Abstract

Cryptocurrencies are under increasing attack from regulators that seek to control the industry. There is a need for cryptocurrencies to evolve in order to provide users the same benefits that made them popular. EthereumDark is one of the pioneers who seek to increase the functionality of the altcoins while improving the security. The first step is achieved by integrating smart contract technology with cross chain payment processing. This will increase what users can do with the ETHD coins in their wallets. Additionally, EthereumDark seeks to make the blockchain more secure by intruding masternodes in the third phase. The masternode technology, coupled with the smart contract algorithms, will allow user-to-user transfer that is truly anonymous. The enhanced anonymity coupled with the greater flexibility in remittance and payment processing will surely endear EthereumDark to the cryptocurrency community. With many regulators like the IRS trying to control the industry, EthereumDark is one of the altcoins that will forge a path to greater anonymity. This is a precursor to the cryptocurrency industry's second resurgence.

Table of Contents

Introduction

When cryptocurrencies were first developed, many people seemed to assume that they would be

a simple fad. However, the skeptics have been proved wrong with cryptocurrencies reaching a

market capitalization of $164 billion. Some experts estimate that the capitalization will pass the

$200 billion market by the end of 2017. This is an indication that this industry is growing at a

rapid rate. Part of the reason for this is the increase in the awareness of the benefits that

cryptocurrencies bring to the financial market.

Reasons for the popularity of cryptocurrencies

The digital currency guarantees complete anonymity. This is unlike the standard currencies used

across the world. For instance, when making a purchase using one's credit card or an ATM card,

one's background information such as personal identity, the physical address is usually attached

to the transaction. The banks have access to an individual information that can be traced back to

the account user. However, cryptocurrencies transactions carry no personal information without you adding it yourself.

Unlike the traditional currency where when you give them access to your credit they can access your funds, cryptocurrencies use techniques that only allows to cryptocurrency recipient to only access what cryptocurrency holder is willing to let them know with no further additional information. Therefore, cryptocurrencies reduce the risk of identity theft, unlike the conventional currencies.

With the invention of various digital platforms, the world is becoming more financially unsafe. This implies that the cryptocurrencies are safe and significantly lower cases of fraud. The digital transactions under the bitcoin platform are very safe and secure. The transactions are less susceptible to credit card frauds for buyers. The recipient of the money sent does not get a

message notifying them of the transaction. This means no niche can be used to steal money from the sender even in the future.


Bitcoin is pseudonymous and not anonymous. Also, transactions made through Bitcoin system can be tracked and are permanently logged in the blockchain. This means that the Bitcoin transaction is easier for law enforcers to follow, monitor and trace the money, diamonds or gold. This guarantees transparency without discrimination since most can monitor the activities taking place and any form of attempted fraud is curbed immediately.

The cryptocurrencies have a decentralized model. Bitcoins draw its advantage from the fact that it has no third party or intermediary whose purpose is to verify the seller and the buyer interactions. The use of third-party implicates the use of transaction cost. This is an added advantage to the use of cryptocurrencies. The use of cryptocurrencies denies the government the power to control and regulate finances based on the monetary policy. Unlike the traditional currencies, cryptocurrencies have no government control on personal financial assets.

