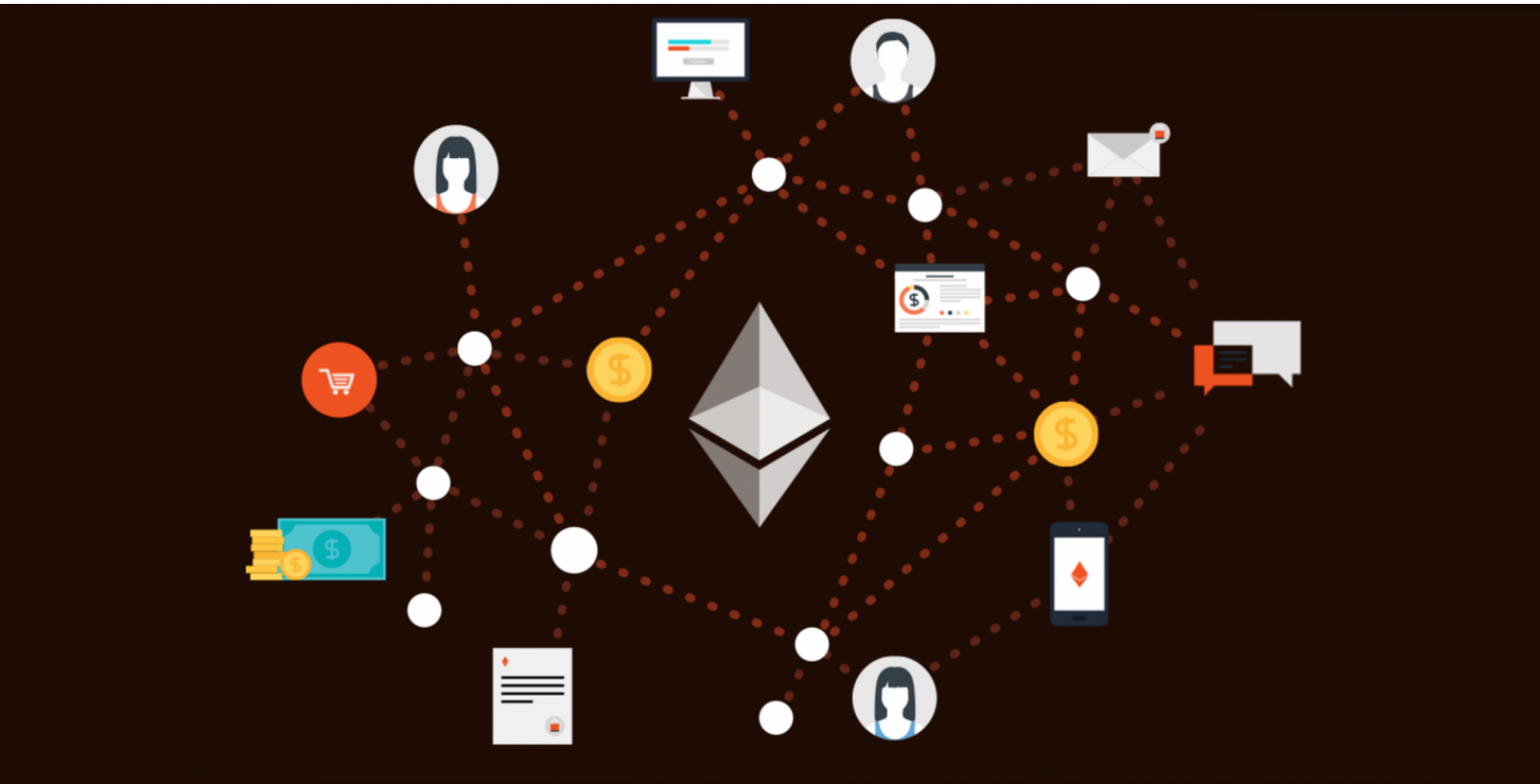
The Modern Ethereum

Ryan F Venter



The Modern Ethereum

Ethereum is the very first available platform that is truly a world computer that is distributed across many machines that will run applications in an unstoppable, uncensorable, trustless manner. It takes the uncensorable nature of a cryptocurrency and extends that to almost any application that you can imagine.

But the coolest thing about Ethereum is that we cannot even begin to imagine the applications that will be built on it. Prepare to be amazed over the next 5 years I think.

Bitcoin is a digital token and is easily tradable and that we use as a currency. The infrastructure that powers this is a distributed ledger called the blockchain. It was the first technology that solved the problem of distributed consensus. The problem is the internal scripting language of Bitcoin is, for understandable security reasons, quite constrained. It does not allow you to construct complex program logic (i.e. loops), it has no access to storage or any other concept of state and, thus, it has proved basically impossible to include any sort of complex program logic that would allow a fuller feature set.

Ever since people people realized the potential for distributed consensus they started thinking about other potential problems that could be solved with this technology. Ethereum has let the cat out of the bag by including a complete state-aware language on top of the Blockchain.

It's really the next logical step post Bitcoin. As inventor Vitalik Buterlin has stated, when the web came out, it was flat HTML files that couldn't really do anything. That's nice, but web applications really came alive when you added in a scripting language (i.e. Javascript). We can expect more or less the same transformation with Ethereum.

Table of Contents

Cryptocurrencies

History

There is little doubt that the twenty-first century is the century of Information Technology, and the Internet is the primary catalyst. It is funny to think that the Internet was once thought of as something slightly better than a fax machine. Not many people had the foresight then to predict the utility of this technology, and the same goes for Blockchain and Cryptocurrency Technologies.

Electronic Commerce requires Electronic Finance and there has been no stopping to the rise of Online Banking. However, in the wake of ever growing fees and the 2008 financial crisis, the world has seen an overall loss of confidence in the traditional banking system.

Interesting fact: When you give money to a bank, that money legally becomes their money. It becomes an asset on the bank's balance sheets. They then have a separate legal contractual obligation to pay you back, they owe you money. They are allowed to use the money which you have loaned to them for any purpose that they wish for.

What happened in the 2008 Financial Crisis was that the miscalculations (taking risk for profits), that banks were making for decades, finally caught up with them and they were about to go bankrupt which would mean a default on all their creditors, the depositors. Luckily the US government stepped in and 'bailed out' these banks at the expense of the US taxpayers but since there have been no sufficient changes in regulations and since banks are speculating with your money still, it is unclear whether the US Government has the funds or the appetite to do so again.

