Security Analysis on Block Chain using the Ecc and Sha Algorithms

B.Aruna , A. Ajay Prakash, M. S. Srinija

Abstract: This paper thinks about blockchain innovation - which is getting solid consideration from the business and furthermore being connected in numerous fields. Passwords assume an imperative job in day by day life in different figuring applications and assume a basic job in online confirmation. The fundamental go for utilizing passwords is to limit unapproved clients to get to the framework. Blockchain, as a new age technology, provides the necessary tools to ensure data integrity and data protection using some encryption. Smaller transaction size and higher transaction efficiency are the essential requirements of the blockchain.

Key words: Block chain, SHA-256, ECC (Elliptic curve cryptography).

I. INTRODUCTION:

A blockchain is an innovation for another age of value-based applications that, through an aggregate accord instrument combined with the utilization of an extensive, decentralized and shared open record book, manufactures trust, responsibility and straightforwardness while streamlining business forms. An assortment of information exchange is made conceivable over the web utilizing different techniques. From these information a portion of the data is exceptionally mystery which requires an extraordinary security, in this manner, a broad security measures must be embraced. Numerous calculations and procedures can be utilized to verify our information or data from dangers. Hashing is the point of cryptography .The cryptography is a method for verifying message and information over the web we realize that, information is available on around the world web is twofold step by step to verify these sort of information we are give a unique mark to its realness .Message Summary is one way where an ace unique finger impression has been produced to provide a message validation code (hash code).The SHA for example Secure Hash Algorithm is fundamentally in view of the idea of hash work. The essential thought of a hash work is that it takes a variable length message as info and produces a fixed length message as yield which can likewise be called as hash or message-digest. The trap behind structure a decent, verified cryptographic hash work is to devise a great pressure work in which each info bit influences however many yield bits as could be allowed. It is utilized with the Digital Signature Standard (DSA) for advanced signature so it has a specific significance. In this we are going to discuss on the security issue of the user privacy. which will be solved by the ECC (Elliptic Curve Cryptography) algorithm which will be based on a mathematical equation and additionally we are adding the Sha algorithm in the System will be the additional.

II. LITERATURE REVIEW

2.1 BBDS: Blockchain-Based Data Sharing for Electronic Medical Records in Cloud Environments

They proposed a blockchain-based data sharing framework that sufficiently addresses the access control challenges associated with sensitive data stored in the cloud using immutability and built-in autonomy properties of the blockchain. Our system is based on a permissioned blockchain which allows access to only invited, and hence verified users.

2.2 Authentication with Block chain Algorithm and Text Encryption Protocol in Calculation of Social Network.

They proposed a calculation named CMCR for a client driven system in Paper, a novel calculation dependent on Clique Theory, PageRank, LDA, and TF-IDF used to tackle the issue. Test results demonstrate that the proposed calculation can beat gauge calculations in some regular criteria. Be that as it may, when planning this calculation, there is a slight absence of client security and client data insurance.

2.3 Implementation of IoT system using block chain with authentication and data protection.

In a square chain IoT condition, when information or gadget confirmation data is put on a square chain, individual data might be spilled through the evidence of-work procedure or address look. In this paper, we apply Zero-Knowledge verification to a shrewd meter framework to demonstrate that a prover without uncovering data, for example, open key, and we have considered how to improve obscurity of square chain for security assurance.

2.4 Block chain based data security enhanced IoT server platform.

They proposed another IoT server stage by presenting a square chain and store sensor information in a square chain. Mobius chose IoT server stage, Mobius validates IoT gadgets complying with oneM2M standard, gets constant sensor information, stores data and information in Mysql server and oversees it.

Revised Manuscript Received on June 07, 2019.

Ms.B.Aruna, Department of ECM, Koneru Lakshmaiah Education Foundation, Vaddeswaram, A.P., India.

A.Ajay prakash,Department of ECM, Koneru Lakshmaiah Education Foundation, Vaddeswaram, A.P., India.

