ISSN: 2350-0328

International Journal of Advanced Research in Science, Engineering and Technology

Vol. 5, Issue 5 , May 2018

BaaS: Blockchain as a Service for Secured Transaction

Remya Stephen, Aneena Alex

P.G. Student, Department of Computer Science, St.Joseph's college of Engineering and technology, Palai
Assistant Professor, Department of Computer Science, ,St.Joseph's college of Engineering and technology, Palai

ABSTRACT:Blockchain is a decentralized innovation. It has tremendous energy to tackle business issues. Cryptography secures the records in a blockchain transaction and every transaction is tied (in the chain) to past exchanges or records. This project works for a transaction using ether. And this should be hosted in the cloud also, it is named as BaaS (Blockchain as a Service). Transactions are validated by some cryptographical methods such as public, private key encryption and digital signature. Blockchain provide transparency, giving each participant the ability to monitor the transactions at any time. Smart contract is used to makes secure transaction which helps to avoid third party interference. Ethereum is used as a platform for this project, it is a decentralized platform that runs smart contracts. This enables developers to create markets move funds in accordance with instructions given long in the past and many other things that have not been invented yet, all without a middle man or counter party risk. The main features of blockchain are Transaction and validation happens in seconds, Decentralization, Immutability and Faster dealings etc.

KEYWORDS: Hashing, Smart contract, Ethereum, BaaS

I.INTRODUCTION

Blockchain technology has huge potential with a variety of applications and provides wide opportunities for various infrastructure. The technology encourages resource management and makes communication both secure and efficient. Trust is increased when conducting noncoal transactions among parties using Blockchain, as it reduces the chances of swindle and automatically produces a record of activities. Creating an automated background check of any member of the system. Due to its decentralized properties, Blockchain creates reliability and reduces the risk faced when looking to enter a business agreement with an unfamiliar party.

Today all people were using advanced technology for communication through internet. Voice call, video call, messages, pictures, are travel directly from sender to receiver over the internet. For this transaction, must maintain a trusted third party between these sender and receiver. When it comes in the case of money transaction, people have to trust a third party for complete this, in traditional system. But in the case of blockchain it will give a perfect security in transaction. A block should record every transaction, it will act like a record book. Once completed a transaction a block goes into the blockchain as a permanent database. If a block is completed a new block is added with this or a new block is generated. Every block carry a hash of the previous block.

Today all individuals were utilizing present day innovation for correspondence through web. Voice and video call, messages, pictures, are head out straightforwardly from sender to beneficiary over the web. For this exchange we should keep up a put stock in outsider between these sender and beneficiary. When it comes on account of cash exchange, individuals host to put stock in a third gathering for finish this, in customary framework. In any case, on account of blockchain it will give an ideal security in exchange. Blockchain is a decentralized application, or it is one of the layers of the decentralized application. A square is the present piece of a blockchain, which records a few or the majority of the current exchanges.

A.The Blockchain Enhanced security

By putting away information over its system, the blockchain takes out the dangers that accompany information being held midway misuse. Its system needs concentrated purposes of helplessness that PC programmers can. Today's web has security issues that are natural to everybody. We as a whole depend on the username/secret word framework to secure our character and resources on the web. Blockchain security techniques utilize encryption innovation. The reason for this are the purported open and private keys. An open key is a client's address on the blockchain. Bitcoins sent across the network gets recorded as belonging to that address. The private key resembles a secret key that gives its proprietor access to their Bitcoin or other computerized resources. Store your information on the blockchain and it is upright. This is valid, albeit securing your computerized resources will likewise require defending of your private key by printing it out, making what's alluded to as a paper wallet.

Benefits

1. In the event that executed in an organization with different branches, the transmission of data will be immediate
2. There would be a more prominent straightforwardness to oblige clients at any branch
3. When leading financial exchange outsiders would dispensed with, making exchange less expensive and speedier
4. Increased unwavering quality, and decrease of misrepresentation and defilement during the time spent game plans
5. Reduces question in new business wanders, the innovation gives a type of protection among accomplices alongside a built up foundation of each parties past connection.

Drawbacks

1. Theopennessofthetechnologyslicesafewlayersoftheprivacyofconnectedparties, it isn't conceivable to pick which data can be seen by others on the framework
2. Thetechnologylackofthirdpartysinteractionsignifiesthatnoonebodycanbeheld responsible or drew closer for an answer in case of a debate or a wrong exchange
3. Transactionsandactionsconductedwiththistechnologycannotbereverseautomatically, a record would be made however to remedy the blunder or get a discount; the second party would need to recognize the error and settle on the final choice
4. Implementation of the innovation isn't momentary, mapping of the part is required and can be tedious relying upon the measure of the foundation consequently it is difficult to in a split second execute the innovation all through in one swoop

II.RELATED WORK

This area exhibits how secure blockchain innovation than other security framework. Focussing on its diverse applications, qualities and its security issues.

