ISSN (Online) : 2348 - 2001

International Refereed Journal of Reviews and Research

Volume 7 Issue 1 January 2019

International Manuscript ID : 23482001V7I1012019-9

(Approved and Registered with Govt. of India)

Blockchain Integrated Security Environment for Assorted Domains

Amit Singla
HOD (Computer Science)
Seth G. L. Bihani S D (PG) College
Sriganganagar, Rajasthan

Abstract

An ever-expanding record set known as a "block" is connected together through cryptography. The preceding block's cryptographic hash, as well as the time stamp and the transaction data, are all included in each block (generally represented as a Merkle tree). In order for a block to be included in a hash, it must contain transaction data that existed at the moment the block was published. Blocks are linked together in a chain because each one has a piece of information about the one before it. A block of blockchain data can't be edited retrospectively without also affecting following blocks, hence blockchains are impermeable to data alteration. As a publicly distributed ledger, blockchains are often administered via a peer-to-peer network that adheres to a protocol for communication and validation of new blocks. A distributed computing system with excellent Byzantine fault tolerance might be described as a "blockchain," even though forks are conceivable in the system. As a public transaction log for the cryptocurrency bitcoin, Satoshi Nakamoto popularised the blockchain in 2008 utilising work by Stuart Haber, W. Scott Stornetta and Dave Bayer. Satoshi Nakamoto's identity is still a mystery. This problem of duplicate spending was initially addressed by bitcoin's use of blockchain technology rather than a third-party authority or central server. Some apps have been influenced by the bitcoin design. and public blockchains, both of which are essential to cryptocurrencies. To put it another way, the blockchain is a sort of payment rail with security environment.

Keywords : Blockchain Technology, Blockchain Integrated Security, Blockchain and Security

Introduction : Blockchain Technology and Case Studies

Blockchain Technology is one of the most important fields of study and implementation in today's world, particularly in the area of Cryptocurrency. A variety of digital cryptocurrencies are now fairly prominent and widely used across the world, despite much criticism and controversy. Some examples of these cryptocurrencies are Bitcoin, Litecoin, PeerCoin, GridCoin, PrimeCoin, Ripple, Nxt, DogeCoin, NameCoin, AuroraCoin and many others. The log of transactions for these blockchain-based cryptocurrencies is not kept by a middle bank or payment gateway. As a result, several nations have banned the use of cryptocurrencies as legitimate forms of payment. Because of this, these blockchain-based coins are extremely popular and widely utilised. There is a block of records in the blockchain network that is linked to dynamic cryptography so that all transactions are encrypted and cannot be sniffed or hacked [1].

The distributed ledger is utilised for transactions in cryptocurrencies, which is where the blockchain technology is most relevant right now. When a digital asset is copied, synced, and shared across several devices, it is considered a distributed ledger, making it impossible for third parties to manipulate the data. It is possible to ensure greater security if a bank adheres to a blockchain-based distributed ledger [2]. This bank's records of transactions will be saved on one million devices if it has a million clients. Rather than just one server, they'll have to hack one million devices in real-time. This is one of the most significant benefits of utilising decentralised blockchains.

If a hacker manages to get access to a bank's server, they will have access to all of the bank's clients' personal information. Those are just two of the many reasons why government organisations should work on decentralising their web-based apps [3].

Decentralized applications may be used to safeguard government servers for land registry, citizen data (including AADHAAR in India), permanent account number (PAN), and a slew of other purposes.

The blockchain based decentralized application can be used for following

- Asset and Land Registry
- (Birth, Marriage and Death) Certificates
- Taxation
- Digital Identity of Government Documents
- Notarized Documents
- Social Welfare and Benefits
- Incorporation Services
- Personalized Government Services
- Polling / Voting / Assembly Elections

Graph showing the size of the Bitcoin blockchain from 2010 to 2018 according to Statista.com research and publications. This graph is in huge demand all around the world.

