**Blockchain Banking**

**ABSTRACT**

The Blockchain is an encrypted database that stores information statistics, or in different words, it is a virtual ledger of any transactions, contracts - that needs to be independently recorded. One of the key capabilities of Blockchain is that this virtual ledger is out there throughout several masses and heaps of computer and isn't always sure to be stored in a single place. Blockchain chain has already commenced disrupting the financial offerings area, and it's far this technology which underpins the virtual currency- bitcoin transaction. The aim of the paper is to conduct research on the effect of blockchain technology on the financial sector. There is no doubt that the world is curious to see how this promising technology will influence or shape the future of banking. Blockchain enhances safety in data storage and transmutation, avails a decentralized and transparent network infrastructure and significantly reduces the costs in operations. These remarkable attributes make blockchain a very promising and in-demand solution even in an industry as restricted as the banking sector.

**INTRODUCTION**

A blockchain is a distributed digital ledger where transactions can be recorded and checked electronically over a network of computers in the absence of a central ledger. Cryptography is used to protect the data from deception or hackers. Blockchain is being called “the new internet”, and is expected to transform businesses across various sectors, most importantly the financial sector. It was invented by “Satoshi Nakamoto” in 2008. A blockchain helps to record all the transactions made so that no alterations can be made later on so as to maintain the security of the data. Today, entities maintain records in their own traditional ledgers for transactions between them. This sometimes leads to transfer or exchange of a considerable amount of data between entities, resulting in an increase in time and cost for them. It also makes the process of any asset transfers inefficient, costly and vulnerable. The duplicated shared ledger concept in blockchain technology can help remove these weaknesses. The use of smart contracts, an application of blockchain technology, can enhance efficiency through event-triggered mechanisms. Most credit and budgetary organizations can't do their work without various go-between, while their interest makes the administrations of these establishments substantially more costly. The execution of blockchain will empower pointless arbiters to be relinquished and give clients and banks less expensive administrations. The fundamental zones in which banks and other budgetary organizations will probably actualize blockchain innovation: Payment, Client Identification framework, Loans, and Credits protection.

**LITERATURE SURVEY**

**Invention and importance of blockchain**

Satoshi Nakamoto sketches out a new method for peerto-peer digital cash gadget, the use of a cryptocurrency known as bitcoin. It became an appreciable improvement. Cryptocurrencies (virtual currencies) aren't constructed or aren't in fee of the government. They have got their own set of policies to follow. This type of association has come to be the very new blockchain era, which was the bottom for the growing numbers of authorizing expended blockchain. Blockchain era permits exchange cash without intermediaries. Thus, humans ship cash immediately and correctly and with none trouble at ten same times. It's miles one of the maximum promising and revolutionizing inventions. Attested to be as large to the internet or energy. Sadly, very few have heard of the era but significant social media coverage is assisting. It is one of the maximum promising and positive new era for the coming era. It’s an allotted ledger generation that roots bitcoin. Presenting a new manner to record, preserve the records and transfer the records. Even greater incredible is the transparent, and secure statistics, this is auditable and proof against blackout.

**Blockchain an underlying technology of bitcoin**

Many humans count on that blockchain and bitcoin are identical. Blockchain is the underlying generation of bitcoin. They're intently associated, however, they're no longer the same factor. In 2008, bitcoin turned into introduced as a form of unregulated virtual currency created through Satoshi Nakamoto. Blockchain was the ledger answer used to safely record facilitating using this new forex when you consider that there has been no bank or government involved to reveal or police the transactions. The confusion between blockchain and bitcoin regularly arises because those two concepts have been introduced at the identical time. The blockchain era as for instance the only used for bitcoin allows for the recording of transactions on an allotted ledger across a community of users. The open-source era allows for the garage of records from the transactions into blocks. Each block consists of a time-stamped report of the transactions with each block related to the previous one, for that reason developing a series. The records saved at the blockchain is absolutely obvious and everlasting without the potential to trade or take away previous transaction facts from the dispensed ledger. This characteristic and answer can be used to resolve many inefficiencies in unique packages and industries.

