentralized. In the case of cryptocurrencies, this means that the data cannot be controlled by any bank or government, making it transparent and incorruptible. [2][6]. Blockchain technology is a disruptive technology because it can be im-

Copyright © 2018 Authors. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

plemented in almost any sector requiring data immutability and transparency [7].

2.2. Forgery and Fraud of Marriage Certificate

Document falsification or forgery is defined as an action that modifies an original document by means such as imitating other people's writing, signature, stamp, adding and subtracting to/from the original content [3].
Several cases have been reported in literature regarding the forgery and fraud of marriage certificates due to various reasons. In [3], a marriage certificate was forged for polygamy, due to groom not being able to obtain the first wife's consent. There are also potential fraud cases involving transgender as currently the National Registration Department (NRD) does not approve the requests of the transgender people to change their names and gender markers on their identity cards [15].
Fraud cases could also occur when a couple decides to marry or elope to other countries with less restrictive registration requirements. These cases usually involve significant repercussions for the children from these marriages as well. For example, there was a case where a Malaysian groom and a Vietnamese bride registered their marriage through an agency outside of Malaysia [4]. The genuineness of the marriage certificate was questioned by the Shariah Court. The consequence was the birth of their newborn child could not be registered by NRD [5] as the marriage was not recognized as legitimate. The child would be declared as illegitimate child by the NRD and according to the current legislation system in Malaysia, there is a very high probability that the child would be returned to the country of origin of its foreign mother or father.

2.3. The Ethereum Blockchain and Smart Contracts

To implement a new recordkeeping system for marriage certificates, the key ingredient is the concept of smart contract - one of the core technologies by Ethereum - an open software platform that enables developers to build and deploy decentralized applications. Currently, Ethereum is the most advanced platform for coding and smart contracts among the current crop of cryptocurrencies. Additionally, it also has an unlimited document processing capability [8].
The Ethereum blockchain is "a blockchain with a built-in fully-fledged Turing-complete programming language that can create contracts for the purposes of encoding arbitrary state transition functions, allowing users to create smart contracts and decentralized applications in which rules can be made according to one's desire, such as rules for ownership and transaction formats" [8].
Ethereum is different from the Bitcoin blockchain as it is not entirely focused on finance like Bitcoin does. The Ethereum blockchain focuses on running the programming code of any decentralized application. Like Bitcoin, Ethereum also has its own currency which is called Ether or ETH. However, the purpose of the currency is different as Ether works as a fuel to execute smart contracts to prevent the abuse of limited network resources. This can also be considered as payment for the transaction fees and services on the Ethereum network [8].
Generally, there are three application categories on top of Ethereum. The first one is financial applications, followed by semi-financial applications and then, decentralized applications. Financial applications, using Ethereum blockchain, are more powerful as users can manage and enter into contracts using their money, in which this may include full-scale employment contracts. An example of semi-financial application are self-enforcing rewards for solutions to computational problems. Finally, decentralized applications are applications that are not focused on finance at all and not controlled by any third party such as voting systems [8].
A smart contract is a computer program that executes on a blockchain in decentralized manner. For Ethereum, the contracts are written in the Solidity programming language. The contracts are executed on the Ethereum Virtual Machine (EVM), a runtime environment for smart contracts, sandboxed and completely isolated - as the code running in the EVM has no access to network, file system or other processes [8]. The code is implemented by inputting proper logic when writing the smart contract. The encrypted code is then sent to other computers or nodes via a distributed ledger. Following that, the execution of the contract is recorded. The result of this execution would be the individual agreement, and this will eliminate the manipulation of a single party [9]. Therefore, the concept of smart contract will be implemented into the new, decentralized application exclusively for marriage certificates.

