Block Chain Technology.

Rajveer Shringi

***Abstract*—This paper describes the concept of Block chain technology, the key components involved in block chain architecture and the set of protocols followed. Block Chain has recently come out as a new generation technology that can be used to support distributed transactional applications. It can provide a mechanism for two parties to get into a "smart contract" capable of establishing trust, accountability and transparency among business processes. We discuss the potential this technology has to transform Business and Society and with big market players such as IBM coming forward to join Linux Foundation to advance Blockchain makes this domain more popular and interesting. The Blockchain concept of distributed, decentralized, shared ledger can be applied to a set of possible use cases of which we focus on - smart contracts between multiple parties who have no reason to trust(or distrust) each other, BitCoin and lightweight financial systems and lastly Provenance tracking. We also discuss the idea of Decentralized Autonomous Organization(DAO) to automate organizational governance and decision-making.**

***Keywords*—*Block Chain, Smart Contracts, BitCoin, Provenance Tracking*.**

I. Introduction

In todays globally distributed yet connected economy organisations are continuously taking part in business spanning across different countries and continents crossing national, geographic and jurisdictional boundaries. This calls the need for transactions which are global in nature and highly distributed. Any object that holds a certain financial value can be described as an asset. Assets can be tangible such as - a car or home or intangible such as - stocks and patents. In such marketplace producers, consumers, buyers, sellers come together to own or transfer the ownership of assets and such activities are termed as Transactions. In present scenario a business transaction generally involve buyer, seller and intermediary such as banks or notaires and involve usage of business agreements and contracts which are recorded in business ledgers. A ledger keeps track of the asset ownership, its transfer among different participants and serves as a systems of records(SORs) for a businesss economic activities. [1]

Taking a minimal transaction of funds transfer as an example - it requires an agreement between payer's bank, a common merchant such as Visa/MasterCard and payees bank. The main role of these intermediaries is to establish a channel of trust among the transaction participants who have no reason to trust or distrust each other. They enforce that both the parties involved in a transaction would deliver what they promised adhering to the pre-agreed terms. The key point in above scenario is the - middleman such as the banks or notaries can range from two-three to almost five to six different organisations just to transfer some money from one part of the world to another. This gives rise to two major problems - latency : it can take days and sometimes weeks for funds to reach correct person, overhead : due to involvement of multiple parties in the transaction there is always a cost associated which is some percentage of the actual amount transfer thus raising costs and making micro fund transactions impractical.

This is where the block chain technology comes into picture. Block chain is trying to do what Internet did in 90s, providing a revolutionary means of communication between people across the world at minimal prices. Although instead of communication, value based on trust is the major commodity that block chain technology promises to provide among different parties spread across the planet. This can significantly bring down the transaction costs and latency which in turn can lead to a revolutionary new ways of carrying out transactions and maintenance of records giving rise to a whole new system of business practices. The block chain technology aims at providing infrastructure to share assets and records in a trusted way among participants. By ensuring transparency, fraud resilience and security, application areas can range from business transactions to provenance tracking and democratic voting.

II. Key Components: Block Chain Architecture

Before starting to discuss the architecture its important to differentiate between BitCoin and Block Chain Technology. Its common to get confused between the two and people use these terms interchangeably. BitCoin is one of the crypto currency system that is based on the block chain architecture, and similar other applications exist such as Ethereum - smart contracts that under the hood rely on block chain methodology. These applications may differ in specific implementations(which we will discuss in later parts of this paper) but the underlying architecture is almost similar.