**Practical byzantine fault tolerance**

This paper describes a new replication algorithm that is able to tolerate Byzantine faults. We believe that Byzantinefault-tolerant algorithms will be increasingly important in the future because malicious attacks and software errors are increasingly common and can cause faulty nodes to exhibit arbitrary behaviour. Whereas previous algorithms assumed a synchronous system or were too slow to be used in practice, the algorithm described in this paper is practical: it works in asynchronous environments like the Internet and incorporates several important optimizations that improve the response time of previous algorithms by more than an order of magnitude. We implemented a Byzantine-fault-tolerant NFS service using our algorithm and measured its performance. The results show that our service is only 3% slower than a standard un-replicated NFS.

**Multi-Chain Private Blockchain**

Bitcoin is now recognized as a cheap, rapid and reliable method for moving economic value across the Internet in a peer-­to-­peer manner. Aside from a brief fork between incompatible versions in March 2013, the bitcoin network has been operating continuously and smoothly for over 5 years. Although there have been losses and thefts of bitcoins belonging to individual holders, the network itself has never been successfully attacked or impeded. Despite bitcoin’s many technical achievements, it is far from reaching mainstream consumer or business adoption. Judging by the current trend in transaction volumes , the sluggish growth of 1 bitcoin usage shows no sign of changing in the foreseeable future. This is despite the availability of many easy ­to ­use bitcoin wallets and the fact that bitcoin can now be spent online at many mainstream businesses such as Microsoft, Dell and Overstock. There are many possible causes of bitcoin’s slow adoption, including: (a) end­user satisfaction with existing payment systems, (b) the practical difficulty of purchasing bitcoins, (c) the volatility of bitcoin’s value relative to government­ issued currencies, (d) the perception that bitcoin is insecure, (e) questions over bitcoin’s legal status, (f) the irreversible and unforgiving nature of bitcoin transactions, and (g) a lack of support for bitcoin in the mainstream financial sector. In the absence of end­user adoption, many have suggested that bitcoin could help improve internal processes within the traditional financial sector, by lowering costs, reducing settlement times and eliminating intermediaries. One immediate theoretical possibility is using bitcoin as a currency and conduit for rapid inter­bank settlement. However the volatility of bitcoin’s value relative to government ­issued currencies renders this unworkable in practice. A more promising direction is to use bitcoin’s infrastructure to transact in assets other than bitcoin itself.

**The quest for scalable blockchain fabric: Proof-of work vs. bft replication**

Bitcoin cryptocurrency demonstrated the utility of global consensus across thousands of nodes, changing the world of digital transactions forever. In the early days of Bitcoin, the performance of its probabilistic proof-of-work (PoW) based consensus fabric, also known as blockchain, was not a major issue. Bitcoin became a success story, despite its consensus latencies on the order of an hour and the theoretical peak throughput of only up to 7 transactions per second. The situation today is radically different and the poor performance scalability of early PoW blockchains no longer makes sense. Specifically, the trend of modern crypto-currency platforms, such as Ethereum, is to support execution of arbitrary distributed applications on blockchain fabric, needing much better performance. This approach, however, makes crypto-currency platforms step away from their original purpose and enter the domain of database-replication protocols, notably, the classical state-machine replication, and in particular its Byzantine fault-tolerant (BFT) variants. In this paper, we contrast PoW-based blockchains to those based on BFT state machine replication, focusing on their scalability limits. We also discuss recent proposals to overcoming these scalability limits and outline key outstanding open problems in the quest for the “ultimate” blockchain fabric(s).

**Difficulty control for blockchain-based consensus systems**

Crypto-currencies like Bitcoin have recently attracted a lot of interest. A crucial ingredient into such systems is the “mining” of a Nakamoto blockchain. We model mining as a Poisson process with time-dependent intensity and use this model to derive predictions about block times for various hash-rate scenarios (exponentially rising hash rate being the most important). We also analyse Bitcoin’s method to update the “network difficulty” as a mechanism to keep block times stable. Since it yields systematically too fast blocks for exponential hash-rate growth, we propose a new method to update difficulty. Our proposed method performs much better at ensuring stable average block times over longer periods of time, which we verify both in simulations of artificial growth scenarios and with real-world data. Besides Bitcoin itself, this has practical benefits particularly for systems like Name coin. It can be used to make name expiration times more predictable, preventing accidental loss of names.