M.S.Srinija, Department of ECM, Koneru Lakshmaiah Education Foundation, Vaddeswaram, A.P., India.

*Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication*

2.5 Bitcoin: A Peer-to-Peer Electronic Cash System.

An absolutely distributed variant of electronic money would permit on the web instalments to be sent straightforwardly starting with one gathering then onto the next without experiencing a monetary establishment. Computerized marks give some portion of the arrangement, yet the primary benefits are lost if a believed outsider is as yet required to avert twofold spending. We propose an answer for the twofold spending issue utilizing a shared system.

III. THEORITICAL ANALYSIS

3.1 Security Analysis using Block Chain

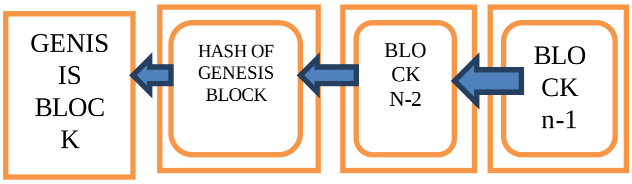
First the User will have the key to authenticate himself then,the issuer generates a set of membership issuing keys and membership verification keys.The issuer then shares the membership verification keys with the verifier. A user who wants tojoin this permissioned group sends a request to the issuer. The issuer is tasked to authenticate the user and accept the user into the group or deny user entry into the group. In the blockchain we all can see the how transition happens as per the constraints that the transaction will take place between two persons and without the third party and it will lead to more Secure and also no problem of leakage of data out from the people who are in the blockchain and no chance of hacking from the third party as there will be only two people in the transaction so if anyone comes in between the transaction and also it will be updated to everyone and that will be the proof of work and which cannot be deleted so that if any kind of activity like checking the data, providing the authorisation and entering the chain for the observing the data etc,. Kind of action will be stored in the blockchain as transactions. For the sack of privacy issue, we are going to add the Elliptic Curve Cryptography (ECC) which will be encrypting the person information who are involved in a transaction where will be two persons be involved in atransaction. So, the transactions will be visible to those who involved in the transaction only remaining people will be kept encrypted but the Accounts and the transactions happened in the chain will be updated for the people in the blockchain in the encrypted form.

3.2 BLOCK CHAIN OVER VIEW:

Blockchain is the decentralized overseeing procedure of Bitcoin, intended for issuing and exchanging cash for the clients of the Bitcoin money.This method can bolster the open record of all Bitcoin exchanges that have ever been executed, with no control of an outsider association [1]. The benefit of Blockchain is that the open record can't be adjusted or erased after the information has been affirmed by all hubs. This is the reason Blockchain is outstanding of its information respectability and security qualities. Blockchain innovation can likewise be connected to different sorts of employments. It can for instance make a domain for advanced contracts and distributed information partaking in a cloud administration.The solid purpose of Blockchain strategy, information trustworthiness, is the motivation behind why its utilization stretches out likewise to different administrations and applications.

3.3. BLOCK DIAGRAM

As a decentralized innovation, the essential capacity of blockchain is to store information and information. It is an arrangement of squares, which holds the total record of transactions like an open record .each square in the chain conveys a rundown of transactions and a hash to the past square.



Tree root hash records all exchanges

When every exchange enters the square, the field should be recalculated for an update. The computerized mark for the most part works at Merkle tree root hash. A digital signature utilizes different encryption calculations to keep noxious clients from changing the information deliberately. These outcomes in making the way toward altering very difficult for the programmers on the grounds that so as to keep away from any discovery of their essence they would need to alter the square containing that record just as the ones connected to it too Blockchain innovation has likewise some specialized difficulties and restrictions that have been recognized. Swan presents seven specialized difficulties and confinements for the adjustment of Blockchain innovation.

