Research Paper
Impact Factor: 4.164
Refereed Journal

IJMDRR
E- ISSN –2395-1885
ISSN -2395-1877

A STUDY ON CRYPTOCURRENCY-CHALLENGES AND OPPORTUNITIES

Dr. V. Babu
Faculty member, Department of Commerce, St. Joseph's College, Lalbagh road, Bengaluru, Karnataka.

Introduction

Today crypto currencies have become a global phenomenon known to most people. While still somehow geeky and not understood by most people, banks, governments and many companies are aware of its importance. Beyond the noise and the press releases the overwhelming majority of people – even bankers, consultants, scientists, and developers – have a very limited knowledge about crypto currencies. They often fail to even understand the basic concepts. Few people know, but crypto currencies emerged as a side product of another invention. Satoshi Nakamoto, the unknown inventor of Bitcoin, the first and still most important crypto currency, never intended to invent a currency.

In his announcement of Bit coin in late 2008, Satoshi said he developed "A Peer-to-Peer Electronic Cash System". His goal was to invent something; many people failed to create before digital cash. The single most important part of Satoshi's invention was that he found a way to build a decentralized digital cash system. In the nineties, there have been many attempts to create digital money, but they all failed. After seeing all the centralized attempts fail, Satoshi tried to build digital cash system without a central entity. Like network for file sharing. This decision became the birth of crypto currency. They are the missing piece Satoshi found to realize digital cash.

Objectives

1. To understand the concept of crypto currency
2. To study the present status of crypto currency and , challenges and opportunities of crypto currency

Methodology

Method of research: Conceptual study
Source of data: secondary data from websites

Crypto currencies - Concepts

A crypto currency is a digital or virtual currency that uses cryptography for security. A crypto currency is difficult to counterfeit because of this security feature. A defining feature of a crypto currency, and arguably its most endearing allure, is its organic nature; it is not issued by any central authority, rendering it theoretically immune to government interference or manipulation.

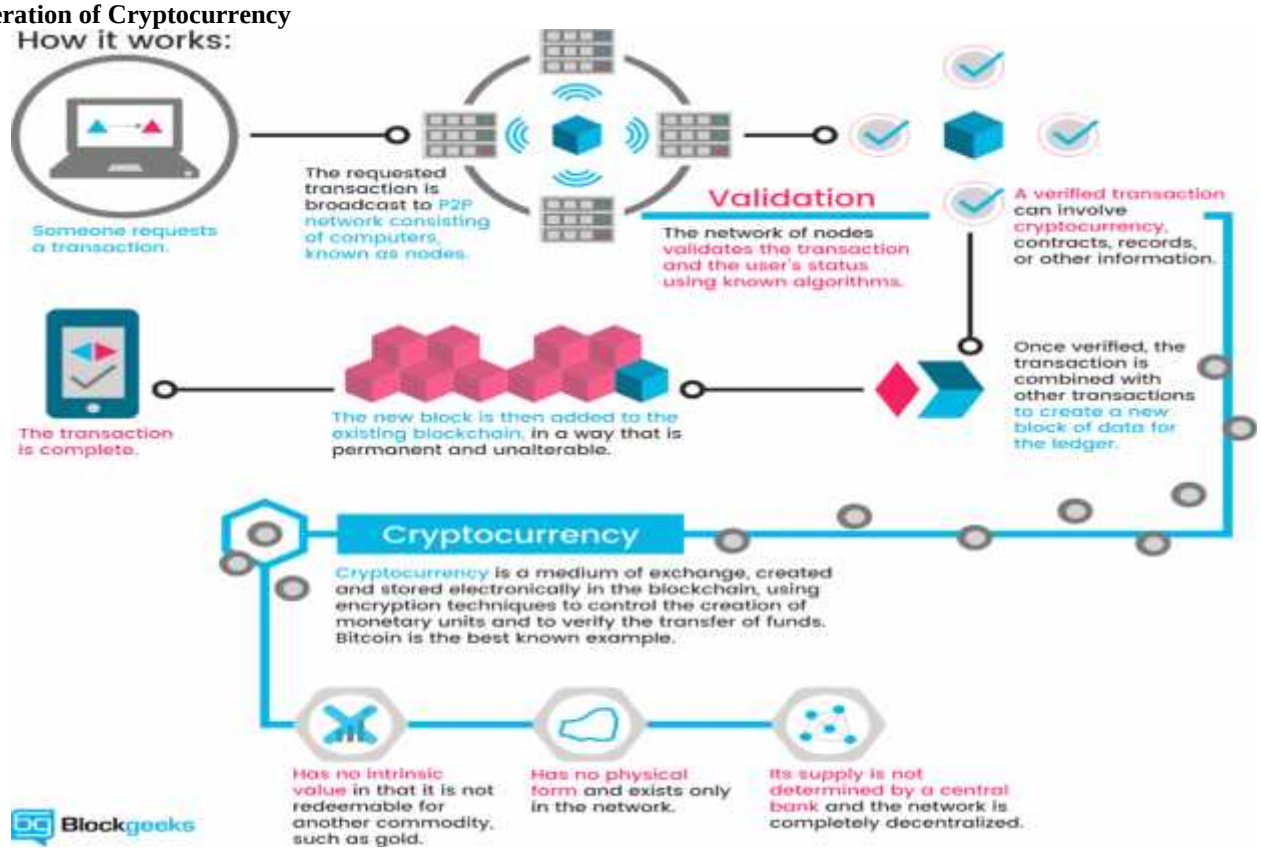
If you take away all the noise around crypto currencies and reduce it to a simple definition, you find it to be just limited entries in a database no one can change without fulfilling specific conditions. This may seem ordinary, but, believe it or not: this is exactly how you can define a currency.

