

Blockchain Hash Function for Secure Biometric System

Rana Aziz Yousif Almuttalibi

Department of Medical Instrumentation Engineering, AL-Mansour University College, Baghdad, Iraq

Abstract: A definition of a blockchain shows that it is formed by serialized databases realizing digital accounts that manifesting register transactions in a network characterized by distribution and decentralization. The challenges to the act of security data against piracy and other negative manifestations such as manipulation and counterfeiting are real in terms of that which entails the process of applying the new technology. This study likes to present its recognition as facilitating user's interaction with the services offered by a blockchain. This is acquired by mere singling out one identity and thus, presenting private user data from being shared by others. What is really transmitted and stored in the server data. The ultimate goal is to achieve the most vehemently secured and an authentic act key words.

Key words: Blockchain, biometric, hashing, security, iris recognition, transactions

INTRODUCTION

The topic of blockchains has recently gained more interest. As a research area, receiving now more attention, an appropriate word for its technology could be a "buzzword". The problem emanates when a digital act represents something and one passes it to another person. Digital transactions are the source of this particular process. This simple process does not acquire physical money. But the technology already mentioned is not that easy. A basic requirement is that the bank should be reliable. What we badly need here is a kind of a technology that is secure and that enables the parties concerned to have direct communication with each other. This kind of technology is named as a blockchain. A person can enter into a transaction twice with using the same money. This is known as double spending, the problem of which could be in the first place solved by the technological process of a blockchain. One does not need a middle way as a bank to solve the problem. Some often technologies have arisen that do the same job as a blockchain which in its work embrace a certain concept, that of a hashchain.

We do have a process known as a hash where a predefined digital string of a fixed length quality results from a data. The most manifest function of a hash is called Modulo to calculate a hash; we have first, to convert a digital string to a number then a constant works to divide the number. A hash value results from that division. The value of a constant is greater than that of a hash value. It is often easy to compute a hash but the difficulty is if one tries to realize its input. If the hash function is characterized by such properties, it suggests itself as a hash function of cryptography.

Figure 1 shows the structure of the hash chain. We observe data chunks linked to each other through hash function (Maxonka, 2016). A hash and payload make up a block. The previous blocks compute the hash value. Arbitrary data contribute to the payload of each block. If data change in a block, they also change in the subsequent blocks. To exemplify things, the payload of a second block changes, if the payload of the block is changed. People are authorized to create new blocks in the chain. "Public Key Cryptography" is responsible for this creation. The process is similar to a one-way function and a hash function. What are involved here are the processes of encryption and decryption. Now a days people use various types of algorithm. In terms of security, two families of hash functions are now being used. These are:

- SHA-2 family (Secure Hash Algorithm)
- SHA-3 (Secure Hash Algorithm)

It is suggested that cryptographic hash functions have a string of any length and a fixed length hash value in hexadecimal (radix 16), e.g., Hexadecimal = Radix 16 (4CF5) $16 = (4 \times 16 + 12 \times 16 + 15 \times 16 + 5 \times 16)$. For security reasons a blockchain usually employs SHA 256 algorithm because in this kind of algorithm, after calculation a string is represented in 256 bit hexadecimal digitals.

The number of outputs in this hash secure algorithm comes up to 256, the internal state size is 1600 bits, the size of the block is 1088 bits, the message size is 24 unlimited rounds, the security bits therein are 128. Figure 2 shows examples of cryptographic hash functions.

