

## Project Final Report

---

**Project Title:** A Survey on Cryptocurrencies

**Name, Surname & ID of group members:**

Erdem Karataş

Yavuz Mehmet Oğuz Şimşek

Ege Bağırsakçı

**Supervised by:** Kamer Kaya

**Month, day, year:** 01/15/2021

## Abstract

Cryptocurrencies are basically digital currencies that aims to serve as alternatives to traditional currencies in order to provide untraceable network among users by using blockchain technology. Blockchain allows cryptocurrency system to be secured and provides a tradeable area. This protection comes from blocks of information including transactions details. Changes in a block, effects the others. Basically, it requires to exact values which outputs must be same and apply to previous blocks. The aim of the project is to conduct a survey on cryptocurrencies' technical details, current state, expectations in order to enlighten people who are interested in investing in specific cryptocurrencies and the ones who want to learn the underlying mechanism. The process of the research will begin by gathering and providing fundamental information about cryptocurrencies and how they work in general then include a report on Classic and Top Coins and DeFi: Derivative Coins. It is expected to provide guidance on potential investment opportunities.

## Introduction

The functionality of cryptocurrencies depends on a peer to peer ledger called blockchain. This ledger is open to everybody and accessible. Blockchain allows cryptocurrency system to be secured and tradable area. This protection comes from blocks of information including transactions details. To construct these blocks, some serious math problems needed to be solved which are almost impossible for human calculations. Since this chain accessible for everyone, people who called miners can construct new blocks by processing the data of transactions. Then because of chain structure, changes in a particular block effects the others due to the Hash function which takes input from previous block then provide an encryption for chain. Basically, it requires to exact values which outputs of the Hash function must be same and apply to previous blocks. Breaking this chain requires vast amount of calculation power so that It should overcome the power of the total and it is simply impossible for individuals. Users' trust on this process resulted from proof of work which is just one way for establishing common consensus

among users. Our goal is analyzing these features of specific coins which are top and DeFi: Derivative coins and reach a conclusion for answer the questions such as “Can cryptocurrencies keep its current functionality” and “Can it contribute to its holders?”.

### Methods & Materials

The research is conducted with the investigation of internet sources. All context related to cryptocurrencies were searched and defined. Then, top coins and DeFi derivatives separated from each other. Each individual coin was investigated in terms of its qualities, features and values. The data and information about coins gathered and written under the relevant coin heading. All the informations were interpreted and analyzed by researchers.

### Results

## WHAT IS CRYPTOCURRENCY

Cryptocurrency is a digital entity that is made for being an option to digital exchange wherein the records of the coin ownership stored in da computerized database using strong cryptography to secure the record of transactions, to control the creation of additional coins, and to approve the transfer of coin ownership (Greenberg, 2011). Jan Lansky stated that cryptocurrency is the system that involves six circumstances which are being decentralized, keeping records of overview of cryptocurrency units and their ownership, defining whether new cryptocurrency unit can be defined to the system, proving the ownership of the cryptocurrency units exclusively cryptographically, allowing transactions to be performed in which ownership of the cryptographic units is changed, and being able to perform the most one of the instructions when there are two different instructions for changing the ownership of the same cryptographic units which are simultaneously entered. (Lansky, 2018)

## ARCHITECTURE OF THE CRYPTOCURRENCIES

The first main keyword about cryptocurrencies is the architecture of them. Architecture of the cryptocurrencies meets with some concepts which are blockchain, timestamping, and mining. Blockchain is the method to prove the validity of each cryptocurrency’s coins. (Narayan, 2016) Blockchain is a growing list of records. These records are called blocks which are linked

and secured using cryptography. Each block has a hash pointer to link to the previous block. Blockchains are inherently immune resistant for modifications of the data as a result of the usage of peer-to-peer network which collectively adhering to a protocol for validating new block. Also, blockchain provides the anonymity of the cryptocurrencies. This anonymity protects people from the leakage its specific keys such as addresses and wallets. Furthermore, blockchains are open and distributed ledgers that can record transactions between two users in an effective and approvable way (Blockchains, 2015)

Timestamping in cryptocurrency is used for proving validity of transactions that added to the blockchain ledger without the need for a trusted third party.

Mining in cryptocurrency is an authentication of transactions and for this endeavour, successful miners earn new cryptocurrency as a reward. The reward of this effort shrinks with the transaction fees. The rate of producing hashes, which authenticate any transaction, has been increased by some machines such as FPGAs and ASICs process difficult hashing algorithms and script them. The reward that the system gives to miners differs by the reward method that cryptocurrencies use. One of the methods is proof-of-work. Proof-of-work is the method that as a result of computing some hash algorithms and finding blocks, the system gives a reward called “block reward”. The other method is proof-of-stake. In proof-of-stake based cryptocurrencies, the producer of the next block is chosen by the random selection and the wealth or age.