A. Security Analysis

Blockchain give preferable security over different applications. The primary favourable position blockchain is, it will maintain a strategic distance from the outsider impedance. Rather than an outsider it will select a record. Record is utilized to store all exchange data.

Utilize ledger . Ledger should record every last exchange in a blockchain. This ledger is changeless. Existing information can't be altered or erased. In blockchain innovation these records is decentralized application. Along these lines, nobody can get to the exchange or even any touchy information from this record [12]. Individuals can just read the data from a record.Another kind of security highlight is the chain of piece. In blockchain each square ought to contain a hash esteem. These pieces are associated by its past hash. Assume an aggressor came to redress the information, at that point its hash will be changed. It will affect the general chain. In this way, it will build the security of touchy information or data.

Blockchain innovation is a decentralized application. Predominantly it will bolster shared correspondence. Along these lines, in a system hub is considered as PCs. These a huge number of hubs ought to have the duplicate of dispersed record. This ought to validate the exchange. On the off chance that any of the hub does not concur an exchange, at that point it can't be continuing. In this way, it will be cancelled [12]. This will shield from an extortion exchange.

B. Applications of Blockchain

1. Charity

Today individuals could gather cash in name of some philanthropy. Regardless, we don’t know where this cash is going, or if the gathered cash is come to at revise goal. Individuals are tricked by these kinds of extortion support. Individuals were supposing they are completing some help for the needy individuals. Be that as it may, the must know course of this cash.Open record is an application to use in this circumstance. Each client in a blockchain ought to have an open record. This record ought to consequently record all exchange. On account of philanthropy, individuals can see the course of cash.

2. Blockchain to protect personal data

Today there is late addition in declared event of security issue in customers singular data. In perspective of this there is a pariah control over the data, who will assemble every individual datum. Blockchain can discard this untouchable and can trade specifically between two social occasions. The measure of data starting late growing in our existence. Facebook, is the greatest online interpersonal organization, accumulated 300 petabytes of individual data. Singular data or sensitive data should not be secure in the hand of outcasts. They are endeavoured to attack and manhandle. Blockchain helps customers that not required to place stock in any outcast. Blockchain sees the customers as the proprietors of their own data. Blockchain should have its own specific rules and control. It is known as splendid contract. Before starting a trade, the entryway director should make a couple of norms and will created as an assertion. It will make a mutual correspondence. Bitcoin has shown in nancial space that is trusted and figuring is possible in decentralized framework. Blockchain is generally proposed to manage the bitcoin, it is a propelled cash.

3. Electronic medical records

Patients can manage electronic remedial records by using the blockchain advancement. Most by far of the prosperity cares foundation should not empower patient to get to their therapeutic data. Patients are getting the chance to be baffled about the security of their remedial records. This all can be avoided by blockchain. In dealing with electronic restorative records, blockchain ought to oversee different diagram work for managing the verification, confidentiality, and obligation. It is generally used when dealing with the delicate data. Online electronic records in blockchain will functioned as decentralized application. In united condition all application should be done at one region. In any case, in decentralized condition application should be done at different zone. Electronic remedial records should act a couple of difficulties and limitations. This structure will go up against some essentialdifficultiesamidtheexecutionofbyandbycontrolled system. That is this eventually controlled records would supplant provider or specialist's office records. Some area of the before long controlled records would be downloaded in to the institutional record to tribute the present data These difficulties can be avoided by blockchain. Since blockchain drives a key exchange-based trade between two social events. Their own particular identity does not pleasure to any others. Since they are simply giving their key identity. Each and every customer in a blockchain should have one open key and one private key.

III.PROPOSED SYSTEM

Figure 1 is the system architecture for this project. In this project a value transacted between two parties. Smart contract, Ethereum, Ledger are used to provide more securitytothis transaction.Etherisusedtomakeatransaction.Ledger,identityservices,crypto services,analytics services are act as middleware tier. Ethereum is the platform for this blockchain technology. These transactionsis also hosted in Microsoft azure cloud. That is BaaS.