A block chain architecture basically consists of - a peer to peer network(P2P), a distributed shared public ledger(database), a set of agreed cryptographic protocols, mathematical computationally expensive tasks that can serve as proof of work. A P2P network consists of participating nodes connected to a random subset of other nodes and each having their own copy of the shared ledger. The nodes can dynamically join or leave the network, and as any designated member of the network can flag a fraudulent entry in ledger the more the participating nodes the stronger the network gets. A distributed and shared ledger(database) of records which resides with every node and acts as the single source of truth. This ledger follows append only mode of operation, so any new entry is appended at the end of already existing records. A set of records in a ledger can be termed as block, when a new transaction happens this is appended in the ledger after repeating the previous existing records forming a new block. This new block of records is then

Rajveer Shringi is with the Department of Informatics - Intelligent Systems, TU Kaiserslautern, Kaiserslautern, 67663 DE e-mail:rshringi@rhrk.uni-kl.de

added to the pre-existing block via a cryptographic signature verifying its authenticity. These repeated blocks of records form a chain structure, leading to the name block chain. The entries in the ledger are encrypted ensuring privacy and time stamped to track the series of events and resolve any disputes. This distributed and encrypted ledger can be used to contain wide variety of information such as - digital or physical assets, personal identity, user reviews and feedbacks leading to a variety of applications. In order to maintain consistency without a central authoritative database it is of prime importance to keep the contents of the distributed ledger synchronised among the network. This leads us to the discussion of how exactly the transactions are initiated, authorised to be authentic, new blocks of records get created and added to the previous chain of records.

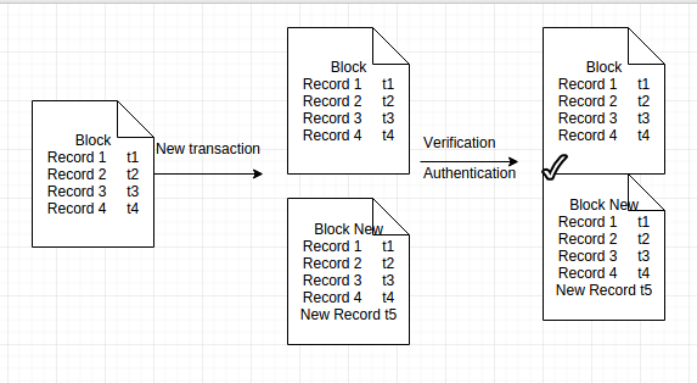

Fig. 1. Shows a block of records, after a new transaction another block is formed and then added to the chain after validation and authentication.

A. Block Chain Algorithm : How it works

Lets consider a P2P block chain network as depicted in Fig. 2. As discussed earlier every member have their own copy of ledger of all the records in the network which in this example is credit history. Now Alice wishes to make a new transaction which involves transferring five dollars to Sarah. In order to achieve this successfully following steps are taken in chronological order -

1. Alice broadcasts the request of transferring of fund to Sarah throughout the network. This request is appended to the already existing set of records but is not verified yet and enters the network as a non verified transaction.
2. Once such a request enters the network many predesignated nodes called miners (here Eve and Dave)take up the task to verify the authenticity of this request. The verification involves checking whether the request is feasible or not in this scenario checking the funds available in Alices account. Such verifications can sometimes involve cross checking the records all the way back in history till the first transaction in the ledger. This task of verification is not much computing expensive. One or many nodes present in the system can choose to be miners depending upon available computing resources at their end.
3. Transactions once verified are then needed to be appended to the existing block chain of records. This is done by generating a hash value which is obtained by solving a mathematical problem of a specific difficulty level depending on the computational cycle in the network. The task of hash generation is termed as proof of work and is a computation intensive process. All the nodes of miner type compete with each other to generate their proof of work as soon as an unconfirmed transaction enters the network. The miner who generates the proof of work earliest wins and gets certain financial incentive for its work.
4. The moment a miner is able to generate a proof of work, it broadcasts this with the validated transaction to all other peers. On the receipt of proof of work other competing miner nodes stop working on this proof of work and try to verify the given block with already provided proof of work as its much easier and cheaper to verify and cross check a proof of work rather than generating it.
5. Miners in the network only accept the new block of transaction once they have verified the proof of work and the involved transactions in that block. Once a specific miner is done verifying it casts a vote to agree or disagree with the new block of records. A consensus is take depending on the agreed protocol, for example if 51 percent of the miners in the network agree to the new block of records then it is added to the existing chain by accepting the hash of new block and setting it as the current hash. In this way the chain of records keep on growing over time.
6. Thus after verification of transaction all the individual copies of records gets updated and synchronised to reflect the network verified credit history at timestamp T2. The workflow of change in ledger can be seen as depicted in Fig 3. The process is designed such that any conflicts regarding entries in the ledger are resolved via P2P network in robust and decentralized consensus.[1]