## **ECONOMY OF CRYPTOCURRENCIES**

The second main keyword about cryptocurrencies is the economy of them. The economy of the cryptocurrencies contains some concepts which are block rewards, transaction fees, exchanges, and atomic swap. In proof-of-work coins, block reward is the reward that miners get by creating a block (Polasik, 2015). On the other hand, in proof-of-stake coins, the miner that earns the block reward is splat by the wealth of the miners.

Transaction fees lean on the supply of network capacity at a certain time, versus the demand from the holder of the currency for rapid transaction. The holder can choose a transaction fee between the highest offered fee to lowest offered fee. For Ethereum, the transaction fee differs by the complexity of the calculation, usage of bandwidth, and the need of

storage (Scalability of the Bitcoin, 2018). For Bitcoin, the transaction fee differs by the size of the transaction and whether the transaction uses SegWit.

Exchanges are allowing the customers to exchange cryptocurrencies for the other entities such as real money, or trade with another cryptocurrency.

Atomic swap provides a mechanism that exchanges one cryptocurrency to another without the need of third party.

## **LEGALITY OF CRYPTOCURRENCIES**

The third main keyword about cryptocurrencies is the legality of them. The legality of the cryptocurrencies differs country to country. There is an “absolute ban” to cryptocurrency in eight countries: Algeria, Bolivia, Egypt, Iraq, Morocco, Nepal, Pakistan, and the United Arab Emirates. There is an “implicit ban” in fifteen countries: Iran, Kuwait, Lesotho, Lithuania, Macau, Oman, Qatar, Saudi Arabia and Taiwan (Regulation of Cryptocurrency Around the World, 2018). Different government departments, agencies, and courts have defined bitcoin differently. For example, in China, China Central Bank banned the usage of Bitcoin in China in 2014. Another example is in Russia, the handling of cryptocurrencies is legal but, the purchase with cryptocurrencies are illegal. Also, cryptocurrency advertisements are illegal in some special media platforms such as Facebook, Twitter, Bing, and LinkedIn (Thomas, 2018).

## **RECEPTION OF CRYPTOCURRENCIES**

The last main keyword about cryptocurrencies is the reception of them. One of the benefits that cryptocurrencies provide is being decentralized with advanced encryption techniques. Because of the decentralized structure of the cryptocurrencies, the governments have taken cautious steps through them as a result of the lack of the central control and the possible effects of the financial security. Regulators were warned against cryptocurrencies and have taken some moves to eloin users in some countries. Cryptocurrencies have been compared to Ponzi schemes, economic bubbles, and pyramid schemes which emphasize that cryptocurrencies are some scams or will be valueless in the long term. Now cryptocurrencies gaining value and prove that ideas wrong. (Paumgarten, 2018)

## **PROS AND CONS OF BLOCKCHAIN**

One of the pros that blockchain provides is the fact that it does not need any trusted third party. Because the structure of blockchain, third party is not necessary to confirm and conclude transactions. Also, as a result of the cancel of the third party, the transaction speed is faster than banks. Furthermore, the transaction fees are lower than banks because of the cancel of the third party. Other pro that blockchain provides is the transparency of the transactions and the security of the system. The decentralized structure of the blockchain provide the security and the transparency of the system.

One of the cons of the blockchain is the control issues of it. For example, when someone forgets their password of cryptocurrency wallets, since there is only one key for one user, the currencies in the wallet cannot be reachable unless the person remembers the password of it. Other con of the blockchain is the cyber-attacks. Blockchain is an online phenomenon, so it can be exposed to cyber-attacks. As a result of cyber-attacks, the transactions can be made involuntarily, and the order of the transactions can be changed. Another con of the blockchain is the operational problems. When a user is having a problem, there are no centralized corporation that user can consult. The last con of the blockchain is the energy efficiency. Blockchains are consuming a great amount of energy. The energy is so great that the energy consumption of blockchains are greater than some countries' energy consumption. (blockchain.com, 2020)

## **BITCOIN**

**Price:** \$33.607,19

**Market Cap:** \$616,041,449,195.42

**Volume:** \$85,783,657,663.42

**Circulating Supply:** 18.589.362 BTC

Bitcoin is a cryptocurrency that is founded in 2008 by a person who uses the name Satoshi Nakamoto (S., 2015). In 2009, the network of Bitcoin was created when Nakamoto mined the first block of the chain. The first coin transaction was received by Hal Finney who made the first reusable proof-of-work system in 2004. From 2009 to today, the growth of Bitcoin continues (Statement of Jeniffer Shasky Calvery, 2013).

Bitcoin uses blockchain which is a public ledger that records transactions as the structure of it (The great chain of being sure about things, 2015). Blockchain consists of blocks and each block contain a hash of the previous block to the first block. Also, blockchain provides the decentralization of the coin. Decentralization contributes the transparency and the security of the coin. Furthermore, it decreases the fees and fasten the transactions (Economist, 2015).

