Abstract

This project aims to evaluate Ethereum, a decentralized platform for the deployment of Smart Contracts on the approach is to initiate a private Ethereum test network, on which I will develop and deploy a decentralized Contract application. The steps towards building the development environment as the created or developed applications are demonstrated in my gathered experiences as the estimation about the potential of the Ethereum project is in my evaluation. I will describe types of Ethereum where we are going to look at the two major types. We will look at the application of Ethereum in our daily lives and how it impacts on us. Later we are going look at the issue of crypto smart currency where we will explain broadly its meaning, the purposes of crypto currency and the application of smart contracts. Lastly, we are going to evaluate the entire document where I will give my final conclusion. At the lower part there is the references.

Introduction

Since its inception in 2008, Bitcoin has managed to gain a lot of momentum and popularity and is now considered a stable alternative currency as a strong subculture movement. The underlyingtechnology of Bitcoin, the blockchain, a distributed database model used to validate the financial transactions in a decentralized manner, is considered tamper For that reason a blockchain based approach can be used for applications beyond monetary, especially in contexts where anonymity , privacy and censorship resistance are important aspects. A new tool called Ethereum Was first described in 2013 and was officially launched in 30 July 2015. Ethereum is a platform designed to run smart contracts over a decentralized network of peers. A smart contract in the context of Ethereum described as an application that runs exactly as programmed without downtimes, censorship, fraud or third party interference' The Ethereum claims that it is to fully decentralize the Internet 'as it was supposed to work by providing a platform on top of which anyone can start a decentralized Internet service, secured by the blockchain. I posed is that Ethereum will make it easy to launch blockchain-based applications without needing to start a new blockchain protocol or crypto currency. (Waters, Richard 2016)

How Ethereum works

Ethereum an open source project first introduced in 2013, initially described as a "Next Generation Smart Contract and Decentralized Application Platform". At first glance Ethereum is a peer-to-peer network and an exchangeable that allows nodes to share computing resources for the execution of programmable smart contracts on the blockchain. There are however multiple different Ways to describe Ethereum depending on point of view. In the official guides Ethereumis also described as a 'World Computer', in that it can be as a single computing platform where anyone in the world is able to use. In this world computer a number of programs can be encoded and executed, and any participating code can interact and have access to the state of each one of these programs. (De Jesus, Cecille 2016)

With Ethereum any user can have access to a cheap, zero-infrastructure, global platform that provides a very interesting set of features:

- User authentication, verified by the cryptographic signatures.

- Easily deployable payment logic. A payment system can be Setup on Ethereum Very quickly with no third party reliance.

• Total DDoS resistance. Each application on Ethereum not executed on any single node; rather it is executed on each and every node on the system. As long as there one node maintaining the blockchain the application will run perpetually and will be able to be interfaced by any joining node.

• Limitless interoperability. Each Ethereum contract can seamlessly interact with any other contract instance via the provided interfaces in the Ethereum ecosystem

• No server infrastructure. As mentioned before Ethereum completely built on top of a Peer-to- Peer network with no central server infrastructure involved. Thus, the deployment of an application on the blockchain does not require the setup and the costs of setting and maintaining servers.

Having said this, I can understand that Ethereum strives to provide a platform where anyone can easily deploy and run Internet services.

Ethereum account types

-

There are two types of accounts in Ethereum

1. Externally Owned Accounts
2. Contracts Accounts

This distinction might be eliminated in Serenity.

1. Externally owned accounts (EOAs)

An externally controlled account has an ether balance,

Can send transactions (ether transfer or trigger contract

code),Is controlled by private keys,

Has no associated code.

2. Contract accounts

A contract has an ether

balance,Has associated

code,

Code execution is triggered by transactions or messages (calls) received from other contracts.

