Block chain technology: Paradigm shift in Business

Alakananda K P [1] Poornima Hegde [2] Sangeetha B K [3] Ramya M [4]
Department of Computer Science [1, 3] Department of Electronics [2, 4]
Trans-disciplinary Research Centre, The National College, Bangalore
And
Florida State International University, USA

Abstract:

Block Chain Technology is creating significant interest across the globe. It has spread its roots into various frontiers like finance, healthcare, industries, forecasting, energy management, payment and money transfers, trade, cyber security, networking and IoT, voting and other application where transparency and decentralization acts as the key players. Block chain technology has a number of features like distributed shared public ledger, digitally signed transactions, chained blocks, public processing nodes, Blockchain integrity algorithm, and flat ledger. These features have the potential to significantly transform financial technology as long as they are tailored to match the confidentiality, data protection, regulatory compliance, reliability, and scalability needs of financial institutions.

Keywords: *Block chain Technology, Intermediary, Smart contract, Ethereum.*

1. INTRODUCTION:

Blockchain technology was first described in a 2008 in pseudonymous paper by Satoshi Nakamoto as a decentralized, public, cryptographically empowered currency system for monetary transaction without going through a financial institution. A block chain is an incorruptible digital ledger of economic transactions that can be programmed to record not just financial transactions but virtually everything of value. [3] Information held on a Blockchain exists as a shared and continually reconciled database. This is a way of using the network that has obvious benefits. The Blockchain database isn't stored in any single location, meaning the records it keeps are truly public and easily verifiable. No centralized version of this information exists for a hacker to corrupt. Hosted by millions of computers simultaneously, its data is accessible to anyone on the internet [1]

Blockchain Technology relies heavily on fundamental tools from Cryptology and Data Security, especially in terms of message authentication targeted towards tamper-evidence and tamper-resilience. In its most abstract form, a Blockchain may be described as a tamper-evident ledger shared within a network of entities, where the ledger holds a record of transactions between

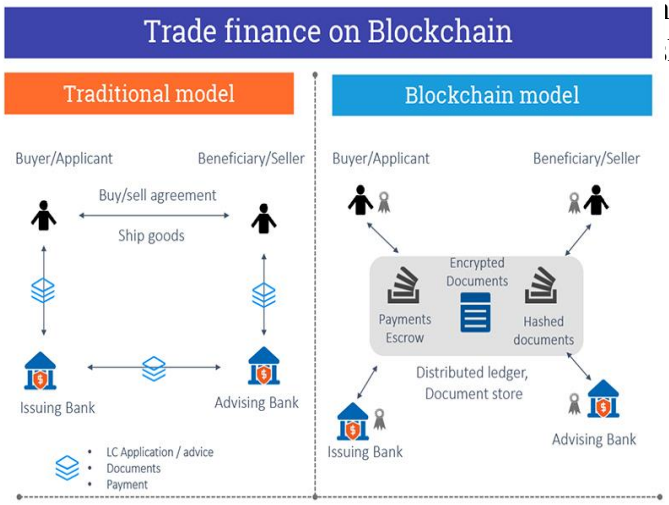


Fig 1: Traditional model v/z Block Chain Model.

