International Journal of Future Generation Communication and Networking
Vol. 13, No. 1s, (2020), pp. 01- 07

Advance Online Payment Security Using Qubits Integrated Blockchain

Bhavin Gajjar [1], Jishant Acharya [2]
[1,2] *Student, University of Mumbai , Atharva College of Engineering,Mumbai*

Abstract

Current era of technology works with cutting-edge computing power, which is evolving incessant. With this, data storage and distribution be imminent. When data distribution we talk about, automatically security comes into the view. Data can be of any type. But the main concern for data transaction is related to the confidential data like business transactions, policies and finance related documents as well as all financial transactions. In those cases, security of all these transactions has utmost importance which can't be oblivious to. Hence, it is important to think whether the existing security methods are enough to actually protect us against the threat lying ahead of us? Now-a-days when we talk about finance and related transactions, avoiding mentioning Blockchains is simply absurd. Blockchain technology invented to tend age-old human trust problem. It emerged in the market by letting digital information distributed in the market but not copied the same transaction by any chance. So, by using the leading and most secured online transaction platform: blockchain and furthermore enhancing it by integrating it with the most promising future technology Qubits, we may can actually overcome the existing security threats. While talking in terms of computer nothing is actually random, everything is algorithm based and predictable, by introducing Qubits we can overcome this loophole.

Keywords: *Online transactions, Quantum bits, Blockchain, Security, payment, gateway.*

1. Introduction

The world is changing at an exponential rate, so are the latest technologies as well as security parameters associated with it. Whereas, when it comes to security one must not forget about the threats and challenges that a certain technology needs to face. The drastic increase in the availability of super computers as well as their incomparable computing capabilities are undoubtedly a major obstacle that world will be facing in the upcoming future [4].

Blockchain is the leading technology in the field of online transactions [6]. Blockchain is basically a series of blocks connected to each other by means of cryptography. Blockchain technology consists of various components including public and private keys. While the public keys are known publicly, private keys are kept hidden and used for encryption purpose [9]. The task to confirm or to authenticate a payment is distributed among several miners and each of them validates the transaction by solving a complex mathematical problem which is also known as proof of work. Once the computation is performed the blocks are generated as per the longest chain rule i.e. miner with the fastest computational power will be able to mine the block and that block will be appended in the current blockchain.

Quantum computers obey the rules of quantum mechanics. Because of the superposition and quantum entanglement states it is possible for a quantum bit (also known as Qubits) to exist in more than one possible state. Hence while a single bit of a classical computer can either represent 0 or 1, due to spin of electron a quantum bit is capable of existing in 0 and 1 state at the same time. In a nutshell we can say that when it comes to computational power, a problem which can theoretically take up to thousands of years for solving can be solved using quantum computers within few seconds [2, 3].

2. Existing System

While using the conventional Online as well as offline payment system Banks have adopted centralized system [10] approach. By centralized approach means, neither for offline banking user need not go physically to the branch of the bank where he/she has registered for banking transactions nor he has separate login branch-wise for doing online transactions. Here when the user wants to perform any kind of transaction online, he/she needs to select activity to be performed.

ISSN: 2233-7857 IJFGCN

Once its selected then user approves for the transaction with the help of OTP or secure PIN. Then his/her details are travelled through a secured gateway to the payment processing authority a.k.a. the bank. Bank further transfer those details to RBI (India) or to central authority who has total hold on all banking transactions. Then RBI (India) validates the transaction and determines whether the transaction can be completed or not and if not, then what is an alternative. Although information passing through the gateways are encrypted using complex algorithms, If the gateway is compromised or say if the algorithm is decoded then the entire payment information is at risk.

Consider an example:

Say a user named 'Bob' wants to make a purchase using the online transaction. He wishes to use his credit / debit card for this purpose. There is a malicious user named 'Amy' who has compromised the gateway security and can access the information. As soon as Bob begins the transaction his details are passed through the gateway, this information contains the payer, payee and amount. As Amy has the access over the gateway channel, she can alter information such as, she can change the 'payee' address or has the control over the 'amount'. At the end of transaction Bob comes to know that double the 'amount' is debited or the transaction is made for some unknown user.

There is another scenario in which the Bank or 'centralized authority' and 'payment processor' is compromised. As the entire processing is handled by a single authority, there security status can be altered.

3. Proposed System

Considering the peculiarity of superposition provided by the quantum bits and a blockchain supported distributed network, we can actually improve the current online transaction security aspects [7]. By using a quantum gateway to convey the information as mentioned further in this paper, the information can be carried out without any insecurity. By converting the centralized entity 'bank' into a dedicated network of computers which will participate in the process of verifying the transaction by solving complex problem using both computation power and sufficient time we can achieve better reliability aspects.