Traditional financial accounts can be frozen completely. This implies that the account holder has no access to their finances in the accounts. Since these digitally available currencies do not operate within the confines of the law and the demands of regulation, then this is an impossible scenario in the use of cryptocurrencies. Only on rare occasions can a bitcoin investor be rendered the access to their funds. This may only take place whenever there are proven illegal activities are binding the case.
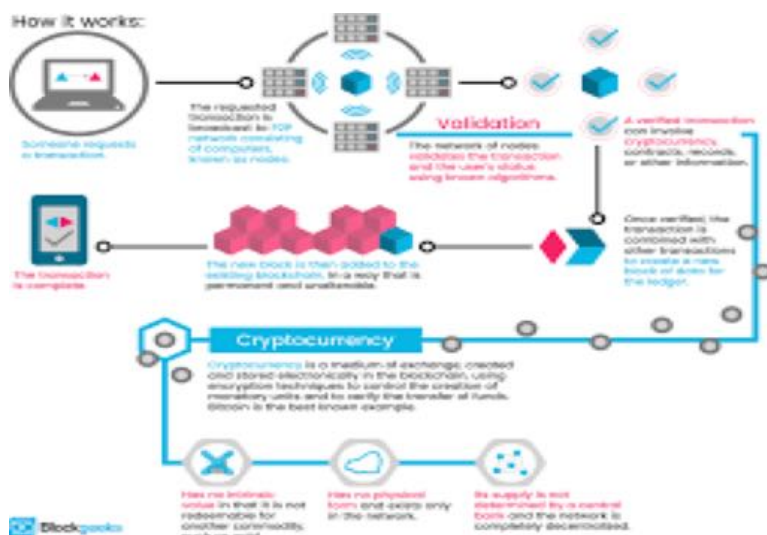
Cryptocurrencies have lower fees as compared to the other available currencies. There are no transaction costs for the cryptocurrency exchanges since the network usually does compensation. Payments using credit cards or even debit cards use up to 3% of the minimum charges when cryptocurrency use only 1% or even in some cases, it is done for free.

Problem

Satoshi Nakamoto's vision was the creation of a digital currency that would be anonymous, confidential and decentralized. This was applied to create the first cryptocurrency, Bitcoin. The original blockchain is barebones in comparison to modern blockchains, but it was specifically created for one purpose, to store wealth. No one can deny that Bitcoin has achieved this goal. At the moment, one Bitcoin is valued at around $4,000. However, experts realized that Blockchain technology could be used for more than just storing wealth.

This led to the development of altcoins that could offer features that the Bitcoin Blockchain did not have. Some of them include payment processing to allow for faster transactions while others

were pegged on fiat currencies and precious minerals. Unfortunately, in the process, the developers seem to have forgotten one of the key philosophies that Nakamoto had for cryptocurrencies, anonymity. He aimed to create a cryptocurrency that was truly anonymous giving clients the utmost confidentiality when they were making their transactions.

Most of the current Blockchain fail to allow the processing of payments for transactions or fail to keep the information away from prying eyes. As a result, the IRS and other institutions are attempting to get access to customer information from cryptocurrency exchanges. Already, the IRS Notice 2014-21 has been published requiring all owners to record cryptocurrencies as property, and the IRS has already started to look for the digital trails of those who do not want to comply with the notice. The court has already granted the IRS John Doe summons, meaning that it can start litigation against anyone they have sufficient information on in the industry. The American government is not alone. A lot of countries in Europe and Asia are trying to regulate the cryptocurrency industry.

This should be a cause for concern for any cryptocurrency investor. At this rate, some governments may get access to the transaction history since it is stored in the ledger. This is an inherent weakness that cannot be ignored. The basic structure the popular blockchain involves saving the transaction history while using pseudonyms to mask user details. However, if governments and other regulatory bodies can get access to cryptocurrency exchanges, they can get the pseudonyms and track the transactions made. This is a weak link that may negate one of the most endearing features of cryptocurrencies, the anonymity of the users. EthereumDark was concerned about this security gap and sought to make a more secure cryptocurrency.

Another issue is improving the speed of the transactions that are made. Bitcoin is the original cryptocurrency, and it is still used as the benchmark for many other alternative currencies. One defining feature of the Bitcoin cryptocurrency is the use of proof-of-work as the protocol used to complete transactions. In essence, this is based on dated technology that was developed more than a decade before Satoshi produced the whitepaper for the cryptocurrency. In specific, it was developed in 1993 at a time when the idea of cryptocurrencies had not been developed. The main problem is that it is specifically built for remittance transactions. This makes it ineffective when it comes to transactions that need to happen in seconds of minutes. However, this can be attributed to the nature of the blockchain source code. This is why Bitcoin and many other altcoins are not effective for payment processing.