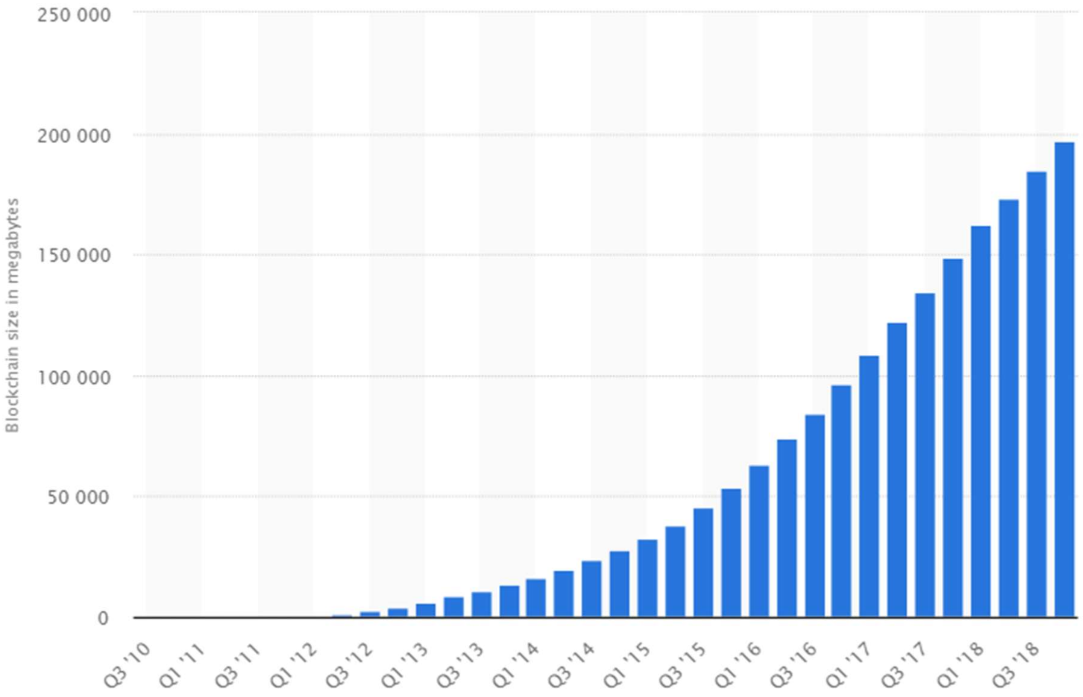


Figure 1: Blockchain Size from 2010 to 2018

A Secured Blockchain for Decentralized Applications (dApps)

The term "decentralised application" (dApp) refers to a piece of software that runs over a network of distributed servers, making it nearly hard to compromise. Centralized applications, on the other hand, are distributed over several servers [4]. The biggest drawback of a centralised solution is that everything on that server can be corrupted or stolen if it is hacked. This means that there is no single server in a decentralised application, and instead, the transaction records are replicated and stored on all client devices. Hacking a decentralised application will be extremely tough in real time utilising smart contracts since the hacker must break into all of the devices connected to the programme. The dynamic token sharing is employed in smart contracts-based dApps to ensure maximal security measures for transactions [5].