Even though gateways and payment processing system are encrypted using highly complex algorithms they are not completely random. These algorithms take considerable amount of computation power by a third – party user for decoding. If we are able to achieve exceptionally higher computation power then all these algorithms are easy to break.

The entire Proposed System can be understood in following points:

1. Replacing Classical bits with the Quantum bits.

2. Using Quantum states to improve security aspects.

3. Converting the centralized system into distributed network.

4. Using blockchain mechanism for verification and storage purpose.

5. Use of 'nodes' as miners in process of verification.

What is the need of Proposed System?

Let's take example of the SHA1 algorithm that was just recently broken by Google using something which is known as a 'collision' [1]. SHA1 was an algorithm that was used as the standard to encrypt any kind of data and it boasted that no two files can have the same hash value that it generated. This was taken up as a project by Google that possess an ample amount of compute. Very recently they broke the algorithm by making a PDF file such that it generated a hash value that was exactly the same as a file that was completely different. This is for sure a one-off occurrence but an occurrence nonetheless. This warrants the answer to the question that if someone with ample resources try to break the payment system. Is the compromise possible? The problem is the pseudo randomness of all the contemporary algorithms. All anyone has to do is to find a

ISSN: 2233-7857 IJFGCN

lacuna in the system and exploit as pleased. This collision attack was a breakthrough for the company but an eye opener for the security of the people that use the public entity of Internet.

As far as true randomness is concerned it can be achieved by using the quantum bits. Quantum bits exhibits the dual nature property hence at any moment position of a quantum bit can be described in terms of probabilities. This nature of quantum bits can be used to achieve unimaginable computing power as well as a solid pillar for future cyber security.

4. Working

This entire process of transaction can be divided into 4 major cycles.

a. Customer Request

b. Payment Gateways

c. Payment Processor

d. Completion of Transaction

Diagrammatic Representation

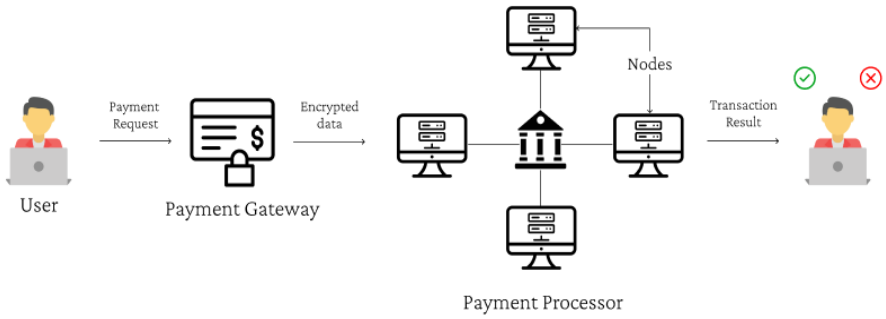


Figure 1. Schematic Workflow

a. Customer Request

A customer is the payer willing to request for a transaction using the online transaction service. At the time of registration, say registration for net banking or registration for debit / credit card the customer is provided with two unique keys. One is the public quantum key and another is the private quantum key. We are using the quantum bits instead of 256-bit keys used in traditional blockchain. The private quantum key is the unique identification for each customer. The public quantum key can be used as payer's or payee's address. i.e. whenever a transaction is requested it is carried out to the public quantum key address or we can transfer money to someone's public quantum address. Customer's public quantum key is sharable while the private quantum key is kept private. Public quantum keys are generated on the basis of private quantum keys using some highly complex algorithm. Now the question may arise that if the public quantum key is generated using some algorithm and the algorithm is known to a third – party user then private key can be easily compromised. But this is when the quantum nature comes to the rescue. As a quantum bit can exist in both 0 and 1 state simultaneously the whole public quantum key is just set of bits which are 0 as well as 1 at the same time. In laymen terms while sharing a public quantum key of 'n' bit length we are providing a set 2^n public quantum key at the same time and one among this is the actual public quantum key generated by the public private key. Once users possess both public quantum and private quantum key, he/she is eligible to participate in the transaction process. Once the customer initializes the transaction all the data including customer's public quantum key and the amount to be paid and payee's public quantum key is passed to the payment gateway.

b. Payment gateway

ISSN: 2233-7857 IJFGCN

Payment gateways are responsible for conveying the data from customer portal to the Payment processor. The gateway is designed for safe data transfer. Once data is entered in the gateway it is encrypted for better security point of view. As data is encrypted in order to obtain the data one needs to decipher the data first, even after deciphering the quantum nature barrier is still present. We are heavily using the term quantum nature so let us understand how a quantum bit is actually more powerful and more secured as compared to classical bit.

Say We want to transfer two bits of data,

- Using the classical bits, we can transfer

  00, 01, 10, 11

  any one of these combinations, one at a time.