When executed - perform operations of arbitrary complexity (Turing completeness) - manipulate its own persistent storage, i.e., can have its own permanent state - can call other contracts

All action on the Ethereum block chain is set in motion by transactions fired from externally owned accounts. Every time a contract account receives a transaction, its code is executed as instructed by the input parameters sent as part of the transaction. The contract code is executed by the Ethereum Virtual Machine on each node participating in the network as part of their verification of new blocks.

This execution needs to be completely deterministic, its only context is the position of the block on the blockchain and all data available. The blocks on the blockchain represent units of time, the blockchain itself is a temporal dimension and represents the entire history of states at thediscrete time points designated by the blocks on the chain.

What is a transaction?

The term “transaction” is used in Ethereum to refer to the signed data package that stores amessage to be sent from an externally owned account to another account on the blockchain.

Transactions contain:

The recipient of the message,

A signature identifying the sender and proving their intention to send the message via the blockchain to the recipient,

VALUE field - The amount of Ii to transfer from the sender to the

recipient,An optional data field, which can contain the message sent

to a contract,

A STARTGAS value, representing the maximum number of computational steps the transactionexecution is alloId to take,

A GASPRICE value, representing the fee the sender is willing to pay for gas. One unit of gascorresponds to the execution of one atomic instruction, i.e., a computational step.

What is a message?

Contracts have the ability to send “messages” to other contracts. Messages are virtual objects that are never serialized and exist only in the Ethereum execution environment. They can be conceived of as function calls. (Schneider, Nathan 2014)

A message contains:

The sender of the message

(implicit).The recipient of the

message

VALUE field - The amount of Ii to transfer alongside the message to the contract

address,An optional data field that is the actual input data to the contract

A STARTGAS value, which limits the maximum amount of gas the code execution triggered by the message can incur.

Essentially, a message is like a transaction, except it is produced by a contract and not an external actor. A message is produced when a contract currently executing code executes the CALL or DELEGATECALL opcodes, which produces and executes a message. Like a transaction, a message leads to the recipient account running its code. Thus, contracts can have relationships with other contracts in exactly the same way that external actors can. (Paumgarten, Nick 2018)

What is EVM?

Ethereum implements an execution environment on the blockchain called the Ethereum Virtual Machine (EVM). Every node participating in the network runs the EVM as part of the block verification protocol. They go through the transactions listed in the block they are verifying and run the code as triggered by the transaction within the EVM. Each and every full node in the network does the same calculations and stores the same values. Clearly Ethereum is not about optimising efficiency of computation. Its parallel processing is redundantly parallel. This is to offer an efficient way to reach consensus on the system state without needing trusted third parties, oracles or violence monopolies. But importantly they are not there for optimal computation. The fact that contract executions are redundantly replicated across nodes, naturally makes them expensive, which generally creates an incentive not to use the blockchain forcomputation that can be done off chain.

When you are running a decentralized application, it interacts with the blockchain to read and modify its state, but these will typically only put the business logic and state that are crucial for consensus on the blockchain.

When a contract is executed as a result of being triggered by a message or transaction, every instruction is executed on every node of the network. This has a cost: for every executed operation there is a specified cost, expressed in a number of gas units.

Gas is the name for the execution fee that senders of transactions need to pay for every operation made on an Ethereum blockchain. The name gas is inspired by the view that this fee acts as crypto fuel, driving the motion of smart contracts. (Schneider, Nathan2014)

The network needs to be rewarded for the amount of computation they provide in order to execute the smart contracts. The amount Of Ether paid for each transaction is reflected in the component of gas. Each computational activity (e.g. a CPU cycle) costs a certain amount of gas units. The total computational complexity within a transaction defines its final gas expenditure.

Each transaction specifies a gas price, i.e. the price the sender is willing to pay for a unit of gasin Ii. "The gas price is an incentive for miners to include the transaction in a block. A miner is free to any transaction with a low gas price. Each transaction specifies a gas limit, i.e. the maximum amount of gas units the sender is willing to expend on transaction. Since predictingthe exact amount of gas each transaction will expend is the sender must set an upper limit of gas they are Willing to pay for the transaction in order to protect themselves from running out for example they invoke an infinite loop).

