Using Blockchain Technology to Validate the Integrity and Confidentiality of Backup Versions on the Cloud

Badr Aleidi[1], Abdulaziz Albesher[1], Mousa Al-Akhras[1+2]
[1]College of Computing and Informatics, Saudi Electronic University, Riyadh 11673, KSA
[2]King Abdullah II School of Information Technology, The University of Jordan, Amman 11942, Jordan
S150004158@seu.edu.sa, a.albesher@seu.edu.sa, m.akhras@seu.edu.sa, mousa.akhras@ju.edu.jo

***Abstract*— The introduction of digital currency (Cryptocurrency) was a consequence of digital revolution that changed the lifestyle worldwide. One of the most successful examples of cryptocurrency is bitcoin, which was established by Satoshi Nakamoto who proposed the establishment of a new financial system based on blockchain technology to enable payment transactions between strangers without the need for a financial intermediary as a third party (bank). This paper aims to find solutions for many issues that are facing researchers who pay huge amounts of money for hosting data on local servers rather than using cloud services. They have several concerns about using cloud services like: Could we host sensitive data in the cloud? Could cloud solutions keep sensitive data safe? Could cloud solutions achieve Confidentiality, Integrity, Availability triad? The paper proposes creating a system with a graphical interface that enables system administrators to take backups of specific data. For example, patient files that saved in an encrypted format using blockchain technique (each backup request means a new transaction based on the previous one). System admin can use the previous key to check the file integrity. Blockchain technique provides strong encryption process that prevents attackers from disclosing confidential data. Moreover, the system admin can detect unauthorized modifications on any version of backup files through reverse hashing operations.**

Keywords—Blockchain; Bitcoin; Cloud; Backup

I. Introduction

The world has witnessed a digital revolution that changed the lifestyle worldwide, from the Internet to the era of social networks, smartphones and cloud computing. This revolution included a radical change in the way of completing transactions from paper to electronic transactions, from fax to email and from traditional currency to digital currency (Cryptocurrency). One of the most successful examples of digital currency was the introduction of bitcoin, which was established by Satoshi Nakamoto [1]. In his article Nakamoto proposed the establishment of a new financial system based on the blockchain technology to enable payment transactions between strangers without the need for a financial third party intermediary such as banks. Bitcoin currency is not scalable for forgery or dual-use, but it provides the users with the advantage of concealing their identities. Moreover, it helps to enhance the conversion speed of financial transactions as well as reduce the cost of financial transactions that remain constant whatever the amount transferred is. Information security experts attempted to generalize the principle of blockchain to use it in solving various problems in several areas [2].

Blockchain technology is a public ledger that contains all transactions that are saved in a chain of blocks, this chain is continuously updated by adding new blocks with every new transaction. There are many characteristics that represent the strengths of blockchain technology in different areas other than the financial field. One of these characteristics is immutable, which means nobody can modify the transactions. Another characteristic is easy to detect modification on any block in the blockchain (as any change is reflected on all subsequent nodes) which gives more reliability and fidelity for this technology. Additionally, there is no single point of failure as blockchain is distributed to the public, which gives more availability. Moreover, blockchain as decentralized service, it does not require an intermediary, just need to consensus algorithms in blockchain that is responsible to maintain data consistency with distributed blockchain, this consequently enhances the performance. Finally, user identity is kept anonymous and auditability is maintained through the ease of verifying and tracking any transactions on the blockchain [3].

The rest of this paper is organized as follows: Section II presents Literature review. Methodology is detailed in section III while implementation details are presented in section IV. Finding and results are presented in section V while conclusions and avenues for future work are presented in Section VI.

II. LITERATURE REVIEW

A. Blockchain Design

Blockchain uses an asymmetric cryptography mechanism to validate the authentication of transactions [3]. Blockchain is a series of blocks that carry transactions information that are related together through parent hash (the hash number of the previous block). The first block in this series is called genesis block which is considered as the core block that does not refer to a previous block, while all other blocks has a reference to a parent block as shown in Figure 1.