3.4 HASH FUNCTION:

A hash work is the major part of a blockchain. Every one of the information in the block is changed over into hash esteem. A blockchain is a type of the hash chain where the latter square contains the hash of the previous square. Such information structure ensures that the information in the square can't be added. In straightforward terms, hashing implies taking an input string of any length and giving out a yield of a fixed length. Some common hash capacities are SHA (Secure Hashing Algorithm) arrangement and MDA (Message Digest Algorithm) arrangement. A hash capacity can be utilized to shroud data being transmitted and make it progressively secure. Be that as it may, it doesn't take into consideration figuring out.

3.5 CRYPTOGRAPHY:-

The quality of Bitcoins is that it utilizes cryptography such that no other framework exists before it really works. It is cash that does not require a focal part to oversee it; everything is characterized by the laws of science. Be that as it may, as Bruce Schneider says, the cryptographic framework can't be as solid as the calculations on which it rests, and when one of them is broken; the framework goes down. This is particularly valid for Bitcoin since it is an exceptionally fabricated framework on cryptographic learning. The disappointment of the calculations for Bitcoin would imply that one of the principle cryptographic frameworks was broken. These are ECDSA, SHA-256 and RIPEMD-160. All are calculations distributed with broad research.

A cryptographic hash work is an uncommon class of hash capacities which has different properties making it perfect for cryptography. There are sure properties that a cryptographic hash work needs so as to be viewed as secure. How about we go through them one by one.

Property 1: Deterministic

This implies regardless of how often you parse through a specific contribution through a hash work you will dependably get a similar outcome. This is basic in such a case that you get distinctive hashes each and every time it will be difficult to monitor the information.

Property 2: Quick Computation

The hash capacity ought to be fit for restoring the hash of information rapidly. On the off chance that the procedure isn't quick enough, at that point the framework essentially won't be effective.

Property 3: Pre-Image Resistance

What pre-picture obstruction states is that given H(A) it is infeasible to decide A, where An is the info and H(A) is the yield hash. Notice the utilization of "infeasible" rather than "incomprehensible". We definitely realize that it isn't difficult to decide the first contribution from its hash esteem. How about we take a model.

Property 4: Small Changes In The Input Changes the Hash.

Regardless of whether you make a little change in your information, the progressions that will be reflected in the hash will be colossal. We should test it out utilizing SHA-256:

What Is Hashing? In the engine Of Blockchain

INPUT	HASH
This is set	CSIAJIODB,BUVUV,!BBKHHKBB
This is set	Ajhkchsih,w1ygcvsvuio8kb,dskq.o9c

You see that? Despite the fact that you simply changed the instance of the main letter set of the information, take a gander at how much that has influenced the yield hash. This is a basic capacity since this property of hashing prompts one of the best characteristics of the blockchain, its changelessness (more on that later.)

3.6. DIGITAL SIGNATURES:-

How does digital signature work?

To make an advanced mark, counterparties sign the archive legitimately. This structure varies from that of the blockchain, where the counterparties sign a hash that speaks to the record. This paper will allude to lopsided or "open key" cryptography, which includes an association among open and private keys. The open key is put away on a server available to different clients on the system, while the private key remains a mystery. Open key cryptography works under a double technique of which marks structure a section. Accepting there are two gatherings, each gathering has a key pair: the general population and private keys. It demonstrates the accompanying procedure: Alice and Bob are individual annalists going to deal with the transmission of an archive. The archive, remaining as another document, should express that it has been confirmed. The subsequent advanced mark is planned to be accessible for anybody to confirm the personality of the gathering that marked the report (for this situation, Alice). The mark will be accessible not exclusively to Bob, yet to ensuing outsiders also. From the perspective of the documenter, the mark is certified in that it is the thing that it claims to be, and it is real in that the components that are required for that legitimacy are available.

IV. PROPOSED SYSTEM

The Proposed system is the data sharing in which is stored in database. All the data sharing transfers are stored in the blockchain which is unchanged without the proof of work.