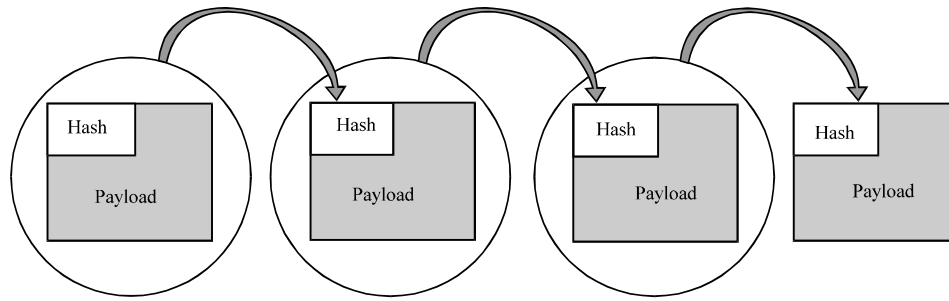


Fig. 1: Hash chain

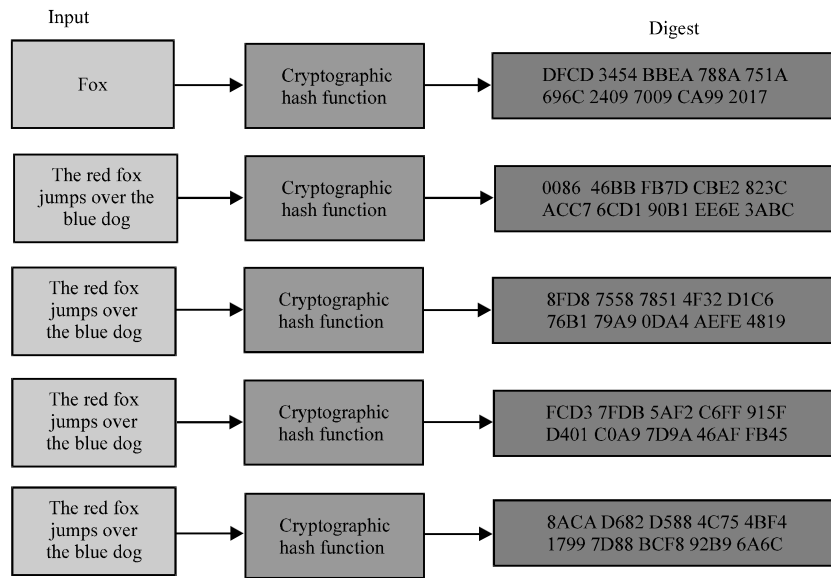


Fig. 2: Cryptographic hash function

MATERIALS AND METHODS

Blockchain architecture: Blockchain architecture is made up of a sequence of blocks. Their job is to store transactions in the same way as a transparent or public ledger (Lee and Chuen, 2015). Every block of blockchain makes use of tree topology. It makes the chain by containing the hash of its preceding block. The size of the transactions decides the size of each block. Similarly, each block chain has only one parent block. In a blockchain structure, all other blocks contains a parent hash value (address or reference) (Buterin, 2014). Figure 3 shows a blockchain structure (Buterin, 2014).

Three elements are realized in each block. These are a blockheader, a parent block hash and a transaction counter. The blockheader has the following parts (Zheng *et al.*, 2017):

- . Block version
- . Marked hash tree
- . Timestamp

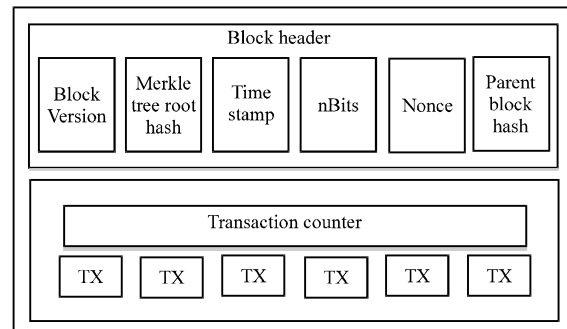


Fig. 3: Blockchain architecture

- . nBits
- . Nonce
- . Parent blockchain

In the first element, that is in block version what validates the block is a set of rules. It also shows the rules to be followed for the process of validation and whether these rules could be the same or otherwise. In a marked

hash tree, each transaction hash has a particular hash value whose job is to identify this block in the whole blockchain in an easy and unique way. Holding the transaction time of a block, the timestamp tries to show the current time of a specified area ever, since, 1st January, 1970. This is the area which shows the place in which the transaction occurs. Significantly, that which shows the limit of a hash value in a valid block is the nbits. A nonce has a 4-byte area starting from 0 and continually increasing on each hash calculation. The nonce value frequently undergoes a change, getting a different hash value and making its transaction more reliable.