Solution

Already, the cryptocurrency industry is under threat from governments and regulatory bodies that would wish to control it. This may potentially make cryptocurrencies lose their anonymity and become less decentralized. In the introduction, some parallels were drawn between the development of the internet and the development of the cryptocurrency industry. There was a time that the same institutions were pushing for greater control over the internet. Fortunately, the internet was able to evolve to the internet 2.0 making it more difficult to control while giving users greater freedom. The same revolution is required in the cryptocurrency industry.

Experts have put forward several different ways that blockchain technology can be enhanced. One way that this is by further embracing cryptography in the blockchain. At the moment, information is encrypted, but anyone on the network can view the transactions. Blockchains can go further to encrypt the transactions to provide a type of double blinding to the information provided. This will mean that the information on the blockchain is protected using pseudonyms and the transactions are inaccessible. Even if regulatory bodies got access to the pseudonyms,

they would be unable to ascertain the transactions made by using the pseudonym discovered.

This can only work when the blockchain is open-source.

Dash offered an intuitive solution to provide users the ability to perform transactions securely.

The masternode approach utilizes multiple servers integrated into the blockchain to allow for the

processing of transactions more securely than in the normal approach. There have to be

safeguards to ensure that the limited number of masternodes are not clogged by users trying to

make even minuscule transactions anonymous. Dash was able to stem this by requiring a

minimum amount of dash coins to be able to use the system.

Masternodes Made Easy

Low Cost Entry
Only 1000 ChainCoin required per masternode.

Masternode dashboard
Monitor your performance and earnings at a glance.

Start Earning
Receive payouts soon after your masternode is online.

Easy Setup
Setup scripts and community help will get you started.

The second problem highlighted is the inability of blockchains to provide payment processing options. This is probably the biggest roadblock to the mass adoption of cryptocurrencies. Bitcoin and other altcoins are based on the proof-of-work architecture that makes it difficult to process payments instantaneously. Instead, a shift to a proof-of-stake architecture may solve the problem. The proof-of-stake architecture relies on algorithms that allocate mining privileges based on the percentage of coins that the individual owns. As a result, miners with a greater number of coins in the blockchain area allowed to work on a similar percentage of the coins.

