**Blockchain Thecnology**

***Analysis of Cryptocurrencies***

Abstract:

Cryptocurrencies have emerged as important financial software systems. They rely on a secure distributed ledger data structure; mining is an integral part of such systems. Mining adds records of past transactions to the distributed ledger known as Blockchain, allowing users to reach secure, robust consensus for each transaction. Mining also introduces wealth in the form of new units of currency. Cryptocurrencies lack a central authority to mediate transactions because they were designed as peer-to-peer systems. They rely on miners to validate transactions. Cryptocurrencies require strong, secure mining algorithms. In this paper we survey and compare and contrast current mining techniques as used by major Cryptocurrencies. We evaluate the strengths, weaknesses, and possible threats to each mining strategy. Overall, a perspective on how Cryptocurrencies mine, where they have comparable performance and assurance, and where they have unique threats and strengths are outlined.

Introduction:

In 2008, an unknown computer programmer or group of programmers using the pseudonym ***Satoshi Nakamoto*** created a computer platform that would allow users to make valid transfers of digital representations of value. The system, called ***Bitcoin,*** is the first known Cryptocurrency. A blockchain is a public ledger to which everyone has to access but without a central authority having a control , it is an enabling technology for individuals and companies to collaborate with trust and transparency. One of the best known applications of blockchains are the cryptographic currencies such as bitcoins , others and many other applications are possible. Cryptocurrency is a digital payment system , it has some popular bitcoins . Bitcoins are generally stored in digital wallets. Nowadays there are lots of applications to buy bitcoins. Mining process is required for getting new and transacting bitcoins which Is done by bitcoin miners. The availability of bitcoins in the entire world is only 21 million. Cryptocurrencies can only stored as digital assets.

Blockchain technology :

What is blockchain ?

**A blockchain is a public ledger to which everyone has to access but without a central authority having a control , it is an enabling technology for individuals and companies to collaborate with trust and transparency. One of the best known applications of blockchains are the cryptographic currencies such as bitcoins , others and many other applications are possible. Cryptocurrency is a digital payment system , it has some popular bitcoins . Bitcoins are generally stored in digital wallets. Nowadays there are lots of applications to buy bitcoins. Mining process**

**How does blockchain works ?**

**Blockchain works via a multistep process, which in simple terms happens as follows: An authorized participant inputs a transaction, which must be authenticated by the technology. That action creates a block that represents that specific transaction or data. The block is sent to every computer node in the network.**

**Blockchain usecase:**

**i] International payments**

**ii] Capital markets**

**iii] Trade finance**

**iv] Regulatory compliancs and audit**

**v] Insurance**

**vi] peer- to-peer transactions**

**vii] Supply chain management**

**Cryptocurrency :**

**Mining is the process that maintains the bitcoin network and also how new coins are brought into existence.**

**All transactions are publicly broadcast on the network and miners bundle large collections of transactions together into blocks by completing a cryptographic calculation that’s extremely hard to generate but very easy to verify. The first miner to solve the next block broadcasts it to the network and if proven correct is added to the blockchain. That miner is then rewarded with an amount of newly created bitcoin.**

**Inherent in the bitcoin software is a hard limit of 21 million coins. There will never be more than that in existence. The total number of coins will be in circulation by 2140. Roughly every four years the software makes it twice as hard to mine bitcoin by reducing the size of the rewards.**

**When bitcoin was first launched it was possible to almost instantaneously mine a coin using even a basic computer. Now it requires rooms full of powerful equipment, often high-end graphics cards that are adept at crunching through the calculations, which when combined with a volatile bitcoin price can sometimes make mining more expensive than it is worth.**

**Miners also choose which transactions to bundle into a block, so fees of a varying amount are added by the sender as an incentive. Once all coins have been mined, these fees will continue as an incentive for mining to continue. This is needed as it provides the infrastructure of the Bitcoin network.**

**Bitcoins :**

**Bitcoin is a digital currency which operates free of any central control or the oversight of banks or governments. Instead it relies on peer-to-peer software and cryptography.**

**Purpose of bitcoins :**

**Bitcoin was created as a way for people to send money over the internet. The digital currency was intended to provide an alternative payment system that would operate free of central control but otherwise be used just like traditional currencies.**

**Bitcoin mining :**

**Mining is the process that maintains the bitcoin network and also how new coins are brought into existence.**

**All transactions are publicly broadcast on the network and miners bundle large collections of transactions together into blocks by completing a cryptographic calculation that’s extremely hard to generate but very easy to verify. The first miner to solve the next block broadcasts it to the network and if proven correct is added to the blockchain. That miner is then rewarded with an amount of newly created bitcoin.**

**Inherent in the bitcoin software is a hard limit of 21 million coins. There will never be more than that in existence. The total number of coins will be in circulation by 2140. Roughly every four years the software makes it twice as hard to mine bitcoin by reducing the size of the rewards.**

**When bitcoin was first launched it was possible to almost instantaneously mine a coin using even a basic computer. Now it requires rooms full of powerful equipment, often high-end graphics cards that are adept at crunching through the calculations, which when combined with a volatile bitcoin price can sometimes make mining more expensive than it is worth.**

**Miners also choose which transactions to bundle into a block, so fees of a varying amount are added by the sender as an incentive. Once all coins have been mined, these fees will continue as an incentive for mining to continue. This is needed as it provides the infrastructure of the Bitcoin network.**

**Merits :**

**Cryptocurrencies represent a new, decentralized paradigm for money. In this system, centralized intermediaries, such as banks and monetary institutions, are not necessary to enforce trust and police transactions between two parties. Thus, a system with cryptocurrencies eliminates the possibility of a single point of failure, such as a large bank, setting off a cascade of crises around the world, such as the one that was triggered in 2008 by the failure of institutions in the United States.**

**Cryptocurrencies promise to make it easier to transfer funds directly between two parties, without the need for a trusted third party like a bank or a credit card company. Such decentralized transfers are secured by the use of public keys and private keys and different forms of incentive systems, such as proof of work or proof of stake and so on..**

**Demerits :**

**Cryptocurrencies represent a new, decentralized paradigm for money. In this system, centralized intermediaries, such as banks and monetary institutions, are not necessary to enforce trust and police transactions between two parties. Thus, a system with cryptocurrencies eliminates the possibility of a single point of failure, such as a large bank, setting off a cascade of crises around the world, such as the one that was triggered in 2008 by the failure of institutions in the United States.**

**Cryptocurrencies promise to make it easier to transfer funds directly between two parties, without the need for a trusted third party like a bank or a credit card company. Such decentralized transfers are secured by the use of public keys and private keys and different forms of incentive systems, such as proof of work or proof of stake.**

**Future scope :**

**Some economic analysts predict a big change in crypto is forthcoming as institutional money enters the market. 3﻿ Moreover, there is the possibility that crypto will be floated on the Nasdaq, which would further add credibility to blockchain and its uses as an alternative to conventional currencies.**

**Conclusion:**

**Like every technologies cryptocurrency too have both merits and demerits. It is something needed to be encouraged for good purposes. we have to invest before getting an clear idea of the concepts as its value is highly volatile. Though this technology is highly impressive. There by concluding by saying think wisely and get a proper knowledge and do further purposes**