Vladislav Savsyuk, Student
Supervisor - Pantileienko K.S., Lecturer
Dnipropetrovsk National University of Railway Transport
named after Academician V. Lazarian

MODERN VIEW ON CRYPTOCURRENCY

A cryptocurrency (or crypto currency) is a digital asset designed to work as a medium of exchange that uses cryptography to secure its transactions, to control the creation of additional units, and to verify the transfer of assets. Cryptocurrencies are a type of digital currencies, alternative currencies and virtual currencies. Cryptocurrencies use decentralized control as opposed to centralized electronic money and central banking systems. The decentralized control of each cryptocurrency works through a block chain, which is a public transaction database, functioning as a distributed ledger.

Bitcoin, created in 2009, was the first decentralized cryptocurrency. Since then, numerous other cryptocurrencies have been created. Theyare frequently called altcoins, as a blend of alternative coin.

Overview

Decentralized cryptocurrency is produced by the entire cryptocurrency system collectively, at a rate which is defined when the system is created and which is publicly known. In centralized banking and economic systems such as the Federal Reserve System, corporate boards or governments control the supply of currency by printing units of fiat money or demanding additions to digital banking ledgers. In case of decentralized cryptocurrency, companies or governments cannot produce new units, and have not so far provided backing for other firms, banks or corporate entities which hold asset value measured in it. The underlying technical system upon which decentralized cryptocurrencies are based was created by the group or individual known as Satoshi Nakamoto.

As of September 2017, over a thousand cryptocurrency specifications exist; most are similar to and derive from the first fully implemented decentralized cryptocurrency, bitcoin. Within cryptocurrency systems the safety, integrity and balance of ledgers is maintained by a community of mutually distrustful parties referred to as miners: members of the general public using their computers to help validate and timestamp transactions, adding them to the ledger in accordance with a particular timestamping scheme. Miners have a financial incentive to maintain the security of a cryptocurrency ledger.

Most cryptocurrencies are designed to gradually decrease production of currency, placing an ultimate cap on the total amount of currency that will ever be in circulation, mimicking precious metals. Compared with ordinary currencies held by financial institutions or kept as cash on hand, cryptocurrencies can be more difficult for seizure by law enforcement.[1] This difficulty is derived from leveraging cryptographic technologies.

Architecture

Blockchain

The validity of each cryptocurrency's coins is provided by a blockchain. A blockchain is a continuously growing list of records, called blocks, which are linked and secured using cryptography. Each block typically contains a hash pointer as a link to a previous block, a timestamp and transaction data. By design, blockchains are inherently resistant to modification of the data. It is "an open, distributed ledger that can record transactions between two parties efficiently and in a verifiable and permanent way". For use as a distributed ledger, a blockchain is typically managed by a peer-to-peer network collectively adhering to a protocol for validating new blocks. Once recorded, the data in any given block cannot be altered retroactively without the alteration of all subsequent blocks, which requires collusion of the network majority.

Blockchains are secure by design and are an example of a distributed computing system with high Byzantine fault tolerance. Decentralized consensus has therefore been achieved with a blockchain. It solves the double spending problem without the need of a trusted authority or central server.

The block time is the average time it takes for the network to generate one extra block in the blockchain. Some blockchains create a new block as frequently as every five seconds. By the time of block completion, the included data becomes verifiable. This is practically when the money transaction takes place, so a shorter block time means faster transactions.[citation needed]

Mining

In cryptocurrency networks, mining is a validation of transactions. For this effort, successful miners obtain new cryptocurrency as a reward. The reward decreases transaction fees by creating a complementary incentive to contribute to the processing power of the network. The rate of generating hashes, which validate any transaction, has been increased by the use of specialized machines such as FPGAs and ASICs running complex hashing algorithms like SHA-256 and Scrypt. This arms race for cheaper-yet-efficient machines has been on since the day the first cryptocurrency, bitcoin, was introduced in 2009. With more people venturing into the world of virtual currency, generating hashes for this validation has become far more complex over the years, with miners having to invest large sums of money on employing multiple high performance ASICs. Thus the value of the currency obtained for finding a hash often does not justify the amount of money spent on setting up the machines, the cooling facilities to overcome the enormous amount of heat they produce, and the electricity required to run them.