This has greatly influenced people's view of the US dollar as the world's reserve currency, not only at the consumer level but among governments and market traders alike. It has become a common believe that the US dollar and other national currencies pegged to it would start to fall in value or perhaps even fail completely.

As if on queue, the world's first cryptocurrency Bitcoin, started life in 2008 as a free, open-source computer program written by a "Satoshi Nakamoto". No one knows if Satoshi Nakamoto refers to one person or several, and the identity of that person or persons remains a mystery to this day.

Nakamoto's genius was in the way he solved the fundamental problems of decentralized digital money and what he created was a decentralized database of addresses that holds tokens that can only be sent to other addresses if one has the password (private key) to do so, and it works!

Transactions are verified by system-supported cryptography that crowd-sources from a global network of computers. This makes Cryptocurrency secure and fast enough to operate on a scale consistent with world currencies. It is easy to use, requires no third party trust (banks) and operates with extremely low transfer fees.

The consequences have been far reaching and because the technology is unstoppable and proven, it is only a matter of time before more and more people begin using it freely. It is uncertain exactly how the world will react to such a massive change in the way we transact going forward, but the disruption is already evident.

Many believe that when the new Cryptocurrency system stabilizes, we will see the decline of the US dollar standard. Money should encapsulate the fair worth of anything that a free market deems so, including goods, services and labor.

As the Internet is prevalent and neutral, there really is no way of stopping or controlling the emergence of this fantastic new and fair way of dealing with money and of global trade. It simply is up to the free markets to decide if it sees Decentralized Cryptocurrencies as beneficial or not, and so far, the trend is that free markets love it!

From the early days of buying a pizza with Bitcoin, to the current market cap of over 15 Billion USD (for all alternative coins and Cryptocurrencies), the popularity and utility of newer and better designed Cryptocurrencies like Ethereum will simply increase and this will mean that the same Ethereum tokens will come to represent an ever larger amount of trade and goods, which are not limited, an inverse inflation.

Current State Of Cryptocurrencies

Today, Cryptocurrencies are already accepted by many merchants for buying goods, making donations, and the list is growing fast. High profile names are pumping millions of USD into it, and now even public bodies want in on the act now.

There is little doubt now that Cryptocurrency technology will form the basis of money in the future, one way or another, and the industry is still wide open for new entrants. Make no mistake about it, those who embrace and learn to survive and thrive in this new world of Cryptocurrencies will become the movers and shakers of the future. So, those businesses and individuals who wish to stay ahead of the pack should endeavor to learn as much about it as possible.

Believe it or not but the most important thing about Cryptocurrency is not that it can be used as a currency, but it is the fact that we are now starting to really discover that we can use the underlying technology for so much more. The Blockchain that makes up the core of Cryptocurrency technology can be used for many decentralized uses such as voting mechanisms, ID verification, legal contracts, and this is where the new revolution in smart contracts will really be the most beneficial and disruptive. A new and better designed Cryptocurrency has been implemented and is set to overtake Bitcoin shortly. This exciting Cryptocurrency is Ethereum, and has set free the potential of what Cryptocurrency and Blockchain technology is able to do.

What Is A Cryptocurrency?

All Cryptocurrencies are simply digital records in an active and growing public ledger (Blockchain), that keeps track of who owns what and what applications where programed within a Blockchain system. It is important to understand that there is no physical cryptocurrency ‘coins’, only records of ownership of units of value.

When a Cryptocurrency token is sent from one person to another it does not actually move anywhere, there is only an alteration in the ledger’s ownership record for that ‘coin’.

The ledger records ownership without revealing any true identities through the use of digital addresses (public keys), which function like pseudonyms. Ownership is ultimately determined by a secret digital key (private key) that affords the holder exclusive rights to transfer Cryptocurrency tokens or to make changes to a programmable contract. When a transaction is made, this secret key is compared with its corresponding public key and if they match then the transaction is allowed (validated). If they do not match, then the transaction is refused (invalidated). This process is known as ‘digitally signing’ a transaction.

The owner is then able to spend these Cryptocurrency tokens on products and services from any business that chooses to accept them.

Reducing the trust required for transactions to occur was one of the primary drivers for the creation of Cryptocurrencies in the first place. As Satoshi’s original paper states in his last paragraph: "We have proposed a system for electronic transactions without relying on trust."

Cryptocurrency As An Investment

There is another reason to own Cryptocurrencies like Ethereum besides the participation of an online economy – investment. There are two primary reasons that people invest in Ethereum.

If central banks across the globe continue to devalue their currencies, then holding Cryptocurrencies could shield against such inflation.

When Cryptocurrencies such as Ethereum become widely adapted, including having easy exchange to and from national currencies, then it will become unimaginably valuable. Each unit worth of Ethereum will essentially increase when it starts to eat up more of the global economy's trade. Some predict prices within the thousands, even tens of thousands, per Ethereum. The potential upside is massive and it should be an essential part of any speculative portfolio.

Why Do People Give Cryptocurrency Value?

Utility

Cryptocurrency can be used to purchase goods and services wherever other currencies aren't accepted or convenient, most notably in dark markets, or developing nations.

Exchange Value

Cryptocurrencies can be exchanged for many different currencies on global exchanges. The term for this is ‘fungible’.

Speculation

Speculators procure Cryptocurrencies with the hopes of creating fast profits by playing the market. So all Cryptocurrencies have value as a speculative asset with a high volume of activity in the marketplace. The term for this is ‘liquidity’.

Cost Of Production

There is an additional reason that a Cryptocurrency can be ascribed value and that is the dollar cost per kilowatt of electricity needed to create (mine) new coins and secure the network.

Fair

It’s an open ledger (Blockchain) consisting all the records of transactions of limited supply units. All the rules of the system are out in the open and all participants can only play by the rules. This means that all parties can in fact ‘trust’ a Cryptocurrency system as the ‘system’ is theoretically un-hackable.

Straightforward

Cryptocurrency is quick and secure!

Blockchain Technology

This article will discuss Blockchain Technology in more detail and will use Ethereum as an example application. It is however very important to note that Blockchain Technology can be used for many more applications.

Interesting fact

There are exactly 2^160 or 1,461,501,637,330,902,918,203,684,832,716,283,019,655,932,542,976 Ethereum addresses. That is why one can simply 'find' an Ethereum address and safely assume that no one else can use it, as they will not have the private key which corresponds with your Ethereum address.