Bitcoin uses proof-of-work as the consensus mechanism. In proof-of-work works with the miner's computer processing power. The proof-of-work, miners need to find a number called "nonce", such that when the substance of the block is hashed along with the nonce, the result is numerically smaller than the difficulty target of network. This calculation is easy for any node in the network to verify, but also the calculation takes time to generate. Miners must try a lot of nonces to meet the difficulty target. In every 2,016 blocks, the difficulty target is determined based on the recent production of the network, with the purpose of keeping the average time between the produced blocks at ten minutes. As a result of this way, the system adapts to the total amount of mining power on the network (Antonopoluos, 2014).

The price of the Bitcoin does not stop growing. It is breaking records every day. The graphs of the growth of Bitcoin emphasizes that the growth of Bitcoin will not stop any time soon. It is a great investment that people can do right now.

## **BITCOIN CASH**

**Price:** \$387,68

**Market Cap:** \$7,331,431,424

**Volume:** \$7,101,707,154.43

**Circulating Supply:** 18.600.863 BCH

Bitcoin Cash is a cryptocurrency that has the same source code with Bitcoin, but independent from it. Bitcoin Cash is an altcoin of Bitcoin which is created in 2017. It is created with the two subsequent chain splits of Bitcoin (Shin, 2017).

Bitcoin has a limited block size that limits the transaction counts. Since Bitcoin spread all around the world, the users of it increase massively and people started to look for solutions for the transaction speed. Bitcoin Cash is created to increase the count of transactions per second. Bitcoin Cash solve this problem with its block size which is bigger than Bitcoin's. The consensus mechanism and the structure of the Bitcoin Cash is nearly same with Bitcoin. It uses proof-of-work system. Miner let the system to use their computer hardware to do calculations for the chain. If miner creates a block, it gets rewarded (Nakamura, 2017).

Bitcoin Cash differs with Bitcoin with some elements. One of them is the size of the blocks. The block size of Bitcoin is 1 mega-byte, but the block size of Bitcoin Cash is 8 mega-bytes. Other one of the differences is the security protocol of them. Bitcoin uses SegWit security protocol, but Bitcoin Cash removed this protocol, and this makes the transactions faster. Another difference between Bitcoin Cash and Bitcoin is the speed and price of them. Bitcoin Cash has a cheaper transaction fee and faster transaction speed than Bitcoin (Larson,2017).

The price of the Bitcoin Cash usually proportional with Bitcoin. Bitcoin breaking records and records in these days, so the rise of Bitcoin Cash would not stop till Bitcoin starts to be more stable. In conclusion, it is a profitable coin.

## **BITCOIN SV**

**Price:** \$171,05

**Market Cap:** \$3,193,266,477.01

**Volume:** \$706,549,598.38

**Circulating Supply:** 18.614.920 BSV

Bitcoin SV (Satoshi Vision) is a cryptocurrency that is created by the split of Bitcoin Cash. It split happened because of a conflict about two camps. One of the camps supported the software entitled Bitcoin ABC, which would make the block capacity 32 mega-bytes. The other camp supported the Bitcoin SV which would make the block size 128 mega-bytes (Kharif, 2018).



Bitcoin Cash was made from Bitcoin's blockchain and Bitcoin SV is one of the parts of the Bitcoin Cash. So, Bitcoin SV uses the chain system with Bitcoin. The consensus mechanism of Bitcoin SV is proof-of-work. Miners let chain to use the computer hardware to make computations and as a result of this computations, a block might be produced, and miner will be rewarded with the block reward.

Bitcoin SV is an investible coin. The graph of Bitcoin SV is proportional with Bitcoin's graph which is peaking. The growth is not as great as Bitcoin, but it is still growing. It may bring money in a long term.

### **Ether (ETH)**

**Price:** \$820

**Market Cap:** \$94,551,390,343

**Volume:** \$28,520,586,699

**Circulating Supply:** 114,097,828 ETH

Ether is the currency that is being used to incentivize the Ethereum Network but what exactly is Ethereum Network? In order to dive deep into Ethereum, some further information about how internet works is needed. Even today, the information submitted by users to most platforms are being saved in servers. Servers are basically online data storage units. Servers today may belong to companies like Google or directly operated by the platform that you submit your information. This structure of internet made servers act like banks and data like money. Just like how bitcoin happened to be a major step at decentralizing money the curiosity aroused if this is possible for internet.

Bitcoin scripts are not "Turing complete" (they don't enable loops) and could store very limited amount of information such as the transaction details "from whom" and "to whom" (Wright, 2016). This incapability of bitcoin network caused Ethereum network to be found. Users can create "smart contracts" using the programming language of Ethereum Network which is Solidity. Solidity is "Turing complete" which means it enables loops to write apps on Ethereum network and unlike bitcoin transactions, smart contracts can store more data to execute smart contracts.

Ethereum was initially proposed by Vitalik Buterin, a programmer and co-founder of Bitcoin Magazine, in late 2013 and brought to life by Vitalik Buterin and seven other programmers, according to Anthony Di Iorio – one of the founders, in 2014 as a platform for decentralized apps (dApps). When an app is deployed to the network, instead of servers many private computers (also called nodes) act as one supercomputer and make sure that the program runs as it was written.