**Bitcoinng: A scalable blockchain protocol**

Cryptocurrencies, based on and led by Bitcoin, have shown promise as infrastructure for pseudonymous online payments, cheap remittance, trustless digital asset exchange, and smart contracts. However, Bitcoin-derived blockchain protocols have inherent scalability limits that trade-off between throughput and latency and withhold the realization of this potential. This paper presents Bitcoin-NG, a new blockchain protocol designed to scale. Based on Bitcoin's blockchain protocol, Bitcoin-NG is Byzantine fault tolerant, is robust to extreme churn, and shares the same trust model obviating qualitative changes to the ecosystem. In addition to Bitcoin-NG, we introduce several novel metrics of interest in quantifying the security and efficiency of Bitcoin-like blockchain protocols. We implement Bitcoin-NG and perform large-scale experiments at 15% the size of the operational Bitcoin system, using unchanged clients of both protocols. These experiments demonstrate that Bitcoin-NG scales optimally, with bandwidth limited only by the capacity of the individual nodes and latency limited only by the propagation time of the network.

**Bitter to better – how to make bitcoin a better currency**

Bitcoin is a distributed digital currency which has attracted a substantial number of users. We perform an in-depth investigation to understand what made Bitcoin so successful, while decades of research on cryptographic e-cash has not lead to a large-scale deployment. We ask also how Bitcoin could become a good candidate for a long-lived stable currency. In doing so, we identify several issues and attacks of Bitcoin, and we propose novel techniques to address them.

**EXISTING SYSTEM**

The banks today are faced with issues such as rising costs of operations, increasing sensitivity to fraud attacks on centralized servers and challenges in ensuring transparency. All this are primarily because most of the banking transactions from opening customer accounts to making global payments- may require intensive manual processing and documentation, involve costly intermediaries and is time consuming as these transactions need to be validated by various participants at various point in time causing the delay thereby resulting in an almost lack of fraud-proof realtime solution. Banks are constantly investigating better approaches to perform exchanges faster for better client administration while guaranteeing cost productivity in their tasks and guaranteeing straightforwardness to clients and controllers. For this, blockchain conceivably gives an answer for banks as it inalienably wipes out middle people, keeps up a changeless log of exchanges and furthermore encourages ongoing execution of exchanges This could potentially reduce the time after time for a banking transaction, reducing costs of manual work, and leading to enhanced customer service and satisfaction. Before we come to recognize or recognize all of the topnotch golden possibilities blockchain eras give us for the banking and economic offerings industry, there are some hurdles and headaches we want to overcome.

Disadvantage

1. Less Security.

2. High Cost.

**PROPOSED SYSTEM**

In this paper author is describing advantages Blockchain over traditional centralized banking application as all bank servers runs on centralized server and this server maintain data only in one place and attackers can hack this server and if this happen then entire bank server will be crashed and to overcome from this problem author is suggesting to revert or add Blockchain to banking application.

Blockchain support decentralized storage which means its data will be stored at multiple nodes as a peer to peer network and Blockchain store each record as BLOCK/transaction and associate each block with unique hash code and before storing any new record then Blockchain will verify hash code of each Block and if this Block not changed then only new Block will be added so it’s impossible to change any Blockchain backend record which make Blockchain as immutable. Blockchain has low maintenance cost compare to traditional cost and Blockchain has inbuilt support data cryptography or encryption or data security.

Above advantages of Blockchain are making almost all application to divert to Blockchain so author suggesting to include Blockchain functionality for banking application where user can send and receive money. All Blockchain bank account can be access by using SOLIDITY code often called as SMART CONTRACT and this code can be deployed on Ethereum tool and then using python WEB3 API we can access that solidity code or function to create use account or to deposit and transfer amount.

advantages

1.More Secure.

2. The timeline of the transaction will be reducing as there will be an automation process of transferring money which will benefit the user sending money in any corner of the world.

**MODULES**

**User Login:** User entered the details and login to application.

**Block Chain:** Block chain contract to store and retrieve USERS and bank transactions details.