What Is A Blockchain

A Blockchain is a public decentralized database, secured by cryptography.

A Blockchain is a public piece of data which means that anyone in the world may view the entire database at any time. It is constantly growing as completed timestamped blocks are added to it with a new set of recordings. The blocks are added to the Blockchain in a linear, chronological order. Once a block is added it can never be changed. This means that information can only be added and never deleted.

To add information to a Blockchain, one must run a transaction on the Blockchain. In order for this to work, one requires a private password (the 'private key'). Anyone with this password can add specific data to the database. Transactions are the content to be stored in the blockchain and are broadcast to the network using software applications.

A block is the 'current' part of a Blockchain which records the recent transactions and once completed goes into the Blockchain as permanent database. Each time a block gets completed, a new block is generated and they are linked to each other in a chain-like, chronological order with every block, containing a hash of the previous block.

Another important feature of Blockchain Technology is that the database is decentralized. What this means is that an exact copy of the entire database exists on multiple independent computers around the world. Each computer which is connected to the network gets a copy of the Blockchain, which gets downloaded automatically upon joining the network. No centralized "official" copy exists and no user is "trusted" more than any other. According to ethernodes.org the Ethereum network currently has over 8,000 such copies running on node computers, this means that no single one needs to be trusted.

Nodes are maintained on the network for an incentive purpose called mining. Nodes compete with each other to see who can first complete the next block and therefore earn tokens for doing so. In a cryptocurrency system, miners collect two types of rewards: a predefined per-block award and fees offered within the transactions themselves, payable to any miner who confirms the transaction.

Also, due to the cryptography used in this technology, it is practically impossible to alter the database in anyway. Without the private keys, additional data cannot be added.

Cryptography

the magic that makes it work securely

Any public Blockchain needs robust security against fraud. The most important concept to grasp in order to be confident that Blockchain technology can't be hacked, is the concept of Cryptography. Cryptography is what is used to encrypt files and data communication over the Internet. Due to how we understand computational complexity, it can be proven that it is relatively easy to encrypt something with a password and on the other hand, it is relatively difficult to decrypt without that password. A good analogy would be to find all the prime factors of a large number. Factorizing a large number is difficult in

comparison to simply taking the calculated factor and then multiplying them to find the original large number again. This is the underpinning of concepts like Cryptography, digital signatures and implementing mechanism against data corruption. In the case of digital signatures, it is relatively easy to find a digital signature of a file, but once we have this signature it is relatively difficult to recreate this file exactly based on the digital signature and any changes made to this file, even swapping a single bit will create an entirely different digital signature. Also, when we say relatively difficult, what is meant is based on the current size of transistors and the explosion in difficulty. In some cases, we would need a computer a billion times the size of our universe and it would take this computer 10 times the age of our universe, in order to compute the answer. So as you can see, this is currently not possible.

Digital signatures are calculated by what is known as a hash function. The hash function used in Ethereum is named KECCAK-256. The output of KECCAK-256 is 256 bits or thirty-two bytes.

Interesting fact

It is only feasibly possible to find a Ethereum address from a private key and not the other way around. An Ethereum address is effectively a public key and in order to use that public key one needs the corresponding private key.

Practical Use Of Hash Functions

As an example, let's say Alice and Bob decide to jointly rent a 2-bedroom apartment. One room is greater than the other, however, they both like the larger room. Neither of them is sure what the extra cost of renting the bigger room should be and neither one desires to be the first to recommend a price as this will weaken their negotiating position. So, they both agree to the following protocol:

1. Each one will write down the price they are willing to pay for the bigger room per month.
2. Each will place the bid face down on the table while not showing the opposite person.
3. Once each bid is placed on the table, flip the papers over to reveal the bids.
4. The higher bidder will get the larger room and the price the winner pays is the average of the two bids.

However, let's say that Bob is out of town on a business trip. Therefore, this method has to be done remotely. If they struggle to negotiate over the phone or email, there's no guarantee that they could come to an agreement before the landlord starts looking for other tenants. The hash functions will solve this problem. Alice and Bob will both write down a sentence like "I'll pay $650" or "$700 is my bid," take the hash, and email each hash to the opposite person. At this time, neither is aware of the other person's bid.

Now both of them may exchange their sentence in order to find out each others bid. Both will rehash the others sentence to verify that the bid given is the one used to create the hash. If one party finds that the hash doesn't match, they'll know that it's time to start looking for a new honest friend. If all the bids conform to the given hashes then they can both be certain that they may fairly proceed with the rules of the protocol and have a happy life in their new apartment.

The point is, we can hash any chunk of data we like to ensure that the info contained within it can never be tampered with. This is because once we know the hash, we also know the resultant output must always be identical to what was put in.

Public-key Cryptography

To understand Blockchain Technology itself, you also need to understand the basic principles of public-key cryptography. This sounds complicated, but it mainly implies that every user who needs to speak with another must have two passwords keys. One key is public; so everybody can see it, while the other is private and known by the user alone.

Here is a basic example of public-key cryptography in action:

To send a secret letter, Alice would encrypt its contents using Betty's public key. Alice would then send her letter and Betty would decrypt it using her non-public key.

The reason public-key cryptography is so powerful is that it does not matter if another person – let's say Charlie – intercepts the letter. Even if he knows Betty's public key he cannot decipher the letter because one always needs the corresponding private key to do so.

This technology allows anyone to send any information out into the public domain (like onto the internet), but only the intended recipient would ever be able to read it.

Interesting fact

You can create an Ethereum address without having to be connected to the Ethereum network. Once you have an address you can ask your friends to send Ether to your address. As long as you have the corresponding private key that unlocks that address, you can spend those Ether, again.

The Ethereum Implementation

So now you understand a little about public-key cryptography, but how is it used within Ethereum?

Consider the Blockchain as having scores of safety deposit boxes, created out of bulletproof glass. The boxes have variable amounts of Ethereum, data and code within them, however they are firmly secured. Even supposing everybody will see what every box contains; only the deposit box owners can unlock them.

Those safety deposit boxes have various amounts of money contained within them and everyone in the world can see how much. However, they are completely secure and each one can only be unlocked by the person who holds the key.

The deposit boxes (addresses) are like public keys. Everybody can see the number strings that make up the keys and therefore finds out how much Ethereum they hold and what code, data and program state they hold. But the actual key to each box is the non-public key held by the owner, so only they can open the box.