One (arguably) downside of smart contracts was the “code is law” principle. Which means that the contracts used to be executed as they are written to the letter until the DAO event. Decentralized Autonomous Organization was a crowd sourced investment dApp on Ethereum network and drained due to vulnerabilities in the code. After the DAO event, Ethereum left the principle of “code is law” in order to prevent victimization and that’s where a disagreement occurred among users of network. The ones that continued to believe “code is law” principle continued their existence under Ethereum Classic network.

Ether is the cryptocurrency used in Ethereum network. Similar to bitcoin, miners are rewarded with Ether for adding blocks to blockchain in proof of work system. Ether is the only way transaction fees are accepted in Ethereum network which also goes to miners in order to incentive miners to adding new blocks to blockchain.

In today’s world users of internet are worried about their privacy and freedom. Examples: In the latest United States elections; Twitter and Facebook could filter out the information they did not want since they were in charge of most social media, the regulations come with DMCA are now started to be applied by big platforms like Twitch and Youtube. That is why Ethereum network can gain further attention and this can evaluate Ether.

### **Ripple (XRP)**

**Price:** \$0.23

**Market Cap:** \$10,119,629,740

**Volume:** \$5,011,269,920

**Circulating Supply:** 45,404,028,640 XRP

In today's world international wire transfers take long times and are costly. The reason behind this is; when transferring money between two banks that are not directly connected, your money travels through different banks and currency conversions might be needed, for example;  
Your money in TRY -> Bank A (Currency conversion from TRY to USD) -> Bank X -> Bank Y  
-> Bank Z -> Bank B (Currency conversion from USD to JPY) -> money transferred as JPY

This money transfer system is what ripple aims to change; the goal is to create the internet for values switching information to values (Takashima, 2018). What makes ripple different from others is; ripple is not against the existence of central authorities such as banks and wants to contribute to traditional system by lowering the transaction fees and time. Even ripple as initial idea is old; it was first stated by Ryan Fugger in 2004 and was called RipplePay. In 2012 it was co-founded by Chris Larsen and Jed McCaleb.

RippleNet is the network which consist computers around the world also known as validators, and just like HTTP of internet, RippleNet uses a protocol called RTXP (RippleNet Transaction Protocol). This network maintains the ledger of transactions and computers of the network validates every transaction according to RTXP protocol (Takashima, 2018).

There are two kinds of tokens that can be transferred using RippleNet and XRP is one of two. IOU's are basically the debts with the information of issuer and can be stored in RippleNet wallet. (IOU Example: USD.Nate(Issuer's Name)) IOU's are trust based since they are issued debts whereas XRP's are real assets.

As RippleNet aims faster international wire transfers XRP transactions are fast (1500 tx/sec while bitcoin is only 7 tx/sec and one transaction takes 4 seconds while it take 9 minutes in bitcoin), XRP's cannot be mined, the validator's duty is to validate the transaction; at least 80% of validators are needed to signal "valid" in order to a transaction to be executed. Initially 100 Billion XRP is pre mined and it is not possible to mine new XRP.

Initial distribution of XRP:

40 Billion XRP in Public hands (including 20 B to founders)

7 Billion to Ripple Labs

Remaining: 1B XRP to Ripple Labs each month.

Ripple Labs is the company that holds RTXP protocol.

Even XRP is claimed to be decentralized, the case of Ripple Labs holding the protocol rules is considered a doubt by users. In each transaction the transaction fees are burned which

decreases the total supply of XRP which results XRP price to go up when other factors are not considered. Also Ripple needs to make agreements with banks in order to be used.

As stated above, XRP's ideal is different; instead of preventing banks to operate money, it serves to banks and customers of banks. When XRP's growth examined it may seem proportional to total market cap of cryptocurrencies; if Bitcoin and most of the other assets reaches their goal of decentralization of money, Ripple is most likely to be eliminated. With this outcome; inversely proportional growth from XRP when compared to cryptocurrency market must not be expected, because XRP is still a crypto asset and if RippleNet ever survive in a cryptocurrency market crash, IOU's are more likely to be the way of transferring money in the network instead of XRP.

One other downside of XRP is validators. There is no reward for validating transactions, and this raises some problems. The first is; since there is no reward, there are not many validators; can cause 80% valid portion to be falsely exceeded and secondly; if there is no reward who is even participating in validation without profiting.

### **Litecoin (LTC)**

**Price:** \$150.23

**Market Cap:** \$10,134,142,348

**Volume:** \$14,016,480,848

**Circulating Supply:** 66,230,155 LTC

Litecoin is a peer to peer cryptocurrency initially released by Charlie Lee and works similar to Bitcoin. Charlie Lee's goal was to create a Bitcoin spinoff which will act as how silver to gold works, as stated by Charlie Lee when interviewed by Mike Green. Litecoin uses a different hashing algorithm called "scrypt" in its blockchain while bitcoin uses "SHA-256" to generate blocks. Even though generating block with "scrypt" requires more work Litecoin is faster than Bitcoin due to having a smaller blockchain. Litecoin transaction takes 2.5 minutes while bitcoin takes 9 minutes.