This eliminates the likelihood that the individual will invalidate any of the transactions. If the miner handles a higher percentage of the block transactions, they have a greater vested interest in the cryptocurrency deterring them from engaging in any nefarious reasons. Why would you perform an action that would jeopardize the value of a cryptocurrency when you have a vested interest in the currency. At the moment, Bitcoin, Litecoin, and other cryptocurrencies still use proof-of-work as their main architecture. The reason for this is that they are more concerned with value creation as opposed to a payment processing option. However, others like Peercoin have combined the two architectures in varying degree. Only NXT and Ethereum blockchains have shifted completely to proof-of-stake as the main architecture.
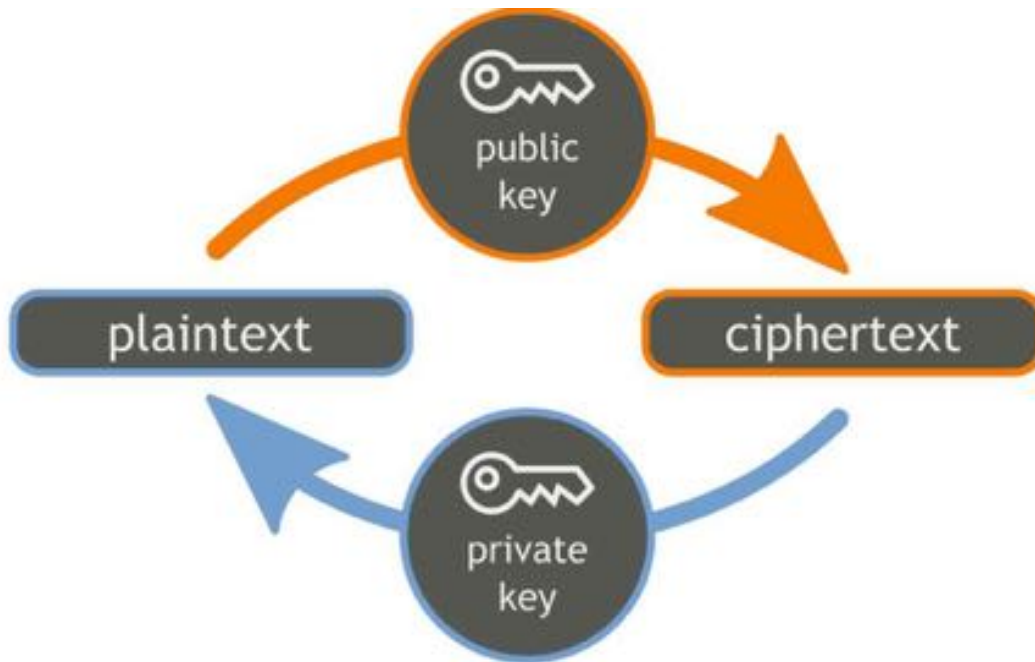
After adoption of the proof-of-stake, a blockchain will be able to use smart contracts or smart transactions. These are two technologies that rely on the same level of authentication to increase the speed of transactions. Smart contracts were developed by Nick Szabo in 1994 as a method of cryptographic self-executing contracts. Instead of relying on a centralized financial or legal body to authenticate the transactions, smart contracts are embedded on the computer nodes in a blockchain. In a sense, the smart contracts avoid using the services of a middleman by approving transactions once certain criteria have been met. This allows the transfer of money, goods, and anything of value in a conflict-free but the transparent way.
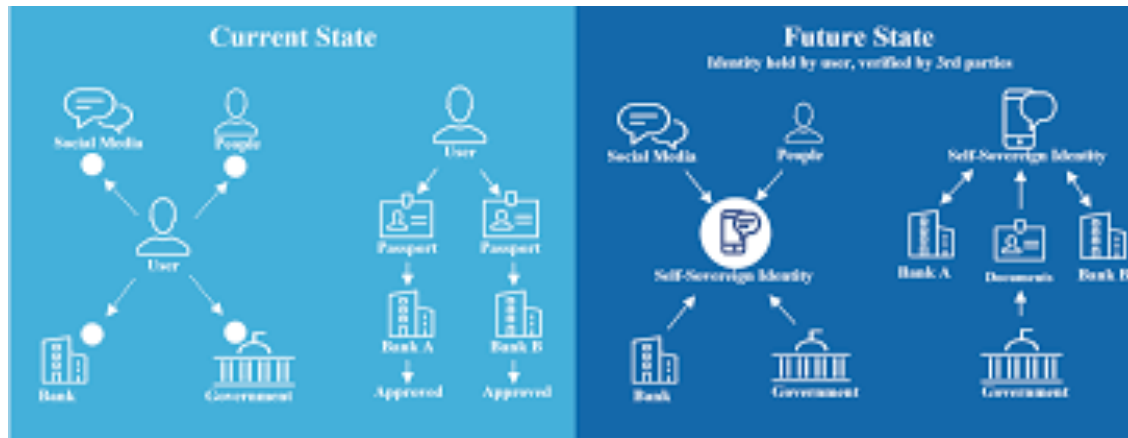
The ingenuity of the smart contracts is that it allows any transaction to be completed using a simple if-then algorithm to complete the transaction. An example would be someone who wishes to pay rent using cryptocurrencies. A virtual contract is created, and a digital key is created. This is linked with the recipient's public key creating the terms of the contract. When that time comes, the money is remitted, and then the recipient accepts the payments, and the entire transaction is recorded in the synchronized blockchain ledger. There are millions of parties that can authenticate that the transaction occurred minimizing the risk of fraud.

Finally, it is also important to use the right e-wallet and exchange to avoid falling victim to the prying eyes of regulators like the IRS or loss of money when these exchanges collapse. Exchanges are the only centralized organizations connecting cryptocurrencies to the financial sector. As a result, choosing the right exchange may protect your wealth. Exchanges have access not only to your e-wallet but also to your pseudonym. As a result, they are the target of multiple cyber-attacks as nefarious characters try to gain access to the cryptocurrencies of unsuspecting users.