Let's look at another example to better explain how it works:

Alice needs to send one Ether to Betty so she sends out a message to the whole network. This message includes Betty's public address (the location of her deposit box and how much Ether is in it), the amount of Ether she needs to send to Betty and her encrypted non-public key that acts as a digital signature to verify that she is the rightful owner of her particular deposit box.

When Alice sends this message out to the network, lots of different network users take a look and verify that this message is correct. If all the numbers match up, then a record of the transaction is placed into a block (a collection of many transactions). The block eventually gets added to the Blockchain, once it is filled with verified transactions.

When that happens, it is a signal that the entire Ethereum network knows and agrees that Alice's safety deposit box contains one less Ether than before, and that Betty's safety deposit box now has one extra Ether inside.

Since the Blockchain is a public ledger that contains records stretching all the way back to the first Ethereum transaction, transactions are never removed from it, then the Ethereum network is always aware of the precise quantity of Ether in each safety deposit box as well as any code, data and program execution that has ever happened in the past on the Ethereum network, forever.

Network Verification

So how is it that this system is unbreakable?

Let us consider the Ethereum network and see how it all works together.

Let's imagine Alice has no Ether in her account but tries to tell the Ethereum network she is sending 5 Ether to Betty. She is welcome to attempt this dishonesty, but it would be virtually impossible to get the network to believe her.

This is precisely because Ethereum's Blockchain is available to all computers operating on the network, so everyone knows whether anyone else has the right to make a transaction and all new transactions must be subsequently validated by the network.

If Alice did try send more coins than she had, the recipient would instantly check her balance, acknowledge the insufficient funds and reject the transaction. That transaction would never be allowed to take its place in the block, and subsequently the Blockchain.

So it is clear that the remainder of the network would never be fooled. Basically, the network remains clean because only verified transactions can ever enter the Blockchain cycle.

The exact same principle applies to the creation, and execution of Ethereum programs ('smart contracts'). Only valid code may be executed and only the holder of the private key to that contract may control it.

Mining

The term used for this processing of Blockchain transactions with a computer is 'Mining'. Mining uses a lot of computing power which needs valuable hardware and expensive electricity. So why would anyone want to get involved with such a process?

Precisely because they are rewarded with tokens for doing so, or in the case of Ethereum, they will receive Ether.

Miners verify transactions and as they are doing so, they are also searching for the answer to a mathematical equation set by the network. The equation is actually unrelated to the transactions being processed, it is simply a way to test the amount of work being done.

If a particular miner is the first to solve the equation, then the Ethereum protocol allows them to publish their block of transactions to the rest of the network. Whomever publishes a block gets a gift from the network of a set number of freshly minted Ether. This gift is known as a 'reward'.

And Then There Was Ethereum!

"Ethereum is the beginning of Web 3.0"

The Offshoots Of Bitcoin

There is currently more than 700 cryptocurrencies, each with their own network of miners and each has its own market value and supply of coins. After the concept of Bitcoin became widespread, more and more independent Cryptocurrencies established themselves on the same technology that bitcoin pioneered. Some of them is simply an attempt to take market share away from the original bitcoin domain and others have sought to address some issues with the current Bitcoin system.

An important thing to note though is that for any Cryptocoin to have any value, it must be traded on an exchange, and most cryptocurrencies are traded directly against Bitcoin, as Bitcoin is still the gold standard of cryptocurrencies.

For the last few years however, there has been lots of talk about improvements for this technology. It became more and more evident that a blockchain could be used for far more than a simple currency system.

One notable contender is Ethereum which has recently sparked a great amount of interest due to the fact that the technology can be used much more than just as a currency system. The largest crowd-sourcing event in history took place on May 28, 2016. An organization called The DAO raised over $164,400,000 in less than a few weeks, with the help of the Ethereum Blockchain Network.

Launched in 2015, Ethereum is based on Blockchain 2.0 or Bitcoin 2.0 technology and allows one to create and execute decentralized turing complete applications and by using the same private key methodology as Bitcoin for trusted verification of transactions.

Ethereum would never have existed without Bitcoin as a forerunner but is making advancements that are core to even basic transactions. It has also created a new generation of developers which never worked with Bitcoin but are interested in Ethereum.

The creator of Ethereum is Vitalik Buterin. After discovering cryptocurrency technologies through Bitcoin, he was immediately adrenalized by the technology and its potential. He co-founded Bitcoin Magazine in September 2011 and after two and a half years looking at what the existing Blockchain Technology and applications had to offer, in the great tradition of Satoshi Nagamoto, he wrote the Ethereum white paper in November 2013.

Ethereum Is Not Just Cryptocurrency

What was discovered was that the use of a Blockchain can enable far more applications than simply enabling a system of token exchange between private key holders- in other words, a cryptocurrency system. In fact, by enabling custom made programs to run in transactions on the Blockchain, it was made possible to create a global decentralized computer.

Example Applications Of Ethereum

Crowdfunding

Kickstarter, Indiegogo, and others have dominated the crowdfunding space for years. A start-up pitches an idea and sets a target for funding. Kickstarter charges 5% and passes the rest on to the start-up. On the Ethereum Blockchain, a start-up pitches an idea and sets a target for funding. If successful, the smart contract automatically sends the money to the startup and takes 0% as a fee.

Decentralized Voting

There is much speculation around the world that many democratic elections are less than democratic indeed. Fraud and tampering are common stories. Ethereum enables us to vote anonymously, but in such a way that each vote it counted openly and transparently. True democracy enabler!

Financial And Legal Contracts

Futures and options contracts, family trusts, marriage contracts and wills. Make your marriage official and put it on the Blockchain. A smart contract can transfer assets to next of kin following death.

Prediction Markets

Prediction Markets offer a way for market makers/speculators to bet on the binary outcome of an event. We will be able to see a new wisdom-of-the-crowd type of governance that has been thought to have many useful applications.

Social Media

A decentralized micro-blogging service running on the Ethereum Blockchain can provide basic Twitter-like functionality to tweet messages of up to 160 characters.

AKASHA is working on decentralizing online communities with a clever rating system. With open source code and rules governed by smart contracts, you should expect to eliminate future censorship scandals.

Managing Identity And Identity Verification

In the digital age, the increasing risk of financial crime arising from fraud and identity theft demonstrates the importance of a reliable means to safeguard the individual's identity.