1.1 The features of Black chain technology are

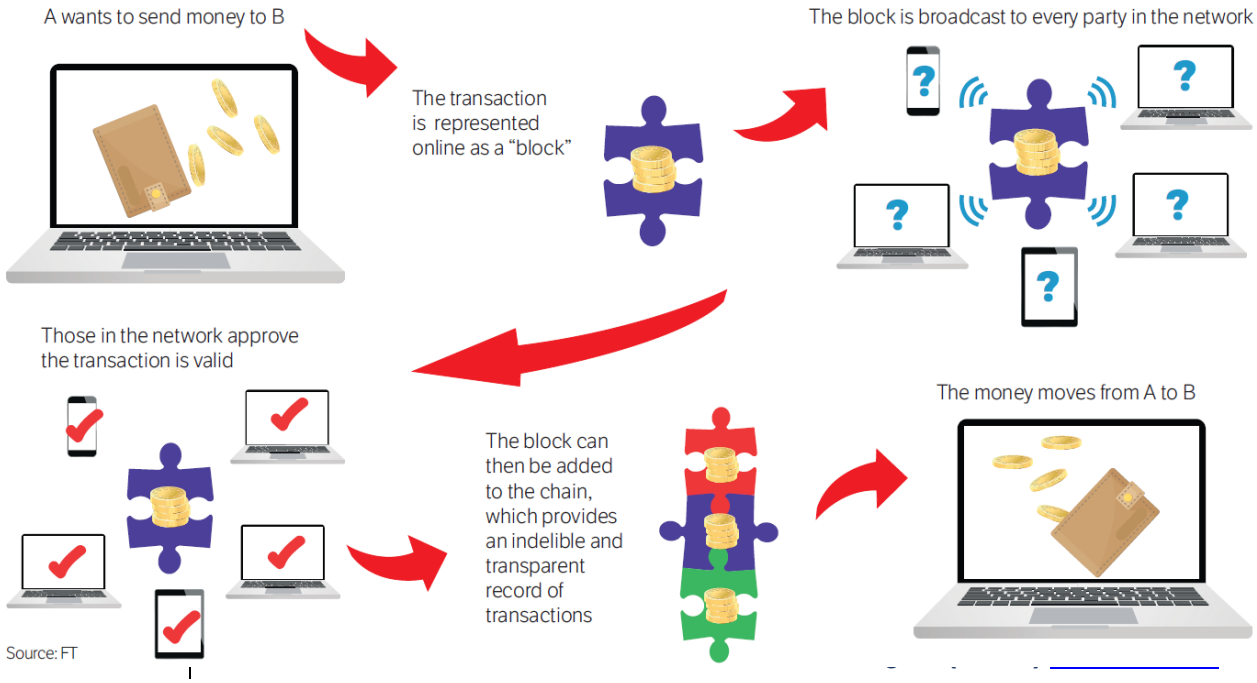
- Block chain cannot be controlled by a single entity.
- They have no single point failure.
- They live in a state of consensus where they check in with themselves for every ten minutes.
- It's a kind of self-auditing ecosystem of a digital value i.e. the network reconciles every transaction that happens in ten-minute intervals.
- The data embedded within the network is transparent.
- The data cannot be corrupted as altering any unit of information on the Blockchain would mean using a huge amount of computing power to override the entire network.
- They are decentralized i.e. the network is referred as a peer-to-peer network were data is not centralized but is visible and accessible by all the peers of the network.
- The network eliminates the middleman.
- Lacks in vulnerability and hence safe from hackers.

Fig 2: Transaction process in Block Chain Technology

- Uses strong encryption technologies.[1]

1.2 Transaction process in a Block Chain Network:

In conventional method the transaction process between two parties A and B would have needed a third party like say a bank or a broker. The Block Chain technology eliminates the third party by means of distributed ledger system. Here the transaction between A and B is transparent to all the other nodes in the Block chain network. These nodes will validate the transaction by checking the previous ledger entries. Once the transaction is authenticated the transaction happens and new transaction block is added to the already existing chain. Once added a block cannot be tampered with science all the nodes on watch for any new transaction or alteration.