To authenticate that the hash value is correct, the nonce of a block has to attain a specified target value. Later, it is sent out to other roles or blocks of a blockchain. The block is to be appended to the blockchain when an existing node in a blockchain allows it. The topology which is decentralized simultaneously permits the addition of more than one valid block in a blockchain. In a block, the hash value of a previous block the size of which is 256 bit is kept by the parent block. The block body realize both the transactions and the transaction counters. The size of the block and the extent of exchange are determined by the greatest number of exchanges that a block can admit. In order to approve the acknowledgement of exchanges, a blockchain makes use of a cryptography component that is a symmetric (Anonymous, 2016).

The technology of the blockchain exercises different effects on certain factors like security, reliability, performance and so on. The security of a blockchain poses a great challenge. The reason relates to associations that have to be pleasant. In addition with regard to the exchange data, it has to be known. A part of the present security arrangement that have encryption calculations that are solid, the concerns of digital security are seen as important and essential components that influence open choices concerning the question of sharing information through the use of blockchain frameworks. The block technology is characterized by

being reliable. The reason is that it is a centralized network. The failure of one node cannot have an effect on the transaction process of other nodes occurring in a network (Morabito, 2017).

The lower cost and the faster transaction of blockchain technology can determine the performance of blockchain technology. A blockchain innovation deeply is able to lessen the expenses and the time of the exchanges by getting rid of outsiders or middlemen. This may be the most notable division of the blockchain which is ultimately connected with the attempt to gradually increase trust between the human and the PC. similarly. This is known as Decentralized Autonomous Association (DAO). It can of itself use people operating the internet to do certain jobs. To create DAO that is self-organizing and self-representing is not an easy task. Yet, if it is once actualized, it can manifestly have affect on modern areas like human services, transportation and shortage that is distributed (Morabito, 2017).

Block: A block may be defined as a single unit in the blockchain (Catalini and Tucker, 2017). Figure 4 shows it as a building block, made of transactions having meta-data. The valid data (transactions) are collected by a miner. These valid data are characterized by certain time interval that forms a block and that calculate the cryptographic hash. At any rate, this hash is of a specific format. It must contain four leading zeroes as manifested in Fig. 4. To get this specific form of hash, the minor must guess in a random manner an arbitrary number, a number that ultimately outputs the hash with four leading zeroes. The number is used once (nonce). A signed block is a block with nonce. Otherwise, it is unsigned. Mining is the process that finds nonce.

Figure 4 shows a sample block. As the figure reveals, a block has three elements. There are nonce, data and a hash. The unique id of the block is the block number, whereas Nonce 72608 is an arbitrary number, a number that is guessed to get the specified format of the hash.

Block:	#	1
Nonce:	72608	
Data:		
Hash:	0000f727854b50bb95c054b39c1fe5c92e5ebc1a4bcb5dc279f56aa96a365e5a	

Fig. 4: Block

Eventually, the data is the digital data of the user. In this particular instance, it is empty. As for the hash, it is the digital fingerprint of the data.

Biometric authentication: To verify that a person is really he who claims to be is authentication. Biometric authentication is a process that attempts to use a physiological trait to achieve this verification. Biometrics gives certain security advantages. It is thus, better than other authentication methods. To exemplify things, a key card may be stolen, a pin or a password may be forgotten. But any eye can neither be stolen or forgotten. When enrolment occurs, an individual may be identified by documents or some other ways. However, for the sake of future comparison, we can capture and store the biometric measure.

Authentically to be useful, a biometric measure has to be unique and constant and readily available to the individual. All users have to cooperate to attain successful implementation of biometric authentication and where proper, training is a necessity to develop user's awareness concerning the vitality and importance of security systems and the role these systems play in the organization (Thavalengal, 2016).

Operational modes of biometric system: Two modes could suggest the work of biometric system. These are enrollment and authentication modes.

Enrollment mode: Enrollment mode requires steps to get discriminating data that separately belong to each individual. In terms of a certain group of individuals, a database having template data can be made. Enrollment can be planned as an instrument that registers new individuals in the database (Monteiro, 2012).

Authentication mode: Often used in the biometric realm, the authentication mode is another name for verifying things. This mode means allowing the individual's identity to be recognized by the system (Drahansky, 2005). These two principal phrases are shown in Fig. 5.