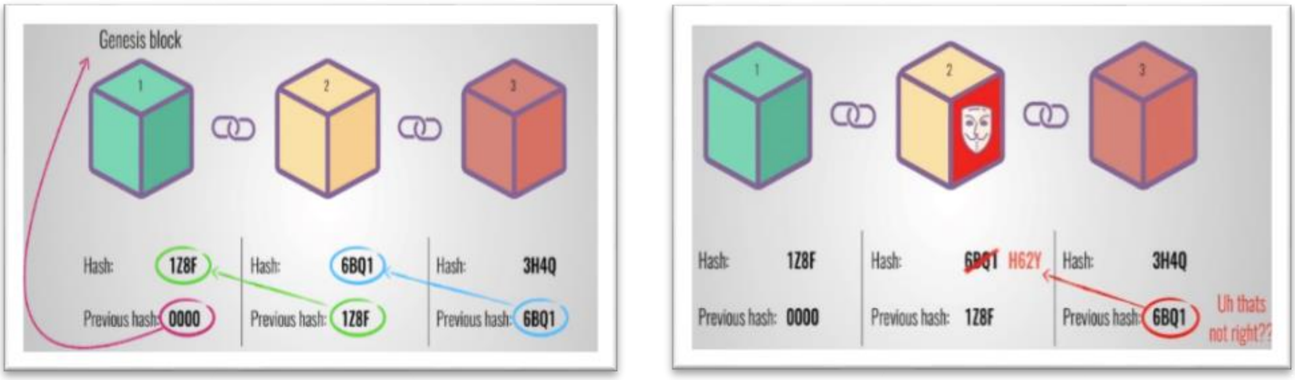


Fig. 1. Blockchain Technology to Validate Integrity and Confidentiality of Backups

B. Blockchain Technology and Bitcoins

Currently, there are various arguments based on the technological terms of blockchain and bitcoin. Both terms are important for financial organizations especially for facilitating a financial transaction. A blockchain is a form of technology that is designed to empower existence of cryptocurrency among other operations in financial transactions. On the other hand, bitcoin is the name utilized for the best-recognized cryptocurrency through which blockchain technology was designed. Moreover, it is essential to understand the meaning of cryptocurrency where as a medium of exchanging currency like dollars, although it is a digital and utilizes encryption methods to control the formation of monetary units and to authenticate the transfer of funds. Blockchain technology and bitcoin are the technologies that have been greatly utilized since 2009 since they were originally designed. The primary factor for the introduction of blockchain technology and bitcoin is the increase in digital era mainly in financial sectors [4].

Bitcoin is usually a model of unregulated digital exchange that was initially designed by Satoshi Nakamoto [1]. This form of technology is also referred to as cryptocurrency, designed with an aim to bypass currency control by the government and streamline online transaction through success clear of third party processing intermediary's payments [5].

C. Blockchain Technology and Bitcoin Operations

Blockchain technology is a form of technology that is easily understood by users. Bitcoin technology is a database and at other times a ledger encompassed of bitcoin transaction files. Considering it as a database operation and it is disseminated across a peer-to-peer network without the need for third-party central authority, participants who are involved in the network are required to agree on the validity of the transaction before they can be filled into the database system. The agreement made by the two parties who are involved in the transaction is known as consensus, and it is attained through mining process. It is essential for the parties involved in the blockchain transactions to be clearly aware of the importance of the transactions conducted and the results of breaching the consensus agreement. The transactions might be conducted for various operations that each of the party is known. After an individual utilizes bitcoin, miner's gets involved in a composite supply-intense computational comparison to verify the legality of the transactions. Over mining, an impervious of effort, which encounters specific qualifications, is designed. A piece of data is regarded as a proof of operation that is expensive and time-consuming to yield, but it can be easily verified through other means. In order to verify the validity of transactions on blockchain, a personal file is required to have a proof of work to indicate that the consensus was attained successfully. Through this method, transaction record cannot be tempered or altered once they have been included in the blockchain [6].

D. Cloud Computing Security Using Blockchain

Companies use cloud components such as Software-as-Service and Platform-as-Service for daily operations and data storage. Therefore, hackers usually make them soft spots for attacks. Blockchain provides several ways for companies to secure their clouds, which can drastically mitigate cyber-attacks. Blockchain sets a model that depends on everyone being vigilant on everyone else in the cloud system. Using this model, users prove their reliability via activities that are validated and written into ledger that all the system users can track. Cryptography algorithm is the exceptional model through which each member validates its identity and activities at any time. Therefore, the authentication process and the cryptography ensures cybersecurity. Blockchain users can apply strong encryption tools, which protects the cloud systems such as e-commerce. In addition, blockchain as a decentralized platform with an advantage that, there is no single access (entry) point that malicious programs can be used for execution. Therefore, using blockchain encryption tools, a company with cloud system can set policies and regulations for their cybersecurity to ensure its critical information is safe [7].