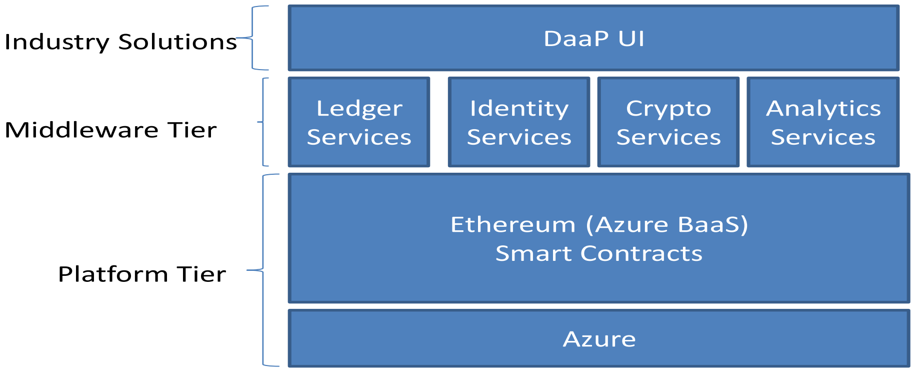


Fig1: System Architecture

A. Ledger Services

Ledger is a decentralized application assigned to each user in a blockchain. After completing a transaction, it will be recorded in the ledger automatically. For example, thereistwo-person AandB. PersonAmustgive100rupeestopersonB.Thereis someotherpersonisthisblockchain. Theyalsohaveaseparateledger. Thisdatawill be automatically updated in everyone's ledger. Person A said that who should only give 10 rupees to B. Then there will be a voting mechanism. This voting mechanism canprovethatthestatementbypersonAisnotvalidated. Therefore,itwillberejected.

B Identity Services

Ascybersecuritythreatsbecomeincreasinglyprevalentandsophisticated,thecasefor blockchain technology as a way to secure and improve identity management grows stronger. Blockchaincangivepeoplemoreproactivecontrolovertheirdataandmake it more difficult for unauthorized users to exploit it. Blockchain start-ups are exploringmoredecentralizeddatamanagementsystemsby,insomecases,teamingupwith financial services, technology, and government organizations to mitigate the risks of large-scale cyber-attacks and identity fraud. There also finding ways to give individuals, includingtheunderserved, accesstoservicesthatrequirevalididentification and they're able to do that much more efficiently than current know your customer processes.

C. Crypto Services

Different types of cryptical methods are used in this project. Such as public and privatekey,hashing,anddigitalsignature.Theprocessofhashingdataisaveryimportant technique using cryptography, and it forms a backbone of what we're going to look at in regards to building up our blockchain implementation. A cryptographic hash functionisanalgorithmthattakesanarbitraryblockofdataandreturnsafixed-sized string, the cryptographic hash value, such that any accidents or intentional change to that data will change the hash value.

Additional signatures is a technique used to help demonstrate that there's authenticity of the message. A valid digital signature gives the recipient a reason to believe that the message was created by a known sender, such that the sender cannot deny having sent that message. Digital signatures give you both authentication and nonrepudiation. Authentication because the signatures had to be created by a user with a valid, private key, and non-repository repudiation as a receiver can trust that the message was signed by a known sender, as only they know the private key.

D. Smartcontract

Smart contract is also known as a crypto contract. Smart contract was proposed by Nick Szabo in 1994. It is a computer program, it directly controls the transfer of digitalcurrency. Thesecontractsarestoredonblockchaintechnology. Smartcontract is a decentralized system. It is existed in two parties.

ISSN: 2350-0328

International Journal of Advanced Research in Science, Engineering and Technology

Vol. 5, Issue 5 , May 2018

E. Ethereum

Ethereum is a decentralized platform that runs the blockchain. That enables developers to build and deploy decentralized applications. Ethereum is similar to Bitcoin. Because it is a distributed public blockchain network. But there are some technical deference between these two. For each Ethereum application the network needs to keep the current state information. Including all users balance, smart contract code and where its all stored.

F. BaaS

Microsoft has recently longed BaaS (Blockchain as a Service) for developers to build Daap or Decentralized application quickly. So now rather than setting up your own Blockchain on Azure platform you can just launch the Blockchain with a click.BaaS offeringsareparticularlyattractivebecausemanyenterprisescanlooktotheircurrent cloud providers to offer them use of the nascent technology.