The consensus mechanisms behind both bitcoin and Litecoin is similar, proof of work. Miners are rewarded for generating new blocks to blockchain, yet Litecoin mining is more

profitable today due to the intense interest on bitcoin mining and Litecoin blockchain being smaller.

### **Binance Coin (BNB)**

**Price:** \$39.41

**Market Cap:** \$5,688,402,498

**Volume:** \$622,443,658

**Circulating Supply:** 144,406,561 BNB

Binance is a cryptocurrency exchange platform founded in 2017 by Changpeng Zhao and as of January 2018 they are the largest platform in terms of trading volume. Total supply cap of Binance Coin decided to be 200 million and 100 million BNB's were offered to public on initial coin offering days – 11 days before the platform went online (Martino et al., 2019).

Initially Binance coin started as an ERC-20 token running in Ethereum platform then ERC-20 BNB's swapped with BEP2 BNB's on a 1:1 ratio and left Ethereum platform to exist in Binance Chain (as stated by coinmarket.com).

Binance platform incentive usage of BNBs by offering lower fees in transactions from and to other assets.

After the initial decision of capping the total supply at 200 million, Binance now plans to decrease the market cap to 100 million. While the coin was a part of the Ethereum platform, Binance used smart contracts to burn 20% of the quarterly profit they made. After migrating to Binance chain they started using a specific function to burn 20% of their quarterly profit in order to cap supply at 100 million. The burning record is accessible at their website.

While Binance Coin doesn't reflect the idea behind most of the top coins; interest to cryptocurrency seems to be growing every other day and Binance is one of the easiest ways to trade in crypto market. Since Binance incentivize the usage of BNB, the price of it seems to follow the cryptocurrency market's trendline.

### **Synthetix Network Token (SNX)**

**Price:** \$8.31

**Market Cap:** \$917,918,329

**Volume:** \$101,561,112

**Circulating Supply:** 110,519,345 SNX

Synthetix Network is a decentralized finance platform on Ethereum Network founded by Kain Warwick. Before proceeding, further information about synthetic assets is needed.

Synthetic assets are the assets that are not real but pegged to a real asset and reflects the changes to the real asset synchronously (Ohorodnik, 2020). Synthetix network is the platform that you can invest on synthetic assets.

Synthetic assets on Synthetix Network:

Fiat synths (sUSD, sJPY, ...)

Crypto synths (sBTC, sETH, ...)

Commodity synths (sGold, sSilver, ...)

Stock synths (sTESLA, sAAPL, ...)

“s” at the front is used to indicate those are synths, there are also inverse synths. “i” at front is used to indicate inverse synths. Investing in any asset’s synth is like betting to the increase of that synth’s value in the environment of platform whereas investing in inverse synth’s is betting on devaluation of that asset. SNX is utility token of the Synthetix network. Users lock SNX to create synths.

Initial 100 million SNXs were issued in March 2018 and total supply is expected to be 250 million by 2024. Currently at 110 million.

SNX works in Proof of Stake mechanism. SNX stakers, who mint sUSD and back it up with 800% collateralization ratio, are rewarded with two kinds of rewards each week on Wednesdays (according to Andrew Trudel – employee of Synthetix Network).

- 0.3% Exchange Fee is distributed among stakers.
- SNX inflationary rewards.

Trading in Synthetix network is different compared to any trade platform consisting real assets after the point of buying SNX.

Trading in Synthetix Network

First step is buying SNX since it is the only currency accepted for creating synths in Synthetix Network. After this point things get a bit more complex because synths are not bought instead created.

Mint and Burn: after owning the enough amount of SNX in order to “mint” a specific synth, locking up the SNX to create synth is needed. Current collateralization ratio in the network is 7.5x which means in order to own 100 sUSDT in network, 750 sUSDT worth of SNX is needed to be locked up. At the moment 880 Million Dollars’ worth of SNX is locked up in the network. In order to leave the system, the inverse process of mint which is called burn is made. Burn is basically destroying the synth in order to free the locked SNX. Like entering and leaving the system, inside is also complex.

Consider there are only two people using the network; person A, person B.

Person A enters the system with 10 SNX worth of Gold. Person B enters the system with 10SNX worth of Silver. Total global debt is 20 SNX and each person owns 50%.

Silver doubles its price: Person B holds 20 SNX worth of Silver Person A still holds 10 SNX worth of Gold and new total global debt is 30 SNX. There is only 20 SNX in the system so system takes 5 SNX from each and adds to total global debt pool. When users decide to leave at this point person A leaves with 5 SNX and B with 15 SNX which caused B to lose money even the gold did not devalue compared to SNX. And that’s why locking up 7.5 times of enough SNX is needed while minting synths.