Blockchain provides modern accessibility tools that its users can utilize to improve system security. For instance, applying blockchain-based smart contract method, cloud operations can be sure that data is only accessible or visible to authorized persons. Smart contract techniques also ensure that data is available promptly to members, which improves the security of the system operations. Smart contract is a digital protocol that facilitates operations to assist users exchange goods and services securely and transparently. That is because smart contract is only visible to users entitled to the blockchain, and bars outsiders from obtaining access. Bitcoin also uses this smart contract technique [8].

E. Blockchain and Network Security

Companies utilize blockchain to set up network security with the aim of making their network architecture resistance to cyber-attacks. For instance, Huawei uses blockchain technology to create a stronger mobile network. Companies can use Blockchain Distributed Ledger Technology (DLT) to facilitate open and trusted exchange over the network without utilizing central network server. DLT technology offers provable and secure digital network activities with rights of ownership confirmation [9]. However, with blockchain technology, companies are able to improve cybersecurity. For instance, implementing blockchain method for storing DNS records improves security by eliminating a single target that threatens an entire network system. Some companies implement Ethereum Blockchain and the Interplanetary File System, which is a distributed substitute for HTTP's centralized configuration to protect its DNS system from Denial of Service attacks. This technique also eliminates DNS redundancies and increases performance nodes that guarantee accessibility of transactions to all peers. Network users and their activities are subject to digital login to confirm authenticity. Consequently, elements of a mobile network under Blockchain technology can enable automatic exchange of user information for access privileges to the network resources. Ideally, using blockchain network-timing procedure ensures cybersecurity [10].

F. The Application of Blockchain Technology in E-government in China

In recent years, many governments around the world have sought to develop smart cities in the culture of innovation. Many studies have pointed to the introduction of blockchain technology as a mean to provide smooth and efficient protection to smart cities and their development, encrypt digital transaction systems and develop a new environmental ecosystem that pushes the economy towards growth. One of the blockchain success stories was when the Chinese government adopted e-government service platform that is based on blockchain technology. This idea aims to enhance the level of mutual trust between Chinese government, enterprises, and citizens. Using this system, citizens can access multiple public services from a single point. The Chinese government aimed to find a solution for the individual credit problem by creating a digital identity system, which depends on blockchain technology to guarantee high level of data confidentiality and integrity during transmission. The Chinese government found that blockchain technology provide high-quality services, create one record per individual that can be used for more than one purpose rather than different records and provide credibility and transparency to the public, and can be governed more effectively. Finally, the purpose of using this technology is the high level provided for security against attacks and resistant to any attempt to tamper with its history [11].

G. Blockchain and Internet of Things

Internet of Things (IoT) offers various competitive advantages for companies. It determines the operations of several companies, not only data, but also how, when, why, and where data is extracted. Because of this complexity, a company can encounter numerous cybersecurity challenges while attempting to create a secure IoT for its operations. Organizations can use blockchain technology to mitigate threats to their IoT-based systems because the technology is scalable, confidential, and reliable. Blockchain technology is engineered to track several linked devices that support secure processing of transactions among devices. In addition, blockchain does not have a centralized database, which implies that it is hard for attackers to exploit its operations. Its decentralized database removes single point of failure, making the system more durable for devices to run on. For an improved defense against cyber-attacks, companies use blockchain to confirm device identity, protect sensitive information in transport, and control access to urban automated facilities [9].

III. Methodology

A. Proposed Idea

This research focuses on using blockchain technique to validate the integrity of backups versions on a server or cloud system. The proposed idea aims to find solutions for many issues that are facing researchers who pay huge amounts of money for hosting data on local servers rather than using cloud services. They have several concerns about using cloud services like: Could we host sensitive data in the cloud? Could cloud solutions keep sensitive data safe? Could cloud solutions achieve Confidentiality, Integrity, Availability (CIA) triad?. The main idea of this research is to create a system with graphical interface that enables the system administrator to take backups of specific data. For example, patient files that saved in an encrypted format using blockchain technique (each backup request means a new transaction based on the previous one). Each time the system admin uses the previous key to check the file integrity, this operation could go many times to reach the first file. Blockchain technique provides strong encryption process to prevent the attacker from disclosing confidential data. Moreover, system admin can detect unauthorized modification on any version of backup files through reverse hashing operations as shown in Figure 2.