Process of biometric authentication

Identification: Systems of identification attempt to answer the following question: 'Who is this individual?' First, the required data are extracted from the biometric system that has been gained. Then to get the best match, the data are tested with the identities that are enrolled. The answer of the system will be the identity of the individual. This identity could be the individual's name or his/her ID number.

Verification: The question "Who he/she claims to be?" is answered by the verification mode in the biometric system. The claim is either accepted or rejected. The procedure occurs through matching the biometric sample with those already registered. Verification occurs when the two samples that are matched relate to the claimed identity. This suggests that the derivation of the two trait signatures from the same individual. Verification means a one-to-one process (Hollingsworth, 2010; Proenca, 2006). The main differences between identification and verification is shown in Fig. 5.

Made of four layers, the iris of the eye is the human organ that can normally be seen. The layers already mentioned are

The anterior border layer: Consisting of fibroblasts and crypts of fuchs, this layer has pigment in case the individual has dark iris that is coloured.

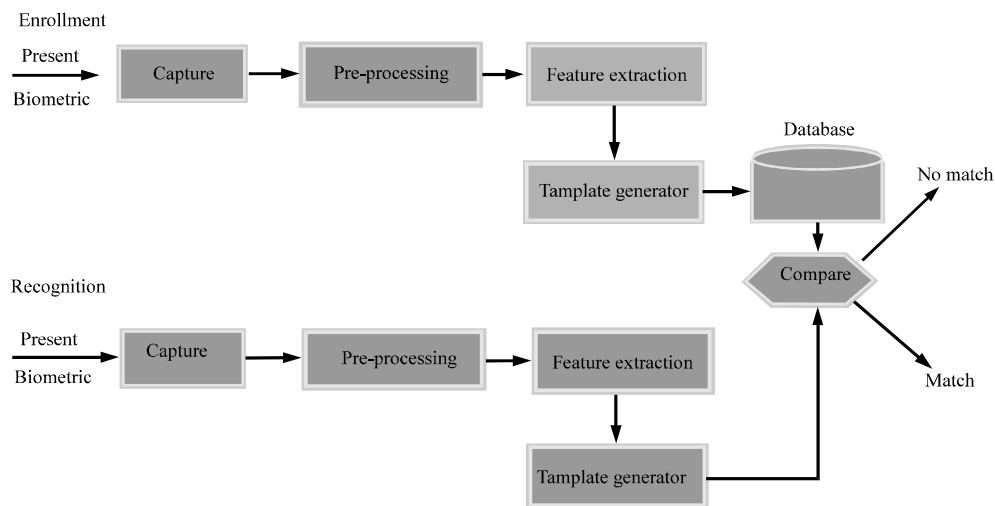


Fig. 5: General operations of biometric system (Kothavale *et al.*, 2004)