Smart Contracts

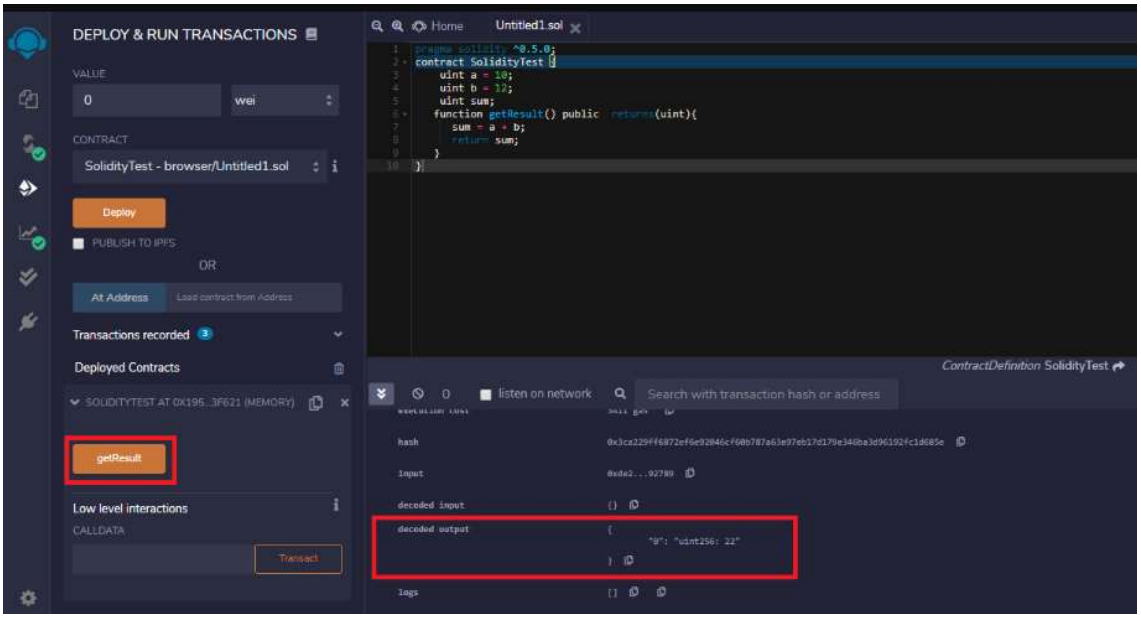
The smart contract programming is required for the globalization based transactions. It means that the transactions can be done across the people who can't communicate because of different continents, languages and traditions. Smart Contracts automatically validate the transactions and business dealings between the people who can't understand the language of each other.

Programming and Scripting with Blockchain Environment for Security

Solidity

For building smart contracts, Solidity is one of the most powerful and high-performance programming languages. There are several blockchain platforms that can be combined with this system since it follows an object-oriented programming model [6] that is more secure and efficient. To run on the Ethereum Virtual Machine, the solidity code is compiled and translated into bytecode (EVM). Since Python, JavaScript, and C++ make up a large part of Solidity Programming's core base, it may be used in a wide variety of contexts and platforms to interface with blockchains. An integrated development environment (IDE) like Remix, EthFiddle, or JetBrains is all that is required to work with Solidity Programming [7].

Remix, an open-source, web-based IDE for Solidity Programming, is a good place to begin learning the language. With Remix IDE's web-based interface, it's simple for programmers to construct Smart Contracts using Blockchain technology.


DEPLOY & RUN TRANSACTIONS
VALUE
0
wei
CONTRACT
SolidityTest - browser/Untitled1.sol
Deploy
PUBLISH TO IPFS
OR
At Address
Load contract from Address
Transactions recorded 3
Deployed Contracts
SOLIDITYTEST AT 0X195...3F621 (MEMORY)
getResult
Low level interactions
CALLDATA
Transact
Home
Untitled1.sol
ContractDefinition SolidityTest
0
listen on network
Search with transaction hash or address