In this we can see the user's data is stored in the Secured database in which there are group of people are keeping their data to keep them safe and, they have their presence in the changing the data of their own data. If the Data is to be taken from that database it must follow some protocols which some keys to authentication and authorisation of the User and the verifier which will have will be explained broadly in the below.

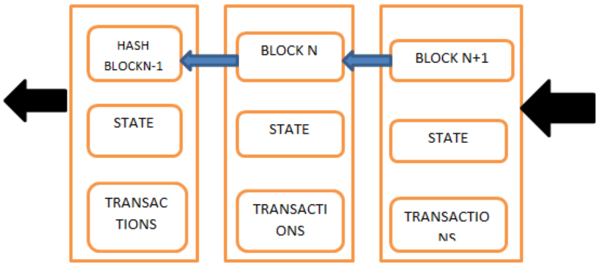


Fig: Blockchain Block Diagram

4.1. Hash function Sha-256, Role of the Hash Code in Blockchain:

Hash function SHA:-

SHA (Secure Hash Algorithm) [18] has been perceived among US principles in 1992 and is connected related with the DSS advanced mark calculation. This calculation acknowledges a message M of any length as the info and conveys 160-piece long yield. Blockchain utilizes SHA-256 hash work with the accompanying attributes: - One-way work: That is, from the underlying message, it is anything but difficult to make a hash esteem. In any case, from the hash esteem, there is no real way to re-establish the first message. The single direction capacity can be developed on the premise of square figure. Crash obstruction. It is hard to discover two distinctive messages that yield a similar hash results. In the event that both of these properties are disregarded, the hash work is no longer usable.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

COLLISIONS SHA-256:

SHA-256 or other hash calculations have two unique assaults that we ought to be worried about: crash and pre-assault. The impact is circumstance where distinctive passages are slashed in similar combination esteem. Finding an impact for a SHA-256 through a crude power assault is conceivable on the grounds that it has a restricted measure of various hash esteems that it can deliver. There are an aggregate of 2256 outcomes for hashing, so impacts are in all respects improbable to happen and we are not worried about such a probability.

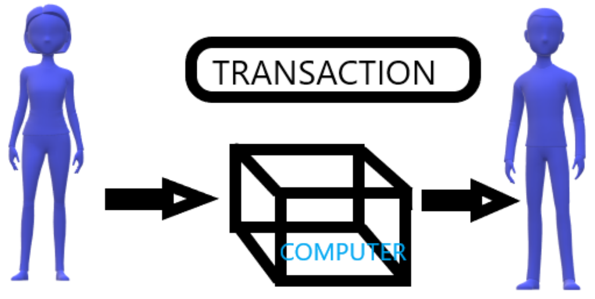
Overall, a great assailant utilizing the birthday mystery further bolstering his good fortune is probably going to discover a crash in "just" 2128 tests for SHA-256 and we need much better to discover an impact to think about a broken calculation. In the event that there is a more straightforward technique for discovering crashes than rough driving as a result of the cryptanalysis.

The first signature of the senders on the exchange hash would be legitimate and, in this manner, the exchange would resemble a substantial exchange. The assailant should locate this quite certain crash rather than a straightforward impact: an exchange message that has its Bitcoin address rather than the goal address ought to have a similar hash. Since these shortcomings found in SHA-1 are by a wide margin insufficient. Also, the aggressor must be quicker than the proprietor of the coins by spending them.

4.2.TRANSACTION:

Start to finish:- Since you've acclimated yourself with the language and assets included, we should plunge into how a digital money exchange really happens from beginning to end. Inside the blockchain arrange, there are three segments which make up the fundamental "players" in charge of everything: clients, hubs, and diggers.

Everything begins with the digital currency client, who could be anybody that utilizes a wallet to store their cryptographic money. Obviously, we realize that these wallets simply hold the open locations of your benefits and not real cryptographic money. Anybody with a wallet can begin an exchange, yet what happens when your exchange is pending? That is the place hubs come in.