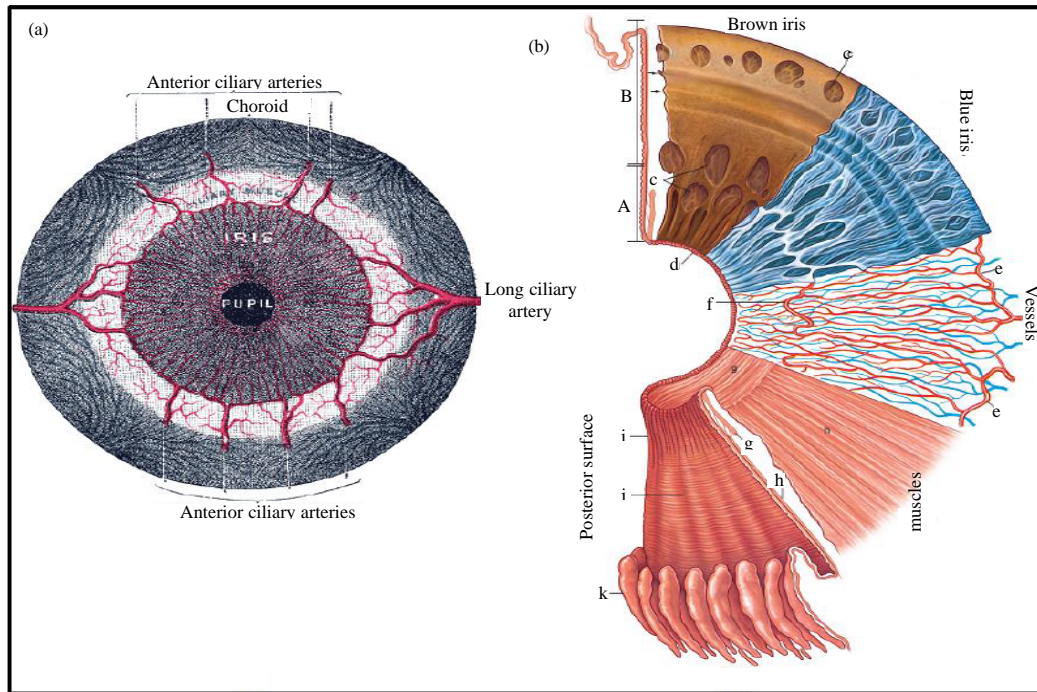


Fig. 6: Human iris: a) Iris front view and b) Composite drawing of the surfaces and layers of the iris

The stroma iridis: Consisting of collagen fibers, most of these fibers radiate towards the pupil of one's age. The latter makes an interwoven structure. The muscles near the pupil of the eye make-up an interwoven structure. These muscles work to regulate the constructions of the pupil. They are also the source of contraction furrows in the iris.

The anterior epithelium: It contains muscles that are arranged in a pattern that can be described as 'radial'.

The posterior epithelium surface: Covered by two layers of pigmented columnar epithelium, this layer is the essential layers that absorbs the light in the it is. The number and the location of the pigmented cells define the colour of the iris. Pigment is absent in the albino. Confined to the posterior epithelium are different shades of blue irises whereas gray, brown and black eyes contain pigment cells in the stroma iridis and the anterior border layer (Irsch and Guyton, 2009).

The iris surface is shown to be divided into two zones. These are inner pupillary zone and outer ciliary zone. What separates these two layers is sinuous structure known as collarette (Strandring, 2016). Depicted in Fig. 6 are complex iris feature which include wofflin spots, iris freckles, pigment frill, crypts of fuchs, crypts in the periphery of iris, iris sphincter, contraction furrows, schwalb's contraction folds and radial furrows.

The structural features of iris play an important role in contributing to a detailed iris pattern within the same



Fig. 7: Unique pattern of the human iris

individual even between his/her left and right eye. A notable trait is that the iris pattern is not genetically determined. It is suggested that even monozygotic twins have patterns of uncorrelated iris (Daugman, 2015; Hollingsworth *et al.*, 2011).

Iris recognition: Iris kind of recognition is a method that attempts to identify people. The method is based on the iris patterns of those people. To define iris it is suggested to be a muscle "that controls the size of the pupil" and that regulates "how much light comes into the eye" (FBI, 2013). Genetically speaking, the colour and anatomy of the iris relate to each other.

However, the patterns which are both random and complex may be described as constant and unique. Figure 7 suggests the complexities of the iris patterns.

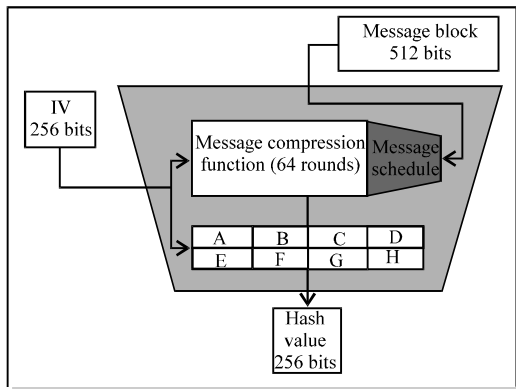


Fig. 8: An overview of the SHA256 hashing algorithm

Iris being considered a robust biometric, iris recognition is now gathering more attention as a research area particularly in the mobile field. Added to this reality is that iris recognition is unlike fingerprints and other kinds of biometrics in the sense that it does not physically require contact with other kinds of biometrics. This is why both companies and researcher try to benefit from iris recognition through exploring the idea to implement it in smartphones. Consumers are now making use of these devices which are available (Fig. 8).