Smart contracts – simple to complex

Digital value exchange	Smart right and obligation	Basic smart contract	Multiparty smart contract	Distributed autonomous business unit	Distributed autonomous organisation	Distributed autonomous government	Distributed autonomous society
A family member sends some bitcoin to another family member	Consumer buys a digital content stream	Landlord remotely locks nonpaying tenant out of apartment	Seller lends buyer funds to buy a house	User of a corporation issues its own bonds, and buyers monitor payments via a shared ledger	Self-driving trucks make P2P deliveries, pay local toll road fees, and buy local electricity	Settlers of a previously uninhabited area code their own self-enforcing government services	Groups of settlers from different areas establish self-enforcing trade agreements

Use case examples

Simple → Complex

The best way to progress blockchain technology would be to combine the different solutions to make the transfer of payments more effective while improving the security of the blockchain. If a blockchain or cryptocurrency can provide all or most of these features, it would be a lot more secure in the long run.

EthereumDark

What is EthereumDark?

EthereumDark is a cryptocurrency that provides its users with anonymity while facilitating fast payment processing. This is achieved by embracing smart contract encryption. Typically, smart contracts are not encrypted by in the Ethereum blockchain. However, EthereumDark offers users absolute anonymity using encrypted smart contract technology. This should not be confused with the Ethereum website. It is a completely independent token represented by the notation ETHD. ETHD will have different features like low fees and instantaneous transactions. These features endear the cryptocurrency to the users who still believe in the anonymity of their transactions.

What does EthereumDark offer?

EthereumDark has a simple strategy to provide everyone an equal opportunity to invest in the coin. Instead of using the common ICO approach, EthrereumDark will raise funds by simply releasing the coin to the market using the blockchain based on the Ethereum platform. The ETHD coins are easy to acquire because they run on the same exchanges that the ETH coins run on. It is easy for any investors to purchase EthereumDark tokens regardless of whether they are using fiat currencies or whether they are using cryptocurrencies. At the moment, the coin is in the first phase.

Once the sufficient number of coins have been distributed, a new coin will be introduced where individuals will be able to swap their old ETHD coins for the new ETHD coins at a rate of 2:1. At this point, the smart contract feature will be activated allowing the use of the ETHD tokens as a means of payment for goods and services. At this point, the value of the ETHD token will continue to appreciate as more people shift to the token as a means of making payments. The final phase involves the introduction of the anonymity feature. EthereumDark will already have the same confidentiality and anonymity features that all the other blockchains tend to have. However, the anonymity will be enhanced by allowing the encryption of the transactions using the smart contract feature introduced in the second phase.

This will make ETHD tokens the ideal cryptocurrency for markets that are somewhat considered risky or confidential. There are always industries that would benefit from a more confidential payment processing system. An example is the online casino industry where consumers prefer keeping their identities a secret. This is the true anonymity that cryptocurrencies were created for by early developers.

Technical aspects

EthereumDark Architecture

EthereumDark is based on a combination of the proof-of-work architecture and the proof-of-stake architecture. Even though the proof-of-stake algorithms are the predominant algorithms in the network, the proof-of-work algorithms allow the cryptocurrency to appreciate in value over time. There will be changes introduced into the blockchain in phases corresponding to the timeline. When the coins are first distributed, a simple e-wallet will be used to store the coins that investors purchase through the dedicated exchanges. This raises revenue for the official launch that will happen in phase two.

In the second phase, the functional blockchain will be launched with smart contract features integrated to allow the processing of payments and remittance of wealth. At this point, investors will be required to swap their old EthereumDark tokens for new ETHD tokens. The reason for this is to crowdfund the cryptocurrency. This is a slightly different take on crowdfunding. Instead of using an ICO, the tokens are initially distributed so that everyone has an opportunity to purchase the cryptocurrency. Thereafter, the initial tokens will be swapped for the usable ETHD tokens at the launch of phase two.