Hubs are essentially PCs utilizing a particular programming to associate with different hubs in the system. These are utilized to approve and some of the time mine coins like Bitcoin, speaking to the initial move towards confirming an exchange. When a hub gets an exchange, it basically downloads the whole edger history and checks that the exchange is substantial. When this happens, hub sends this to every other hub over the world—acting like the "cameras" in the previously mentioned analogy—to completely approve the exchange. At long last, the exchange requests are presently pending and anticipate the excavator to carry out its responsibility.

Diggers can likewise be anybody with appropriate equipment and web get to, assuming a urgent job in the exchange procedure. Actually, the vast majority with hubs are additionally diggers, as any individual who just runs a hub independent from anyone else does as such exclusively to secure the honesty of the blockchain. Pending exchanges are sent to diggers, who can pick and check one of them. When an excavator understands the comparing hash confuse, every single other digger in the system are informed and the subsequent square is sent back to the hubs.

Rundown: through and through, an exchange on the blockchain is taken care of by three jobs: the client, excavator, and hub. When a client begins an exchange, it's checked by all hubs and is sent in a pool of pending exchanges to diggers. From that point, excavators unravel a hash baffle and send the subsequent square of exchanges alongside the hash arrangement back to the hubs, where the square is endorsed and spared into the constantly developing chain of squares… blockchain!

4.4. ECC (Elliptic Curve Cryptography):

Basics of Elliptic Curve

Prime field: The condition of the elliptic curve on a prime field Fq is y2 (mod q) = x3 +a× x +b, where 4a3 ECDD+27b2 (mod q) ≠ 0. Here the components of the limited field are the whole number among 0 and q-1 [7]. All activities, for example, point-expansion, point-subtraction, point-division, and point- Augmentation includes the whole number among 0 and q-1. The prime q is picked with the end goal that there is a limitedly substantial number of focuses on the elliptic curve to make the cryptosystem secure.

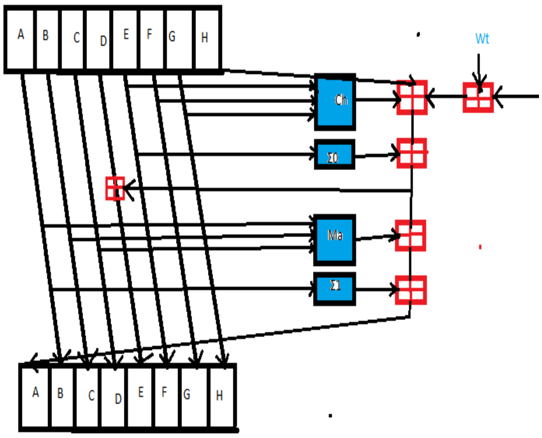
Binary field: The condition of the elliptic curve on a double field F2 m is $y^2 + x\times y = x^3 + ax^2 + b$, where b ≠ 0. Here components of a limited field are whole numbers. These components are picked with the end goal that length of each ought to be at most m bits. These numbers can be viewed as a twofold polynomial having degree m-1. In twofold polynomial, the coefficients must be 0 or 1. All tasks include polynomial of degree m-1 or lesser. Them is picked with the end goal that there is a limitedly expansive number of focuses on the elliptic curve to make the cryptosystem more secure.

Elliptic Curve Group:When the point expansion task is considered as a gathering activity, an added substance gathering that comprises of the arrangement of arrangements of the elliptic curve condition and an excellent point O called point-at-unendingness is framed. It is outstanding that E/Fq with a parallel task, called expansion of focuses and signified by +, is an Abelian amass with O∞ as the personality component. The gathering is signified by E(Fq).