A trusted gatekeeper would perform an individual check on a user's ID using KYC and authenticate them. The files would be stored in a distributed database system, which can later be retrieved by the trusted gatekeeper, or the user, to demonstrate with certainty that the ID is genuine.

By proving that you own the private key associated with that verified ID on the Blockchain, you can verify that you are in fact who you claim to be.

Payment System

The primary use case of Bitcoin can also be run on the Ethereum network.

Internet Of Things

The IoT will become a multi-trillion dollar market.

Online Gambling And Lotteries

On the Ethereum platform, you can code provably fair casino style gambling. What this means is that a casino can prove to you that they are in fact paying out in accordance to set rates and not that they may be cheating you.

Web Hosting

Decentralized web hosting means that a website is hosted by everyone at once, meaning that it cannot be DDoS attacked or censored by any government. So what we have here is a potentially censorship-free Internet.

Cryptocurrency Exchange

EtherEx is a decentralized exchange in the works for cryptocurrencies.

Other Use Cases

Escrow, time stamping, proof of work delivery and content creation verification.

Smart Contracts

Smart contracts are the building blocks for decentralized applications. A smart contract is equivalent to a little program that you can entrust with a unit of value (as a token or money), and rules around that value. The basic idea behind smart contracts is that a transaction's contractual governance between two or more parties can be verified programmatically via the Blockchain, instead of via a central arbitrator, rule maker, or gatekeeper. Why depend on a central authority when two (or more) parties can agree between themselves? And when they can make the terms and implications of their agreement programmatically and conditionally?

The starting point that you assume when applying smart contracts is that third-party intermediaries are not needed in order to conduct transactions between multiple parties. Instead, the parties define and agree on rules and they embed them inside the transactions, enabling an end-to-end resolution to be self-managed between computers that represent the interests of the users. Smart properties are digital assets which can identify who their owners are. Their ownership is typically linked to the Blockchain.

Smart contracts represent an "intermediate state" between parties and we will trust these smart programs to verify plus take action based on the logic behind these state changes.

Key Technologies For Developers

Solidity is a Javascript-like programming language of choice for smart contract development on Ethereum. There is also Serpent (Python based) and LLL (Lisp based). They all run on the Eithereum Virtula Machine, just like Java runs on the JVM.

Web3.js is the javascript browser interface to the Blockchain. The web graphical user interfaces, or front ends running in your browser can make use of web3.js in order to interface directly with Ethereum client.

Ether

Ether is the token of the Ethereum system. Like a Bitcoin unit is to the bitcoin system. And although Ether is also a crypto currency (because it has all the properties of any cryptocurrency), the main idea behind Ether is that it is used to pay for running contracts on the Ethereum network. Just like on Bitcoin network there are also miners who mine for Ether. It can be bought and sold on many exchanges, just like bitcoin, but it allows the main fuel used to pay for running the smart contracts on the Ethereum Network.

Noteworthy Exchanges To Buy, Sell And Hold Ether

http://www.kraken.com/

http://www.cex.io/

http://www.bitstamp.com/

http://www.shapeshift.io/

http://www.poloniex.com/

More Information Online

Notable websites where you may find more information about the Ethereum ecosystem and about existing DApps, as well as the laters news and developments:

http://coinmarketcap.com/

http://ether.fund/

http://dapps.ethercasts.com/

https://www.youtube.com/user/EtherCasts

http://www.myetherwallet.com/

How To Learn About Ethereum

This guide is for people who wish to learn about Ethereum, smart contracts and decentralized blockchain technology. At present, the Ethereum ecosystem is in very fast development mode and as such most of its users are also developers focusing on features rather then interface.

Learning about Ethereum is as much about using existing Đapps (smart applications that run on the Ethereum blockchain network), as it is about learning how to create your own Đapps.

The Ethereum ecosystem is still in its infancy and Đapps it's unfortunate that at the present time it is too advanced for most people who are not technically savvy enough to access the fantastic features it delivers. For starters, at the moment most Ethereum services make use of the web3.js framework. While this has the benefit of fully decentralizing applications, the problem with web3.js is that it requires an end user to have a fully working Ethereum node installed on their computer. Currently the Ethereum blockchain is more then 30GB in size and growing at apace of about 1.5 GB per month. Not many people are willing to install over 30GB of data simply to use Ethereum services. Hardcore users who really wishes to run Đapp applications on their own node may opt to use a web3.js version of an application, which will enable the user to verify any Ethereum Đapp on the blockchain.

As the Ethereum community continues to grow, I suspect that most Ethereum applications and services will become more readily available in that they will run a full stack of Ethereum services on their servers (as most websites do today) but with the added facility to check the blockchain code when needed.

Lite Clients

Another workable solution will come in the form of what is know as "partially light clients". A light client can be viewed as an Ethereum node that downloads block headers by default, and verifies only a small portion of what needs to be verified, using a distributed hash table as a database. These partially light client nodes, will processes everything but will store almost nothing of the blockchain.

In the future it is expected that all Ethereum nodes except for a few archive nodes intended to be run by businesses, block explorers, will eventually be set up as light clients with respect to all history older than a few thousand blocks.

There are however various good reasons to install an Ethereum node today. For starters you could use it to start mining your own Ether (the token currency of Ethereum), or as part of a platform to be able to learn how to develop your own smart contracts!

The most popular node, geth (short for Go Ethereum) is still beta testing its light client functionality, but if you wish to start running your own Ethereum node now as a light clients, you should try the Parity Ethereum Node.

According to the Parity website, Parity is a high performance, lightweight Ethereum node providing you with access to all the features of the Ethereum network including powerful Decentralized applications. What really sets Parity apart is the fact you can download a smaller version of the Ethereum blockchain at just over 4 GB. Installation is simple and there are distributions for all 3 major operating systems, and once you have installed and synchronized your blockchain, you can start writing smart contract and deploy transactions on the main Ethereum blockchain.

Private Test Blockchain

Another viable option if you want to learn about Ethereum is to simply run your own private Ethereum test network for development and testing purposes. This private blockchain will be separate from the main Ethereum blockchain and all changes and usage of it will be solely for you own personal usage. It is usually hard to try to explain to someone what Ethereum is and what it can do, just as it is hard to explain how to do programming, one needs to use a new technology and practice with it in order to learn it and to understand what it is about and what it can do.