B. Block Chain Algorithm : Security

As already discussed each new block in the block chain is added to the existing chain via a cryptographic key that takes into account all previous records and appends the new record. This hash key generation takes place through a mathematical task which requires - computing resources and luck. It can be considered as analogous to winning a lottery where computing resources play the role of lottery tickets. HIgher number of lottery tickets increases your chances of winning the lottery but does not guarantee that you will land a winning ticket. The mathematical task of generating a proof of work is unrelated to the network transaction but is an integral part of the security of the system. As generating proof of work is computationally expensive task while its verification is not, any fraudulent proof of work or invalid transaction would be observed by peers easily and rejected. Thus its only logical and profitable to broadcast valid transactions once a miner has spent certain resources on generating the proof of work. This highlights another impressive aspect of this algorithm that takes mutual human distrust as a resource and harness it to validate and strengthen the updates using a P2P validation methodology. In order for a node to add a fraudulent transaction it would be required to fork the block chain at a specific place to insert the

block with fraudulent transaction, generate the proof of work in a timely manner to keep up with the chain length as the miner nodes accept the longest chain or the chain with maximum proof of work as the only valid chain. This is an immensely computation expensive task and thus would be illogical and unprofitable to do when compared to the expected profit made. If a node has access to such computation resources then the only logical way to turn it profitable would be to use them to generate proof of works in timely manner and validate honest transactions and gain the financial incentive provided at every proof of work.[2]

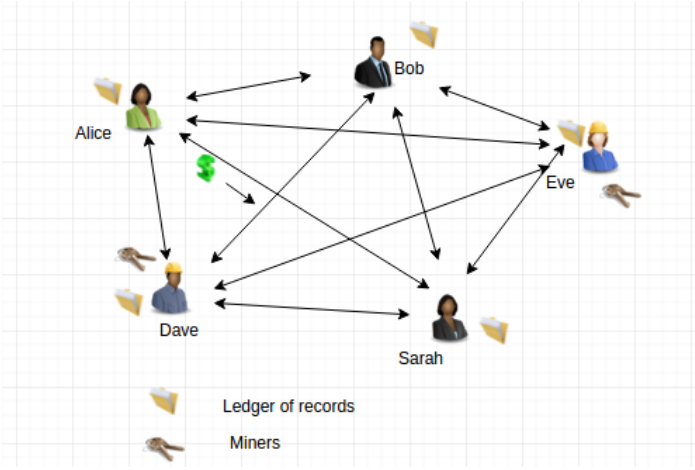

Fig. 2. Shows a P2P block chain network with some nodes acting as miners. In this network Alice initiates a transaction of $5 transfer to Sarah.

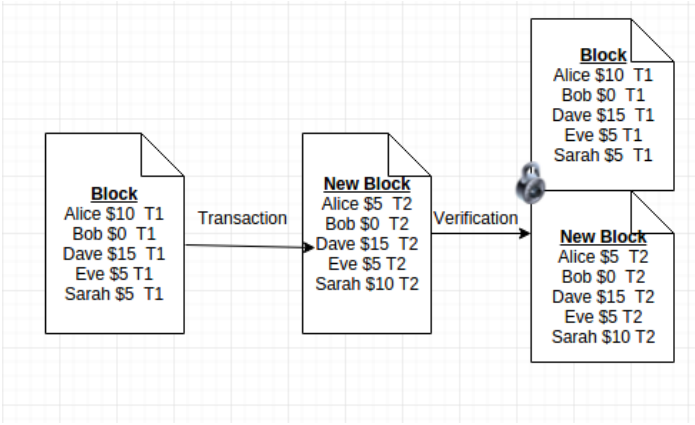

Fig. 3. Shows a block of records before the transaction was initiated, after a new transaction another intermediate block is formed and then added to the chain after validation and authentication. Note that all the records have time stamps.