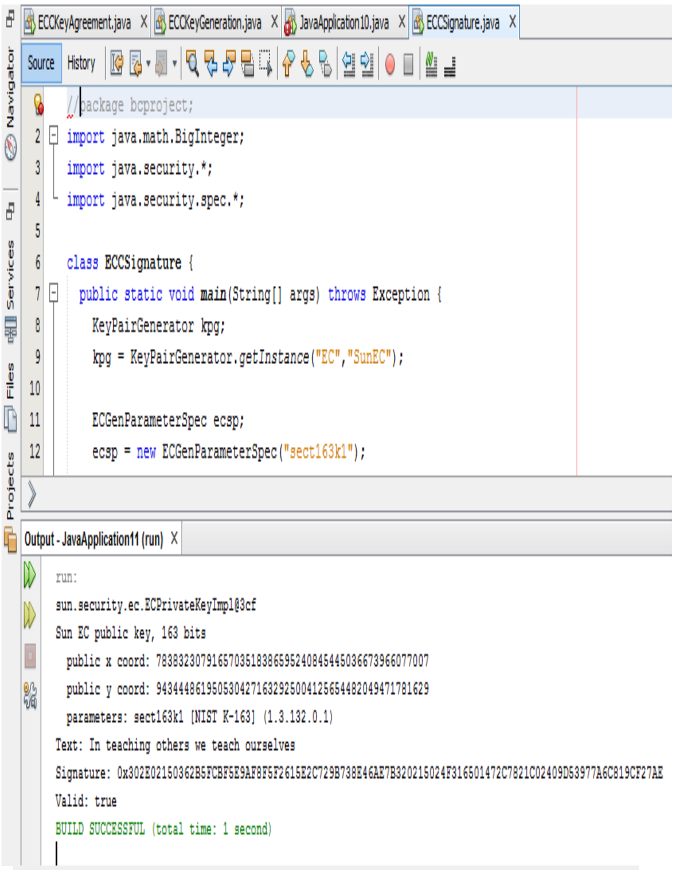
V. 5. IMPLEMENTATION AND RESULTS

SHA-256 ALGORITHM:

```
Same pre-processing, same initialization of W1 - W15
//Extend the 16 32-bit words into 64 32-bit words:
for t from 16 to 63
s0=(Wi-15>>>7 )⊕(Wi-15 >>>18)⊕(Wi-15 >>3)
s1=(Wi-2>>>17)⊕(Wi-2 >>>19)⊕(Wi2 >>10) Wt =
Wi-16 + s0 + Wi-7 + s1
//Initialize hash value for this chunk:
A = h0 B = h1 C = h2 D = h3 E = h4 F = h5 G = h6 H = h7
Same pre-processing, same initialization of W1 - W15
 //Main loop: for t from 0 to 63
s0=(A>>>2)⊕(A >>>13)⊕(A >>>22)
maj =(A ∧ B) ∨ (B ∧ C) ∨ (C ∧ A)
 t0=s0+ maj
s1=(E>>>6)⊕(E >>>11)⊕(E >>>25)
ch =(E ∧ F) ∨ (¬E ∧ G)
t1 = H + s1 + ch + Kt + Wt H = G G = F F = E E = D + t1 D
= C C = B B = A A = t0 + t1
 SHA-256 Algorithm
//Add this chunk's hash to result so far:
h0 := h0 + A
h1 := h1 + B
 h2 := h2 + C
 h3 := h3 + D
 h4 := h4 + E
h5 := h5 + F
 h6 := h6 + G
 h7 := h7 + H
//Output the final hash value (big-endian): digest = hash = h0
|| h1 || h2 || h3 || h4 || h5 || h6 || h7
```



