BITCOIN

Shaikh Imran, Ansari Afroz, Sayed Azhar, Lanjekar Javed
Computer Department,
Anjuman.Islam.Abdul.Razzak.Kalsekar.Polytechnic, Panvel, India

1. Abstract : Along the history, people organised in communities needed payment means in order to exchange goods or deliver services. From beads and feathers to metal and paper money they have always improved the way transactions were made. The invention of the Internet opened new doors in the field of payments, through the quick access to information and the emergence of significant international online communities. The members of these communities became aware of the importance of decentralising the way they acquire goods or services, thus eliminating the middlemen. Cryptocurrencies represent the response of these communities to he old centralised means of payment, controlled by the bankers, politicians and interest groups. Our paper aims to analyse the cryptocurrency phenomenon revealing some of its advantages and disadvantages, to increase the awareness on the topic. We based our research on the existing literature, the relevant international databases, the official positions of the financial and regulatory institutions on the analysed matter.

Key-Words: Bitcoin, Nakamoto, cryptocurrency, altcoins, blockchain, ethereum, security.

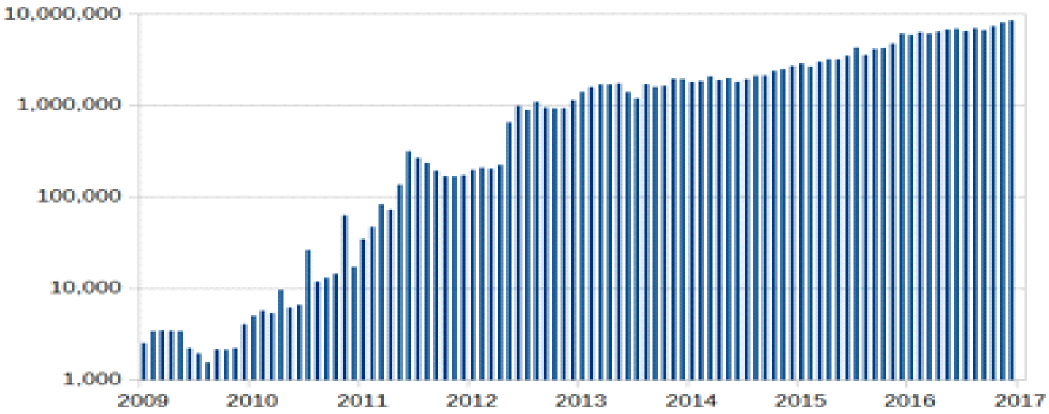
2. Introduction:

Bitcoin is a cryptocurrency, a form of electronic cash. It is the world's first decentralized digital currency, and it was designed to work without a central bank or single administrator.

Bitcoins are sent from user to user on the peer-to-peer bitcoin network directly, without the need for intermediaries. Transactions are verified by network nodes through cryptography and recorded in a public distributed ledger called a blockchain. Bitcoin was invented by an unknown person or group of people using the name Satoshi Nakamoto and released as open-source software in 2009. Bitcoins are created as a reward for a process known as mining. They can be exchanged for other currencies, products, and services. Research produced by the University of Cambridge estimates that in 2017, there were 2.9 to 5.8 million unique users using cryptocurrency wallet, most of them using bitcoin.

3. History of bitcoin :

Bitcoin is a cryptocurrency, a digital asset designed to work as a medium of exchange that uses cryptography to control its creation and management, rather than relying on central authorities. The presumed pseudonymous Satoshi Nakamoto integrated many existing ideas from the cypherpunk community when creating bitcoin. Over the course of bitcoin's history, it has undergone rapid growth to become a significant currency both on and offline – from the mid 2010s, some businesses began accepting bitcoin in addition to traditional currencies.



4. Bitcoin Creator :

Satoshi Nakamoto is the name used by the unknown person or people who developed bitcoin, authored the bitcoin white paper, created and deployed bitcoin's original reference implementation. As part of the implementation, they also devised the first blockchain database.In the process they were the first to solve the double-spending problem for digital currency using a peer-to-peer network. They were active in the development of bitcoin up until December 2010.