Even though trendline of SNX price follows the cryptocurrency market, SNX is a utility token used in Synthetix Network. However; buying SNX without even entering the Synthetix network can be considered due to the rewarding proof of stake mechanism.

## **AUCTUS (AUC)**

**Price:** \$0.1061

**Market Cap:** \$3,519,824

**Volume:** \$16,363

**Total- Circulating Supply:** 65,829,631- 31,260,935 AUC

([coinmarketcap.com/currencies/auctus/](https://coinmarketcap.com/currencies/auctus/))

Auctus is a decentralized platform built on Ethereum which allows users to trade and mint with call and put options without an obligation to rely on third parties.

ERC-20 Token

Secured by OpenZeppelin

**Developers:** Felix Hartmann, Vinicius Melo, Thiago Araujo, Ariny Guedes, Iuri Santos

### **DeFi Products of Auctus:**

#### **ACO Tokens (Auctus Crypto Options)**

Auctus has both Call and Put options for customers. Each option token is attached to a smart contract.

Each token consists of 4 elements:

- 1- Symbol of the underlying asset
- 2- Strike Price
- 3- Option Type
- 4- Expiration Time

Call Option Token:

ACO **ETH-200USDC-C-26JUN20-0800UTC** (Call Option Token Sample)

Above token indicates a call option which is able to transfer one ETH for 200 USDC.

Put Option Token:

ACO **ETH-160USDC-P-26JUN20-0800UTC** (Put Option Token Sample)

Above token indicates a put option which is able to transfer 160 USDC for one ETH.

Everyone who has one of the option tokens above can execute smart contract by giving USDC (call option) or giving ETH (put option) at the strike price before expiration date. These options makes token holders invulnerable to market changes by establishing a strike price (docs.auctus.org, 2018).

### **dPiggy:**

dPiggy is another project of Auctus for investors to invest without any loss. dPiggy platform has a basic, customer-friendly interface which takes a few input such as amount of DAI that will be invested and allocation of assets for investment. The platform automatically makes investment according to your choices to minimize the loss during investments.



**Advantageous:**

- Auctus platform fees are used to burn tokens, so that inflation will be prevented
- Simple interface platform that users can benefit easily
- Long term savings via call and put options

**Investment Advice:**

Auctus is still developing itself and creating new products. Platform started with retirement saving platform, but it transformed to a much bigger investment and long term saving platform. The team also prevents inflation by burning coins so it seems that AUC will not lose value soon. They also try to join different areas with different DeFi products such as dPiggy. Therefore, investment on Auctus may be a good idea for an investment since the team and platform still remaining their success and popularity.

**AUGUR (REP)**

**Price:** \$17.99

**Market Cap:** \$16,094,724

**Volume:** \$15,970,931

**Total - Circulating Supply:** 11,000,000 - 11,000,000 REP

([coinmarketcap.com/currencies/augur/](https://coinmarketcap.com/currencies/augur/))

Transparent exchange platform with no limits and no limited context, users can bet on everything and bet any amount that they desire.

ERC-20 Token

**Developers:** Forecast Foundation

**Mechanism:**

Augur Platform enables users to bet on everything with a simple interface.

Every market created by users follows the way:

- Market Creation
- Trading

- Report
- Settlement

**Market Creation:** A User who wants to create a bet can start by forming a market which includes bet context.

**Trading:** Any user can participate by buying shares of the current bet via smart contracts.

**Report:** Any user can report outcome of the context by staking REP. If the reporter's claim is parallel with consensus, reporter can take back the stake.

**Settlement:** After the report phase establishes the outcome regarding consensus among users, any user who has share can quit by either selling their share or getting assets equivalent to their share. When transactions occurred, it's called traders settled with market (origin.augur.net/whitepaper.pdf, 2019).

#### **Advantageous:**

- Augur has no limits on payouts, trades, deposits and withdrawals
- Low fees, approximately 1%, for operations
- Bets can depend on anything, not restricted to sports and politic as local bet markets do.
- Global market
- Platform getting no profit over bet markets

#### **Disadvantageous:**

- Although Augur is a fully decentralized platform, people beware due to bets that are not legal

#### **Investment Advice:**

Augur achieved an unseen success by establishing some kind of bets that nobody ever dare such as war bet, election bet. Augur is the only place for users who seek for these kind of bets. That's why it can be said that the platform will gain more popularity and attention from people. Yet, there is a risk that platform can be blamed as illegal by local governments or institutions although the platform guarantees user's privacy. It is suggested that even if you are going to invest on Augur, the amount of investment shouldn't be huge.

#### **MCDEX (MCB)**

**Price:** \$4.33

**Volume:** \$399,445

**Total Supply:** 50,263,002 MCB

([coinmarketcap.com/currencies/mcdex/](https://coinmarketcap.com/currencies/mcdex/))

The mission of MCDEX is to make investing in DeFi more accessible by creating a secure and easy-to-use blockchain-based decentralized financial platform.