2.4. Related Works

This section details several researches works in blockchain technology. In [10], a blockchain based voting protocol application was presented for board meetings. Its objectives are to provide maximum voter privacy and the complete elimination of any trusted authority for tally computation. The Ethereum blockchain was used as it offers smart contract capabilities. Traditionally, the voters' privacy relies on the role of a third party, who would be decrypting and tallying the votes in a verifiable manner. The role of the third party was completely removed with the implementation of blockchain as the voting and the tally computation can be done without any assistance. The proposed implementation has two smart contracts. The first contract is the voting contract, while the other one is called cryptography contract. The voting contract includes the voting protocol, the controls of the election process and the verifications of the zero-knowledge proofs (protocols in which one can prove a statement without leaking the information to another). As for the cryptography contract, it is related to the proofs and the voters can use the same cryptography code locally without interacting with the Ethereum network. A consensus mechanism was used to enforce the execution of the protocols stated above. Therefore, the paper has presented a smart contract implementation that provides maximum voter privacy and can be publicly verified.
In [11] presented blockchain based Internet of Things (IoT) application for thing-to-thing electricity micro payment. The implementation of a proof-of-concept of a smart cable that connects to a smart socket and the electricity payments will be made without any human interaction. The micro payment is well suited for this application as it is small, numerous and autonomous. Several blockchains, including Bitcoin, were examined in terms of its properties and feasibilities in handling thing-to-thing payment. Bitcoin was chosen because of its decentralized structure and ease of account creation. The implementation uses a smart cable that automatically makes payment for the electricity it provides to the devices connected at the end of the cable.
In [12] presented a volunteer service time record system based on a new blockchain called Timecoin. The paper aims to replace the conventional time record system using a, which lacks in data security and to improve credibility and traceability of volunteer service time management. Unlike Bitcoin, the transaction is not strictly for financial purposes as they are used to execute instructions such as storing, querying and sharing data. The volunteers' service time certification was achieved using smart contract. When a volunteer finishes his service time in a way that satisfies the predefined requirements, the relevant award was given to the volunteers. The advantage of the proposed approach was data transparency. Every volunteer and manager could check and monitor the service time record through their addresses as blockchain is a public ledger. An additional advantage was tamper-resistance as modifications are not allowed using blockchains.
In [13], a decentralized application to record electronic medical records (EMRs) was proposed. Using blockchain technology, medical information can be accessed, while recording patient records using comprehensive and immutable logs. The blockchain application also handles critical tasks such as authentication, con-

fidentiality, accountability and sharing of sensitive medical data information. The system relies on medical stakeholders, such as researchers and public health authorities to maintain and secure the network via Proof of Work (PoW) mechanism, which provides guaranteed data integrity and tamper-resistance. The system was implemented as several smart contracts deployed over the Ethereum blockchain. Smart contracts were used to automate and track certain state transitions, such as a change in viewership rights or the creation of a new record in the system. To control access, a log in mechanism was created, in which patient-provider relationships were defined to associate them with medical records and viewing permissions. Medical providers can add a new record to the log regarding a patient and the authorization of sharing the records between providers can be made by the patient themselves. Patients were constantly informed regarding their medical records using an automated notification when new information was updated to the log. New information was first verified before insertion into the blockchain.

In [14] proposed a blockchain-based security framework for data communication in a smart city. The project aims to provide better services to people while ensuring that the available resources can be utilized efficiently using a data communication platform that features privacy, integrity and data confidentiality. Smart cities provide open data services or facilities like smart terminals, in which they offer bicycle rental terminals, self-service machines and information kiosks. The idea behind the adoption of blockchain was to fend off cyber-attacks attempting to steal personal and financial information. The security framework implemented four layers - physical, communication, database and interface. Smart contracts were applied in the communication layer to act as protocols for different types of applications. In the database layer, a decentralized and distributed ledger stores data, in which the scalability, performance and security for real time applications are ensured. Therefore, this project promises a platform that can be used by all devices in the smart city to communicate with each other securely in a distributed environment.

3. Methodology

As shown in Figure 1, the project was generally divided into three main phases. They are described in detail in Section III-A to Section III-C.

3.1. Concept and Design Planning

This phase involves a study of the requirements for the project and planning out the appropriate block design to accommodate the required functionalities for the system.