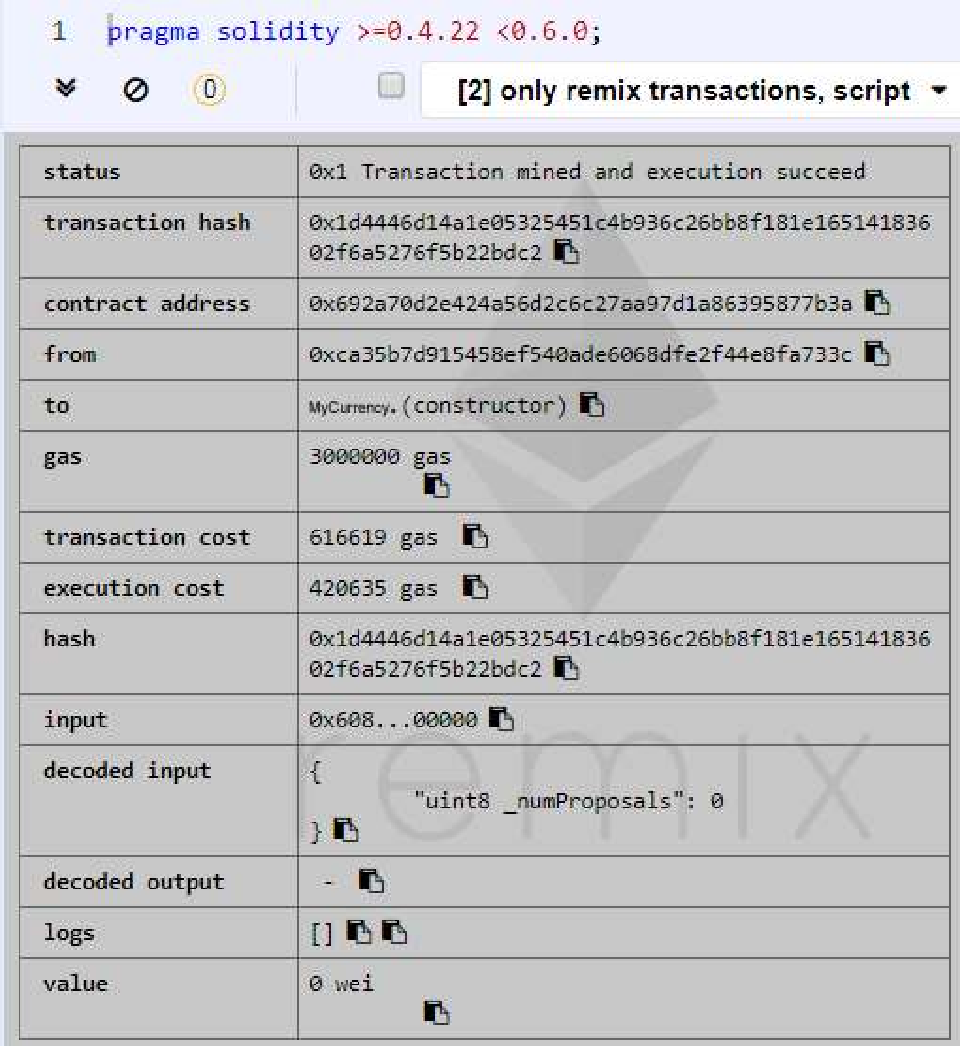
```
pragma solidity ^0.5.0;
contract SolidityTest {
    uint a = 10;
    uint b = 12;
    uint sum;
   function getResult() public  returns(uint){
      sum = a + b;
      return sum;
   }
}
```

```
hash              0x3ca229ff6872ef6e92046cf00b787a63e97eb17d179e346ba3d96192fc1d685e
input             0xde2...92789
decoded input     {}
decoded output    {
                      "0": "uint256: 22"
                  }
logs              []
```

Figure 2: Remix IDE for Blockchain Programming

```
pragma solidity ^0.4.18;
contract MyCurrency {
string public name = 'MyCurrency';
// Name of the New Currency
string public currencyName = 'Currency1.0';
// Select Currency
mapping (address => uint) SecuredTransactions;
// Key-Value Pair for Address-Account
event Transfer(address _sender, address _receiver, uint256 _value);
// Log Recording
constructor() public {
// Constructor on Creating the Contract
SecuredTransactions[SecMessage.sender] = 100000;
// SecuredTransaction Confirmation
}
function sendSecuredPayment(address _receiver, uint _SecuredPayment) public returns(bool
sufficient) {
if (SecuredTransactions[SecMessage.sender] < _SecuredPayment) return false;
// Authentication of the Transfer
SecuredTransactions[SecMessage.sender] -= _SecuredPayment;
SecuredTransactions[_receiver] += _SecuredPayment;
emit Transfer(SecMessage.sender, _receiver, _SecuredPayment);
// Commit of Payment Transfer with Transaction Recording
return true;
}
function getSecuredTransaction(address _addr) public view returns(uint) {
// Checking the SecuredTransaction
return SecuredTransactions[_addr];
}
}
```