ERC-20 Token

Secured by OpenZeppelin and ConsenSys

**Founder:** Liu Jie

### **MCDEX Platform**

Platform main product is its Decentralized Perpetual Contracts including three smart contracts which control funding, leverage and liquidity.

Platform enables users to trade up to 10x leverage with long and short positions controlled by smart contracts. For example, having a long position means that when prices are suitable to buy bitcoin, long positions holders have a right to borrow dollars from short positions. Conversely, if short positions holders are strong in market then they have a right to borrow bitcoin to buy dollars. According to which position is strong in the market, interest of that positions rises parallel to the price of dollars or bitcoins ([mcdex.io/references/#/en-US/white-paper](https://mcdex.io/references/#/en-US/white-paper)).

### **Advantageous:**

- Platform allows 10x leverage unlike current low leverage trading.
- Platform performs better trading system via its robo-trade system “AMM”

### **Disadvantageous:**

- Even though platform facilitate trading mechanism, it is not recommended for finance beginners.

### **Investment Advice:**

MCDEX has a great system for investors who seek leverage trading. MCDEX supports up to 10x leverage which means users get vast amount of profit. Also, MCDEX is not a cruel platform if you fail. Liquidation of your account does not occur rapidly, system gives a chance to user. However, if you are not an expert on economy, you may prefer not to get involved because you may lose much. Relatively to that, even though MCDEX is a great chance for investors, their target group is experts. MCB price may increase, but it would be a rapid and huge increase.

### **Numeraire (NMR)**

**Price:** \$26.54

**Market Cap:** \$127,602,798

**Volume:** \$10,535,355

**Total- Circulating Supply:** 11,000,000 - 4,465,650 NMR

([coinmarketcap.com/currencies/numeraire/](https://coinmarketcap.com/currencies/numeraire/))

Numerai proposes Numeraire, a new cryptographic token that can be used in a novel auction mechanism to make overfitting economically irrational.

ERC-20 Token

**Founder:** Richard Craib

### **Numerai**

Numerai is a platform for scientists to develop AI to solve various problems established by the platform. The competition keeps going according to an auction mechanism. Auction mechanism takes inputs “Stake” and “Confidence” from competitors. Then, each competitor listed according to s/c rate. Each machine learning mechanism are tested for current problem. If mechanism success on the problem depending on evaluation mechanism of  $\logloss^2$ , the competitor earns DAI equivalent to its s/c rate. The process keeps going until the prize pool depletion. After depletion no one can earn although their mechanism success (numer.ai/whitepaper.pdf, 2017).

**Advantageous:**

- Platform has a novel auction mechanism that never seen in CeFi projects
- Numerai has no rival currently so that it gains more popularity and interest

#### **Disadvantageous:**

- It is beneficial for only scientist and machine learning experts
- There could be participation problem if prize pool becomes very small resulting participants lose their interest.

#### **Investment Advice:**

Considering nowadays investment and developments on technology especially on AI technology, machine learning technology and things that related to this area are most likely to get more attention and interest by investors and users. Although it limited to only scientist and experts, soon, more people will get involved in this area. Investing on this kind of highly potential area may provide huge profit for investors.

### **NXT**

**Price:** \$0,01099

**Market Cap:** \$10,985,661

**Volume:** \$563,704

**Circulating Supply:** 998.999.942 NXT

NXT is an open-source, decentralized cryptocurrency that was created in 2013 by an anonymous developer called BCNext. It created with a total of 1 million coins. NXT uses proof-of-stake as its consensus mechanism. The developer asked for bitcoin donations to determine the distribution of the initial stake. BCNext announced that an altcoin which called “Ignis” will be created and the people who buy two NXT coin will be rewarded with one Ignis coin. This increased the sales of the NXT and when Ignis came out, the value of NXT be stable.

NXT applies a new feature called “Transparent Fogging” which will allow NXT to approach the common payment systems’ rate of transactions. The transaction rate is high because of the transparency that NXT provides in the protocol will let each user’s client to determine which node will be generated the next block. Security mechanism is another aspect that Transparent

Fogging provides. This mechanism prevents forked chains from being forked by high-stake nodes (nsxcrypto.org, 2014).

NXT uses proof-of-stake as its consensus mechanism. Block generation with their transaction fees are completed for proportional to all active wallets based on the amount of NXT a wallet has. So, if a wallet has 1 million NXT in their wallet, they have one in a thousand chance of creating a new block and receiving any transaction fees in that block. So instead buying equipment for mining, buy NXT to create more NXT (nsxcrypto.org, 2014).

NXT as an investment is not a great idea. The graph of NXT's price and volume, the money that circulating in this cryptocurrency is depleting. The graph of the price is stable, so money cannot be earned from this coin (nsxcrypto.org, 2014).