Some miners pool resources, sharing their processing power over a network to split the reward equally, according to the amount of work they contributed to the probability of finding a block. A "share" is awarded to members of the mining pool who present a valid partial proof-of-work.

One company is operating data centers for mining operations at Canadian oil and gas field sites, due to low gas prices.

Given the economic and environmental concerns associated with mining, various "minerless" cryptocurrencies are undergoing active development. Unlike conventional blockchains, some directed acyclic graph cryptocurrencies utilise a pay-it-forward system, whereby each account performs minimally heavy computations on two previous transactions to verify. Other cryptocurrencies like Nano utilise a block-lattice structure whereby each individual account has its own blockchain. With each account controlling its own transactions, no traditional proof-of-work mining is required, allowing for feeless, instantaneous transactions.

As of February 2018, the Chinese Government halted trading of virtual currency, banned initial coin offerings and shut down mining. Some Chinese miners have since relocated to Canada. According to a February 2018 report from Fortune, Iceland has become a haven for cryptocurrency miners in part because of its cheap electricity. Prices are contained because nearly all of the country's energy comes from renewable sources, prompting more mining companies to consider opening operations in Iceland. However, the cryptocurrency mania might have gone a little too far in Iceland. The region's energy company says bitcoin mining is becoming so popular that the country will likely use more electricity to mine coins than power homes in 2018.

In March 2018, a town in Upstate New York put an 18 month moratorium on all cryptocurrency mining in an effort to preserve natural resources and the "character and direction" of the city.

Wallets

A cryptocurrency wallet stores the public and private "keys" or "addresses" which can be used to receive or spend the cryptocurrency. With the private key, it is possible to write in the public ledger, effectively spending the associated cryptocurrency. With the public key, it is possible for others to send currency to the wallet.

Ton

Telegram creators Pavel and Nikolai Durov have filed a "Notice of Exempt Offering of Securities" with the US Securities and Exchange Commission (SEC) Feb. 13, reporting $850 mln raised under the SEC exemption Rule 506(c) from 81 investors for "the development of the TON Blockchain, the development and maintenance of Telegram Messenger."

The type of securities offered in the SEC filing are described as "Purchase Agreements for Cryptocurrency", and are filed under the Rule 506(c) exemption that means that US citizens who invest must be accredited investors — those worth more than $1 mln or that have an annual income of $200,000 — in order for the tokens to not have to be registered with the SEC as securities.

The Eastman Kodak Company, which had announced the launch of their own ICO under the same exemption in early January, 2018, has postponed their ICO to take more time to verify their investors' accredited status.

The date of the first sale for the Durovs' ICO is noted as Jan. 29 of this year. By filing with the SEC, the Durovs are preparing to allow for US citizens to legally invest in their project, and implying that US citizens may in fact be some of the 81 investors.

Although the SEC filing did not contain the names of any investors in the Durov's securities offering, Russian news outlet Vedomosti revealed today the names of some of the largest alleged investors, citing inside sources.

Russian billionaire Roman Abramovich, who purportedly has already invested in cryptocurrencies, reportedly was one of the first Russian citizens to be approved to invest in the project. One source allegedly close to the billionaire told Vedomosti that Abramovich had invested as much as $300 mln, however another source claimed the sum was closer to $20 mln.

Sergei Solonin, CEO of Russian payment service provider QIWI, invested $17 mln, Vedomosti writes. David Yakobashvili, co-founder of Russian-based dairy product company Wimm-Bill-Dann, told the publication that invested $10 mln in the project.

At the moment, the government of Russian federation plans to block the crypto currency of Pavel Durov, referring to terrorism

Reference:

1. https://en.wikipedia.org/wiki/Cryptocurrency

2. https://cointelegraph.com/news/durov-brothers-file-telegram-and-ton-with-sec-report-850-million-already-raised

3. https://t.me/Blockchain_TON