Difference B/W Ethereum and Bitcoin

Bitcoin

The easiest way to define Bitcoin is to call it a “digital dollar.” That’s really all it is—minus all the formal regulations that come with a bank (which is what makes it such a disruptive concept). It’s not a technology. It’s not a company. It’s money, held in a digital form.

Some people buy Bitcoin because they want to store their money somewhere other than a bank. Some buy Bitcoin as an investment, believing that its price a few months or years from now will be substantially higher than it is today. And some people purchase Bitcoin as a means of investing in companies that raise money through an ICO, since equity in those companies cannotbe purchased with traditional currency. You can only purchase tokens with Bitcoin or Ether, which is Ethereum’s crypto currency. (Finley, Klint 2014)

Ethereum

Ethereum is another crypto currency, and one many people see as potentially overtaking Bitcoin as the dominant coin in the market.

What makes Ethereum different is its technology, not the fact that it's yet another crypto currency. Ethereum's coin value is referred to as "Ether," and just like Bitcoin is bought and sold,and used by investors to buy into ICO opportunities.

The difference between Ethereum and Bitcoin is the fact that Bitcoin is nothing more than a currency, whereas Ethereum is a ledger technology that companies are using to build new programs. Both Bitcoin and Ethereum operate on what is called "blockchain" technology, however Ethereum's is far more robust. If Bitcoin was version 1.0, Ethereum is 2.0, allowing for the building of decentralized applications to be built on top of it.

Furthermore, there is heavy support behind Ethereum's technology in what is called The Enterprise Ethereum Alliance. This is a super-group of Fortune 500 companies that have all agreed to work together to learn and build upon Ethereum's blockchain technology — otherwise referred to as "smart contract" technology. In this case, "smart contracts" mean that demanding business applications can automate extremely complex applications.

What has so many people excited about Ethereum’s technology is its potential to impact projects and processes across all industries. It’s by no means a perfect technology yet, but it has opened the door for a wide variety of unique innovations.

Crypto Smart Contracts

What is Smart Contracts?

A smart contract is a computer protocol intended to digitally facilitate, verify, or enforce the negotiation or performance of a contract. Smart contracts allow the performance of credible transactions without third parties. These transactions are untrackable and irreversible.

Smart contracts are self-executing contracts with the terms of the agreement between buyer and seller being directly written into lines of code. The code and the agreements contained therein exist across a distributed, decentralized blockchain network.

Smart contracts permit trusted transactions and agreements to be carried out among disparate, anonymous parties without the need for a central authority, legal system, or external enforcementmechanism. They render transactions traceable, transparent, and irreversible.

Proponents of smart contracts claim that many kinds of contractual clauses may be madepartially or fully self-executing, self-enforcing, or both. The aim of smart contracts is to provide security that is superior to traditional contract law and to reduce other transaction costs

associated with contracting. Various crypto currencies have implemented types of smart contracts.

A crypto currency (or crypto currency) is a digital asset designed to work as a medium of exchange that uses strong cryptography to secure financial transactions, control the creation of additional units, and verify the transfer of assets. Crypto currencies use decentralized control as opposed to centralized digital currency and central banking systems. The decentralized control of each crypto currency works through distributed ledger technology, typically a blockchain, that serves as a public financial transaction database.

Purpose of Smart Contracts?

Smart contracts help you exchange money, property, shares, or anything of value in a transparent,conflict-free way while avoiding the services of a middleman. The best way to describe smart contracts is to compare the technology to a vending machine. Ordinarily, you would go to a lawyer or a notary, pay them, and wait while you get the document. With smart contracts, you simply drop a Bitcoin into the vending machine (i.e. ledger), and driver’s license, or whatever drops into your account. More so, smart contracts not only define the rules and penalties around an agreement in the same way that a traditional contract does, but also automatically enforce those obligations.