Ethereum was chosen as the blockchain platform due to its ability to execute smart contracts. Based on Section II-C, the smart contract will be deployed as a decentralized application. The system was designed such that it would be managed by a registration officer from the Department of Islamic Affairs. To register a marriage, the officer would check and verify all the documents submitted to him. He would also check the existing data on the blockchain to ensure that no elements of fraud has occurred. Once this is done, the officer would then proceed to enter the data into a block and adding it to the blockchain by executing a smart contract. Once the registration data has been entered and the block validated, the data would be copied to participating nodes globally. The permanently stored data can be examined using the Ethereum blockchain explorer. The data is also unchangeable, and any new modifications would have to be included in a new block. Therefore, this mechanism creates a data storage that has high integrity, reliability and redundancy.

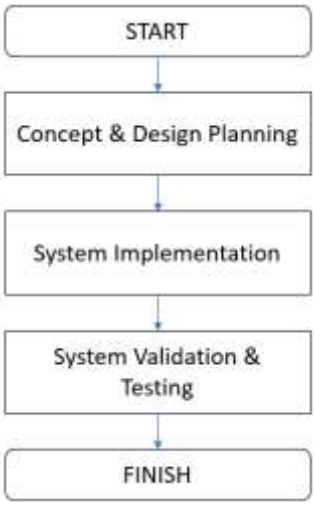


Fig. 1: Project flowchart

Since the platform of choice is Ethereum, the execution of the smart contract would require some fees in the form of Ether (the currency powering Ethereum). In this test version, the transaction may be completed using simulated Ether. However, for implementation in the mainnet, real Ether would have to be used, and they can be purchased by exchanging them with fiat currency through various exchanges worldwide.

3.2. System Implementation

To implement the project, the Ethereum testnet, also known as Ropsten testnet, was used as the blockchain database to develop the application. It is a testing network that runs the same protocol as Ethereum. Using the testnet, several tests can be conducted before deploying the smart contract on the main network. Another reason for using the Ropsten network was to avoid losing real money for transaction fees and smart contract deployments when building and experimenting with the system.

For the smart contract, a programming language called Solidity was used. The smart contract is compiled and deployed by Remix, a browser-based compiler and Integrated Development Environment (IDE) that enables users to build Ethereum contracts with Solidity language and it can be used to debug transactions.

The user interface was designed to make data entry easier. Hypertext Markup Language (HTML) and Javascript were the languages used to create the interface. Metamask was needed to use the interface as it is a tool that provides the browser the capability to make Ethereum transactions through a regular website using the web3.js Javascript library developed by the Ethereum Core developers. In other words, it was used to connect the regular website to an Ethereum node or interact with the blockchain. The user interface asks for various information of the groom, bride, wali and witnesses. The information is then stored into the smart contract which is deployed inside the blockchain system.

3.3. Blockchain System Evaluation

The smart contract was written, modified and deployed according to the planned concept design. The user interface was tested by entering data into the system. Etherscan (a Ropsten blockchain explorer) was used to verify whether block insertion was successful. In a summary, the overall system was tested several times to ensure that the blockchain works properly as it is the most vital part of the project.

4. Results and Discussion

The user interface for the developed system is shown in Figure 2. The user interface is connected and can interact with the written smart contract which has been deployed through Remix as MetaMask plugin has been installed into the browser. The Ethereum blockchain was deployed on the Ropsten testnet. The current design of the smart contract would restrict the use of the system to only one person for data entry due to security considerations. Therefore, it is suggested that the owner should be an officer attached to the Islamic Religious Department as managers of the registration process.

Referring to Figure 3, before any data can be submitted into the blockchain, an account with MetaMask is required. In the current implementation, the smart contract owner is assumed to be the owner of Account 1 with the address 0x06F7e902871ef5CCe22859F329E659c04173537b. This address uniquely identifies the user and is to be referred for any future transactions.