The official NIST standard offers a detailed description of the SHA256 hashing algorithm (Kim *et al.*, 2016). This study offers an overview of the SHA256 algorithm. The latter may be regarded as forming the backbone of the Bitcoin ecosystem. Depending upon the two elements of the pre-image resistance of the SHA256 hashing algorithm and that of collision is the integrity of Bitcoin transactions. It has to be remembered that the SHA256 hash is computed twice in Bitcoin protocol.

The length of input of the SHA256 is <264 bits. Representing a sequence of 16 bits 32-bit words is the block size of 512 bits. The function this 512 bit block is known as the message of comprehension function in words consisting 32 bits. Later, all these relevant details are discussed. The 512 bit message is expanded through the message scheduler into words amounting to sixteen 32 bit words. Performed on words of 32-bit length are the operations that are inside the SHA256 hashing algorithm. These operations employ some light working variables, names known as A-H. The variables are 32 bits in length. Computed at every round are the value of these variables with this process continuing, until the completion of 64 rounds. Additions mentioned henceforth in this text should be interpreted as additions performed module 2³².

A 256 bit Initialization Vector (IV) that is being fixed for the first message block is also taken by SHA256.

Obtained at the end of the first 64 rounds serving as the IV for the next message block is an intermediate message digest. Built by units Davies-Meyer constructions is the SHA256. Here, added to the output at the end of 64 rounds is the IV. The algorithm works to produce an intermediate message digest of 256 bits after the addition of the IV and 64 rounds of the message comprehension function. The complete message blocks having been hashed, we obtain a value of 256 bits. Now, we will have the final message digest of the input message. Now comparable to a block cipher of a 256 bit message block size is the SHA 256 hashing algorithm.

In addition, a 512 bit key (message block is expanded into sixteen 32 bit round keys, using the message schedules for each of the 64 rounds of this block cipher. It is the job of the next section to dive deeply into the insides of the SHA256 algorithm.

Proposed model authentication: This proposed model contains five phases. There are iris data sensor, feature extraction, hash function, hash value and hash chain.

It is obvious that Fig. 9 shows that the principal iris authentication frame work requires, as suggested above, five phases, each one having sub-stages that asks for certain steps to achieve user's enrollment, the final goal of the steps already mentioned.

Iris data sensor phase: The iris image is scanned in this phase for the benefit of the user who participation in the system of iris identification and verification. The phase contain various stages. There are the acts of pre-processing iris data segmentation and iris data normalization.

Feature extraction phase: The processed data extract features from the iris image after being scanned and obtained, later, from the iris image.

Hash function phrase: The hash function which this phase uses is that of secure hash algorithm SHA-256 inputs.

Hash value phase: The output obtained from SHA-256 has a fixed length and a unique quality (256 bits). Having a specific format like the hash value, it is characterized by having leading four zeroes as the figure shows.

Hash chain phases: The structure of the hash chain shows itself as a sequence of four blocks which is a hash function attaches them to each other. A hash and a payload make a block whose hash value is computed throughout the preceding blocks.