I. Source: FT

2 BLOCK CHAIN TECHNOLOGY IN FINANCE:

Block chain technology can be applied to financial services in the following areas:

- Smart Securities via Smart Contracts
- Post Trade Processing and Settlement
- Loan Origination and Servicing
- Foreign Exchange Markets
- Derivatives Markets
- Record-Keeping Processes
- Auditing and Corporate Compliance

2.1 The advantages of block chain technology in finance are

- **Cost saving:** the commission paid to the bank in order to facilitate a transaction can be eliminated.
- **Efficiency:** the transactions can be secure and speed of transactions can be included.
- Wrong entries are avoided since all the peers can monitor the transaction record.
- **Smart contracts** can be drawn using block chain technology for timely trading between traders.
- **The trust** a party has on the bank is replaced by the peer-to-peer network i.e. the transaction records of both the parties are transparent to the other which enables fair trading environment. [4]
- **Fully Distributed System:** No centralized authority like banks.
- **Transparency:** All transactions are publically recorded and available for scrutiny.
- **Security:** The ledger is distributed across thousands of computers, meaning a practical hack is near-impossible.
- **Risk:** No single authority has control, which means if there is a fault, the rest of the network continues.
- **Privacy:** The user is anonymous and doesn't need to provide ID credentials.
- **Dependency:** Use of the block chain eliminates dependency on the base layer service for functionality.
- **High Network Effects:** There can be substantial benefits from very large groups of people (or even everyone) using the same service.

2.2 Limitations and Challenges:

Blockchain technology has also some technical challenges and limitations that have been identified. They are

- Throughput
- Latency
- Size and bandwidth
- Security
- Wasted resources
- Usability
- Corporate Shareholder Voting
- Reducing Counterparty Risk
- Cross-Border Payments

3 Block Chain technology in Capital market:

Banks and financial institutions maintain assets like cash, equity, bonds, and open derivate contracts in customer accounts. These accounts are maintained in their internal accounting systems like core banking systems or position management systems in the form of ledgers. One key function of these institutions is to enable the movement of assets across customers and entities. In the case of cash, it is about fund transfer, online or offline payments, bill payments, and more. In the case of capital markets, it is about security issuance, position maintenance, asset servicing, trading, clearing, and settlement. For the movement of assets from one institution to another, the ledger balances of these assets have to move [2].

The number of messages to be exchanged and ledgers to be updated, increases proportionately with the number of intermediaries in the transaction. For instance, in the capital markets industry, there are several intermediaries like exchanges, Central Counter Parties (CCPs), Central Securities Depositories (CSDs), brokers, custodians, and investment managers that help complete the investment transaction of a customer.

These intermediaries need to update their respective ledgers based on the messages exchanged between them to complete a business transaction. Thus, every time a transaction flows through an intermediary, it involves additional messaging, delays, and costs. Sometimes, to enable a particular transaction and the corresponding ledger updates, intermediaries may need to complete a few additional ledger transfers in the form of realignment, securities borrowing, or cash management. This introduces additional delays in the transaction lifecycle and is usually referred to as a settlement cycle in capital markets. [2]

Blockchain can help banks transform from isolated, hierarchical ledgers with point to point communication models (that exist today) to shared flat ledgers with an ability to process peer-to peer transactions. Digital signatures and encryption ensure necessary data protection and privacy needed for financial data. Immutability and 'append-only' data structures enable improved auditability and replication among financial institutions.

However, there are additional benefits to blockchain that are not feasible with existing technology. Having all participants operating from their own local version of the golden source reduces system duplication, with the associated cost and risk of errors. There is no mass demand placed on any central authority, reducing the risk of it being overloaded. Counterparties can bilaterally reveal information to each other without querying the centre. With no central authority, there is no single point of failure. Entries into the blockchain are irrevocable once agreed, so there is a reduced risk of manipulation (to change an entry, one needs to change all subsequent versions of the ledger, although this presents certain challenges that are discussed later). Distributed ledger functionality also allows more sophisticated smart contracts to be used, and the full benefits to be realised. [2]

4 Block Chain in Banking Sectors:

Block Chain Technology has the potential to replace the conventional method of trading or financial transaction eliminating the role of a bank as the financial intermediary. A financial intermediary is a financial institution such as bank, building society, insurance company, and investment bank or pension fund. It offers services to help an individual or a firm to save or borrow money.