- But if we use quantum bits, we can transfer multiple states of bits at the same time. As quantum bits exist in 0 and 1 state simultaneously at the same time, we can say that each bit of the two data bit is also present in superposition state.
- Because of superposition we are transferring 4 states of 2 data bits simultaneously.
- Henceforth while the classical bit transfers 1 combination of all 4 possible state at a time the quantum bit is transferring all 4 states.
- Hence quantum bits are responsible to convey 2^n states where 'n' is the length on bits for this particular case, length of data bits is 2 hence $2^2 = 4$ quantum states.
- This is an exponential function hence the number of states will keep increasing with increase in exponential power.

  $2^3 = 8$ quantum states

  $2^4 = 16$ quantum states

  $2^5 = 32$ quantum states

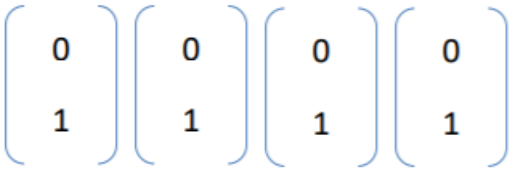
- So, let's say the gateway channel is compromised and the malicious user has control over the gateway and knows about the decoding algorithm

In case of classical bits,

- Encrypted message is: ZhY6721
- But the malicious user has the decoding algorithm and he/she can decode the encrypted message.
- Decrypted message: 1011
- Which is the original public key of the user (Note: Here we have used only 4 bits for the sake of simplicity in explanation the original public key may contain a greater number of bits)

If the same scenario happens during the transfer of quantum public key let's see what happens

- Encrypted message is: ZhY6721
- As mentioned above malicious user can decipher this message but when he/she does the following output is obtained
- Decrypted message:



ISSN: 2233-7857 IJFGCN

Note: This is diagrammatic representation to describe the superposition state.

As seen above this is how the message is decrypted. If we form set of all possible states it will be something like following:

- Quantum states = { 0000, 0001, 0010, 0011,

  0100, 0101, 0110, 0111,

  1000, 1001, 1010, 1011,

  1100, 1101, 1110, 1111 }

  This are all the possible combinations which are getting transferred at the same time the possible public quantum key could be a one of the above combinations or set of more than one combination.

- As explained above use of quantum keys drastically increases the security of the payment gateway.

Once the data is transferred through the gateway it reaches the payment processing.

c. Payment processor

Payment processor receives data through the gateway. Payment processor is responsible to authenticate the transaction. Hence at the end of a process Payment processor decides whether the transaction requested is valid or not. The transaction will be discarded if public quantum key is tempered or insufficient funds are available in customers registered account. The additional security feature that will be added during this process is hash value for the verified transaction. Each transaction is saved as blocks of information. These blocks contain the information obtained from gateway as well as the hash value. The hash value is also responsible to identify the block adjacent to current block. If by any external source the information present in a block is tempered then a new block is added to the consisting sequence hence it follows functionality of blockchain. All the blocks are immutable which makes this method more secure.

In the traditional payment verification technique either bank or the payment processor companies are responsible to verify the transaction but again this is a centralized system which can be improved using a distributed computer network. Thus, this advance payment processing system consist of distributed network, in which all computer present within network works as a node which are responsible for verification of incoming transaction.

- **Nodes**

Nodes are nothing but computer present within distributed network which will verify the transaction by solving a complex mathematical problem. In blockchain architecture proof-of-work is mandatory because the network is established worldwide and all the miners get mining fees hence, they need to show the proof-of-work. But our system is close to a private blockchain where only authorized computers get the chance to participate in verification of transaction.

This proof-of-work will benefit us in two ways first it will delay the process of adding new blocks in existing chain and hence it will become more and more difficult to alter the entire blockchain data. Secondly this proof of work will be used as the hash value for a block. As transaction is verified by more than one node present in computer network, only the transaction which was approved by more than 51% of nodes is allowed to enter in the blockchain, and the hash value of this newly mined block is complex combination of hash values obtained by different computers present in that network.

Not all nodes verify a single transaction, but an algorithm is used to determine how many nodes will participate in a network, based on amount to be transferred. Hence multiple transactions can be verified depending upon the computational power of network.

ISSN: 2233-7857 IJFGCN

Once this network of nodes verifies transaction a new block is mined and is added to the blockchain. This blockchain is downloaded on a computer whenever a new computer is added into the system. Hence even if some of the computers are tempered even then the transaction can be verified using 51% majority policy.

Another update algorithm is used to update the corrupted nodes within a network as it can become expensive to replace a computer every time a node is tempered.

After the successful verification of a transaction the result is passed to the final stages and system proceeds towards completion of transaction.

d. Completion of transaction

After the transaction is verified through the payment processor, transaction obtains a tag of complete or failed if transaction is completed successfully then amount is debited from payer's account and is credited in payee's account. Otherwise there is no change.

The failed transactions are also added to the chain just to keep a tab on the transactions and also to refer back to them in case they are needed to be shown as a proof of failure in the future.