IV. EXPERIMENTAL RESULTS

A. STORING TRANSACTIONS IN BLOCKS

First, goingtohave blocks with asingletransaction. Create theability to link blocks together, so that if any of the blocks are modified after it has been added to the block chain, thentheremainderofthechainwillfailtoverify.Thenwehaveblockswithmultiple transactions, so that each block contain various different transactions instead of just one. We'll do this using a technique and a data structure called a miracle tree. Finally, we'll extend this version further by creating a transaction pool that feeds a block chain, which newer implementation might be a message queue or a remote repository of transactions. We'll also extend the applications or use authenticated hashes and calculate a four-digital signature for each block that is entered onto the chain. Finally, we'll talk about versioning of blocks to support the rotation of authenticated hashing keys. As I mentioned earlier, in this project, all the sample applications have been written to support .NET Core 2.0. This means you can execute the samples on Windows, MacOS, and Linux, using IDE, such as Microsoft's Visual Studio on Windows, Visual Studio for Mac, Visual Studio Code.

a. MicrosoftAzureCloud

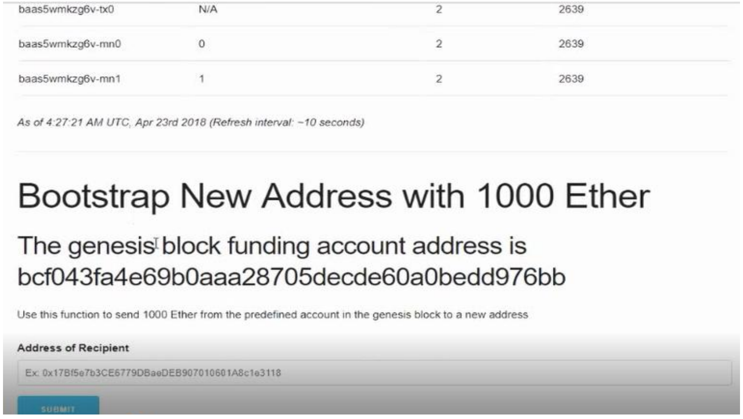
Microsoft Azure, formerly known as Windows Azure, is Microsoft's public cloud computingplatform. Itprovides arrange ofcloudservices,includingthoseforcompute, analytics, storage and networking. Users can pick and choose from these services to develop and scale new applications, or run existing applications, in the public cloud.Blockchain can be easily built using Microsoft Azure and the whole process takes slightlyoverahalfanhour. FirststepistocreateaMicrosoftazureaccount. HereIamused a free trial account.After creating an account we got one user name and password. Using this user ID we can login the account from portal azure login.

b. Metamask

Metamask is used to bring Ethereum to browser.Metamask is a bridge that allows you to visit the distributed web of tomorrow in your browser today. It allows you to run Ethereum dapps right in your browser without running a full Ethereum node.Metamask includes a secure identity vault, providing a user interface to manage your identities on different sites and sign blockchain transactions.We can install the Metamask add-on in Chrome, Firefox and Opera.

c. Ether Transaction

Ether exchange is done through metamask. I am already facilitated baas on purplish blue cloud. At that point I replicating the administrator site and glue it into the program. The I got one page including the Ethereum hub status.There is a deliver for sending ether to other record. fig 2.



baas5wmkzg6v-tx0	N/A	2	2639
baas5wmkzg6v-mn0	0	2	2639
baas5wmkzg6v-mn1	1	2	2639

As of 4:27:21 AM UTC, Apr 23rd 2018 (Refresh interval: ~10 seconds)

Bootstrap New Address with 1000 Ether

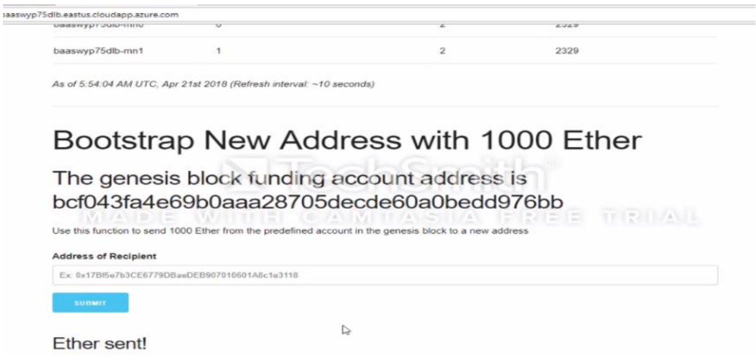
The genesis block funding account address is bcf043fa4e69b0aaa28705decde60a0bedd976bb

Use this function to send 1000 Ether from the predefined account in the genesis block to a new address

Address of Recipient: Ex: 0x17Bf5e7b3CE6779DBaeDEB907010601A8c1e3118

Fig2 : Ethereum node status

Here we can be copying the recipient address in the given box and click on submit button.Next login the metamask account and create one account.Every account should have one address. Copying the address of metamask account one and paste it in to the box like figure 2. then click on submit button. After that we can see that ether has been sent.