After the launch, EthereumDark will launch phase three where anonymity will be enhanced even in the transaction process. In particular, the technical process that will be used is the introduction of masternodes. Masternodes are servers connected to the blockchain network with limited functionality to allow perform limited tasks. In particular, the masternodes introduced on the EthereumDark blockchain will allow smart contract transactions to be conducted anonymously.

Knowledge of cryptocurrencies remains limited

Please describe the extent to which you are familiar with cryptocurrencies

83%

slightly familiar/not at all familiar

Source: 2015 PwC Consumer Cryptocurrency Survey.

6%

very familiar/ extremely familiar

Everyone will have access to the nodes allowing them to send and receive ETHD tokens anonymously. However, there are some restrictions placed to ensure that the masternodes are utilized effectively without bloating the network. The sender and the receiver will all require having at least 1000 ETHD. This amount does not have to be in the masternode, but it should be in an e-wallet that is transparent to everyone else in the network.

Any spending or moving of those coins will cause the masternode to stop working. In a sense, this will allow everyone to be their private financial regulator without relying on any regulatory organization. This will increase the appeal of the ETHD tokens to merchants and individuals who value their confidentiality and anonymity. The target is to ensure that there are around 50,000 masternodes in the system within one year after the third phase is launched.

EthereumDark supply and mining rewards

Whenever you are trying to launch a cryptocurrency, there is a need to balance the supply while rewarding miners for every new coin. If the supply is insufficient, the cost may deter investors from purchasing coins. However, if the supply is too much, it may water down the value of the cryptocurrency. In order to avoid this, EthereumDark will be limited to 4.2 million ETHD coins. This number is adequate to ensure that there are enough coins in circulation. The initial supply in

the first phase will be 2,940,000 coins. After swapping this will be slightly less than 1.5 million coins in supply. The rest of the coins will be held by the development team for gradual release to prevent a market crash.


Those who want to mine the coin will be able to do so based on the following proof-of-work and proof-of-stake difficulty. The proof-of-work difficulty will be 0.05650192 while the proof-of-stake difficulty will be 0.00024414 based on the initial supply of 2,940,000 coins.

EthereumDark distributions

The release of the coins will be based on the following distribution. The three members of the development team will receive a total of 10 percent of the coins. This is 3.333 percent per person that can be released in future to prevent any form of market collapse. The marketing and public