Banks intermediates transaction between two parties, who might be strangers to each other but have trust on the bank to smoothen the transaction. Banking is all about trust. Trust plays an important role in trade and a bank provides a secure environment for transactions to take place between two parties.

We trust that the bank will have our money for us when we go to get it. We trust that it will honour the checks we write to pay our bills. The thing that's hard to grasp is the fact that while people are putting money into the bank every day, the bank is lending that same money and more to other people every day.

4.1 Role of a bank as a financial intermediary:

Financial intermediation is the process performed by banks of taking in funds from a depositor and then lending them out to a borrower. The banking business thrives on the financial intermediation abilities of financial institutions that allow them to

lend out money at relatively high rates of interest while receiving money on deposit at relatively low rates of interest. Direct lending between savers and borrowers is like barter, inefficient. In order for financial transactions to be completed there must be a double coincidence of wants. People with saving will have a given amount of funds that they will want to lend for a particular time period[7]. They will need to find someone to lend to with matching circumstances, the same approximate amount of funds and the same time period.

Another problem encountered by lenders is that they will have limits ability to diversify and minimise their exposure to default risk. Financial intermediation resolves this problem. A financial intermediary offers a service help an individual or firm to save or borrow money. Some of the roles played by banks as financial intermediaries are as follows

- Pooling the resources of small savers.
- Mobilising wholesale finance and lines of credit.
- Providing safekeeping, accounting and payments mechanism for resources.
- Providing liquidity.
- Diversifying risk.
- Collecting and processing information [7].

4.2 Some of the advantages of having financial intermediaries include the following:

- Lower search coast: A person doesn't have to search for the right lenders.
- Spreading risk: An individual's money is lent to a variety of borrowers which will reduce the risk of loss of ones funds.
- Economies of scale: a bank can become efficient in collecting deposits, and lending. This enables economies of scale-lower average costs.
- Convenience of amounts: if a person want to borrow $1000 it would be difficult to find someone who wanted to lend exactly $1000. But, a bank may have 1000 people depositing $10 each.[7]

4.3 Potential Problems of Financial Intermediaries:

- There is no guarantee that a bank will spread the risk. Due to poor management, they may risk depositor's money on ill-judged investment schemes.
- Poor information.
- They rely on liquidity and confidence. To be profitable, they may only keep reserves of 1% of their total deposits. If people lose confidence in the banking system, there may be a run on the bank as depositors ask for their money back. But the bank won't have sufficient liquidity because they can't recall all their long-term loans. [7]

5 Smart Contracts:

The challenge of latency in block chain technology is due the quick transfer of money but there might be a delay in the delivery of the goods purchased because of the distance between the trading parties. In these cases a contract has to be drawn. Traditionally physical contracts, such as those created by legal professionals today, contain legal language on vast amounts of printed documents and heavily rely on third parties for enforcement. This type of enforcement is not only very time consuming, but also very ambiguous.

