ABSTRACT

Cryptocurrency is a digital currency which is created for the purpose of transaction as a normal currency. It uses Cryptography and Blockchain technology to secure its exchanges and limit the production of a particular type of cryptocurrency and keep track of each and every transaction in whole network. The Cryptocurrency laden with so much new age technologies and a huge market presence all over the world, but still, even after a decade of its existence, it has not attained an established image as a new age currency system among majority of the countries in the world and people are still sceptical about its worth. It's almost a decade that Cryptocurrencies are existing in all over world but still its status has not been idented as whether it will ever attain the actual currency status or it will remain as a part of investment portfolio. To know the awareness and perception level of cryptocurrency in Bangalore as it is a cosmopolitan city, the study has been carried out. Bitcoin has emerged as the most successful cryptographic currency in history. Within two years of its quiet launch in 2009, Bitcoin grew to comprise billions of dollars of economic value despite only cursory analysis of the system's design. Since then a growing literature has identified hidden-but-important properties of the system, discovered attacks, proposed promising alternatives, and singled out difficult future challenges. Meanwhile a large and vibrant open-source community has proposed and deployed numerous modifications and extensions. We provide the first systematic exposition Bitcoin and the many related cryptocurrencies or 'altcoins.' Drawing from a scattered body of knowledge, we identify three key components of Bitcoin's design that can be decoupled. This enables a more insightful analysis of Bitcoin's properties and future stability. We map the design space for numerous proposed modifications, providing comparative analyses for alternative consensus mechanisms, currency allocation mechanisms, computational puzzles, and key management tools. We survey anonymity issues in Bitcoin and provide an evaluation framework for analysing a variety of privacy-enhancing proposals. Finally we provide new insights on what we term disintermediation protocols, which absolve the need for trusted intermediaries in an interesting set of applications. We identify three general disintermediation strategies and provide a detailed comparison

WHY BITCOIN IS WORTHY OF RESEARCH

Consider two opposing viewpoints on Bitcoin in strawman form. The first is that "Bitcoin works in practice, but not in theory." At times devoted members of the Bitcoin community espouse this philosophy and criticize the security research community for failing to discover Bitcoin, not immediately recognizing its novelty, and still today dismissing it due to the lack of a rigorous theoretical foundation. A second viewpoint is that Bitcoin's stability relies on an unknown combination of socioeconomic factors which is hopelessly intractable to model with sufficient precision, failing to yield a convincing argument for the system's soundness. Given these difficulties, experienced security researchers may avoid Bitcoin as a topic of study, considering it prudent security engineering to only design systems with precise threat models that admit formal security proofs.

To the second viewpoint, we contend that Bitcoin is filling an important niche by providing a virtual currency system without any trusted parties and without pre-assumed identities among the participants. Within these constraints, the general problem of consensus in a distributed system is impossible [7], [93] without further assumptions like Bitcoin's premise that rational (greedy) behaviour can be modelled and incentives can be aligned to ensure secure operation of the consensus algorithm. Yet these constraints matter in practice, both philosophically and technically, and Bitcoin's approach to consensus within this model is deeply surprising and a fundamental contribution. Bitcoin's core consensus protocol also has profound implications for many other computer security problems beyond currency1 such as distributed naming, secure timestamping and commitment, generation of public randomness, as well as many financial problems such as self-enforcing ("smart") contracts, decentralized markets and order books, and distributed autonomous agents. In short, even though Bitcoin is not easy to model, it is worthy of considerable research attention as it may form the basis for practical solutions to exceedingly difficult and important problems.

Introduction

The origin of blockchain and cryptocurrencies dates back to 2008, when Satoshi Nakamoto – the pseudonymous developer of blockchain and the cryptocurrency bitcoin – posted a paper to a cryptography forum entitled "Bitcoin: A Peer-to-Peer Electronic Cash System" The paper described a revolutionary technology to create a genuine decentralized peer-to-peer monetary system, arguing that "a purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution" (. Blockchain is defined as "a digital, distributed transaction ledger, with identical copies maintained on multiple computer systems controlled by different entities". Cryptocurrencies are based on blockchain but are not the only possible application. There is a dangerous relationship between blockchain and cryptocurrencies, being necessary to underline that cryptocurrencies are one of the multiple possibilities of blockchain technologies. According to the World Economic Forum (2015) 10% of GDP will be stored in blockchain by 2027 (World Economic Forum, 2015), with an average annual growth rate of 62.1% until 2025 (Business Wire, 2017).

