Security analysis of cryptocurrency and blockchain

Engineering, Computer Security

Abstract

The major intention of this paper is to discuss about the role of cybersecurity in the field of cryptocurrency, figure out the current threats and vulnerabilities, and the countermeasures to minimize the cyberattacks on them. There is a plethora of cybercrimes happening in the field of cryptocurrencies like Coincheck, Parity, Bitfinex, NiceHash, FacexWorm and CoinDash. In this paper we have provided a detailed description of blockchain security measures of different cryptocurrency and their future scope.

Introduction

Cryptocurrency is a virtual or digital currency. It has value like money and can be lent, exchanged or borrowed but it doesn’t have a physical presence. Currencies are value deposits that we can use to buy goods or services and most cryptocurrencies cannot be exchanged for anything other than a cryptocurrency. This currency is not handled by banks or some central authority. The transactions get recorded in a digital public ledger called blockchain. It ensures the transactions occur without any interference. The first crypto currency introduced was Bitcoin, in October 2008. This is believed to be done by a person (or a group of people) called Satoshi Nakamoto. Many other crypto currencies were launched following the success of bitcoin. There are more than around 1300 crypto currencies present today. All these currencies work using the block chain technology.

Blockchain

Blockchain is a group of blocks where each block signifies a transaction or record of exchange. It is a decentralized, distributed database that maintains a list of transactions. Each block consists of various valid transactions which are hashed and added to the list. Each transaction includes a timestamp and a link to the previous transaction. Hence, if someone tries to modify a record, a new hash will be produced even if a small change is made as it will not contain the information of the previous records. This method confirms the integrity of the previous block and all the way back to the original one: [1]. A transaction requires two things: a wallet and a private key. A wallet is assigned to an individual, which is basically an address to uniquely identify a user. And this address is public, whereas the private key (i. e. , a string of random numbers) must be kept a secret. Once the transaction is requested, it is broadcast to the blockchain network where it will be verified. After verification and validation, this transaction is added as a block and no changes can be made after that: [2]. What makes this system theoretically tamper proof is the cryptographic fingerprint unique to each block, and a “ consensus protocol,” by which the nodes in the network agree on a shared history. The fingerprint i. e. , the hash, takes a lot of computing time and energy to generate initially. It serves as a seal, since altering the block would require generating a new hash. Then whether or not the hash matches its block is verified and after that, the nodes update their respective copies of the blockchain with the new block: [3]. These hashes also serve as links in the blockchain. The major goal of a hash is to convert data of any size in to a string of a fixed size taking an arbitrary amount of input data applying some

algorithm and engenders finite amount output. Each block comprises the previous block’s distinctive hash. In case if user want to modify an entry in the ledger retroactively, user must manipulate a new hash not only for the block it’s in but also for every subsequent block. and user have to do this rapidly than the other nodes can add new blocks to the chain. If user have computers that are more significant than the rest of the nodes combined, any blocks one adds will have contention with existing ones, and the other nodes will spontaneously reject the changes. This is what makes the blockchain tamper proof, or “ immutable. ”

1. Guardtime detects and mitigates cyberattacks in real-timeGuardtime, founded by Estonian cryptographer Ahto Buldas, is a date security company started in 2007. The company has created Keyless Signature Infrastructure (KSI), using blockchain which is a replacement for the more traditional Public Key Infrastructure (PKI). It uses asymmetric encryption and a cache of public keys maintained by a centralized Certificate Authority (CA). Guardtime is now the world’ largest blockchain company. In 2016 the company achieved an incredible milestone as it successfully secured all of Estonia’s 1 million health records using its technology.
2. REMME is making passwords obsoleteWith REMME’s blockchain, the authentication of system and user are done without any password. Because it removes the human factor from the authentication process, it prevents from becoming a potential attack. Alex Momot, founder and CEO of REMME, said that the use of simple logins and a centralized architecture are a big weakness of traditional systems. “ No matter

how much money a company spends on security, all these efforts are in vain, if customers and employees use easy passwords which can be easily cracked or stolen. Block chain takes the responsibility for strong authentication, resolving the single point of attack at the same time. In addition, the decentralized network helps us to provide agreement between parties for their identification. ” REMME used a distributed public key infrastructure to authenticate users and devices. Instead of a password, it gives each device a specific SSL certificate. The certificate data is managed on the Block chain, which makes it virtually impossible for malicious hackers to use fake certificates. The platform uses two-factor authentication for enhancement of the security.

3. Obsidian ensures the privacy and security of chatsObsidian uses the block chain de-centralized network, which cannot be censored or controlled by any single source. In addition, communications meta-data is scattered throughout the distributed ledger and cannot be gathered at one central point, reducing the risk through such digital fingerprints. Users need not to link to their email addresses or telephone numbers, thereby increasing privacy.

Future Of Cryptocurrency

The risks of fraud and theft has prompted governments to regulate cryptocurrency completely out of existence. South Korea and India have signaled their willingness to outlaw crypto exchanges. Some EU countries have started following strict regulation or blacklisting of crypto markets. Even the EU’s upcoming data privacy regulation, the Global Data Protection Regulation (GDPR), may be incompatible with blockchain’s decentralized

structure. China has interestingly fasten down harshly on cryptocurrency and its markets while still indicating its support for blockchain technology. The following three could be the future of cryptocurrency: [9]A. Security Tokens: Security tokens are crypto tokens issued to investors in a sale or ICO for the exchange of their money. Security tokens pays dividends, share profits, pays interest or invests in other tokens or assets to generate profits for the token holders. B. Air Gapped Networks: This is the process of keeping the devices that have wallets and cryptocurrencies details disconnected from the internet. Also called as cold storage, this network is about the safest way to keep your cryptocurrency tokens safe and secure from security breaches. C. Polymath Networks: Polymath network and its idea of creating a security token platform where an individual can hold its token sale for investors are far too unique. The company behind Polymath network is Saint George Barbados-based Software Company which was founded back in 2017. Polymath is the only crypto project which is aiming to create a link between securities and blockchain so as to keep the investments of a crypto trader safe and promote crypto trading by enhancing its security and lowering the risk.

Conclusions

The whole point of using a blockchain is to let people—in particular, people who don’t trust one another—share valuable data in a secure, way. This is possible because blockchains store data using sophisticated math and innovative software rules that are extremely difficult to be manipulated by attackers. But the security of even the best-designed blockchain systems can fail sometimes where the math and software rules come in contact with

humans, who are skilled cheaters, in the real world, where things can get messy. But the blockchain technology used by bitcoin is by far the most secure way of transferring or sharing digital currency.