CRYPTO TRACKER

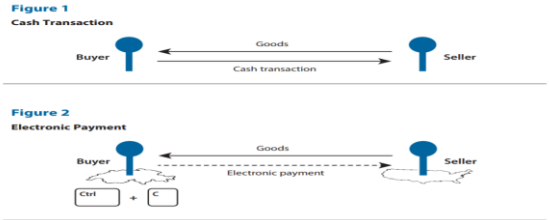
[1]Harshit Aggarwal, [2]Prof. Savita
[1]Student, [2]Associate Professor
Department of Electronics and Communication Engineering
Mahavir Swami Institute of Technology, Sonipat, India

Abstract: - cryptocurrency is decentralized digital money that's based on blockchain technology. You may be familiar with the most popular versions; Bit coin and Ethereum, but there are more than 5,000 different cryptocurrencies in circulation. You can use crypto to buy regular goods and services, although most people invest in cryptocurrencies as they would in other assets, like stocks or precious metals. While cryptocurrency is a novel and exciting asset class, purchasing it can be risky as you must take on a fair amount of research to fully understand how each system works.

1. INTRODUCTION

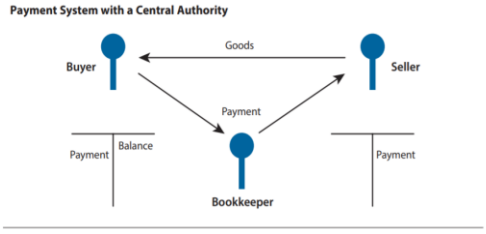
Bitcoin originated with the white paper that was published in 2008 under the pseudonym "Satoshi Nakamoto." It was published via a mailing list for cryptography and has a similar appearance to an academic paper. The creators' original motivation behind Bitcoin was to develop a cash-like payment system that permitted electronic transactions but that also included many of the advantageous characteristics of physical cash. To understand the specific features of physical monetary units and the desire to develop digital cash, we will begin our analysis by considering a simple cash transaction.

CASH:
Cash is represented by a physical object, usually a coin or a note. When this object is handed to another individual, its unit of value is also transferred, without the need for a third party to be involved (Figure 1). No credit relationship arises between the buyer and the seller. This is why it is possible for the parties involved to remain anonymous. The great advantage of physical cash is that whoever is in possession of the physical object is by default the owner of the unit of value. This ensures that the property rights to the units of value circulating in the economy are always clearly established, without a central authority needing to keep accounts. Furthermore, any agent can participate in a cash payment system; nobody can be excluded. There is a permission less access to it. Cash, however, also has disadvantages. Buyers and sellers have to be physically present at the same location in order to trade, which in many situations makes its use impracticable.



DIGITAL CASH:
An ideal payment system would be one in which monetary value could be transferred electronically via cash data files (Figure 2). Such cash data files retain the advantages of physical cash but would be able to circulate freely on electronic networks.1 A data file of this type could be sent via email or social media channels. A specific feature of electronic data is that it can be copied any number of times at negligible cost. This feature is highly undesirable for money. If cash data files can be copied and the duplicates used as currency, they cannot serve as a payment instrument. This problem is termed the "double spending problem."

Electronic Payment Systems:
To counteract the problem of double spending, classical electronic payment systems are based on a central authority that verifies the legitimacy of the payments and keeps track of the current state of ownership. In such systems, a central authority (usually a bank) manages the accounts of buyers and sellers. The buyer initiates a payment by submitting an order. The central authority then ensures that the buyer has the necessary funds and adjusts the accounts accordingly. Centralized payment systems solve the double spending problem, but they require trust. Agents must trust that the central authority does not misuse the delegated power and that it maintains the books correctly in any state of the world—that is, that the banker is not running away with the money. Furthermore, centralized systems are vulnerable to hacker attacks, technical failures, and malicious governments that can easily interfere and confiscate funds.



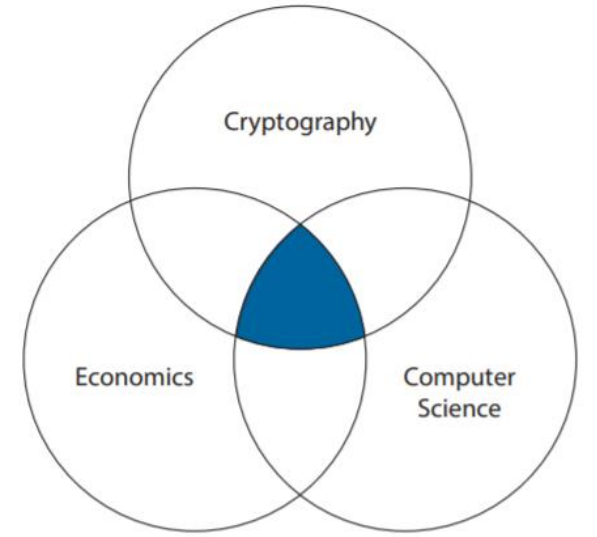
2. BITCOIN TRANSACTIONS

The complexity of the present material is due to interdisciplinary. To understand the Bitcoin system, it is necessary to combine elements from the three disciplines of economics, cryptography, and computer science.
Having presented a broad overview of the Bitcoin system, we will explain a few technical elements of the system in greater detail. Blockchain uses proven technologies and links these in an innovative way. This combination has made the decentralized management of a ledger possible for the first

time. Berentsen and Schär (2017) argue that transaction processing demands that three requirements are satisfied: (1) transaction capability, (2) transaction legitimacy, and (3) transaction consensus. These three requirements will now be considered. In particular, we will explain how these conditions can be satisfied in the absence of a central authority.