Take the money on your bank account: What is it more than entries in a database that can only be changed under specific conditions? You can even take physical coins and notes: What are they else than limited entries in a public physical database that can only be changed if you match the condition than you physically own the coins and notes? Money is all about a verified entry in some kind of database of accounts, balances, and transactions.

IJMDRR
E- ISSN –2395-1885
ISSN -2395-1877

Source:https://blockgeeks.com

Operation of Cryptocurrency



Source:https://blockgeeks.com

Challenges of Crypto currency

Irreversible: After confirmation, a transaction can‘t be reversed. By nobody. And nobody means anybody. Not you, not your bank, not the president of the United States, not Satoshi, not your miner. Nobody. If you send money, you send it. Period. No one can help you, if you sent your funds to a scammer or if a hacker stole them from your computer. There is no safety net.

Pseudonymous: Neither transactions nor accounts are connected to real-world identities. You receive Bitcoins on so-called addresses, which are randomly seeming chains of around 30 characters. While it is usually possible to analyze the transaction flow, it is not necessarily possible to connect the real world identity of users with those addresses.

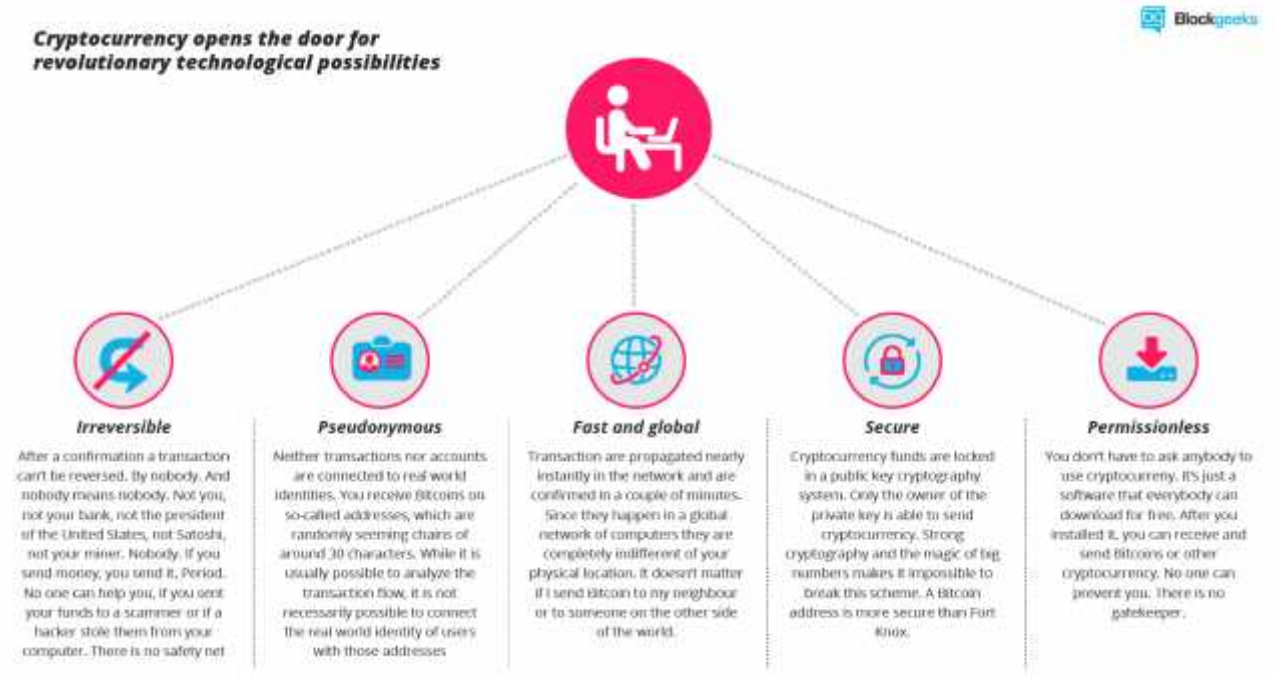
Fast and global: Transaction are propagated nearly instantly in the network and are confirmed in a couple of minutes. Since they happen in a global network of computers they are completely indifferent of your physical location. It doesn‘t matter if I send Bitcoin to my neighbour or to someone on the other side of the world.