Your best option for running a private blockchain is the geth node because on geth you can easily create a private testnet blockchain on which you can deploy smart contracts and transactions just as you would on the main live Ethereum blockchain.

Simply download geth from https://github.com/ethereum/go-ethereum/wiki and after installation run the following command:

```
geth --dev --unlock 0 console
```

geth will start by asking you for a Passphrase. This will be your testnet account password and you will use it to access your accounts later. Type in your Passphrase and remember it.

Then type in:

```
miner.start()
```

This will start a fully working test node that you can use to connect all existing Ethereum applications to.

Then there is also the Ethereumjs testrpc. Testrpc is an even lighter-weight test node for running test Ethereum systems. The problem with testrpc is that, since it is a heavily open source application it is difficult to install in on Windows and Mac Os. Various libraries and dependencies are required, and any missing piece will make the entire installation fail. If you want to try testrpc it is advisible to install it on a virtual Linux machine on Windows or Mac OS or to install it natively on a Linux distribution. Currently the most popular visualization software for Windows ad Mac OS is called VirtualBox.

After having installed and tried both geth and testrpc, my advice is to just use geth. Geth also happens to be the most popular Ethereum node at the present moment and it has lots of additional functionality which is not found in testrpc.

A third and new option is Metamask. Metamask is a new concept in that it allows you to run Ethereum Đapps 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.

The Power Of The Blockchain

So now that you have either a full or test node running, what now? The next step would be to install the official Ethereum-Mist Wallet Application.

Styled as a decentralized application discovery tool, Ethereum-Mist Wallet is meant to serve as a wallet for smart contracts that features a graphical interface and allows users to dynamically set transaction fees and manage custom tokens. Ethereum-Mist Wallet enables you to transfer Ether, and deploy Ethereum transaction and new smart contracts.

Again, the best way is to see for yourself by downloading the latest version from the official open source Github repository Ethereum Mist

From here you will have the power of the Ethereum blockchain at your fingertips and be able to further explore other areas such as creating your own custom cryptocurrency tokens or even writing your own smart contract and Đapps. Let your journey begin!

Ethereum Wallets

Ethereum as an investment vehicle makes more and more sense. The Ethereum platform is gaining a lot of attention globally these days as it is the 1st major decentralized applications platform and its underlying cryptocurrency Ether (which is meant to be serve as payment for executing application code) can only gain in value. The main reason for this is that Ether has now become a permanent store of value, such as other cryptocurrencies, but Ethereum will nave much broader utility then other cryptocurrencies going into the future.

There are several ways to get Ether. All new Ether comes into existence by a process know as mining. Ethereum miners are computers who enable the network to operate securely and decentralized and in exchange for mining, they receive payment in the form of new Ether. Anyone with sufficient computing capabilities can run a mining node, however the easiest way to obtain Ether is most probably to just buy it from other traders on one of the major cryptocurrency exchanges such as Kraken, Cex, Bitstamp or Shapeshift.

The Ethereum blockchain is a ledger which records ownership of Ether without revealing any true identities through the use of digital addresses (public keys), which function like pseudonyms. Ownership is ultimately determined by a secret digital key (private key) that affords the holder exclusive rights to transfer Ether. When a transaction is made, this secret key is compared with its corresponding public key and if they match then the transaction is allowed (validated), if they do not match, then the transaction is refused (invalidated). This process is known as 'digitally signing' a transaction.

In the physical world, we tend to store our cash in a physical wallet. Ether is also stored in a wallet, except that it is a digital one. An Ethereum wallet is a software file containing your private-key, public-key (address) and your balance. Wallet files are loaded into wallet software so that they can be used. Wallet software is available in numerous forms, and for various devices. Of course, it is always important to encrypt and make backup copies of your Ethereum wallet files, and you can even make paper wallets if you do not wish to store these on a computer. To be technically correct, you do not actually store Ether anywhere. What you store in a wallet, are the secure digital keys used to access your public Ethereum addresses, these in turn are stored on the global blockchain.

Online Wallets

In light of recent hacks at large cryptocurrency exchanges, something which had nothing to do with cryptocurrency and blockchain technology's security models, it would be very wise to keep any cryptocurrencies such as Ether safely in your own cryptowallet and not on a wallet stored on a server on the internet.

Online wallets defeats the purpose of decentralization and poses the risk of hacks and theft. Because they require your personal keys to be placed under the control of whatever organization owns the web-based wallet service, taking your Ether out of your control and involving a third party.

There are some advantages to using online wallets such as

- No syncing is necessary, your Ether is instantly accessible.
- They can be accessed from many places other than your computer; all you need is an online browser.
- You can integrate your wallet with browser plugins that make using Etherum online much easier.
- Your coins are not held on one single hard drive, so if your PC crashes, they will remain safely in the cloud.

However the disadvantages outweigh these as:

- You must trust a third party with your Ether. While many online wallet service providers have a good name, it is still always risky to let another party hold onto your non-public keys.

- If you are connected to the internet you are already at some risk of malicious attackers who might try to steal your coins. But internet-based wallets are often even more vulnerable to attack.
- Many online wallet services have indeed been attacked and many have closed shop following such an attack, and they have not refunded all of their users.

For small amounts of currency they can be a very convenient choice. It is much easier to simply log onto a website to move your Ether and let them do all the hard work of syncing for you. It is especially beneficial if you are planning on leaving your home for a few days and do not want to take a laptop. However, these services should not be used for any amount of Ether that you cannot afford to lose.

Software Wallets

There is currently a good selection of Ethereum wallet software which will enable you to keep your Ether safely secured. One thing that you MUST remember is that since you are in control of your Ether, you must keep your "private keys" encrypted and backed up at all times.

Mist Ethereum Wallet

Mist Ethereum Wallet is the most popular software wallet at the moment but required an Ethereum node to be installed and running. As such you may want to consider one of the other options until the time when "light client nodes" become available in the near future.

MyEtherWallet

Running a full node is an important part of any cryptocurrency's ecosystem, as it helps keep the system decentralized and secure. But as a user, not everyone has the resources to broadcast and store the blockchain in their computer, which is strictly required when running Mist or any other full node wallet solutions. Mist can be used as a simple wallet to send and receive payments, but it requires users to run a full node and it takes a while to sync. If you want to create a new wallet without having to download the blockchain or simply haven't done so in a long time and don't wish to download a big part of it, you can simply use the web based application, MyEtherWallet.