aaswyp75dlb.eastus.cloudapp.azure.com

baaswyp75dlb-mn1	1	2	2329

As of 5:54:04 AM UTC, Apr 21st 2018 (Refresh interval: ~10 seconds)

Bootstrap New Address with 1000 Ether

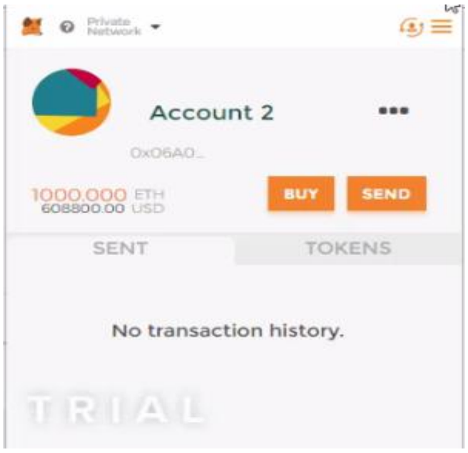
The genesis block funding account address is bcf043fa4e69b0aaa28705decde60a0bedd976bb

Use this function to send 1000 Ether from the predefined account in the genesis block to a new address

Address of Recipient: Ex: 0x17Bf5e7b3CE6779DBaeDEB907010601A8c1e3118

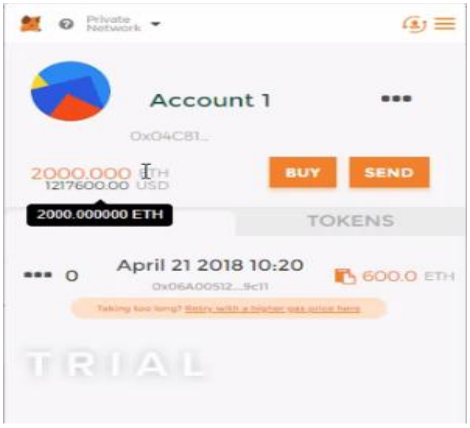
Ether sent!

Fig 3: Ether Sent



No transaction history.

Fig 5 :Before receiving ether



Account 1

0x04C81...

2000.000 ETH
1217600.00 USD

2000.000000 ETH

0 April 21 2018 10:20 600.0 ETH
0x06A00512...9c11

Taking too long? Retry with a higher gas price here

Fig4 :After receiving ether

V.CONCLUSION

Blockchain is an amazing topic in recent year, it will support different applications. Blockchain will give Better security during transaction of any value. This technology is mainly proposed to handling bitcoin transaction. Smart contract, Ethereum and distributed ledger are some applications of blockchain, This will also give more security.
Best suited and mostly used application of blockchain bitcoin. Blockchain gives faster and cheaper transaction than any other application. It will provide a better security especially to sensitive data. Blockchain applications often see additional benets in its transparency and immutability.

REFERENCES

[1] http://www.blockchain4innovation.it/wp-content/uploads/sites/4/2017/05/Blockchain
[2] https://www.coindesk.com/information/who-created-ethereum
[3]https://www.business2community.com/tech-gadgets/issues-blockchain-security-02003488
[4] A. Azaria, A. Ekblaw, T. Vieira, and A. Lippman, Medrec: Using blockchain for medical data access and permission management, in 2016 2nd International Conference on Open and Big Data (OBD), Aug 2016, pp. 2530
[5] C. Decker and R. Wattenhofer, Information propagation in the bitcoin network, in IEEE P2P 2013 Proceedings, Sept 2013, pp. 110.
[6][G. Zyskind, O. Nathan, and A. . Pentland, Decentralizing privacy: Using blockchain to protect personal data, in Security and Privacy Workshops (SPW), 2015 IEEE, May 2015, pp. 180184.
[7A.Mehmood,M.M.Umar,andH.Song,Icmds: Secureinter-clustermultiple-keydistribution scheme for wireless sensor networks, Ad Hoc Networks, vol. 55, pp. 97106, 2017.
[8] A. Azaria, A. Ekblaw, T. Vieira, and A. Lippman, Medrec: Using blockchain for medical data access and permission management, in 2016 2nd International Conference on Open and Big Data (OBD), Aug 2016, pp. 2530.
[9https://www.researchgate.net/publication/319058582 Blockchain Challenges and Opportunities A Survey
[10]https://www.dotmagazine.online/issues/innovation-in-digital-commerce/what-can-blockchain-do/securityand-privacy-in-blockchain-environments