Secure: Cryptocurrency funds are locked in a public key cryptography system. Only the owner of the private key can send cryptocurrency. Strong cryptography and the magic of big numbers makes it impossible to break this scheme. A Bitcoin address is more secure than Fort Knox.

Permissionless: You don‘t have to ask anybody to use cryptocurrency. It‘s just a software that everybody can download for free. After you installed it, you can receive and send Bitcoins or other cryptocurrencies. No one can prevent you. There is no gatekeeper.

Controlled supply: Most cryptocurrencies limit the supply of the tokens. In Bitcoin, the supply decreases in time and will reach its final number somewhere in around 2140. All cryptocurrencies control the supply of the token by a schedule written in the code. This means the monetary supply of a cryptocurrency in every given moment in the future can roughly be calculated today. There is no surprise.

No debt but bearer: The Fiat-money on your bank account is created by debt, and the numbers, you see on your ledger represent nothing but debts. It‘s a system of IOU. Cryptocurrencies don‘t represent debts. They just represent themselves. They are money as hard as coins of gold.



Source: https://blockgeeks.com

Current Profile of Crypto currency

The anonymous nature of crypto currency transactions makes them well-suited for a host of nefarious activities, such as money laundering and tax evasion.

The first crypto currency to capture the public imagination was Bit coin, which was launched in 2009 by an individual or group known under the pseudonym Satoshi Nakamoto. As of September 2015, there were over 14.6 million bit coins in circulation with a total market value of $3.4 billion. Bit coin's success has spawned a number of competing crypto currencies, such as Litecoin, Namecoin and PPCoin.

#	Name	Market Cap	Price	Available Supply	Volume (24h)	% Change (24h)	Price Graph (7d)
1	Bitcoin	$11,382,240,050	$712.76	15,969,336 BTC	$67,288,200	-1.60%	
2	Ethereum	$904,848,975	$10.54	85,831,133 ETH	$4,069,260	-1.21%	
3	Ripple	$290,446,848	$0.008121	35,765,131,899 XRP *	$2,386,420	0.26%	
4	Litecoin	$184,904,214	$3.82	48,378,029 LTC	$2,258,970	-1.05%	
5	Monero	$83,466,495	$6.27	13,311,446 XMR	$3,134,490	5.38%	
6	Ethereum Classic	$80,817,441	$0.942637	85,735,486 ETC	$803,573	2.21%	
7	Dash	$66,519,213	$9.68	6,874,532 DASH	$596,632	-0.77%	
8	Augur	$52,038,360	$4.73	11,000,000 REP *	$396,072	6.38%	
9	NEM	$37,322,550	$0.004147	8,999,999,999 XEM *	$86,817	4.40%	
10	Waves	$35,727,500	$0.357275	100,000,000 WAVES *	$133,650	-3.94%	