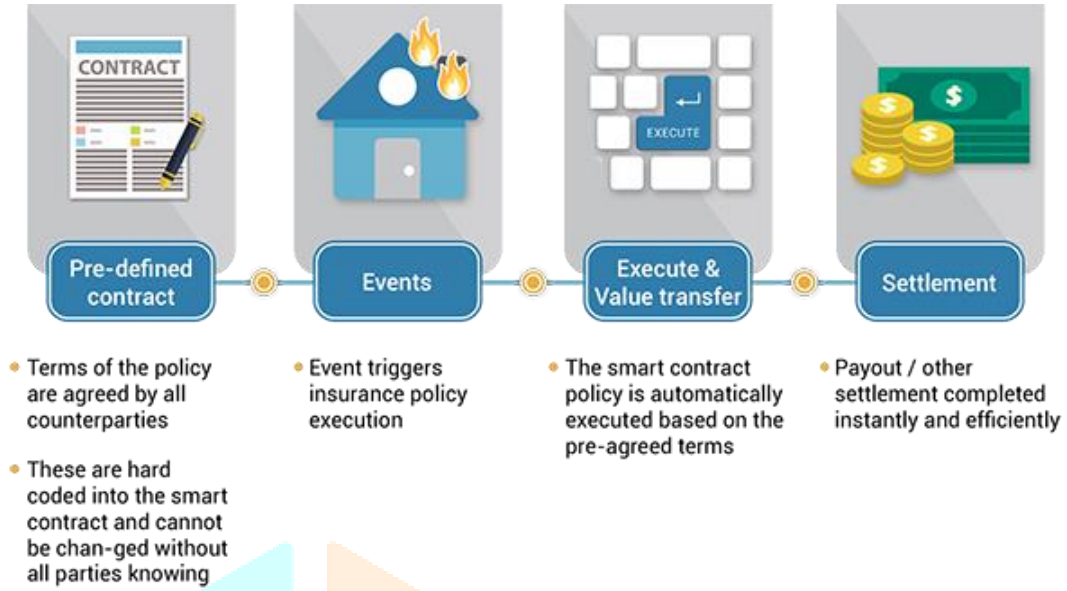


Fig 3: working of a Smart Contract

If things go astray, contract parties often must rely on the public judicial system to remedy the situation, which can be very costly and time consuming [8]

To overcome such risks a smart contract can be used. Smart contracts are also called as digital contracts, they are simply computer programs that act as agreements where the terms of the agreement can be pre-programmed with the ability to self-execute and self-enforce on its own. The main goal of a smart contract is to enable two anonymous parties to trade and do business with each other, usually over the internet, without the need for a middleman. Smart contracts helpsoneto exchange money, property, shares or anything of value in a transparent, conflict-free way, while avoiding the services of a middleman. [9].Smart contracts solve the problem of intermediary trust between parties to an agreement, whether that is between people transferring assets like property, or executing decisions between the two parties as specified in the contract. [10]

Smart contracts not only define the rules and penalties around an agreement in the same way that a traditional contract does, but also automatically enforce these obligations. [9]

For example if A wants to buy anitem from B and want to pay $xxx at a specific time in future then a set of preconditions are met, the conditions, payout, and parties' details would be programmed into a smart contract. Once the defined conditions are met, Money would be released and sent to the appropriate party as per terms. [9]

Smart contracts represent a next step in the progression of block chains from a financial transaction protocol to an all-purpose utility. They are pieces of software, not contracts in the legal sense, that extend block chains' utility from simply keeping a record of financial transaction entries to automatically implementing terms of multiparty agreements. [11]

Smart contracts are executed by a computer network that uses consensus protocols to agree upon the sequence of actions resulting from the contract's code. The result is a method by which parties can agree upon terms and trust that they will

be executed automatically, with reduced risk of error or manipulation [11]

For example, suppose Sam wants to rent an apartment from Dan. Sam can do this through the block chain by paying in crypto currency. He will get a receipt which is held in the virtual contract. Dan will give the digital entry key which comes to Sam by a specified date. If the key doesn't come on time, the block chain releases a refund. If Dan sends the key before the rental date, the function holds it, releasing both the fee and key to Sam and Dan respectively when the date arrives. The system works on the If-Then premise and is witnessed by hundreds of people, so one can expect a faultless delivery. If Dan gives the key to Sam, then he is sure to be paid. If either one fails on the terms agreed then the document is automatically cancelled after the time, and the code cannot be altered by either party without the other knowing, since all participants are simultaneously alerted. [9]

6 Ethereum

Ethereum is an open-source, public, block chain-based distributed computing platform featuring smart contract (scripting) functionality, which facilitates online contractual agreements. It is a decentralized hence runs smart contracts applications that run exactly as programmed without any possibility of downtime, censorship, fraud or third party interference. In Ethereum all smart contracts are stored publicly on every node of the block chain, [12]