Management

The blockchain not only provides a single ledger as a source of trust, but also shaves possible snarls in communication and workflow because of its accuracy, transparency, and automated system. Ordinarily, business operations have to endure a back-and-forth, while waiting forapprovals and for internal or external issues to sort themselves out. A blockchain ledger streamlines this. It also cuts out discrepancies that typically occur with independent processing and that may lead to costly lawsuits and settlement delays.

Automobile

There's no doubt that progression from slothful pre-human vertebrates to super-smart robots. Think of a future where everything is automated. Google's getting there with smartphones, smartglasses, and even smart cars. That's where smart contracts help. One example is the self- autonomous or self-parking vehicles, where smart contracts could put into play a sort of 'oracle' that could detect who was at fault in a crash; the sensor or the driver, as Ill as countless other variables. Using smart contracts, an automobile insurance company could charge rates differently based on where, and under which, conditions customers are operating their vehicles.

Real Estate

You can get more money through smart contracts. Ordinarily, if you wanted to rent your apartment to someone, you'd need to pay a middleman such as Craigslist or a newspaper to advertise and then again you'd need to pay someone to confirm that the person paid rent and followed through. The ledger cuts your costs. All you do is pay via Bitcoin and encode your contract on the ledger. Everyone sees, and you accomplish automatic fulfilment. Brokers, real estate agents, hard money lenders, and anyone associated with the property game can profit.

Healthcare

Personal health records could be encoded and stored on the blockchain with a private key which would grant access only to specific individuals. The same strategy could be used to ensure that research is conducted via HIPAA laws (in a secure and confidential way). Receipts of surgeries could be stored on a blockchain and automatically sent to insurance providers as proof-of- delivery. The ledger, too, could be used for general healthcare management, such as supervising drugs, regulation compliance, testing results, and managing healthcare supplies.

How do Smart Contracts works?

In order to understand how a smart contract works, let's take an example where you wish to sell a property of your own. The process of selling properties demands a lot of paperwork as Ill as communication with multiple parties. Other than the communication complexity, it also involves the risk of frauds. In the current times, most of the people who want to deal in properties make their way ahead through real-estate agents. These agents are responsible for dealing with the paperwork and markets. They act as intermediaries in the overall process and work on negotiations and overseeing deal.

In such cases, you can't rely on the person that you're dealing with therefore, the agencies provide escrow services which transfer the funds from one party to the other. When the deal is finalized, you will have to pay both, the agent and the escrow service their commission in terms of the decided percentages. This leads to an extra loss of money and more risk on the seller'send.

Enter Smart Contracts. Using smart contracts in such situations can result in more effectiveness by reducing the burden. Smart contracts are designed to work on condition-based principle (if this then that), which will resolve the ownership issue by transferring it to the buyer only when the monetary, as Ill as other conditions, are agreed upon. Moreover, when it comes to escrow services, smart contracts can replace those too.

Both money and the right of possession of the property can be stored in a distributed system which can be vied by the involved parties in real-time. Since the money transfer will bewitnessed by all the network participants, the chances of fraud are eliminated. Moreover, there's no chance of an intermediary to be involved as the trust between parties is not an issue anymore. All the functions performed by the estate agent can be coded into the smart contract, thus, savinga considerable amount of money on both, buyer and seller end.

Evaluation

I will present the experiences I gathered, using Ethereum from an operational as Ill as a development point Of Generally, Ethereum has brought some extremely powerful concepts into life and can certainly be a huge leap forward towards the decentralization of the Internet. However, it is still under heavy development and suffers from low maturity and lack of proper documentation. It demonstrates certain performance and stability issues and the security status of the platform is largely uncertain. Indeed, the official guides warn strongly against running anything production ready on the current version of the Ethereum. Below I share some of our insights regarding different aspects of my evaluation.