5. Roadblocks

The technology being in the absolute nascent stage as it is, the first and the obvious roadblock comes in the form of the cost of adaptation of the technology. This can be seen in example of displays where the obscure 4K panels that used to cost an arm and a leg just 5 years ago have gone down in price significantly due to the popularity of the tech.

Quantum technology is relatively new; it is in fact the newest and the most promising field that the scientists have devoted themselves to. The breakthroughs are of the magnitude that a particular problem that could have taken more than 10,000 years was done in fewer than 10 mins. This magnitude of improvement will help implement this very compute heavy task faster. The assumption was appropriately made that in the future we might have the power of unlimited compute. This was in lieu of the current breakthroughs in the technology. Google's achievement of quantum supremacy using a mere 54 Qubits is a huge push towards the technology getting available to the masses and not being obscure as it is right now. Quantum Supremacy means that the complexity of the gates emulated by the quantum computer are impossible to be emulated by classical supercomputers

This is quite complex to setup and the compute needs are going to be through the roof, if we try to implement this now there are going to be many questions that we will need answers to, but the main thing that we should focus for now is that if this mechanism falls into place and works harmoniously the payment systems will be hack free.

The miscreant will have to go to the very basics involving electrons to break it, which is, as we all know never going to be easy as the variables are just not something we can take into account.

6. Future scope

This system can make blockchain payments a thing that is not just limited to the niche of the crypto-currency realm but is present to the masses and makes the payments more secure than ever. The development of this can very efficiently make blockchain payments more secure and also with the performance improvements that are going to be through the roof make it available to the masses and make security a democratic affair.

Currently, the non-truly random algorithms have succumbed to numerous hacks and have led to a loss of a very big number of people. The system will change the internet for the better because truly random nature of this implementation will make internet the most secure thing.

The future of this implement is as vivid as the imagination can get and also is as vast as one can imagine. It can be used to make the authentication process secure where the data goes in a

ISSN: 2233-7857 IJFGCN

quantum hash form. This can be used to store sensitive data on the internet more securely as we can make use of the very basic random nature of the implementation and exploit it in a manner that we see fit. We can even make the most secure messaging application that can only be seen by the sender and the receiver. Evidently, the scope is limited by imagination and not by implementation. The most important thing that we have to take care of is that this is a technology that has to be used by all but in a very streamlined manner because the encryption can also do more harm than good in the wrong hands or with the wrong implementation of it.

7. Conclusion

We have proposed a scheme for upgradation of current online transaction method, to sustain security aspects. By implementation of a quantum gateway and converting transaction processing system into a distributed system we can enhance the functionality and restrict the susceptibility against possible threats. Considering all the good and counter points written in this paper it is safe to assume that quantum technology is promising for the upcoming future and if we use it we can achieve things that were once unimaginable.

References

1. Google Security Blog February 23, (**2017)** By, Marc Stevens (CWI Amsterdam), Elie Bursztein (Google), Pierre Karpman (CWI Amsterdam), Ange Albertini (Google), Yarik Markov (Google), Alex Petit Bianco (Google), Clement Baisse (Google) .https://security.googleblog.com/2017/02/announcing-first-sha1-collision.html
2. D. Chaum," Blind signature for untraceable payments", in: Advances in cryptology, Proc. of CRYPTO'82, Springer, pp. 199-203, **(1983).**
3. M. Nikooghadam and A. Zakerolhosseini, "An efficient blind signature scheme based on the elliptic curve discrete logarithm problem, "The ISC Intl J. of Inf. Security vol. 1, no. 2, pp. 125-131, **(2009).**
4. C. Bennett and D. DiVincenzo, "Quantum information and computation," Nature, vol. 404, pp. 247-255, (**2000).**
5. M. Nikooghadam, A. Zakerolhosseini and M. E. Moghaddam," Efficient utilization of elliptic curve cryptosystem for hierarchical access control," The J. of Systems and Software, vol. 83, pp. 1917-1929, (**2010).**
6. Zheng Z, Xie S, Dai H, et al. An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends[C]. IEEE International Congress on Big Data. IEEE, (**2017).**
7. C. Elliott, D. Pearson and G. Troxel, "Quantum cryptography in practice," in: SIGCOMM03: Proc. of the Conf. on Apps.,Tech., Arch., and Protocols for Comp. Commun., ACM Press, New York, pp. 227- 238, (**2003).**
8. P. Dirac, "The principals of quantum mechanics," 4th Ed., Oxford university press, New York, 1858.
9. Satoshi Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System, 2008, Online, http://bitcoin.org/bitcoin.pdf.
10. Haiping Wang, "Online transaction process: An experience perspective" ,(**2010)** 2nd International Conference on Industrial and Information Systems.

ISSN: 2233-7857 IJFGCN