III. Cryptocurrency and BitCoin

Historically we have been using currency in the form of gold, silver, precious stones and more recently the bank notes for trading of goods and services. The reason for existence of currency is the inherent trust and value that is packaged in them due to the reasons such as scarcity for gold, silver etc or government backing up incase of bank notes such as - US Dollars or EU Euros. There are several flaws in both of these previous means of currency - safe storage, fraudulent currency, currency track and control to name a few. This is where the idea of digital currency or crypto currency comes into picture. Digital currency can be defined as the means of currency whose sole existence relies and is governed by the digital network and its protocols. Its called crypto currency because of the usage of several cryptographic algorithms(MD5/SHA-256) for the management and transfer operations. And users respect and value such currencies for the same earlier reasons of being scarce, reliable and fault tolerant.

BitCoin system is one of such digital currencies or electronic payment systems that is based on block chain technology for its operation. There exist several other alternatives such as - Litecoin, Opencoin, Dash but of these BitCoin is the most widely known and accepted and we focus our discussion on BitCoin henceforth. A computer programmer or a group of programmers aliasing under the name - Satoshi Nakamoto proposed BitCoin in a white paper published in 2008 as an open source, peer-to-peer, digital currency. Since then the network has gained popularity with user base doubling every 8 months and the current number of coins reaching to a number of 14 million approximately two third of the maximum limit set.

A. How it works-

Essentially bitcoin network is identical to the block chain P2P network discussed earlier, where distributed ledger keeps track of the number of bitcoins in the network and their ownership transference.

1. In order to transfer funds from one account to another, the nodes generally install a service in form of a e-wallet which takes care of the cryptographic signing involved to initiate and validate transactions.
2. The cryptographic process involves the use of digital signatures using algorithms such as RSA/DSS. Before initiating a transaction every node generates two sets of keys - private key and a public key. The private key is used for signing purposes while the public key is used for validation, getting tied to the identity of user in the network. For every transaction a node wants to initiate it encrypts it with its private key and broadcasts the result to the network. Other nodes on the network can authenticate these set of transaction to be truly initiated by the correct node via using the public key of the initiator node which is available publicly throughout the network.
3. After authentication these set of transaction are still unconfirmed and need to be verified for validity and a proof of work has to be generated before they can be appended to the existing chain of records.
4. All the miner nodes in a network start competing by taking such unconfirmed transactions in a given time window and ensemble them into a block, each of them adding their own

unique extra transaction involving the transaction fee they charge.
5. After this they start to validate these transactions which is followed by generation of proof of work for the new set of records. A sample proof of work generation may look like - pairwise hashing of the new set of transaction in a tree structure and then finally hashing it to the earlier existing block of records to generate a new block of record. After this the miner node need to compute a sequence of numbers which when hashed with the cryptographic hash value of the new block of records leads to an output with a specific number of leading zeroes(for example 32 or 40 leading zeroes).
6. Once a miner finds such a sequence it broadcasts the result with the new block of records to the network. The new block is accepted as the current block in the chain after verification of proof of work and consensus voting.