Difficulty

There is a clear imbalance between the difficulty of setting up and operating a development environment and actually developing an Ethereum application. Ethereum consists of several different components and its foundation lies in complex concepts in cryptography, mathematics, economics, etc. While a deep understanding of these concepts is not mandatory setting up an Ethereum client or a private network of peers, the user a lot of times has to rely on outdated or unclear guides, spread around different sources that sometimes conflict with each other. Moreover, the guides often reference other sources that have been abandoned deleted.

Developing, on the other hand, is much more intuitive since it largely resembles traditional object oriented although the solidity tutorial is itself also not completed, and sometimes introducing fundamental concepts for the first time, it is relatively easy for anyone with programming experience to rapidly develop and deploy complex smart contracts.

Computational Power and Storage

I have mentioned before that the Ethereum network new blocks every 12 seconds. This means that there is a release of a burst of computational power each time a block is discovered and the State of the Blockchain is updated. While this is an acceptable waiting time for a number of applications, such as every day financial transactions (transferring funds can take a few days if a foreign bank is involved for example), it is forbidding for certain time critical applications such as industrial operations or health Moreover, a big scalability issue becomes apparent if I think that the state of the blockchain has to be stored in each individual client.

Security

An interesting security question might arise. Can malware be built in the Blockchain? The intuitive answer is that this is not possible. While Ethereum can map anything that can be programmed into a Block-chain smart contract, smart contracts are applications that hold enforce certain logic and relationships between entities and other programming models, smart contracts do not handle files or initiate network connections. However, the security of the whole platform depends on the security Of the Ethereum Virtual Machine (EVM) and each client implementation. In theory if there is an implementation flaw in the Ethereum client a contract could try and print an executable command that Will actually have impact on the client (e.g. initiate an Ether transfer from an unlocked account).

Conclusion

I will present my conclusions in regard to how they will show the benefit overall of this research. Ethereum be directly used to rapidly deploy meaningful and sufficiently performing trusted with added value over traditional approaches this can be argued to be true I have

demonstrated that a full decentralized application can be developed and launched with minimal effort to the Ethereum network. The application I have developed is much more than a trivial 'Hello World' project and it is fully decentralized which adds great value.

Application performance even With the currently present constraints If I can look past the 12 second block time problem, I can achieve performance which for a large number of is totally What the time needed for an Ethereum to be developed and launched Development time, however, depends heavily on the experience of the developer and complexity of contract in question. However, since there is no infrastructure involved, the overhead of having to setup servers and database systems waived, which greatly speeds up the process. (Waters, Richard 2016)

The added value Of Ethereum becomes apparent by the fact that every application is decentralized and is controlled by no single authority. In a traditional client-server approach one would have to trust the operational authorities for ensuring the security of the system and not tampering themselves with the data. In the case of Ethereum trust eliminated samong the nodes.

References

Waters, Richard (2016). "' brought to earth by crypto currency". ft.com. The Financial Times. Retrieved 19 October 2018.

Waters, Richard (2016). "Ether thief remains mystery year after $55 million heist". www.bloomberg.com. Bloomberg News.

De Jesus, Cecille (2016). "The DAO Heist Undone: 97% of ETH Holders Vote for the Hard Fork". Futurism, LLC. Archived from the original on 7 August 2017. Retrieved 16 May 2017.

Paumgarten, Nick (2018). "The Prophets of Cryptocurrency Survey the Boom and Bust". The New Yorker. Retrieved 4 February 2019.

Finley, Klint (2014). "Out in the Open: Teenage Hacker Transforms Ib Into One Giant Bitcoin Network". Wired. Archived from the original on 18 March 2016. Retrieved 21 March 2016.

Schneider, Nathan (2014). "Code ymy own utopia: Meet Ethereum, bitcoin's most ambitious successor". Al Jazeera. Archived from the original on 23 February 2016. Retrieved 21 February 2016.

Schneider, Nathan (2014). "The Entrepreneur: Joe Lubin, COO of Ethereum". Epoch Times. Archived from the original on 25 April 2016. Retrieved 31 March 2016.