In the case of cryptocurrencies, it is the supporting software that both verifies ownership and executes transfers.[Footnote3] There is no requirement for a 'trusted third party'.[Footnote4] This approach though requires a complete historical record of previous cryptocurrency transfers, tracing back each holding of cryptocurrency to its initial creation. This historical record is based on a "blockchain", a linking of records ("blocks") to each other in such a way that each new block contains information about the previous blocks in the growing list ("chain") of digital records. So that every participant in the cryptocurrency network sees the same transaction history, a new block is accepted by agreement across the entire network. The applications of this technology are not necessarily finance-related; it can be applied to any form of record-keeping; however if the block refers to a financial transaction then each transaction in the blockchain, by definition, includes information about previous transactions, and thus verifies the ownership of the financial asset being transferred. Falsifying ownership, i.e. counterfeiting (which, one could imagine, is easy, as digital objects can be easily duplicated by copying), is impossible because one would have to alter preceding records in the whole chain. Since records are kept in the network of many users' computers, a "distributed ledger", this is rather unthinkable.

There is a substantial computer science literature on the supporting cryptocurrency technologies, including on the security of public key cryptography, efficient search tools for finding transactions on the blockchain, and the 'consensus' mechanisms used to establish agreement on ledger contents across the network.[Footnote5] Commentators expect new more efficient approaches will replace the mechanisms currently used in Bitcoin and other cryptocurrencies.[Footnote6] This though would not affect our definition of cryptocurrencies (as an asset and some technology which verifies ownership of the asset), which is independent of any particular technological implementation.[Footnote7]

Cryptocurrencies can be seen as part of a broader class of financial assets, "cryptoassets" with similar peer-to-peer digital transfers of value, without involving third party institutions for transaction certification purposes. What distinguishes cryptocurrencies from other cryptoassets? This depends on their purpose, i.e. whether they are issued only for transfer or whether they also fulfil other functions. Within the overall category of cryptoassets, we can follow the distinctions drawn in recent regulatory reports, distinguishing two further sub-categories of cryptoassets, on top of cryptocurrencies:[Footnote8]

Blockchain

The decentralized blockchain technology on which many of today's biggest cryptocurrency coins are built act as public ledgers where all of the transactions that have been performed within the network are stored for anyone to independently verify. Public ledgers are what make trust less peer-to-peer transactions possible, because the users of that digital currency know that all of the transactions on the network will be concerted and displayed on the blockchain. On a blockchain, transactions are recorded chronologically, forming an immutable chain, and can be more or less private or anonymous depending on how the technology is implemented. The ledger is distributed across many participants in the network — it doesn't exist in one place. Instead, copies exist and are simultaneously updated with every fully participating node in the ecosystem. A block could represent transactions and data of many types — currency, digital rights, intellectual property, identity, or property titles, to name a few.

Cryptocurrencies and neoclassical finance

Cryptocurrencies can be used both as a means of payment and as a financial asset. Glaser et al. (2014) provide evidence that, at least for the Bitcoin, the main reason to purchase a cryptocurrency is speculative investment. Financial securities, such as ETNs (exchange traded notes) and CFDs (derivative products) that replicate Bitcoin's price performance are made available by brokers, expanding the speculative investment opportunities to an even larger set of investors. With this in mind, it makes sense to evaluate cryptocurrencies as financial assets.

On the positive side, the development of the cryptocurrency market contributes to the dynamics of access to finance). The advent of the blockchain technology allowed entrepreneurial teams to raise capital in cryptocurrencies and fiat money (which has to be exchanged into a cryptocurrency) through the issuance of digital tokens (Initial Coin Offerings, ICOs) and the development of 'smart contracts'). Tokens give their buyers a right to use certain services or products of the issuer, or to share profits, in which case they resemble equity. Special crypto exchanges then serve the secondary market for tokens. The OECD lays out basic principles and typical steps of an ICO. An important distinction between tokens and cryptocurrencies is though that there is a liability or some sort of commitment behind the token, and this liability determines its value. Now that this crypto asset bears more similarity with traditional assets, one would expect also the main predictions of neoclassical finance to come true. In fact, in a recent empirical study of crypto tokens, Howell et al. demonstrate the effects of asymmetric information on tokens trading: their liquidity and trading volume are positively associated with the information inflow. The latter is achieved through voluntary disclosure of information (including the operating budget and their business plans), and quality signalling (e.g. information on prior venture capital funding of the issuer).