SHA-256

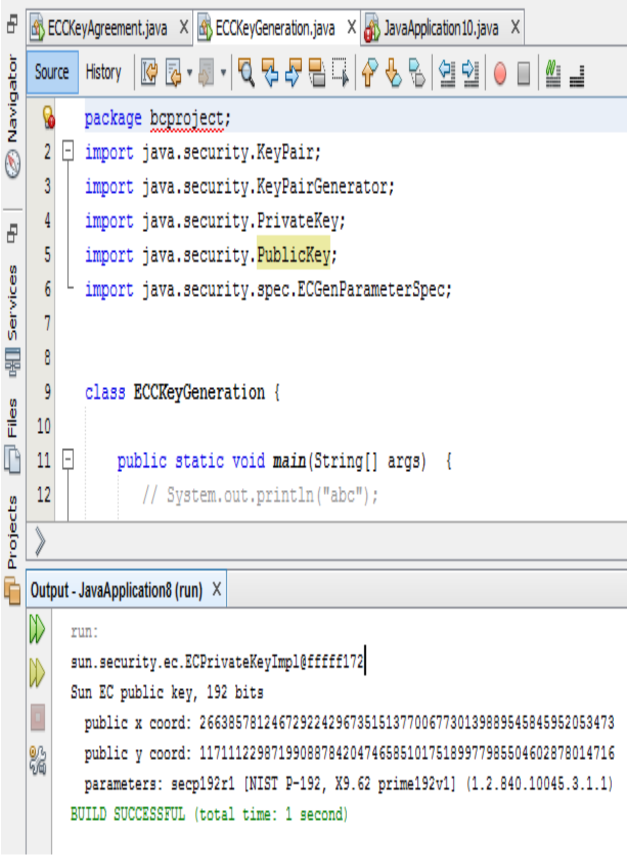


```
//package bcproject;
import java.math.BigInteger;
import java.security.*;
import java.security.spec.*;

class ECCSignature {
  public static void main(String[] args) throws Exception {
    KeyPairGenerator kpg;
    kpg = KeyPairGenerator.getInstance("EC","SunEC");

    ECGenParameterSpec ecsp;
    ecsp = new ECGenParameterSpec("sect163k1");
```

```
run:
sun.security.ec.ECPrivateKeyImpl@3cf
Sun EC public key, 163 bits
  public x coord: 7838323079165703518386595240845445036673966077007
  public y coord: 9434448619505304271632925004125654482049471781629
  parameters: sect163k1 [NIST K-163] (1.3.132.0.1)
Text: In teaching others we teach ourselves
Signature: 0x302E02150362B5FCBF5E9AF8F5F2615E2C729B738E46AE7B320215024F316501472C7821C02409D53977A6C819CF27AE
Valid: true
BUILD SUCCESSFUL (total time: 1 second)
```



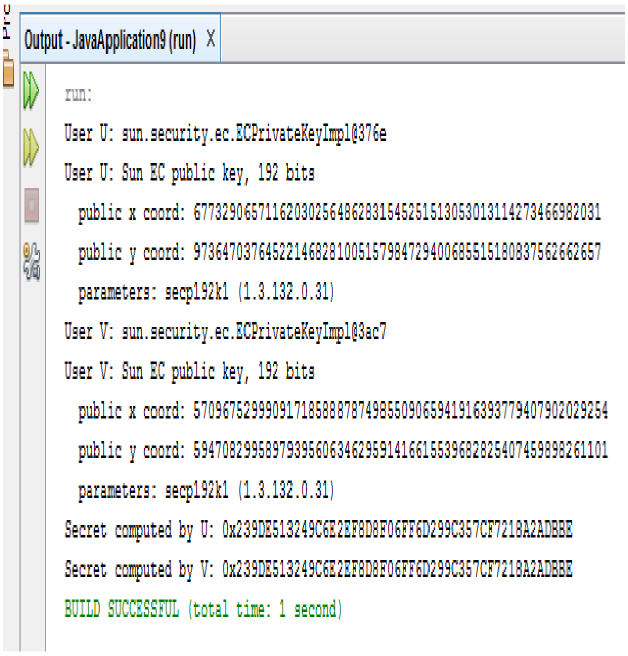
```
package bcproject;
import java.security.KeyPair;
import java.security.KeyPairGenerator;
import java.security.PrivateKey;
import java.security.PublicKey;
import java.security.spec.ECGenParameterSpec;


class ECCKeyGeneration {

   public static void main(String[] args)  {
     // System.out.println("abc");
```

```
run:
sun.security.ec.ECPrivateKeyImpl@fffff172
Sun EC public key, 192 bits
  public x coord: 2663857812467292242967351513770067730139889545845952053473
  public y coord: 1171112298719908878420474658510175189977985504602878014716
  parameters: secp192r1 [NIST P-192, X9.62 prime192v1] (1.2.840.10045.3.1.1)
BUILD SUCCESSFUL (total time: 1 second)
```