B. Money Generation and Flow -

A miner node in this process gets incentive via - a transaction fee that they charge and certain amount of bitcoins which get generated in the process and assigned to it with every successful proof of work. This is how the new bitcoins get generated in the network. When started in January 2009, the reward for every proof of work was 50 bitcoins. And the network controls the currency generation by slicing the rewards into half after every 210,000 blocks of records. Also as discussed before there is a certain difficulty level involved in generating proof of work at every stage of the chain which can also be controlled and modified to control the generation of new coins in the network. BitCoin network maintains that every 10 minutes a random miner would be able to generate a proof of work and thus adding a new block to the chain every 10 minutes. This provides a metric to monitor and control of the growth of coins in the network. For every 2016 blocks added the time taken to add them is checked and compared with ideal time required of 2 weeks, calculated by assuming every new block takes 10 minutes. Based on this observation the difficulty level of proof of work problems is increased or decreased. In our example say to find a sequence of digits with 41 leading zeroes(higher difficulty) or 39 leading zeroes(lower difficulty). The fact that the reward given to miners which is also the new coins added to the network gets halved every 210,000 blocks(which takes around 4 years) by year 2140 the network would reach its maximum permissible coin amount which is 21 million coins.[4]
Due to this limited and constant decrease in issuance of new coins in the network over the time makes BitCoin currency deflationary. Which is in direct contrast with most of the currency systems prevalent today which are inherently inflationary in nature. By the rule of demand and supply once the supply is constant and the demand rises the value of the currency will keep on increasing. The current value of one BitCoin is around 868 Euros at the time of writing of this paper. An inherent problem that comes with such a currency is if the holder of one bitcoin can buy a car, how does he buy lesser goods such as bread or water. This is termed as the problem of divisibility in currencies and bitcoin system addresses it by being highly divisible and traded in fraction. The network permits value as low as one millionth of a bitcoin to be used in transactions. Another issue that comes into light is once the network reaches its maximum value of coins there will be no new reward given to miners for a proof of work and then what incentive would motivate them to keep working. One of the hypothesis is that once the network reaches such state there will be enough people in the network leading to a high number of transactions. And as every miner charges a transaction fee for every block it ensembles, this fee should grow proportionally to the number of transactions taking place providing enough monetary incentive for the miners. [4][5]

C. Advantages over Traditional Systems-

1) Privacy: Typical transactions involving credit-debit cards, cheques and other such methods always leave a footprint behind exposing user's transaction history. On contrary Bitcoin promises the same or more anonymity involved as during a cash transaction without leaving any digital track of users transaction history. A user interacts in bitcoin network via its alphanumeric coded account linked to its e-wallet. Every transaction is encrypted and a user can be associated with one or more accounts in the network. The network keeps track of all the transactions happening but it would not be possible to link it back to any specific user.

2) Open: This system of currency is open and available to anyone at the disposal of a network connection(internet) increasing its user reach to developing and under developed regions of the world. A user does not need to register with a bank, credit or debit card to start a transaction.

3) DeCentralised: As there is no one central authority that controls the network, there is no central authority controlling the money supply and currency flow. This reduces bottlenecks leading to payment latencies. This also reduces transaction costs involved thus making micro payments possible and practical.

4) Safety Against Double Spending: A physical form of money is safe from double spending as it can only be in one place at one given time, while a digital currency is susceptible to this problem. The problem of spending the same digital currency twice is termed as double spending. BitCoin deals with this via making sure that the currency can only be transferred within the network. And underlying block chain network maintains the ledger tracking the ownership of every single bitcoin throughout their creation to every subsequent transaction,, thus eliminating the double spending problem. [3]

IV. Ethereum and Smart Contracts

Earlier parts of this paper describe how Bitcoin technology uses blockchain infrastructure to facilitate transfer of currency among nodes in a decentralized yet reliable manner. Now consider this transfer of currency from say, Alice to Bob happening if and only if Bob completes certain task that Alice agreed upon for example - make a good meal for her. This is a simple example of a smart contract. Smart contracts can be defined as a pre specified set of instructions(for example - transfer of money) that gets executed automatically once