MyEtherWallet is not an online wallet as it does not allow you to create an account and to store your Ether on their servers. MyEtherWallet simply allow you create a wallet, which is yours to store and keep safe, and to broadcast your transactions on the blockchain through their full node.

With MyEtherWallet you can:

- create a wallet
- send a transaction
- make an offline transaction

You can create an Ethereum wallet within seconds and easily send a transaction without the need to download and broadcast the blockchain! And you can even protect yourself against nasty hackers and evil-doers by generating a transaction offline and broadcasting it on an online computer.

JAXX

Jaxx is a multi-platform open source Ethereum and Bitcoin wallet which offers a client-side security model, with private keys hosted locally and never sent to any servers.

With a focus on unifying the look and feel across devices and focusing on customer service, security, design, and user experience, their goal is to make the Jaxx Ethereum wallet default wallet of choice for the masses.

Icebox

Icebox is a simple Ether cold storage solution which makes it easy to securely generate new keys and addresses on an airgapped device as well as spend from those addresses.

EtherLi

EtherLi is a multi-signature wallet where multiple signatures are necessary before funds can be transferred. Etherli uses a two of three multi-signature scheme which means that at least two signatures are necessary to validate a transfer of funds. Multi-signature wallets are more secure because an attacker must obtain at least 2 keys and gain access to multiple devices in order to obtain access of a users funds. The use of 2FA and server-side security of the co-signer key dramatically lowers risks posed by malware, phishing, weak passwords, and hacks. You can still recover funds if you lose data for a single key, or forget the password to one of the keys.

Threats

So, you have an idea of the various ways to store your Ether, but is there really a need to keep them safe?

Most definitely Yes!

There are many threats to your digital cash, and being attentive to them will greatly increase your chances of avoiding them.

Yourself

You are the biggest threat to your Ether. That might sound strange, but it is true.

There are a great many horror stories of individuals being careless and losing their cryptocurrencies, and it is usually one of two major mistakes that they tend to make: The first is to encrypt their wallet and then forget the password, and the second is to leave their wallet on a hard drive which then breaks, causing it to be lost forever.

Most of the standalone Ethereum wallet programs allow you to encrypt your wallet file. This is sensible, and you should do it, because it stops people accessing your PC and getting to your coins, however many people make the password and then forget it because it could be months later when they come to access their coins again. And if this happens to you, you are sunk, because there is no way to recover those coins, none at all, ever!.

When you choose a password you must write it down and put it in a safe place. This is even truer if you have multiple wallets, don't use your wallet often, or use web wallets.

Make sure you put your written password and backup copies in a safe place!

Physical Theft

Theft is a very common threat, whether you have a paper, mobile, or desktop wallet, there are always ways for a thief to walk off with your coins. If they can access your wallet in any way, then they will transfer your Ether to an address they own and you will not even be able to find out who did it.

Hacking

There are many tech-savvy criminals out there who are making it their business to hijack as many cryptocoins and Ether as they can. They primarily target exchanges or online wallets were there are millions of users and lots of coins. Several exchanges have been hacked within the past few years, resulting in many lost coins, and they are seldom recovered or the perpetrators identified.

Luckily, they cannot hack the encryption in Ethereum itself, so individual users are only in danger when holding coins online with vulnerable web-based services.

As the Ethereum community and infrastructure grows, it is likely that more professional and mature firms will populate it. They will have the finances and experience to deal with hackers, and to implement much more stringent safety measures. But until then, the best approach is to only store small amounts of coins with exchanges and online wallet providers.

Malware

Passive attacks are carried out by somehow implanting malicious code on your computer. They are a much bigger threat to the average Ethereum users than active hacks because they target an individual's PC.

The malicious code will often record all keystrokes, and then send them to the hacker. If the hacker can use a keylogger to find out your password, then he can get to your Ether.

These types of attacks will usually get in via a browser when you click some shady looking link and it permits a bad script to run. Sadly, malware like this is very easy to pick up, particularly if you don't have good protection against it and are dangerous with your web browsing habits.

Securely Storing your Ether

The final topic to cover before you go experimenting with Ethereum is secure storage. Storing your Ether securely does require some technical ability but it is not overly complicated.

It is not advisable to skip this topic, because not securing your funds correctly is like leaving the doors and windows of your house unlocked while you go out, and just hoping nobody decides to come in and steal something.

Ethereum tokens are literally in their deposit boxes (their public addresses) on the Ethereum blockchain, and a wallet is just a file with all of the information about your deposit boxes into one place so you can gain access to them.

Think of a wallet as your own little bank. With it you can look at your row of deposit boxes, and you have the keys to those boxes too. So, whenever you want to look inside, remove, or add Ether to any of your public addresses, the wallet allows you to do so.

Backups

It is easy to deal with the problem of hard drive failures. All you need to do is make copies of your wallet file and save them to a USB drive, or a web storage system like Google Drive or Dropbox.

Always remember to encrypt it before making a backup, and then to write down the password first and put it in a safe, memorable place.

Paper Wallets

The safest and most cost-effective option for keeping your Ether safe, but also a little bit inconveniant are paper wallets. Also some people do not want to use computer, internet or smartphone-based wallets.

But you are probably wondering why on earth anyone would want to keep digital coins on paper. Well, there is an easy answer: Paper wallets are by far, the safest method of storing your Ether. So if you do not need to use your coins regularly, and just want to store them long term, then you might want to look into using a paper wallet.

You might wonder how it is possible that Ether, a digital currency can be stored on something as primitive as a piece of paper. But remember that the genius of Ethereum lies in public-key cryptography, and its public ledger, the blockchain.

So, to make a paper wallet, all you have to do is create a public Ethereum address, place some Ether within it, and then print off the private key and store it somewhere safe.

To use your Ether later, you would find your piece of paper and input that private key from it. Often paper wallet generators print this as a QR code in the first place, so you may only have to scan the non-public key. One such paper wallet generator can be found at ethaddress.org, which is an open source project with lots of features.

The good thing about paper wallets is that their personal keys are not stored digitally, and so cannot be subjected to cyber-attacks or hardware failures, however the bad thing about them is that they might be damaged in a fire or flood, you may lose them, or someone might steal them from your pocket, and there is no backup!

Starting Your Own Cryptocurrency on Ethereum

The notion of cryptocurrencies have come along way from its inception in the Satoshi Nagamoto white-paper. There is currently almost 100 million people using cryptocurrencies around the word, and with more then 700 different Bitcoin clones out there, the key question then becomes, do we need any more cryptocurrency coins. The answer is yes.