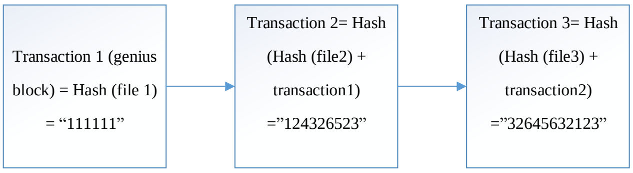

Transaction 1 (genius block) = Hash (file 1) = “111111”
Transaction 2= Hash (Hash (file2) + transaction1) =”124326523”
Transaction 3= Hash (Hash (file3) + transaction2) =”32645632123”

Fig. 2. Detection of Unauthorized Modification

In the implementation of this research, there is considerable reliance on processes provided by Microsoft.Net environment. Especially with the great capabilities that are provided in information security with “Security.Cryptography” library in addition to relying on the principles of encryption, digital signature and hashing. Each time the system calculates the hash value it encrypts the file before saving it in the cloud system to ensure the confidentiality and interconnection of files/data. The main algorithm used for encryption is Rijndael, due to its significant properties that it has resistance to all major known types of attacks, high speed and simplicity of design. On the other hand, MD5 function is used to calculate the hash value, due to easy implementation and difficult penetration. This research attempts to utilize of the properties that enabled blockchain technology to spread globally and the security design applied to secure organization and individuals. This research focuses on how to use blockchain technique to validate the integrity of backup versions on cloud system. The proposed idea aims to find solutions for many issues that are facing researchers who pay huge amounts of money for hosting data on local servers rather than using cloud services.

B. System Analysis

The current system allows system admin to create unlimited backups for the whole database, then the system produces the hash number, which reflects the stage of the backup series. This number is the mean to ensure backups copies in the cloud server are not manipulated since the first backup and even the existing version. Additionally, the system administrator can retrieve any previous version by entering the hash number. The system runs a function that goes over all previous versions and calculates a series of hash values until the current version as shown in Figure 3.

C. Use Case Diagram

The proposed system allows system administrator (user) to sign into the blockchain system to perform four main tasks. Figure 4 shows the Use Case Diagram:

- Take full backup for Microsoft SQL server database.
- Retrieve secure and correct backup version any time from the cloud.
- Validate encryption method: allow admin to try to retrieve backup version without decryption.
- Simulation attack that allows system admin to simulate attacker behavior by retrieving any backup version to the local machine, and make some modification on it and encrypt it again to the cloud. When the system admin attempts to retrieve backup version, the system allows retrieving any version before modification and denies retrieve versions that were exposed to modifications and any later version.

D. Flowchart

The main page of the project is a dashboard that contains links to others pages that contain different functions such as Retrieve, Create Backup, Simulation attack and Try to retrieve backup encrypted. Figure 5 shows the general flowchart of the system.

Figure 6 explains the essential functions in the system that simulates an attack.

IV. Project Implementation

A. Software Requirements

The code was written using Microsoft Visual Studio 2013 and .Net Framework 4.5 as C#.net web application, and targeting data that is saved in Microsoft SQL server 2008 database. In the implementation some of the famous .NET libraries were used to help to use different tools that are already provided by visual studio software such as:

- System.Security.Cryptography.RijndaelManaged: A library that gives the ability to call encryption method (RijndaelManaged).
- System.Security.Cryptography. MD5: A library that gives the ability to call the HASH method.
- Microsoft.Office.Interop.Excel: A library that gives the ability to create, read and write excel sheet.