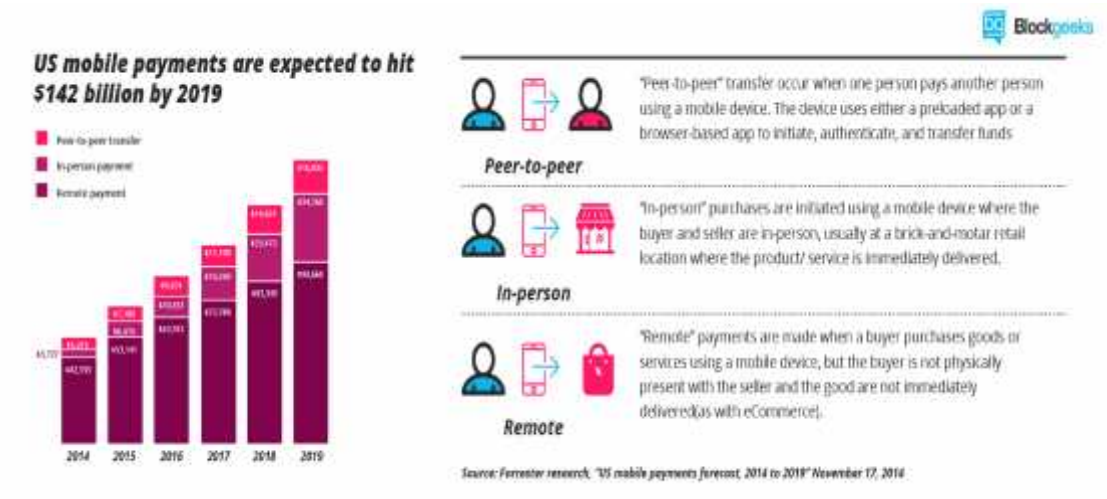
Source:https://blockgeeks.com

Opportunities for Crypto currencies

The market of crypto currencies is fast and wild. Nearly every day new crypto currencies emerge, old die, early adopters get wealthy and investors lose money. Every crypto currency comes with a promise, mostly a big story to turn the world around. Few survive the first months, and most are pumped and dumped by speculators and live on as zombie coins until the last bagholder loses hope ever to see a return on his investment.

Markets are dirty. But this doesn't change the fact that cryptocurrencies are here to stay – and here to change the world. This is already happening. People all over the world buy Bitcoin to protect themselves against the devaluation of their national currency. Mostly in Asia, a vivid market for Bitcoin remittance has emerged, and the Bitcoin using darknets of cybercrime are flourishing. More and more companies discover the power of Smart Contracts or token on Ethereum, the first real-world application of blockchain technologies emerge.

The revolution is already happening. Institutional investors start to buy cryptocurrencies. Banks and governments realize that this invention has the potential to draw their control away. Cryptocurrencies change the world. Step by step. You can either stand beside or observe – or you can become part of history in the making.



Source:https://blockgeeks.com

New Trend in Currency Transaction

Mostly due to its revolutionary properties cryptocurrencies have become a success their inventor, Satoshi Nakamoto, didn‘t dare to dream of it. While every other attempt to create a digital cash system didn‘t attract a critical mass of users, Bitcoin had something that provoked enthusiasm and fascination. Sometimes it feels more like religion than technology.

Cryptocurrencies are digital gold. Sound money that is secure from political influence. Money that promises to preserve and increase its value over time. Cryptocurrencies are also a fast and comfortable means of payment with a worldwide scope, and they are private and anonymous enough to serve as a means of payment for black markets and any other outlawed economic activity.

But while cryptocurrencies are more used for payment, its use as a means of speculation and a store of value dwarfs the payment aspects. Cryptocurrencies gave birth to an incredibly dynamic, fast-growing market for investors and speculators. Exchanges like Okcoin, poloniex or shape shift enables the trade of hundreds of cryptocurrencies. Their daily trade volume exceeds that of major European stock exchanges.

At the same time, the praxis of Initial Coin Distribution (ICO), mostly facilitated by Ethereum‘s smart contracts, gave live to incredibly successful crowdfunding projects, in which often an idea is enough to collect millions of dollars. In the case of “The DAO” it has been more than 150 million dollars.

In this rich ecosystem of coins and token, you experience extreme volatility. It‘s common that a coin gains 10 percent a day – sometimes 100 percent – just to lose the same at the next day. If you are lucky, your coin‘s value grows up to 1000 percent in one or two weeks.

While Bitcoin remains by far the most famous cryptocurrency and most other cryptocurrencies have zero non-speculative impact, investors and users should keep an eye on several cryptocurrencies. Here we present the most popular cryptocurrencies of today.

Bitcoin

The one and only, the first and most famous cryptocurrency. Bitcoin serves as a digital gold standard in the whole cryptocurrency-industry, is used as a global means of payment and is the de-facto currency of cyber-crime like darknet markets or ransomware. After seven years in existence, Bitcoin‘s price has increased from zero to more than 650 Dollar, and its transaction volume reached more than 200.000 daily transactions.