## References

Auctus: Getting Started. Auctus. Retrieved on December 30, 2020, from  
<https://docs.auctus.org/>

*Blockchain Advantages and Disadvantages*. (2020, October 21). Binance Academy.  
<https://academy.binance.com/en/articles/positives-and-negatives-of-blockchain>

Blockchains: The great chain of being sure about things (2015). *The Economist*.

Coinmarketcap. "Coins". Retrieved on December 30, 2020, from  
<https://coinmarketcap.com/coins/>

Craib, R., Bradway, G. Xander, D. & Joey, K. (2017). Numeraire: A Cryptographic Token for Coordinating Machine Intelligence and Preventing Overfitting.

Finance Subcommittee on Economic Policy (2013). *fincen.gov*. Financial Crimes Enforcement Network.

Greenberg, A. (2011). Crypto Currency. *Forbes*.

Jie, L. MCDEX: DeFi Platform for Trading Perpetuals. Retrieved on December 30, 2020, from <https://mcdex.io/references/#/en-US/white-paper>

Kelly, Jemima (2018). Bitcoin cash is expanding into the void. *Financial Times*.

Kharif, Olga (17 November 2018). Bitcoin Cash Clash Is Costing Billions With No End in Sight. Bloomberg.

Lansky, Jan (2018). Possible State Approaches to Cryptocurrencies. *Journal of Systems Integration*. 9/1: 19– 31. doi:10.20470/jsi.v9i1.335.

Larson, Selena (2017). Bitcoin split in two, here's what that means. *CNN Tech*. Cable News Network.

Martino, P., Wang, K. J., Bellavitis, C., & DaSilva, C. M. (2019). An introduction to blockchain, cryptocurrency and initial coin offerings. *New Frontiers in Entrepreneurial Finance Research*, 181-206.  
[https://doi.org/10.1142/9789811202766\\_0007](https://doi.org/10.1142/9789811202766_0007)

Nakamura, Yuri; Kharif, Olga (4 December 2017). Battle for 'True' Bitcoin Is Just Getting Started. *Bloomberg Businessweek*.

Narayanan, Arvind; Bonneau, Joseph; Felten, Edward; Miller, Andrew; Goldfeder, Steven (2016). Bitcoin and cryptocurrency technologies: a comprehensive introduction. *Princeton: Princeton University Press*. ISBN 978-0-691-17169-2.

Ohorodnik, V. (2020, September 25). *Synthetic assets: Learn why they are necessary and how to use them*. BTC-Alpha. <https://btc-alpha.com/en/stories/what-are-synthetic-assets-and-how-do-they-work>

Paumgarten, Nick (2018). The Prophets of Cryptocurrency Survey the Boom and Bust. *www.newyorker.com*. The New Yorker.

Polasik, M., Piotrowska, A. I., Wisniewski, T. P., Kotkowski, R., & Lightfoot, G. (2015). Price fluctuations and the use of bitcoin: An empirical inquiry. *International Journal of Electronic Commerce*, 20(1), 9-49. Bitcoin's Legality Around The World Archived 16 September 2017 at the Wayback Machine, Forbes.

Polgar, David. Cryptocurrency is a giant multi-level marketing scheme. *Quartz*. Quartz Media LLC. Archived from the original on 1 March 2018.

Peterson, J., Krug, J. Micah, Z. Austin, K. Williams, A. & Stephanie, A. (2019). Augur: a Decentralized Oracle and Prediction Market Platform (v2.0). Forecast Foundation.

Regulation of Cryptocurrency Around the World (2018). Library of Congress. *The Law Library of Congress, Global Legal Research Center*. pp. 4–5.

S., L. (2015). Who is Satoshi Nakamoto?. *The Economist*. The Economist Newspaper Limited. Archived from the original on 21 August 2016.

Scalability of the Bitcoin and Nano protocols: a comparative analysis (2018), *Blekinge Institute of Technology*

Schwartzkopff, Frances (2013). Bitcoins Spark Regulatory Crackdown as Denmark Drafts Rules. *Bloomberg*.

Shin, Laura (2017). "Will This Battle For The Soul Of Bitcoin Destroy It?". *Forbes*.

Statement of Jennifer Shasky Calvery, Director Financial Crimes Enforcement Network United States Department of the Treasury Before the United States Senate Committee on Banking, Housing and Urban Affairs Subcommittee on National Security and



International Trade and Finance Subcommittee on Economic Policy. (2013). *fincen.gov*.  
Financial Crimes Enforcement Network.

Takashima, I. (2018). *Ripple: The ultimate guide to the world of ripple Xrp, ripple investing, ripple coin, ripple cryptocurrency, cryptocurrency*. Createspace Independent Publishing Platform.

The great chain of being sure about things (2015). *The Economist*. The Economist Newspaper Limited.

Wilson, Thomas (2018). Twitter and LinkedIn ban cryptocurrency adverts – leaving regulators behind. *Independent*. Reuters.

Wright, C. S. (2016). Turing complete bitcoin script white paper. *SSRN Electronic Journal*,  
1. <https://doi.org/10.2139/ssrn.3160279>