A Technical Overview We present Bitcoin's three main technical components: transactions (including scripts), the consensus protocol, and the communication network. Bitcoin is exceedingly complex—our goal is to present the system with sufficient technical depth that the literature on Bitcoin and be reviewed and evaluated in later sections of this paper. In particular, a key benefit of our three-component breakdown is that it makes evaluating and systematizing proposed changes (Sections VI & VIII) insightful by "decoupling" concepts that may be changed independently. Sources of information on Bitcoin. Bitcoin can be difficult to define as there is no authoritative formal specification. The original Bitcoin white paper [90] provides a good overview of Bitcoin's design philosophy but many important technical details are omitted or outdated. The reference implementation bitcoin is considered a de facto specification, with further knowledge scattered across a series of "Bitcoin Improvement Proposals" (BIPs), forum postings, online wiki articles, the developer mailing list, and logged IRC discussions.3 We systematize these sources into a precise technical introduction, putting forward the components of the system we consider to be independent design decisions.

. THREATS REGARDING CRYPTOCURRENCY

Cryptocurrency when it was being used for the first time, no one knows about it and only • handful of persons knows what cryptocurrencies is. It was mostly used to do illegal deals by drug dealers, smugglers and black marketers for the transaction of their funds as it is the safest, untraceable and fastest method to doall over the world. After the introduction of new cryptocurrencies in the market, few companies started taking interest in the digital mode of cryptocurrencies and invented their own cryptocurrencies like Litecoin etc. India assets in digital world has grown tremendously in the last few years but it also going through a phase of uncertainty. Uncertainties also created various types of complications in the industry of digital assets in country mainly for the digital exchanges. Various exchanges of digital had a mission to involve India into blockchain technology but as per the new RBI guidelines, banks have been told to not to continue with any services which involves virtual currencies which leaves all the virtual currencies into the question of legal challenge. It is also a warning sign for all the investors who will deal with these types of virtual cryptocurrencies. 4 There are many risks involve in investing cryptocurrencies: -

1) Entrance is wide, but exit is narrow-As clear from the heading it is easy to invest in Bitcoin because all the things have been done digitally so it creates a less barrier for the cryptocurrency and a very high risk to exist from the digital world of Bitcoin.

Intangible and Unsecured-The intangible and unsecured form of nature of cryptocurrencies. The blockchain technology-based cryptocurrencies has eliminate the bank and banker which can act as an intermediary in between and which can also solve the issue of unsecured cryptocurrency, but this feature captured the thing of security which can be assured by banks.

2) Manipulation by extortion-even though the amount is nominal there is no way that the investors will not be prepared in any way to lose their ownership as a crypto holder and they easily become victim of social engineering as well as misinformation risks. So, market manipulation and extortion risk are more common in the investment of cryptocurrency.

3) Protection, Care and Control-Although cryptocurrencies are intangible in form and act as an asset which is digital in nature. It became one of the biggest issues for the care, control and custody of the cryptocurrency as wealthiest investors will invest in security vault to take care of their cryptocurrency but those who can't afford it will easily become target of the frauds and the hackers for the custody of their cryptocurrency.

4) Cyber risks always-It is obvious that cyber threats will always be there to keep the cryptocurrency. Risks are always involved for the ransomware attack and various types of viruses which can attack to the cryptocurrency and create many problems to the investors of the cryptocurrency.

In today's world, cryptocurrency is becoming the target for the cybercriminals as they can easily demand from the crypto holders the ransomware in the form of cryptocurrency. It is also becoming famous because in this no one will block the address of you,no one will catch you and moreover there is very less chance of being tracked by the officials. Web mining is another technique used in browser with a special script which is installed in the web browser and the attackers are well known about the fact that it is very easy to upload such type of web page in the browser and can easily mining the things out of the cryptocurrency holders. So, the nature of the cryptocurrency is becoming more and more dangerous as cyber threats are increasing day by day for example by changing the address of the electronic wallet and stealing the electronic wallet are the things which can be done by the hackers. So, in other way we can say that cryptocurrency have opened the new and unprecedented ways to monetize the activities which are done maliciously

Banks versus Cryptocurrency

As we all know banks have both primary and secondary functions. Cryptocurrency has been acclaimed to carry out the same primary functions as of bank. The objective of this is to aid as a mediator between the fund gathering and allocation of it. Cryptocurrency is also giving the same intermediary role and the most important thing is the boycott of the supervision of each transaction. Now a day's internet has become worldwide popular, depositors will deal with cryptocurrency in a more convenient method and it also provide to the users the intermediate actions. It will make the banks to focus on their functions which are secondary in nature for their survival. Cryptocurrency collision on all the banks of centre and the government is the removal of issuance of fiat currency by them. A large drive by the banks of centre to dissolve the money which has been going long enough before the arrival of cryptocurrencies. Technology is giving the central bank attempts to issue the money which is digital in nature. According to some sources, 79% of cryptocurrency amount of the firms have introduced to introduce some relationship with banking institutions, but it is difficult in attaining and maintaining this relationship is challenging due to competition.