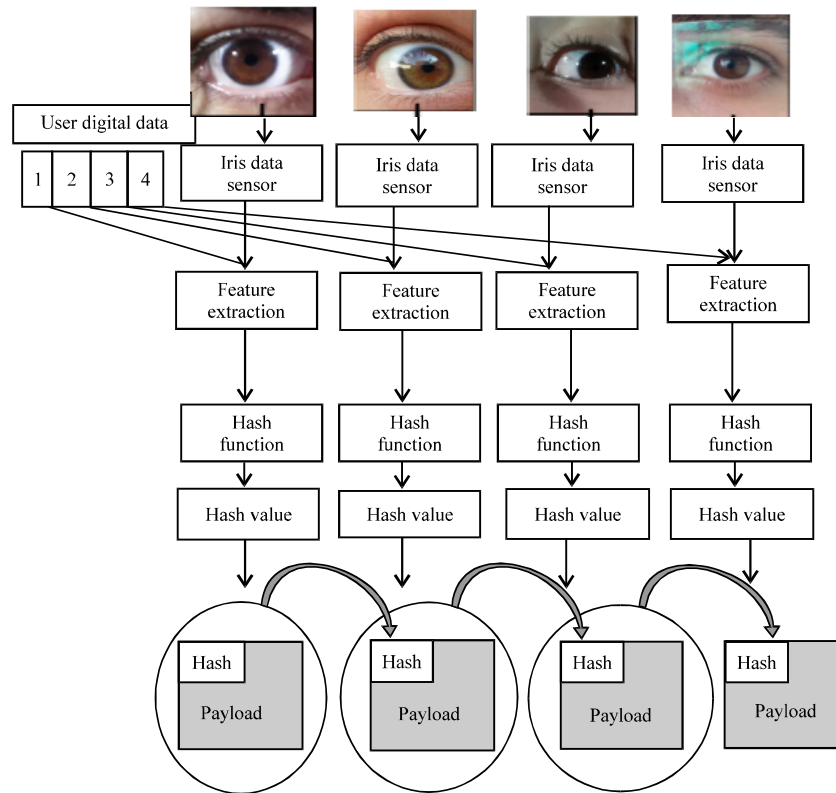






Fig. 9: Proposed model authentication

Table 1: Feature extraction

Images	M1	M2	M3	M4	M5	M6	M7	M8	M9
	0.31482	0.04547	0.35024	0.06840	0.28838	0.49115	0.09441	0.84713	0.08360
	0.31519	0.04555	0.34844	0.06874	0.28941	0.49864	0.09416	0.85176	0.08407
	0.13703	0.03734	0.33530	0.05763	0.30087	0.55470	0.07454	0.89342	0.07040
	0.31392	0.03217	0.34723	0.04913	0.29724	0.51374	0.06524	0.87174	0.05894

RESULTS AND DISCUSSION

The results of the suggested system that has been fully described in the previous study. Are the main concern of this study. The proposed system as this study shows has been represented on a hash chain consisting of four blocks. They system is flexible in the sense that it can be expanded in accordance with our needs. We have employed the MICHE-1 database, after implementing certain procedures on iris data (procedures as preprocessing, segmentation, normalization and enhancement). Feature extraction has been obtained by using a certain method, that is the Zernionike moments.

Table 1 shows this method which uses coefficient of order 9 for the normalized image. The Zernionike moments have the quality of being invariant to rotation.

Table 2 is designed to show the hash value of each block of blockchain after using the algorithm SHA-256. Here, the input is the user's iris feature with its data whereas the output is 256 bits.

The nonce of the block is shown in Table 3. This nonce is a random arbitrary number used to get the specific format of the hash.

Figure 10 shows a sample blockchain. Here, four blocks are chained together, thus, making a blockchain. Each block shows that it has a block number, a nonce

(a)

Block: # 1

Nonce: 11316

Data:

Prev: 00

Hash: 0000ba6817bf3f02efca141410de6dae3332e00371b396244a9cb140ee61f33521aa

(b)

Block: # 2

Nonce: 35230

Data:

Prev: 000017bf3f02efca141410de6dae3332e00371b396244a9cb140ee61f33521aa

Hash: 000017bf3f02efca141410de6dae3332e00371b396244a9cb140ee61f33521aa

(c)

Block: # 2

Nonce:

Data:

Prev: 00006a61d30736b5e5c1d69f0c3ef03da33cc45964f02bd7fb6ecedd419db065

Hash: edc56e3c9904fb3281a9c6e984173a67f1802a43a427900e047d32cce7102cd0

(d)

Block: # 2

Nonce:

Data:

Prev: edc56e3c9904fb3281a9c6e984173a67f1802a43a427900e047d32cce7102cd

Hash: d39b276304624d6cd05e2ce3a6ae8fec7b18250694a2d5b696ab48efb205d30

Fig. 10: a-d) Blockchain

Table 2: Hash value

No. of blocks	Hash values
#1	ba68117bf3f02efca141410de6dae3332e00371b396244a9cb140ee61f33521aa
#2	228f6a61d30736b5e5c1d69f0c3ef03da33cc45964f02bd7fb6ecedd419db065
#3	edc56e3c9904fb3281a9c6e984173a67f1802a43a427900e047d32cce7102cd0
#4	d39b276304624d6cd05e2ce3a6ae8fec7b18250694a2d5b696ab48efb205d30

Table 3: The nonce of blocks

No. of blocks	Nonce	
#1	(ba68) ₁₆	47720
#2	(228f) ₁₆	8847
#3	edc5	60869
#4	s39b	54166

hash, a current block of blockchain. However, the hash of the previous hash points is null (0000000000000000) integer whereas block H-H, as Fig. 4 shows are the second, third and the fourth block of the blockchain. These have the hash points of the previous block.