Like the Ethereum mainnet, the application requires Ether to execute the smart contract. This Ether is required to reward miners responsible for validating smart contract transactions. Since the smart contract is connected to the Ropsten network (a testing environment), no real money is used. In the actual implementation, Ether needs to be purchased with fiat currency. Simulated Ether can be added to the account for the testing and development purposes (Figure 3). Figure 3 shows the amount of simulated Ether was added into the account which 9.320 ETH.

Data was to be inputted accordingly in which the user interface asks for the names and the number of identity cards of the groom, bride, wali and witnesses. When a user clicks the "Submit Data" button, a notification regarding transaction confirmation will pop out automatically. This can be seen in Figure 4.



Fig. 2: The user interface

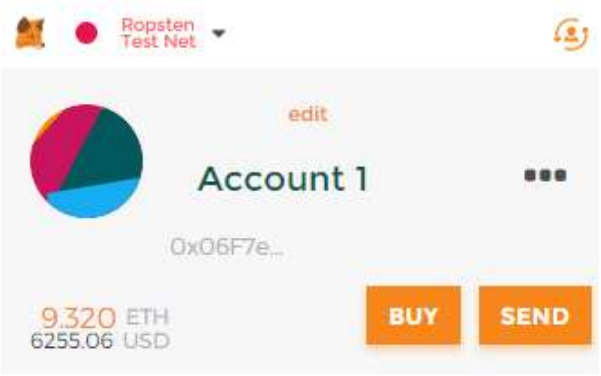


Fig. 3: Account 1 creation in MetaMask

When a user clicks "Submit" button in the MetaMask notification, it took a few minutes for the input data from the user interface to be pushed into the blockchain. When the transaction was successful, this indicates that the data is now in the Ropsten blockchain. This can be proven using Etherscan, a Ropsten blockchain explorer. By entering the account address of the owner in the explorer, the overview of each transaction information can be viewed such as in Figure 5. It shows all the input data that is stored into the blockchain.



Fig. 4: Transaction confirmation in MetaMask

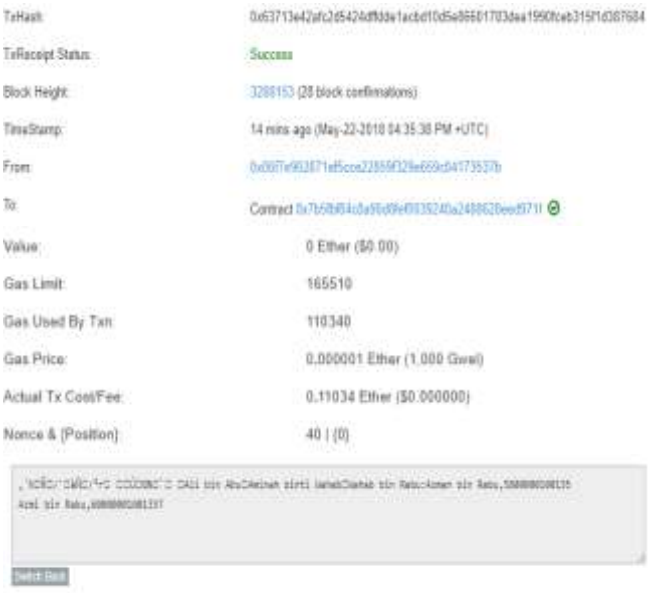


Fig. 5: Transaction overview in Etherscan

In the user interface, the stored data can be called from the blockchain once it has been submitted (Figure 6). The first input would be the information of the applicant, followed his or her partner, wali and the witnesses.

5. Conclusion

Blockchain technology is an online ledger that records every transaction made in an immutable fashion. The highlight of this technology is that it cannot be controlled or modified by a third party. Any transaction that uses this technology can be tracked all over the network, making it very difficult to be hacked and counterfeited. Therefore, the records are transparent and have integrity.