FUTURE OF CRYPTOCURRENCY IN THE PRESENT WORLD

The market of the cryptocurrency is wider than any other currency in the world. Even though the development of blockchain technology is a new concept for all but still all the new coins are competing with each other in order to stay in the market of the cryptocurrency. In future we can say that there will be only three or four coins to be in working mode for the entire payment, trading and other banking infrastructures. It will be expected to say that every person in future will use the application of blockchain in the modern era. Central Banks and other banks are of the view that cryptocurrencies are a long run thing and are here to stay for quiet long time. Bitcoins are rapidly in the process of converting and act as a real money that will give a competition to the centralised bodies of government. Bitcoins have a very bright future in the coming era. This currency is of this type that is decentralised, and anyone can use it which is eliminating the rates of exchange in the market of the world makes the future by becoming centralised across the country and the days are not far away when there will be one world and one currency.

CONCLUSION

With the revolutionary changes in the cryptocurrency the future of the virtuality cannot be determined in near future. Moreover, virtual currency is illegal in almost all over the world. Some organisations are still using this currency, but majority of companies completely ban them in transaction. If the cryptocurrency in the modern era have become famous, then it is impossible for the countries to completely ignore it. Moreover, cryptocurrencies have the power to become one global currency. There is legality to the use of Bitcoin is a debate, but the acceptance of cryptocurrencies can be happened in the next few years in the digital world.11Eventually we can say that needs of the customers for the cryptocurrency application it is essential to note that that what are the main success factors for learning the application on cryptocurrency. One obvious thing we see for the use of cryptocurrency is that the people who are the investors in cryptocurrency are having the income which is higher from others and they are also possessing the other methods of investment. By keeping in mind, the importance of cryptocurrency those persons who are investing their profiles can be decided and which results in the m-learning application of cryptocurrency which is the main planning of the customer caring. One more thing is to be added also that by using the deductive logic the application which we use in mobiles the success factors can be used for the application of cryptocurrency also and highest factor rate can be given special attention for the safeguard, accomplishment, easy use and invention in order to design the application of mobile. However, the most important feature in using the m-learning on cryptocurrency is that it will become the one stop app for the persons who are interested in cryptocurrencies. The only problem comes after researching on this topic is that the concept of blockchain technology and the cryptocurrency is totally new to the people and it is known mainly to the IT field department. The market of cryptocurrencies are growing day by day and all the spotlight are on the concept of new ecosystem of cryptocurrencies.

The second issue, widely debated in the cryptocurrency literature, is whether cryptocurrencies have a fundamental own value. Dwyer (2015) conjectures the limitation of the quantity produced can create an equilibrium in which a digital currency has a positive value: this limitation is a form of commitment, replacing the implicit obligation of Central banks to exchange fiat money into gold. Hayes (2017) advocates the cost of production view on cryptocurrency pricing; yet, as we discussed earlier, from a market equilibrium perspective, being sunk cost (as in Dwyer 2015), it does not matter for the pricing of existing coins.[Footnote14] A concurrent work by Bolt and Van Oort (2019) outlines three key elements of the cryptocurrency value: convertibility into fiat money or ability to buy goods and services, investors' expectations, and factors that determine acceptance of the cryptocurrency in the future, by both vendors and buyers. Simultaneously, Schilling and Uhlig (2019) offer a model where cryptocurrencies are a reliable medium of exchange and compete against fiat money: this role implies the current price of cryptocurrencies is the expectation of their future value (a martingale), yet interestingly, competition and substitutability between the two imply in their analysis cryptocurrencies should disappear in the long run equilibrium. The authors admit that their analysis abstracts away such distinctive features of cryptocurrencies as "censorship resistance, transparency, and speed of trading". Above we have provided a simplified argument explaining that cryptocurrencies may have a value by offering features, such as anonymity of transactions, not covered by traditional currencies. Many findings, also those included in this special issue, point towards the intangible nature of the cryptocurrency value. Knowing more about it, we would be better equipped to understand the price dynamics and, reciprocally, the price dynamics would improve our understanding of decisions made by investors. So far, we remain very much agnostic in this respect.

The third issue is the societal role of cryptocurrencies and their regulation. While many discussions of cryptocurrencies stress that they are free of regulation, and the desire to be unregulated was one of drivers behind their creation, there is considerable controversy both about the application of existing regulation to cryptocurrencies and other crypto assets+ and also what if any new regulations may be needed to protect investors, prevent financial crime and ensure financial stability. Are crypto investments securities and therefore subject to securities law (in the US this has been determined by the so-called Howey test)? What about the regulation of crypto exchanges and the problems of hacking with some prominent examples of theft and failure to enforce "know-your-customer" (KYC) and anti-money-laundering (ALM) regulations?