These apps run on a custom built block chain, an enormously powerful shared global infrastructure that can move value around and represent the ownership of property. This enables developers to create markets, store registries of debts or promises, move funds in accordance with instructions given long in the past (like a will or a futures contract) and many other things that have not been invented yet, all without a middle man or counterparty risk.[13]

Ethereum includes a digital currency called ether. Ether has a lot in common with the famous digital currency Bitcoin. Both are a purely digital store of value and means of exchange that cannot be counterfeited. Both are implemented so that no one can manipulate the currency supply. Both can be transferred around the world, like email, and in a very final way, like cash. Both have value today because users expect them to have value tomorrow, and because they can do things traditional money can't. [13]

Ethereum's other half is a complete programming language, sometimes called EtherScript. A programming language is how people tell computers what to do. Computers are not able to guess at what humans really intend, so instructions written in any programming language are precise. There is no ambiguity about how a computer will run a program. Under the same conditions, it will always run in the same way. This feature would be great to have in legal contracts and human law. [14]

6.1 Advantages of smart contract

- **Autonomy** – You're the one making the agreement; there's no need to rely on a broker, lawyer or other intermediaries to confirm. Incidentally, this also knocks out the danger of manipulation by a third party, since execution is managed automatically by the network, rather than by one or more, possibly biased, individuals who may error.
- **Trust** – Your documents are encrypted on a shared ledger. There's no way that someone can say they lost it.
- **Backup** – Imagine if your bank lost your savings account. On the blockchain, each and every one of your friends has your back. Your documents are duplicated many times over.

- **Safety** – Cryptography, the encryption of websites, keeps your documents safe. There is no hacking. In fact, it would take an abnormally smart hacker to crack the code and infiltrate.
- **Speed** – You'd ordinarily have to spend chunks of time and paperwork to manually process documents. Smart contracts use software code to automate tasks, thereby shaving hours off a range of business processes.
- **Savings** – Smart contracts save you money since they knock out the presence of an intermediary. You would, for instance, have to pay a notary to witness your transaction.
- **Accuracy** – Automated contracts are not only faster and cheaper but also avoid the errors that come from manually filling out heaps of forms.[10]

CONCLUSION: The use of block Chain technology in the field of finance has many merits over the conventional methods. It helps to smoothen the trade process with an unknown party without a financial intermediary. It avoids faking of the transaction history and has a transparency due to which the risk of forging is completely eliminated.

REFERENCES:

[1] "Application of Blockchain Technology to Banking and Financial Sector in INDIA" An IDRBT Publication, January 2017.
[2] Blockchain in Capital Markets, the Prize and the Journey February 2016 by Oliver Wyman.
[3] https://blockgeeks.com/guides/what-is-blockchain-technology
[4] Jesse Yli-Huumo1, Deokyoon Ko2, Sujin Choi4*, Sooyong Park2, Kari Smolander3 , "Where Is Current Research on Blockchain Technology?—A Systematic Review", PLOS ONE | DOI:10.1371/journal.pone.0163477 October 3, 2016 1 / 27
[5] Health care usecase: catalyst .nejm.org/decoding_blockchain_technology_health
[6] www.thebalance.com
[7] www.wikihow.com
[8] www.herald.co.zw/importance-of-financial-intermediation
[9] www.blockchaintechnologies.com
[10] www.huffingtonpost.com
[11] www.blockgeeks.com/guides/smart-contracts
[12] www.Deloitte.com,DeloitteUniversity press
[13] www.wikipedia.com
[14] www.Etheruem.com
[15] www.Etherscripter.com

FIGURE:

1.http://www.virtusapolaris.com/images/content/blockchain/4.jpg
2.https://fhhwz.ch/content/uploads/2016/08/bidl-blockchain-bitcoin-technology-banking-fintech-FT.png
3. https://www.draglet.com/wp-content/uploads/2017/02/Smart-contracts-in-insurance-policies.png