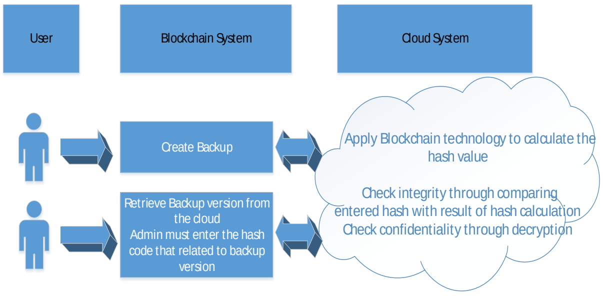

User
Blockchain System
Cloud System
Create Backup
Retrieve Backup version from the cloud
Admin must enter the hash code that related to backup version
Apply Blockchain technology to calculate the hash value
Check integrity through comparing entered hash with result of hash calculation
Check confidentiality through decryption

Fig. 3. System Description

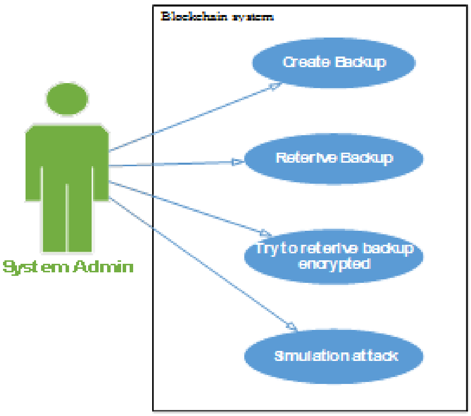


Fig. 4. Use Case Diagram

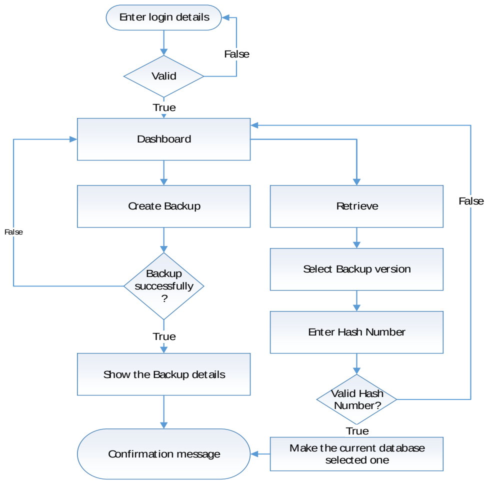


Fig. 5. General Flowchart for the system

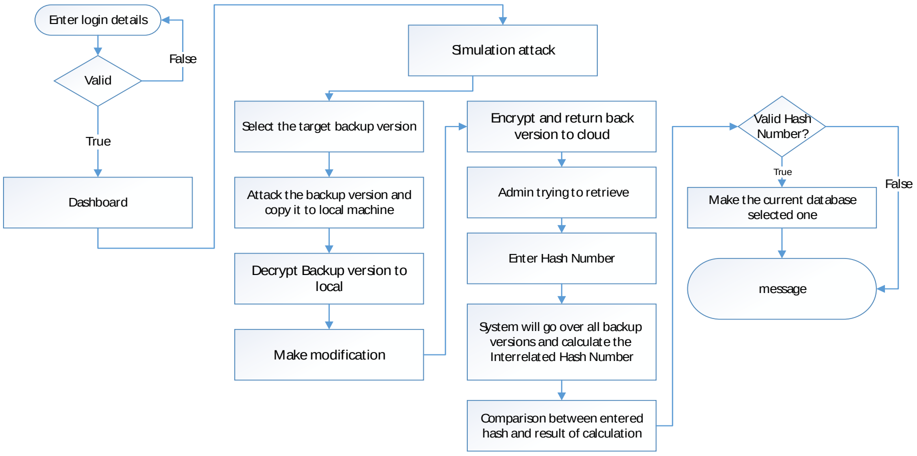

Enter login details
Valid
False
True
Dashboard
Simulation attack
Select the target backup version
Attack the backup version and copy it to local machine
Decrypt Backup version to local
Make modification
Encrypt and return back version to cloud
Admin trying to retrieve
Enter Hash Number
System will go over all backup versions and calculate the Interrelated Hash Number
Comparison between entered hash and result of calculation
Valid Hash Number?
True
False
Make the current database selected one
message

Fig. 6. Simulation attack flowchart

B. *Software Model*

1) *Blockchain:*

This model provides the user with the ability to view current system data (shows the main table that is called "data" in the table) and it allows adding data to this table through a simple form. In addition, it allows the user to create a backup version (.bak), which is considered as the main function in this page. This model uses Rijndael algorithm to encrypt and decrypt data. It also uses MD5 to calculate a hash value as shown in Figure 7.