Fig. 6: Displaying data in user interface

The scalability of blockchain technology is very large as it can be applied almost any industry requiring data integrity and transparency. As a legal document issued by the government, marriage certificate is important as it is an integral part of Islamic marriage. The use of smart contracts in the Ethereum Ropsten blockchain to store Islamic marriage certificates have been demonstrated in this paper. Using specialized plugins to connect to the blockchain network, data was successfully entered into the blockchain. This has been proven with the Etherscan blockchain explorer.

Acknowledgement

Authors gratefully acknowledge the financial support from Ministries of Higher Education Malaysia and Institute of Research Management and Innovation (IRMI) Universiti Teknologi MARA Grant No: 600-RMI/NRGS 5/3 (3/2013).

References

[1] Chek, R. (2010). Konsep perkahwinan dalam Islam dan Kristian: Kajian perbandingan. Masters thesis, University of Malaya.
[2] Aste, T., Tasca, P., & Di Matteo, T. (2017). Blockchain technologies: The foreseeable impact on society and industry. Computer, 50(9), 18-28.
[3] Ismail, W. A. F. W. (2017). Forms of document falsification in Malaysia's Syariah courts. Geografia-Malaysian Journal of Society and Space, 11(9), 32-39, 2015.
[4] Leng, C. H. (2011). International marriages in Malaysia: Issues arising from state policies and processes. In G. W. Jones, T. H. Hull, & M. Mohamad (Eds.), Changing Marriage Patterns in Southeast Asia: Economic and Socio-Cultural Dimensions, Routledge Contemporary Southeast Asia Series. Abingdon: Routledge, pp. 185-201.
[5] Yusof, N., & Shukor, H. A. (2013). Status Anak Dalam Perkahwinan Sindiket Menurut Perspektif Syarak Dan Akta Undang-Undang Keluarga Islam Wilayah Persekutuan 1984. Proceeding of the International Conference on Social Science Research.
[6] Pilkington, M. (2016). 11 Blockchain technology: Principles and applications. In by F. X. Olleros, & M. Zhegu (Eds.), Research Handbook on Digital Transformations. Cheltenham: Edward Elgar Publishing, pp. 225-253,
[7] Mattila, J. (2016). The blockchain phenomenon – The disruptive potential of distributed consensus architectures. http://www.etla.fi/wp-content/uploads/ETLA-Working-Papers-38.pdf.
[8] Divers, D. (2015). Ethereum white paper: A next generation smart contract. https://www.ethereum.org/pdfs/EthereumWhitePaper.pdf.
[9] Blockchain Technologies. (2017). Blockchain explained - Distributed ledgers and blockchain technology. http://www.blockchaintechnologies.com/blockchain-smart-contracts.
[10] McCorry, P., Shahandashti, S. F., & Hao, F. (2017). A smart contract for boardroom voting with maximum voter privacy. Proceedings of the International Conference on Financial Cryptography and Data Security, pp. 357-375.
[11] Lundqvist, T., de Blanche, A., & Andersson, H. R. H. (2017). Thing-to-thing electricity micro payments using blockchain technology. Proceedings of the IEEE Global Internet of Things Summit, pp. 1-6.
[12] Zhou, N., Wu, M., & Zhou, J. (2017). Volunteer service time record system based on blockchain technology. Proceedings of the IEEE 2nd Advanced Information Technology, Electronic and Automation Control Conference, pp. 610-613.
[13] Azaria, A., Ekblaw, A., Vieira, T., & Lippman, A. (2016). Medrec: Using blockchain for medical data access and permission management. Proceedings of the IEEE International Conference on Open and Big Data, pp. 25-30.
[14] Biswas, K., & Muthukkumarasamy, V. (2016). Securing smart cities using blockchain technology. Proceedings of the IEEE 18th International Conference on High Performance Computing and Communications; IEEE 14th International Conference on Smart City; IEEE 2nd International Conference on Data Science and Systems, pp. 1392-1393.
[15] Human Rights Watch. (2017). Human Rights Watch submission to the Committee on the Elimination of Discrimination against Women concerning Malaysia. https://www.hrw.org/news/2017/05/24/human-rights-watch-submission-committee-elimination-discrimination-against-women.