The connected transaction's blockchain logs may be examined in detail. The transaction log contains a number of parameters, including the Gas Limit. Smart Contract Programming's Gas Limit refers to the transaction's related effort or throughput [8]. For JavaScript-based programming, NodeJS is an open source cross-platform platform. Blockchain development, smartphone apps, distributed web apps, noSQL processing, big data analysis and machine learning are just a few of the numerous applications that may be built using this technology.



```
pragma solidity >=0.4.22 <0.6.0;
```

status	0x1 Transaction mined and execution succeed
transaction hash	0x1d4446d14a1e05325451c4b936c26bb8f181e165141836 02f6a5276f5b22bdc2
contract address	0x692a70d2e424a56d2c6c27aa97d1a86395877b3a
from	0xca35b7d915458ef540ade6068dfe2f44e8fa733c
to	MyCurrency.(constructor)
gas	3000000 gas
transaction cost	616619 gas
execution cost	420635 gas
hash	0x1d4446d14a1e05325451c4b936c26bb8f181e165141836 02f6a5276f5b22bdc2
input	0x608...00000

decoded input	{
	"uint8 _numProposals": 0
	}

decoded output	-
logs	[]
value	0 wei

Figure 3: View Logs and Transaction Details

Web3JS and NodeJS are used for blockchain development. The term "Web3JS" refers to a collection of blockchain-based libraries and tools.

Conclusion

There is a pressing need to address privacy and resource optimization challenges in the developing field of blockchain development. There are concerns about the security and integrity of data in blockchain and decentralised apps since data is copied across several devices. The performance of blockchain-based solutions may be improved with the creation and deployment of new algorithms. The data structure created by blockchain technology has built-in security properties. Using cryptography, decentralisation, and consensus principles, it ensures the trustworthiness of every transaction. Some distributed ledger technologies (DLTs), such as blockchains, organise transactions or bundles of transactions into blocks that may be linked together. In a cryptographic chain, each new block is inextricably linked to the ones that came before it, making tampering very difficult. There is a consensus process in place to ensure that all transactions in the blocks are correct and truthful. Members of a distributed network can participate in decentralisation through the use of blockchain technology. There is no single point of failure and a single user cannot change the record of transactions. However, certain essential features of security differ between blockchain and other systems. Public blockchain networks typically allow anyone to join and for participants to remain anonymous. To verify transactions and reach consensus, a public blockchain makes use of computers connected to the internet. Using "bitcoin mining," Bitcoin is one of the most well-known examples of a public blockchain. By solving a difficult cryptographic issue, the Bitcoin network's "miners" produce proofs of work, which are then used to validate transactions. There are little identity and access protections other than public keys in this sort of network.

References

[1] Lin, I. C., & Liao, T. C. (2017). A survey of blockchain security issues and challenges. Int. J. Netw. Secur., 19(5), 653-659.

[2] Minoli, D., & Occhiogrosso, B. (2018). Blockchain mechanisms for IoT security. Internet of Things, 1, 1-13.

[3] Khan, M. A., & Salah, K. (2018). IoT security: Review, blockchain solutions, and open challenges. Future generation computer systems, 82, 395-411.

[4] Karame, G. (2016, October). On the security and scalability of bitcoin's blockchain. In Proceedings of the 2016 ACM SIGSAC conference on computer and communications security (pp. 1861-1862).

[5] Moubarak, J., Filiol, E., & Chamoun, M. (2018, April). On blockchain security and relevant attacks. In 2018 IEEE Middle East and North Africa Communications Conference (MENACOMM) (pp. 1-6). IEEE.

[6] Stephen, R., & Alex, A. (2018, August). A review on blockchain security. In IOP Conference Series: Materials Science and Engineering (Vol. 396, No. 1, p. 012030). IOP Publishing.

[7] Halpin, H., & Piekarska, M. (2017, April). Introduction to Security and Privacy on the Blockchain. In 2017 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW) (pp. 1-3). IEEE.

[8] Wang, H., Wang, Y., Cao, Z., Li, Z., & Xiong, G. (2018, August). An overview of blockchain security analysis. In China Cyber Security Annual Conference (pp. 55-72). Springer, Singapore.