2) *Retrieve Backup:*

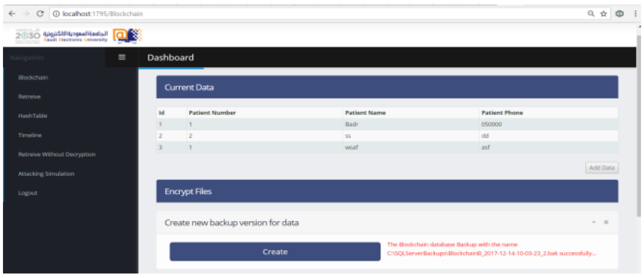
This model provides the user with the ability to retrieve any previous backup version, the only condition is entering the correct hash code that is related to the correct version. The system can detect any manipulation in any previous version of backup files. Every time the user enters retrieve button the system starts calculating the hash value since the first backup file, then it compares the result with the entered one by the user. This model uses Rijndael algorithm to encrypt and decrypt data. Furthermore, it uses MD5 to calculate the hash value as shown in Figure 8 (Retrieve page).

3) *Attacking Simulation:*

This model simulates the attacker behavior by enabling the admin to select one backup version from the list, decrypt the selected version in another folder (attacker device), make changes to the backup version, encrypt the backup version on the cloud again and attempts to retrieve the file. In addition, the system displays "The Entered Hashing code is not correct, there are some modification on backup file" for a version that is manipulated or any version that comes after the manipulated one in addition to the corrupted backup file.

V. Finding and Results

Blockchain is a technology for a new generation of applications that provide trusted, reliability, and transparency to run business processes efficiently. Blockchain is a public or common record that keeps all transactions and allows the subscriber network to electronically access a copy of this record, and add a new transaction to it (in block shapes). Moreover, this technology helps to maintain lists of resistance to tampering with growing data records, and allow the secure exchange of valuable material such as funds, stocks or data access rights. Unlike conventional trading systems, there is no need for a broker or central registration system to follow the movement of exchange as all parties are dealing directly with each other. The simple and effective nature of blockchain technology enhances security and reduces risks associated with digital certificates and certification authorities. Blockchain is a good way to keep CIA traid, by preventing unauthorized users from disclosing and manipulate confidential data, in addition to providing data in public record which ensures data availability in a suitable place and time. The great success and significant impact achieved by blockchain technology in the economical field was due to the provision of a direct, efficient and secure financial transaction which motivated individuals, companies and countries to conduct further research. The research results conducted from this technology contributed in providing better services and reduce costs for other fields.



Current Data

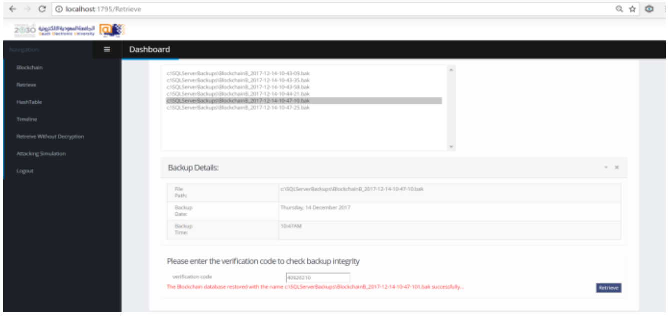
Id	Patient Number	Patient Name	Patient Phone
1	1	Badr	050000
2	2	ss	dd
3	1	wsaf	asf

Encrypt Files

Create new backup version for data

The Blockchain database Backup with the name C:\SQLServerBackups\BlockchainB_2017-12-14-10-03-23_2.bak successfully...

Fig. 7. Take Backup page



c:\SQLServerBackups\BlockchainB_2017-12-14-10-43-09.bak
c:\SQLServerBackups\BlockchainB_2017-12-14-10-43-35.bak
c:\SQLServerBackups\BlockchainB_2017-12-14-10-43-58.bak
c:\SQLServerBackups\BlockchainB_2017-12-14-10-44-21.bak
c:\SQLServerBackups\BlockchainB_2017-12-14-10-47-10.bak
c:\SQLServerBackups\BlockchainB_2017-12-14-10-47-25.bak

Backup Details:

File Path:	c:\SQLServerBackups\BlockchainB_2017-12-14-10-47-10.bak
Backup Date:	Thursday, 14 December 2017
Backup Time:	10:47AM

Please enter the verification code to check backup integrity

verification code: 40926210

The Blockchain database restored with the name c:\SQLServerBackups\BlockchainB_2017-12-14-10-47-101.bak successfully...