relations departments will receive five percent to aid in their objectives while another five percent will be used as giveaways in the EthereumDark reward system.
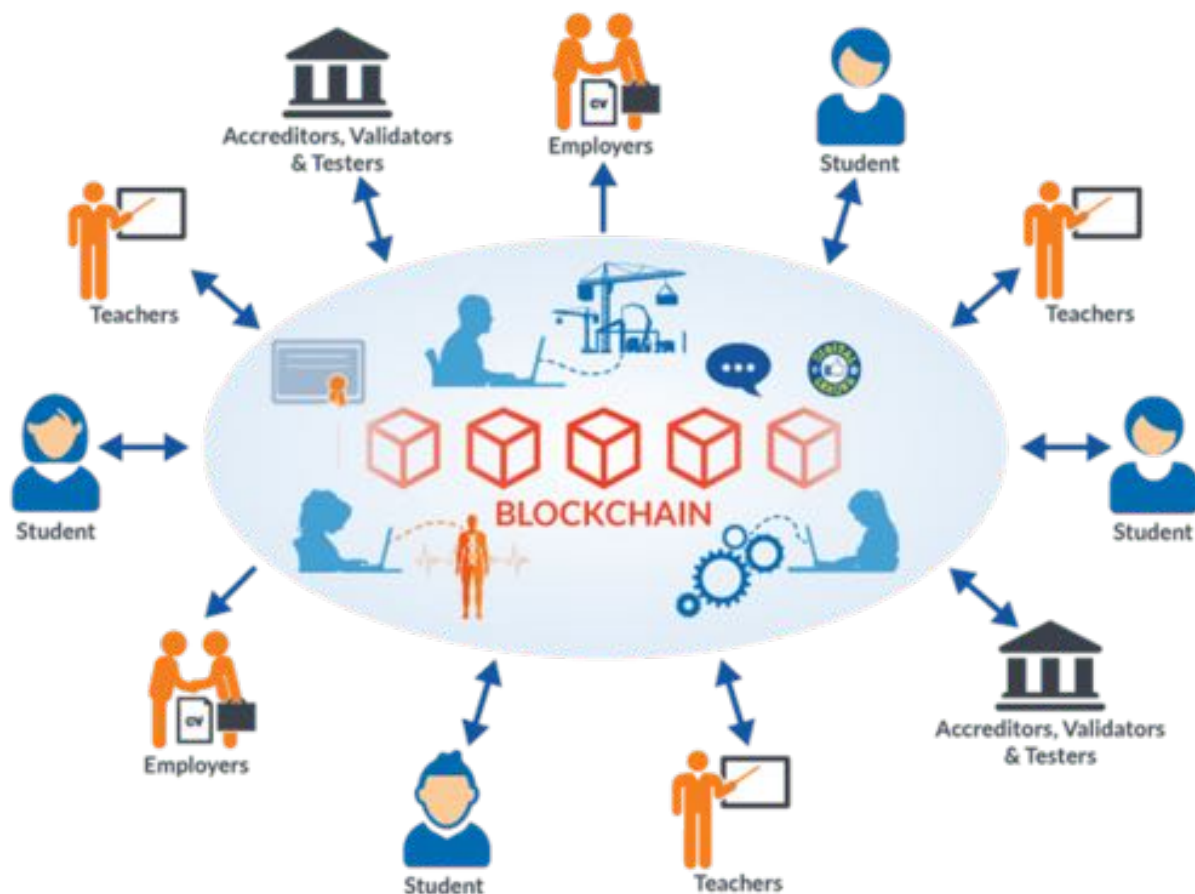
Getting listed on an exchange is another important milestone and EthereumDark has set aside five percent of the coins to be distributed to anyone who can get the coins registered in an exchange. This is one percent per exchange. An additional 10 percent of the coins will be set aside for bounties and airdrops. At the moment, the first two have already been done, but the date of the third and the fourth will be revealed soon to investors.

There will be five percent to be used to pay for developments in the different phases. These include the smart cards, merchant services, and online shopping payment platforms that will increase the payment processing capabilities of the coin. Similarly, 10 percent will be set aside for the development of the subsequent phases. These include e-wallet redesign, the introduction of masternodes and improvement of the cryptographic encryption in the blockchain. Five percent more of the income will be used in the maintaining the blockchain to ensure it runs smoothly without any hitches.

There will be ten percent set aside for translators and modulators who will be paid once a week until the coin supply allocated to them is over. Finally, there will be five percent set aside for the lottery program where four winners will receive 336 coins each week. The lottery program will last 156 weeks and act as a motivator for investors.

Distribution	Percentage
Development team	10
Marketing and public relations	5
Reward system giveaways	5
Incentive for listing on exchanges	5
Bounties and airdrops	10
Development of merchant service, shopping platform, and smart cards	5
Development of the architecture to include masternodes and redesigned e-wallets	10
Maintenance of the blockchain	5

Translators and modulators	10
Lottery program	5

Investor opportunities

Most cryptocurrencies raise money through ICO. However, this has been exploited by certain startups that only seek to raise funds without investing in any technology. The EthereumDark developers wanted to try a different approach that shows the seriousness to become more than just an altcoin that had an ICO. The approach chosen was a distribution of coins to everyone for a limited period before the official launch of the token.

In essence, two launches will occur. The first is for investors to acquire ETHD tokens and the second is the launch of the payment processing and smart contract aspects to the public. At this point, every two tokens will be swapped for a new ETHD coin that can be used for smart

contract transactions. As an investor, acquiring a significant quantity of ETHD coins before the appreciation happens will give you a chance to earn a handsome profit.