a specific predefined condition(for example - doing certain task) is met. The underlying idea behind smart contracts remains the same as of blockchain - decentralizing a certain centralized(monitoring) service to increase transparency and reduce the need for trust in a single central authority. The term smart contracts was coined by cryptologist Nick Szabo in 1997, where he defines smart contracts as tool to combine set of digitally defined rules and user interface in order to express a contract.[8]
Smart contracts are of further two types - deterministic and non-deterministic. A deterministic smart contract can determine the preconditions required to trigger the set of instructions from the block chain network itself without being dependent on an external entity. While a non deterministic contract depends on external entities called - Oracle to determine if the preconditions are met before triggering the set of instructions.
While a basic bitcoin currency exchange can be made to work following a specific set of instructions via a script, encoding more complicated set of instructions that suits a business logic needs a dedicated service to itself. This is where Ethereum comes into picture. Ethereum is a crowdfunded project founded in Spring 2015 which can be defined as a block chain platform providing rich API interfaces to developers to support development of decentralised applications(DApp) on top of it. Smart contracts is one of the significant features provided by Ethereum. Ethereum aims to decentralize any and all interactions happening over a network in a similar way Bitcoin decentralized value and trust. It runs on a blockchain with a native currency called - ether, has 1400 nodes and has a blockchain speed(the rate at which new blocks get added to the chain) of around 12-17 seconds per block. One of the main goal behind ethereum is to decentralize the internet via DApp concept, the idea being instead of hosted on a specific central servers in a server farm, the application(s) can reside throughout random nodes of P2P network of the underlying blockchain just like bitcoins.
Ethereum supports smart contracts by providing a blockchain packaged with a Turing-complete programming language. This enables any organisation or individual to encode a business logic in form of computer program and implement it as a smart contract to control asset ownership and funds transfer. It should be noted that contracts here can be termed as individual autonomous entities existing inside Ethereum execution environment. These autonomous entities always execute a specific set of instructions when triggered by a message or transaction and have a direct control of their own assigned assets and database.[7]

An Ethereum based smart contact is a computer program with its own small database and assigned assets, which can only be modified by the owning program. Once such a contract is created it exists passively in the Ethereum execution environment waiting for it to be activated via a certain message or transaction. And once activated this program executes modifying its own database, triggering other events and sending a response to the activating message. All of these steps are performed in the exact same way at all the nodes in the network generating precisely exact results and thus maintaining consistency.

These are the basic five steps in which an Ethereum based smart contract work -
1. Encoding a complex business logic in terms of computer programs.
2. Listing the events that would trigger the computer program into execution.
3. Using digital signatures to verify the ownership of the triggering events.
4. Deploying the computer program, events and digital signatures on the block chain.
5. On receipt and verification of triggering event on every node executing the specific computer program on every node of the network. [6]
Computer programs are deterministic in nature, meaning a program should essentially produce the exact same output at one node that it produced at any other node given the same input variables. This makes the last step in the above algorithm a bit of overkill and waste of computation resources as the program can be executed at specific predesignated nodes and changes can be synchronised with all other nodes. The last step of execution of program at every single node on receipt of triggering message also leads to- halting problem where a node is not sure when the specific program will finish execution and if a node is allowed to kill execution in middle, there will arise inconsistent copy of records about the result of that computation. Concurrency is another problem faced by nodes in such networks when all of them try to run a computer program based on some input messages. As we know that messages coming to nodes in a block chain are in no specific order but the program in the contract might contain instructions that are dependent on the order of execution generating different results if executed in different order. Thus the transactions can not be processed until their order of execution is determined in the blockchain.[6]

V. DAO and Provenance Tracking

Decentralized autonomous organisations(DAO) can be essentially described as an organisation without a central control structure such as a CEO or Board of directors. Instead in such an organization control is decentralized and distributed among the nodes of the P2P network which forms the structure of this organisation. All the decision making process is reached via a majority consensus over this network. Thus DAO in simple terms is a network of people interacting with each other to reach a consensus on execution of certain action. The BitCoin blockchain network is a very basic example of a DAO where people interact and come to a consensus regarding the decision of currency/value transfer. In the current economic scenario it can be observed that different parties involved in an organisation are bound by certain legal contracts. As humans we end up making this scenario complicated as - sometimes knowingly or unknowingly people do break rules and also not everybody agrees on what the rules actually imply. With the advent of crowdfunding techniques this scenario gets more complex, on one hand it makes it easier for minor investors to