Most cryptocurrencies in existence today are mere clones of the original bitcoin idea, some even using the exact same code but with just a different name and on a different blockchain network. This is a very expensive waste of energy just to maintain the different networks.

Instead of having to create entirely new decentralized blockchain networks in which to run yet more cryptocurrencies, why not just use the existing Ethereum global computer, with infrastructure already setup and all the safety guarantees to go with it. Also you would not need to run your own node in order to make sure that your network keeps running as its should, but instead outsource that functionality again to the Ethereum world computer.

That was the whole premise for the creation of Ethereum as its creator realized that blockchain technology could be used for far more applications not just cryptocurrencies, so why not use Ethereum to do this basic functionality for us?

In Ethereum there is already a standardized form of cryptocurrencies, and although anyone can create an entirely new way of implementing a cryptocurrency, if you use the Ethereum standardized method, your new token can instantly become recognizable in existing Ethereum wallet software, which means you will also already have wallet software made for you.

The Code

What you will see below is an Ethereum smart contract written in a language called Solidity. Solidity is the standardized programming language of Ethereum used to create smart contracts. Although you won't need to fully understand Solidity in order to create your own cryptocurrency, it is definitely worth learning it at some point in the near future. It would also be worth it to take a little bit of time to see if you can understand what the code is doing.

```
contract tokenRecipient { function receiveApproval(address _from, uint256 _value, address _token, bytes
_extraData); }


contract MyToken {
    /* Public variables of the token */
    string public standard = 'Token 0.1';
    string public name;
    string public symbol;
    uint8 public decimals;
    uint256 public totalSupply;

    /* This creates an array with all balances */
    mapping (address => uint256) public balanceOf;
```

```
    mapping (address => mapping (address => uint256)) public allowance;

    /* This generates a public event on the blockchain that will notify clients */
    event Transfer(address indexed from, address indexed to, uint256 value);

    /* Initializes contract with initial supply tokens to the creator of the contract */
    function MyToken(
        uint256 initialSupply,
        string tokenName,
        uint8 decimalUnits,
        string tokenSymbol
        ) {
        balanceOf[msg.sender] = initialSupply;              // Give the creator all initial tokens
        totalSupply = initialSupply;                        // Update total supply
        name = tokenName;                                   // Set the name for display purposes
        symbol = tokenSymbol;                               // Set the symbol for display purposes
        decimals = decimalUnits;                            // Amount of decimals for display purposes
        msg.sender.send(msg.value);                         // Send back any ether sent accidentally
    }

    /* Send coins */
    function transfer(address _to, uint256 _value) {
        if (balanceOf[msg.sender] < _value) throw;           // Check if the sender has enough
        if (balanceOf[_to] + _value < balanceOf[_to]) throw; // Check for overflows
        balanceOf[msg.sender] -= _value;                     // Subtract from the sender
        balanceOf[_to] += _value;                            // Add the same to the recipient
        Transfer(msg.sender, _to, _value);                   // Notify anyone listening that this
transfer took place
    }

    /* Allow another contract to spend some tokens in your behalf */
    function approveAndCall(address _spender, uint256 _value, bytes _extraData)
        returns (bool success) {
        allowance[msg.sender][_spender] = _value;
        tokenRecipient spender = tokenRecipient(_spender);
        spender.receiveApproval(msg.sender, _value, this, _extraData);
        return true;
    }

    /* A contract attempts to get the coins */
    function transferFrom(address _from, address _to, uint256 _value) returns (bool success) {
        if (balanceOf[_from] < _value) throw;                 // Check if the sender has enough
        if (balanceOf[_to] + _value < balanceOf[_to]) throw;  // Check for overflows
        if (_value > allowance[_from][msg.sender]) throw;   // Check allowance
        balanceOf[_from] -= _value;                           // Subtract from the sender
        balanceOf[_to] += _value;                             // Add the same to the recipient
        allowance[_from][msg.sender] -= _value;
        Transfer(_from, _to, _value);
        return true;
    }
```

```
    /* This unnamed function is called whenever someone tries to send ether to it */
    function () {
        throw;     // Prevents accidental sending of ether
    }
}
```

How To Deploy

Open the Ethereum Wallet, go to the contracts tab and then click "deploy new contract".

Paste the source code from above into the "Solidity source field".

You should now see a "pick a contract" drop down on the right and select the "MyToken" contract. On the right column you'll see all the parameters you need to personalize your own token. In this tutorial you should use these parameters:

10,000,000 as the supply

Any name you want

"%" for a symbol

2 decimal places

Your app should be looking like this:

Scroll to the end of the page and you'll see an estimate of the computation cost of that contract and you can select a fee on how much ether you are willing to pay for it. Any excess ether you don't spend will be returned to you so you can leave the default settings if you wish. Press "deploy", type your account password and wait a few seconds for your transaction to be picked up.

You'll be redirected to the front page where you can see your transaction waiting for confirmations and after about a minute you should see that your account will show that you have all the tokens that you have just created. To send some to a few friends: select "send", and then choose the currency you want to send, paste your friend's address on the "to" field and press "send".

If you send it to a friend, they will not see anything in their wallet though. This is because the wallet only tracks tokens it knows about, and they will have to add these manually. Go to the "Contracts" tab and you should see a link for your newly created token. Click on it to go to its page. Since this is a very simple contract page there isn't much to do here, just click "copy address" and send that Ethereum address to your friend.

For you friend do add a token to watch, they must go to the contracts page and then click "Watch Token". A pop-up will appear and they need to put in that contract address. The token name, symbol and decimal number should be automatically filled but if it's not they can put anything you want (it will only affect how it displays on their wallet). They will automatically be shown the balance they have of your new token and they will also be able to send it to anyone else. That's all you have to do to have created your own cryptocurrency.

Conclusion

Hopefully, I have made the potential uses of Blockchain Technology and smart contracts a little bit clearer to you in this article. The power of Blockchain Technology comes from its diversity of use cases and just how many use cases are out there that haven't even been discovered yet? Ethereum has only been in the development for two years and is by all accounts still raw and unfinished. Its potential as a game changer coupled with some smart and creative thinkers will only mean incredible applications and valuable real life utility which will improve the quality of our lives.

Ethereum is opening the door to a new class of applications that has never been seen before, it will change the world in fundamental ways.