5. Advantages of Using Bitcoin :

- Greater Liquidity Relative to Other Cryptocurrencies
- Increasingly Wide Acceptance as a Payment Method
- International Transactions Easier Than Regular Currencies
- Generally Lower Transaction Fees

WHY USE BITCOIN ?
INSTANT
PAYMENT SETTLEMENTS
NETWORK CENTRIC
IRREVERSIBLE PAYMENTS
DIGITAL
GLOBAL ACCEPTANCE
DECENTRALISED
NO CENTRAL POINT OF FAILURE
OPEN SOURCE
VOLUNTARY AND FREE TO JOIN
SECURE
CRYPTOGRAPHIC FUNCTIONS
UNOCOIN

6. Disadvantages of Using Bitcoin :

- Black Market Activity May Damage Reputation and Usefulness
- No Chargebacks or Refunds
- Susceptible to High Price Volatility
- Potential to Be Replaced by Superior Cryptocurrency

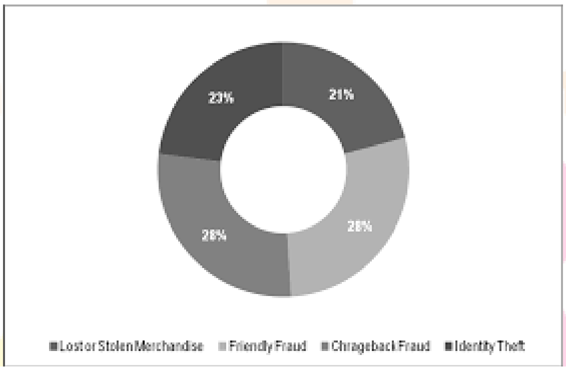


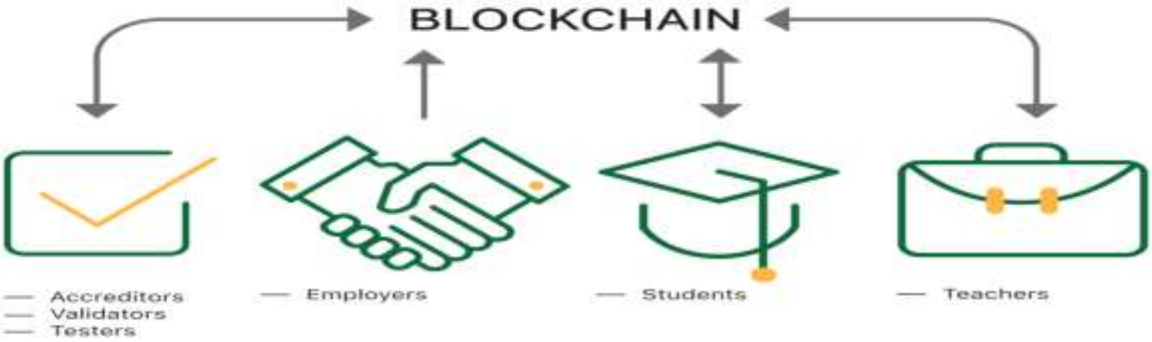
Table 1. Cryptocurrencies Market Capitalizations on the 16th of November 2017

Rank	Name	Market cap ($)	Price ($)	Circulation supply	Volume (24h) ($)	% change in 7 days
1	Bitcoin	124,915,866,558.00	7,487.76	16,682,675.00	4,157,970,000.00	3.78%
2	Ethereum	31,718,817,624.00	331.23	95,761,281.00	696,121,000.00	3.42%
3	Bitcoin Cash	18,052,542,573.00	1,074.23	16,805,100.00	1,963,800,000.00	70.87%
4	Ripple	8,238,610,568.00	0.21	38,622,892,459.00	122,815,000.00	-2.36%
5	Litecoin	3,428,420,697.00	63.67	53,850,357.00	169,528,000.00	0.86%
6	Dash	3,236,113,295.00	420.72	7,691,919.00	94,258,500.00	28.64%
7	IOTA	2,243,039,245.00	0.81	2,779,530,283.00	105,177,000.00	43.35%
8	Monero	1,904,116,137.00	123.97	15,359,615.00	64,204,600.00	6.90%
9	NEO	1,892,371,000.00	29.11	65,000,000.00	40,880,000.00	-9.74%

7. Blockchain :

The bitcoin blockchain is a public ledger that records bitcoin transactions. It is implemented as a chain of blocks, each block containing a hash of the previous block up to the genesis block of the chain. A network of communicating nodes running bitcoin software maintains the blockchain. Transactions of the form *payer X sends Y bitcoins to payee Z* are broadcast to this network using readily available software applications.

Network nodes can validate transactions, add them to their copy of the ledger, and then broadcast these ledger additions to other nodes. To achieve independent verification of the chain of ownership each network node stores its own copy of the blockchain. About every 10 minutes, a new group of accepted transactions, called a block, is created, added to the blockchain, and quickly published to all nodes, without requiring central oversight. This allows bitcoin software to determine when a particular bitcoin was spent, which is needed to prevent double-spending. A conventional ledger records the transfers of actual bills or promissory notes that exist apart from it, but the blockchain is the only place that bitcoins can be said to exist in the form of unspent outputs of transactions.