Fig. 8. Retrieve Page

Many researches have been conducted in an attempt to take advantage of the blockchain technology to maintain information security like using blockchain technology in: Identity protection [12], maintain privacy, maintain anonymity [13], secure data storage, secure cloud computing, network security, Internet of Things. Blockchain technology demonstrated high efficiency in maintaining information security through providing a hash function that ensures the integrity of data and encryption method, which makes sure information are kept confidental from unauthorized persons.

It is possible to take advantage of this technology in helping system administrators maintain integrity and confidentiality of backup files in databases. This can be done by enabling two key functions which are encryption and hashing. This research can be utilized to achieve effective data protection and help in achieving CIA triad.

VI. Conclusions and Future work

Blockchain is a technology for storing and verifying digital transactions on the Internet with high security and encryption, which are not feasible to break under the technologies available today. The technique was developed in 2009 by Satoshi Nakamoto who created an electronic currency called Bitcoin, which is fully encrypted based on blockchain. Bitcoin is not governed by any central authority and is not subject to any central laws. Therefore, the exchange currency is directly between the dealers without the presence of intermediary process, which completely abandons the role of the bank-sector from the business transactions. There are numerous applications for blockchain technology, a factor that makes it suitable to be facilitated in business for security purposes while transacting finances. This is a new technology that has greatly improved the global economy since it is possible for parties to trust each over a long distance through the blockchain records and be able to conduct business operations suitably. It is important for the technology to be more facilitated on its numerous operations to achieve better future for currency transaction and improve trust amongst business operators.

There are many benefits of blockchain technology, but on the other hand, there are some limitations such as: the time required to calculate the value of the hash each time, the expected problems of growth (scalability) and the need to know the hash number associated with its backup version.

This research can be extended to protect backups of systems, not just databases, detect any manipulation in files and enable researchers of placing data in the cloud with a guarantee of integrity and confidentiality.

References

[1] S. Nakamoto, Bitcoin P2P e-Cash Paper, Originally published in The Cryptography Mailing List (Mailing list), October 2008. Retrieved from https://www.mailarchive.com/cryptography(metzdowd.com/msg09959.html

[2] A. Nordrum, Wall street occupies the blockchain - Financial firms plan to move trillions in assets to blockchains in 2018," in IEEE Spectrum, vol. 54, no. 10, pp. 40-45, October 2017.

[3] Z. Zheng, S. Xie, H. Dai, X. Chen and H. Wang, An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends, 2017 IEEE International Congress on Big Data (BigData Congress), Honolulu, HI, 2017, pp. 557-564.

[4] T. Laurence, Blockchain for Dummies, Hoboken, New Jersey: John Wiley & Sons, 2017.

[5] A. M. Antonopoulos, Mastering Bitcoin: Unlocking Digital Cryptocurrencies, Sebastopol, CA, USA:O'Reilly Media, Inc, 2014.

[6] M. Swan, Blockchain: Blueprint for a New Economy, US:O'Reilly, 2015.

[7] J. Wertz, Cybersecurity: How Blockchain is helping e-commerce business protect their data, 31 October, 2017. Retrieved from Forbes : www.forbes.com/

[8] D. Drescher, Maintaining the History of Transfer. In Blockchain Basics: A Non-Technical Introduction in 25 Steps. Frankfurt: Apress, 2017, pp. 66-70.

[9] E. Langberg, Blockchains in Mobile Networks, 25 June, 2016. Retrieved from Hiawei: http://e.huawei.com/en/publications/global/ict_insights/201703141505/core-competency/201703150928

[10] S. Foresti, Cryptology and Network Security, 15th International Conference on Cryptology and Network Security, Milan, 14-16 November 2016, pp. 147-152.

[11] H. Hou, The Application of Blockchain Technology in E-Government in China, 2017 26th International Conference on Computer Communication and Networks (ICCCN), Vancouver, BC, 2017, pp. 1-4.

[12] D. Tapscott, A. Tapscott, "The Blockchain Revolution: How the Technology Behind Bitcoin is Changing Money Business and the World", Portfolio, 2016.

[13] S. Raval, Decentralized applications: Harnessing Bitcoin's Blockchain technology. O'Reilly, 2016.