CONCLUSION

To recapture things, this study attempts to propose a new authentication model for the blockchain. Within the context of an autonomous network, this kind of authentication stands as a secured decentralized storage and a trust information as well. Based on hash function (SHA-256), this iris authentication model reveals quite clearly how the blockchain is used immediately to offer solutions to a problematic area in the field of decentralized an-hoc networks.

In a precise sense, we have shown in this study, the possibility of building a thorough solution that is apt to provide both authentication mechanisms and trust evaluation in a network that can safely be described as both self-organized and evaluative.

ACKNOWLEDGEMENTS

This research was supposed by the AL-Mansour University College, Medical Instrumentation Engineering, Baghdad, Iraq.

REFERENCES

- Anonymous, 2016. Survey on blockchain technologies and related services. Nomura Research Institute, Chiyoda, Tokyo, Japan. http://www.meti.go.jp/english/press/2016/pdf/0531_01f.pdf
- Catalini, C. and C. Tucker, 2017. When early adopters dont adopt. *Sci.*, 357: 135-136.
- Drahansky, M., 2005. Biometric security systems fingerprint recognition technology. Ph.D Thesis, Department of Intelligent System, Brno University of Technology, Brno, Czech Republic.
- Hollingsworth, K., K.W. Bowyer, S. Lagree, S.P. Fenker and P.J. Flynn, 2011. Genetically identical irises have texture similarity that is not detected by iris biometrics. *Comput. Vision Image Understanding*, 115: 1493-1502.
- Hollingsworth, K.P., 2010. Increased use of available image data decreases errors in iris biometrics. Ph.D Thesis, The University of Notre Dame, Notre Dame, Indiana.
- Irsch and D.L. Guyton, 2009. Anatomy of Eyes. In: *Encyclopedia of Biometrics*, Li, S.Z., (Ed.). Springer, Berlin, Germany, ISBN:9780387730028, pp: 11-16.
- Kim, D., Y. Jung, K.A. Toh, B. Son and J. Kim, 2016. An empirical study on iris recognition in a mobile phone. *Exp. Syst. Appl.*, 54: 328-339.
- Kothavale, M., R. Markworth and P. Sandhu, 2004. Computer security SS3: Biometric authentication. Master Thesis, The University of Birmingham, Birmingham, UK.
- Lee, D. and K. Chuen, 2015. Handbook of Digital Currency. 1st Edn., Elsevier, Amsterdam, Netherlands, ISBN:9780128023518, Pages: 612.
- Monteiro, J.C.D.S., 2012. Robust irish recognition under unconstrained Settings. MSc Thesis, University of De Porto, Porto, Portugal.
- Morabito, V., 2017. Blockchain Value System. In: *Business Innovation through Blockchain*, Morabito, V. (Ed.). Springer, Berlin, Germany, ISBN:9783319484785, pp: 21-39.
- Proenca, H., 2006. Towards non-cooperative biometric iris recognition. Ph.D Thesis, Department of Computer Science, University of Beira Interior, Portugal.
- Standring, S., 2016. Grays Anatomy: The Anatomical Basis of Clinical Practice. 41st Edn., Elsevier, Amsterdam, Netherlands, ISBN:9780702052309, Pages: 1562.
- Thavalengal, S., 2016. Contributions to practical iris biometrics on smartphones. Ph.D Thesis, College of Engineering and Informatics, National University of Ireland, Galway, Ireland.
- Zheng, Z., S. Xie, H. Dai, X. Chen and H. Wang, 2017. An overview of blockchain technology: Architecture, consensus and future trends. *Proceedings of the 2017 IEEE International Congress on Big Data (BigData Congress)*, June 25-30, 2017, IEEE, Honolulu, Hawaii, USA., ISBN:978-1-5386-1997-1, pp: 557-564.