invest in large projects and the entrepreneurs to receive funds which were not so easily available in the past. This can lead to a scenario where minor investors might feel that they do not have much say in the corporates decision making process because of their low stakes. And thus they might disagree and undermine the decisions taken by such crowdfunded projects. On the other hand the decision makers in such projects might feel under pressure to take the decision that they consider profitable and go under a business risk, without a majority consensus of the people funding the project. The idea of a Decentralized Autonomous Organisation aims to address these problems by making - participants of the organisation in direct control of the available funds and decision making process, by formalizing and deploying the binding organisation rules in terms of contracts(computer programs) over the network.[9]
Provenance Tracking is another important use case of block chain architecture. In current production-supply scenario, supply chain might be highly distributed and involve several parties. This leads to the room for cheating and theft over the ownership of expensive products involved such as - electronics, pharmaceuticals, diamonds/jewellery, heavy machinery etc. The blockchain method of tracking of ownership can provide a safe way to interact and transfer such high value resources among the network without being worried about false change of ownership. This process works by generating a digital token whenever a product of high value is created in the network, which authenticates the origin of product. Every time the product changes custody in the physical world, the token is moved in parallel thus tracking the real world custody transfers of the product in the blockchain. Once the end user gets this product, it can verify the origin and track the chain of custody all the way back to origin with the help of this digital token. This system of tracking the product in supply chain works better than a database maintained by producer or delivering- middleman organisations because it eliminates the need for a central database which might be controlled by a single organisation. The records of custody are maintained in a blockchain making it more secure, robust and tamper proof, also providing anonymity and privacy to the end user. Similar to high value goods, the provenance of property such as a piece of land or a house can also be monitored and recorded using a blockchain system. This kind of system can give rise to a whole new way of provenance tracking contrast to current existing systems - making them totally decentralized without involvement of any federal organizations.[10]

VI. Conclusion

In this paper we discussed the basic building blocks of a blockchain architecture and its functionality. We discussed in detail about well known applications of blockchain such as BitCoins and Ethereum Smart Contracts. Finally we also mentioned about some other efficient use cases of this technology such as - DAO and Provenance tracking. The blockchain technology is still young and nascent and needs more vision and experiments to see what use cases it efficiently fits in and what does not work. But it would be safe to conclude that this technology has the potential to become one of the ground breaking techniques developed that would change the entire way business work today leading to a decentralized, fully automated economy. A blockchain service can be loosely compared to a service such as Wikipedia whose contents are generated and maintained by the network of users. Thus the service can be as good as its users and peer reviewers and in order to get the full potential out of blockchains we need to make them simpler and more readily available to end users with minimum technical know how. There have been past incidents such as - Silk Road(drug trafficking via bitcoins) and Ethereum DAO hacks that put this whole technology into shadow, but it is important to understand that any piece of technology comes with its pros and cons. And in order to derive successful benefits out of it we need to focus more on the positive aspects while continuously striving towards eliminating the negative parts.

Acknowledgment

The author would like to thank Dr Ansgar Bernardi for the conitnous help and metoring provided.

References

[1] Sloane Brakeville (sbrakev@us.ibm.com) and Bhargav Perepa *Blockchain basics: Introduction to business ledgers - Get to know this game-changing technology and IBM's contribution to it* 2016.

[2] Khan Academy Bitcoin: Transaction block chains.

[3] The block is hot: a survey of the state of bitcoin regulation and suggestions for the future. Misha Tsukerman

[4] Mastering BitCoin - http://chimera.labs.oreilly.com/book

[5] Bitcoin wiki https://en.bitcoin.it/wiki

[6] Smart contracts:The good, the bad and the lazy. Posted November 2, 2015 by Gideon Greenspan (http://www.multichain.com/blog/author/gdg/) in Private blockchains (http://www.multichain.com/blog/category/private-blockchains).

[7] A Next-Generation Smart Contract and Decentralized Application Platform (https://github.com/ethereum/wiki/wiki/White-Paper)

[8] Formalizing and Securing Relationships on Public Networks, 1997 Nick Szabo

[9] Decentralized autonomous organization to automate governance final draft. Christoph Jentzsch

[10] Four genuine blockchain use cases. Posted May 10, 2016 by Gideon Greenspan (http://www.multichain.com/blog/author/gdg/)in Private blockchains (http://www.multichain.com/blog/category/private-blockchains/).