8. Transactions :

Transactions are defined using a Forth-like scripting language.Transactions consist of one or more *inputs* and one or more *outputs*. When a user sends bitcoins, the user designates each address and the amount of bitcoin being sent to that address in an output. To prevent double spending, each input must refer to a previous unspent output in the blockchain. The use of multiple inputs corresponds to the use of multiple coins in a cash transaction. Since transactions can have multiple outputs, users can send bitcoins to multiple recipients in one transaction. As in a cash transaction, the sum of inputs (coins used to pay) can exceed the intended sum of payments. In such a case, an additional output is used, returning the change back to the payer. Any input *satoshis* not accounted for in the transaction outputs become the transaction fee.

8.1 Units :

The unit of account of the bitcoin system is a *bitcoin*. Ticker symbols used to represent bitcoin are BTC and XBT. Small amounts of bitcoin used as alternative units are millibitcoin (mBTC), and *satoshi* (sat). Named in homage to bitcoin's creator, a *satoshi* is the smallest amount within bitcoin representing 0.00000001 bitcoins, one hundred millionth of a bitcoin. A millibitcoin equals 0.001 bitcoins, one thousandth of a bitcoin or 100,000 *satoshis*.

8.2 Transaction fees :

Though transaction fees are optional, miners can choose which transactions to process and prioritize those that pay higher fees. Miners may choose transactions based on the fee paid relative to their storage size, not the absolute amount of money paid as a fee. These fees are generally measured in *satoshis per byte (sat/b)*. The size of transactions is dependent on the number of inputs used to create the transaction, and the number of outputs.

8.3 Mining :

Mining is a record-keeping service done through the use of computer processing power. Miners keep the blockchain consistent, complete, and unalterable by repeatedly grouping newly broadcast transactions into a *block*, which is then broadcast to the network and verified by recipient nodes. Each block contains a SHA-256 cryptographic hash of the previous block,thus linking it to the previous block and giving the blockchain its name.

To be accepted by the rest of the network, a new block must contain a so-called *proof-of-work* (PoW). The system used is based on Adam Back's 1997 anti-spam scheme, Hashcash. The PoW requires miners to find a number called a *nonce*, such that when the block content is hashed along with the nonce, the result is numerically smaller than the network's difficulty target.This proof is easy for any node in the network to verify, but extremely time-consuming to generate, as for a secure cryptographic hash, miners must try many different nonce values (usually the sequence of tested values is the ascending natural numbers: 0, 1, 2, 3, ...) before meeting the difficulty target.

Every 2,016 blocks (approximately 14 days at roughly 10 min per block), the difficulty target is adjusted based on the network's recent performance, with the aim of keeping the average time between new blocks at ten minutes. In this way the system automatically adapts to the total amount of mining power on the network. Between 1 March 2014 and 1 March 2015, the average number of nonces miners had to try before creating a new block increased from 16.4 quintillion to 200.5 quintillion.The proof-of-work system, alongside the chaining of blocks, makes modifications of the blockchain extremely hard, as an attacker must modify all subsequent blocks in order for the modifications of one block to be accepted.As new blocks are mined all the time, the difficulty of modifying a block increases as time passes and the number of subsequent blocks (also called *confirmations* of the given block) increases.

9. Conclusions :

As we emphasised, the phenomenon of cryptocurrencies is developing at a high rate. Bitcoin is for the time being the king of virtual money regarding market capitalisation, and daily transactions. The developed countries are more open to adopting cryptocurrencies than developing countries. In such developed countries Bitcoin is regarded as private money, money service businesses, financial service, means of payment, electronic service, decentralised virtual currency and so on. Some developing countries consider bitcoin, and other cryptocurrencies illegal because they are not issued and controlled by a government and can be involved in “dubious activities” such as money laundering, terrorism financing, human and drug trafficking, tax evasion, illegal payments. There are several countries (Ecuador, China), that consider implementing their cryptocurrencies. Bitcoin has several advantages that can help its development in the following years. Personal data protection of the users is better ensured. In case a retailer is compromised by a security breach, customers` data are still safe. The transaction costs are over five times lower than the ones made by credit card. On the merchants` side, it offers more protection in case of charge-back fraud, the transactions being confirmed in 10 to 30 min, giving the seller time to receive the money before delivering the ordered goods. The monetary inflation of Bitcoin will decrease in time until it reaches the limit of 21 million mined bitcoins. On the downside, we identified that the anonymity of the transactions in bitcoins could not be 100% ensured. Keeping safe the private key to the wallet might also prove to be a problem in the case of computers connected to the Internet, or if an attacker has physical access to one`s storage device. As we showed, some scams are being operated by criminals against bitcoin owners (Ponzi schemes, mining devices never delivered, buffer wallets and exchange scams). No system is perfect, but the dynamic of the cryptocurrencies phenomenon, the intentions of some developed states and large private companies to adopt blockchain to improve the financial and administration systems indicate that there are other opportunities to be explored in the future.