Ethereum

The brainchild of young crypto-genius VitalikButerin has ascended to the second place in the hierarchy of cryptocurrencies. Other than Bitcoin its blockchain does not only validate a set of accounts and balances but of so-called states. This means that Ethereum can not only process transactions but complex contracts and programs.
This flexibility makes Ethereum the perfect instrument for blockchain -application. But it comes at a cost. After the Hack of the DAO – an Ethereum based smart contract – the developers decided to do a hard fork without consensus, which resulted in

the emerge of Ethereum Classic. Besides this, there are several clones of Ethereum, and Ethereum itself is a host of several Tokens like DigixDAO and Augur. This makes Ethereum more a family of cryptocurrencies than a single currency.

Ripple

Maybe the less popular – or most hated – project in the cryptocurrency community is Ripple. While Ripple has a native cryptocurrency – XRP – it is more about a network to process IOUs than the cryptocurrency itself. XRP, the currency, doesn‘t serve as a medium to store and exchange value, but more as a token to protect the network against spam.

Ripple Labs created every XRP-token, the company running the Ripple network, and is distributed by them on will. For this reason, Ripple is often called pre-mined in the community and dissed as no real cryptocurrency, and XRP is not considered as a good store of value. Banks, however, seem to like Ripple. At least they adopt the system with an increasing pace.

Litecoin

Litecoin was one of the first cryptocurrencies after Bitcoin and tagged as the silver to the digital gold bitcoin. Faster than bitcoin, with a larger amount of token and a new mining algorithm, Litecoin was a real innovation, perfectly tailored to be the smaller brother of bitcoin. “It facilitated the emerge of several other cryptocurrencies which used its codebase but made it, even more, lighter“. Examples are Dogecoin or Feathercoin. While Litecoin failed to find a real use case and lost its second place after bitcoin, it is still actively developed and traded and is hoarded as a backup if Bitcoin fails.

Monero

Monero is the most prominent example of the cryptonite algorithm. This algorithm was invented to add the privacy features Bitcoin is missing. If you use Bitcoin, every transaction is documented in the blockchain and the trail of transactions can be followed. With the introduction of a concept called ring-signatures, the cryptonite algorithm was able to cut through that trail.
The first implementation of cryptonite, Bytecoin, was heavily premined and thus rejected by the community. Monero was the first non-premined clone of bytecoin and raised a lot of awareness. There are several other incarnations of cryptonote with their own little improvements, but none of it did ever achieve the same popularity as Monero.

Monero‘s popularity peaked in summer 2016 when some darknetmarkets decided to accept it as a currency. This resulted in a steady increase in the price, while the actual usage of Monero seems to remain disappointingly small. Besides those, there are hundreds of cryptocurrencies of several families. Most of them are nothing more than attempts to reach investors and quickly make money, but a lot of them promise playgrounds to test innovations in cryptocurrency-technology.

Conclusion

As money with a limited, controlled supply that is not changeable by a government, a bank or any other central institution, cryptocurrencies attack the scope of the monetary policy. They take away the control central banks take on inflation or deflation by manipulating the monetary supply.Cryptocurrencies make it easier to transfer funds between two parties in a transaction; these transfers are facilitated through the use of public and private keys for security purposes. These fund transfers are done with minimal processing fees, allowing users to avoid the steep fees charged by most banks and financial institutions for wire transfers.

Central to the genius of Bitcoin is the block chain it uses to store an online ledger of all the transactions that have ever been conducted using bitcoins, providing a data structure for this ledger that is exposed to a limited threat from hackers and can be copied across all computers running Bitcoin software. Many experts see this block chain as having important uses in technologies, such as online voting and crowdfunding, and major financial institutions such as JP Morgan Chase see potential in cryptocurrencies to lower transaction costs by making payment processing more efficient.

However, because cryptocurrencies are virtual and do not have a central repository, a digital cryptocurrency balance can be wiped out by a computer crash if a backup copy of the holdings does not exist. Since prices are based on supply and demand, the rate at which a cryptocurrency can be exchanged for another currency can fluctuate widely.
Cryptocurrencies are not immune to the threat of hacking. In Bitcoin's short history, the company has been subject to over 40 thefts, including a few that exceeded $1 million in value. Still, many observers look at cryptocurrencies as hope that a currency can exist that preserves value, facilitates exchange, is more transportable than hard metals, and is outside the influence of central banks and governments.

References

1. https://www.investopedia.com.
2. https://www.blockgeeks.com.