Figure 7

Interdisciplinarity



Transaction Capability

What has to be resolved is how transactions can be initiated if there is no central authority. In a classical banking system, a client talks to his or her advisor or submits his or her payment instructions via the bank's online banking service. The infrastructure provided by the commercial bank and other central service providers ensures that the transaction will be communicated for execution. In the absence of a central authority, communicating a payment order in this traditional sense is not possible. In the Bitcoin system, a payment order can be communicated to any number of network nodes. The network nodes are linked together in a loose network and forward the message until all nodes have been informed about the transaction (Figure 8). The decentralization of the system has many advantages. In particular, it makes the system extremely robust. There is neither a central point of failure that can be attacked nor any system relevant nodes that could cause the system to collapse. Therefore, the system functions even when some network nodes are unreachable, and it can always establish new connections and communication channels.

Transaction Legitimacy:

Every participant can generate new payment orders and spread them across the network. This feature carries the risk of fraudulent messages. In this respect, there are two important questions that arise:

1. How do the nodes know that the initiator of the transaction is the rightful owner and that he or she is thereby entitled to transfer the Bitcoin units?
2. How can one ensure that the transaction message will not be tampered with before it is passed from one node to the next?

Figure 8

Bitcoin Transaction Communicated to Network Nodes

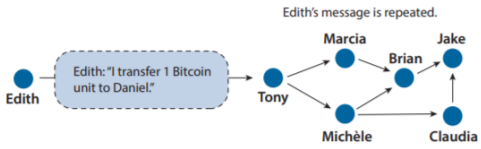
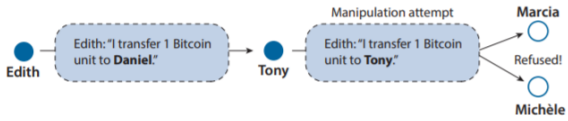


Figure 9

Bitcoin Transaction Manipulation Attempt



3. RISKS

Much like any other key innovation, blockchain technology introduces some risks. The following sections will consider some of these risks. As we mentioned in Section 3, we would like to note that this list is non-exhaustive.

Forks:

As discussed above, the Bitcoin protocol can be altered if the network participants, or at least a sufficient number of them, agree on the suggested modification. It can happen (and in fact has happened) that a blockchain splits because various groups cannot agree about a modification. A split that persists is referred to as a "fork." The two best-known examples of persistent splits are the Bitcoin Cash fork and Ethereum's ideological dissent, which resulted in the split to Ethereum and Ethereum Classic.

Energy Wastage:

Proof-of-work mining is expensive, as it uses a great deal of energy. There are those that criticize Bitcoin and assert that a centralized accounting system is more efficient because consensus can be attained without the allocation of massive amounts of computational power. From our perspective, however, the situation is not so clear-cut. Centralized payment systems are also expensive. Besides infrastructure and operating costs, one would have to calculate the explicit and implicit costs of a central bank. Salary costs should be counted among the explicit costs and the possibility of fraud in the currency monopoly among the implicit costs. Moreover, many cryptoassets use alternative consensus protocols, which do not (solely) rely on computational resources.

Bitcoin Price Volatility:

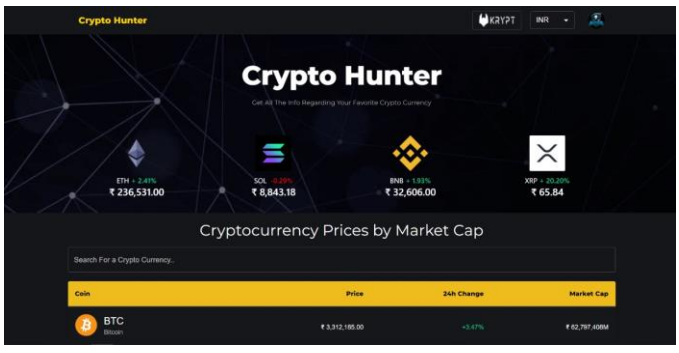
The price of Bitcoin is highly volatile. This leads us to the question of whether the rigid predetermined supply of Bitcoin is a desirable monetary policy in the sense that it leads to a stable currency. The answer is no because the price of Bitcoin also depends on aggregate demand. If a constant supply of money meets a fluctuating aggregate demand, the result is fluctuating prices. In government-run fiat currency systems, the central bank aims to adjust the money supply in response

to changes in aggregate demand for money in order to stabilize the price level. In particular, the Federal Reserve System has been explicitly founded "to provide an elastic currency" to mitigate the price fluctuations that arise from changes in the aggregate demand for the U.S. dollar. Since such a mechanism is absent in the current Bitcoin protocol, it is very likely that the Bitcoin unit will display much higher short-term price fluctuations than many government-run fiat currency unit

4. CONCLUSION

The Bitcoin creators' intention was to develop a decentralized cash-like electronic payment system. In this process, they faced the fundamental challenge of how to establish and transfer digital property rights of a monetary unit without a central authority. They solved this challenge by inventing the Bitcoin Blockchain. This novel technology allows us to store and transfer a monetary unit without the need for a central authority, similar to cash. Price volatility and scaling issues frequently raise concerns about the suitability of Bitcoin as a payment instrument. As an asset, however, Bitcoin and alternative blockchain-based tokens should not be neglected. The innovation makes it possible to represent digital property without the need for a central authority. This can lead to the creation of a new asset class that can mature into a valuable portfolio diversification instrument. Moreover, blockchain technology provides an infrastructure that enables numerous applications. Promising applications include using colored coins, smart contracts, and the possibility of using fingerprints to secure the integrity of data files in a blockchain, which may bring change to the world of finance and to many other sectors

5. OUTPUT



References

1. https://stackoverflow.com/
2. https://faucet.egorfine.com/
3. https://tailwindcss.com/
4. https://www.coingecko.com/
5. https://www.alchemy.com/