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication



```
run:
User U: sun.security.ec.ECPrivateKeyImpl@376e
User U: Sun EC public key, 192 bits
  public x coord: 6773290657116203025648628315452515130530131142734669820З1
  public y coord: 9736470376452214682810051579847294006855151808375626626 57
  parameters: secp192k1 (1.3.132.0.31)
User V: sun.security.ec.ECPrivateKeyImpl@3ac7
User V: Sun EC public key, 192 bits
  public x coord: 5709675299909171858887874985509065941916393779407902029254
  public y coord: 5947082995897939560634629591416615539682825407459898261101
  parameters: secp192k1 (1.3.132.0.31)
Secret computed by U: 0x239DE513249C6E2EF8D8F06FF6D299C357CF7218A2ADBBE
Secret computed by V: 0x239DE513249C6E2EF8D8F06FF6D299C357CF7218A2ADBBE
BUILD SUCCESSFUL (total time: 1 second)
```

VI. CONCLUSION:-

From the above System Description, we conclude that the problem we took from the reference that's talks about the one of the flaws in the blockchain is the privacy issue between the Users inside the Blockchain. This can be rectified by the ECC (Elliptic curve cryptography) and SHA algorithm.

REFERENCES:

1. http://www.ijircce.com/upload/2015/sacaim/30_212.pdf
2. https://www.researchgate.net/publication/327392778_Analysis_of_Secure_Hash_Algorithm_SHA_512_for_Encryption_Process_on_Web_Based_Application
3. https://pdfs.semanticscholar.org/b111/0264f5efa9848bfa647cc8f7f8ea7ecebc34.pdf
4. http://www.ijaret.org/2.10/SECURED%20HASH%20ALGORITHM-1%20Review%20Paper.pdf
5. http://paper.ijcsns.org/07_book/201812/20181202.pdf
6. https://www.researchgate.net/publication/330832141_A_Multidimensional_Adversary_Analysis_of_RSA_and_ECC_in_Blockchain_Encryption
7. http://www.icommercecentral.com/open-access/blockchain-bitcoin-wallet-cryptography-security-challenges-and-countermeasures.php?aid=86561
8. https://blockgeeks.com/guides/what-is-hashing/
9. https://www.researchgate.net/publication/330125746_A_survey_of_blockchain_from_security_perspective
10. file:///C:/Users/personal/Downloads/Analysis_of_a_SHA-256_Variant%20(1).pdf
11. https://www.researchgate.net/publication/326009898_Review_Paper_on_Secure_Hash_Algorithm_With_Its_Variants
12. https://pdfs.semanticscholar.org/1749/6c347e05ef2681473a0648ae11696796829d.pdf
13. http://gauss.ececs.uc.edu/Courses/c6053/lectures/PDF/mdalgs.pdf
14. [14].https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0163477
15. https://link.springer.com/chapter/10.1007/978-3-319-56925-3_2
16. https://ieeexplore.ieee.org/document/8100712
17. https://ieeexplore.ieee.org/document/8343261#s

AUTHORS PROFILE

Ms.B.Aruna, Department of ECM, Koneru Lakshmaiah Education Foundation, Vaddeswaram, A.P., India.

A.Ajay prakash,Department of ECM, Koneru Lakshmaiah Education Foundation, Vaddeswaram, A.P., India.

M.S.Srinija, Department of ECM, Koneru Lakshmaiah Education Foundation, Vaddeswaram, A.P., India.