Furthermore, since the supply is capped at 4.2 million coins, there will a definite increase in the value. This gives you a chance to use ETHD coins as a long-term investment vehicle. Additionally, once the masternodes are developed, there will be a demand for coins so that users can meet the 1000 ETHD minimum required to use the masternode. The developers estimate a massive rise in the value as the demand will be more than the supply. Since only 10 percent will be held by the developers, the rest of the supply has to be met by early adopters.

Roadmap

When altcoins were developed, they aimed to provide additional features and services that were not available on the Bitcoin blockchain. The EthereumDark vision is to ensure that the users can get access to payment processing and remittance services while maintaining their confidentiality and security. As a result, the roadmap will keep evolving as more features keep being added into the blockchain. However, the current roadmap can be subdivided into three phases.

Phase one

This is the initial release of the coin to the market. This includes the initial e-wallet that features cross-platform compatibility, allowing users to purchase Ethereumdark coins using any

cryptocurrency or fiat currency. This phase also involves the bounty reward system that will be used to increase market awareness to the benefits that the EthereumDark blockchain offers clients. A subreddit has already been released allowing tech-savvy individuals to scrutinize the EthereumDark offering. Finally, a whitepaper will be created for investors who would like a more detailed review of the information.

Phase two

The second phase involves the release of the more effective e-wallet that will be used in swaping the initial EthereumDark coins for the new coins. The new wallet will be able to run on all iOS, Linux, Windows, and Android operating systems. Additionally, smart contracts will be integrated into the blockchain allowing for the full use of the coin in remittance, payment processing, and shopping. In this phase, some additional products may be developed including smart cards that allow the processing in specific online and offline stores. Finally, cross chain swapping will be developed to allow the easy exchange of different cryptocurrencies.

Phase three

This part involves the addition of masternodes on the blockchain network. These masternodes will be able to enhance security and anonymity of the user who meets the criteria to use them. With time, the number of masternodes will be increased to make it more effective. Additionally, more features will be added to the blockchain to make it more popular in the cryptocurrency industry. Some of these features include user-to-user anonymous transfers and online point-of-sale systems. The android application will be fully developed to help achieve these features.

Phase	Activity
Phase one	Initial distribution of the coin to the market

	The first cross-platform e-wallet is produced to facilitate access to ETHD coins
	Bounty reward system is implemented
	Subreddit is started
	Whitepaper is written
Phase two	Release of the advanced e-wallet
	Integration of smart contract functionality in the blockchain
	The ability to remit coins and process payments is opened to the public
	Swapping the initial coins with the new coins at a ratio of 2:1
	Cross chain swapping is introduced to the blockchain to increase liquidity
Phase three	Masternodes are introduced to the blockchain
	Customers can anonymously transfer payments to others on the blockchain
	Online point-of-sale systems are integrated into the blockchain

Conclusion

Blockchain technology was used to create the first cryptocurrencies that served as a disruption of the financial industry as constituted. The decentralized nature, security, and anonymity made them popular to users. However, governments and industry regulators have since started to push back. In 2014 the IRS published notice 2014-21 with the aim of controlling the industry. Since

then, it has made efforts to open litigation suits against exchanges that fail to give sensitive information of cryptocurrency users to it.

This is the first of many attempts all over the world to control the cryptocurrency market. As recently as September, China has closed down and started legal proceedings against one of the largest cryptocurrency exchanges in Asia. It is evident that more should be done in the cryptocurrency industry to protect users.

EthereumDark seeks to do this by introducing a more secure and anonymous method of making transactions. This is achieved using the masternode technology integrated with smart contract technology to provide anonymous but transparent in intra and inter blockchain transactions. This is done using a different approach from the normal ICO approach most altcoins prefer using. Instead, coins have been distributed allowing everyone an equal opportunity to profit from the cryptocurrency. In the next few months, the second phase will begin where users will be able to swap coins and e-wallets to activate the smart contract technology. The final phase will involve the introduction of masternodes to facilitate truly anonymous transactions in the EthereumDark network.