A BRIEF ANALYSIS ON PREDICTED FUTURE VALUE OF PI NETWORK ON THE BASIS OF BITCOIN

K.M. SADAT SAMIN, BIJOY KUMAR DESHMUKHYA, FARHAN BIN ALAM

DAFFODIL INTERNATIONAL UNIVERSITY

DHAKA, BANGLADESH

sadat15-11930@diu.edu.bd

Abstract

Nowadays, blockchain based cryptocurrency is known to all. Bitcoin is one of the highest value and high demand crypto currencies. Bitcoin is not available for all platforms. Also, not much user-friendly cryptocurrency. But there is an upcoming user-friendly cryptocurrency. Pi Coin, it is designed to be accessible to the general public. This can create a huge impact on the future and also can be a high demand cryptocurrency. Bitcoin already created its crypto demand. On the side, Pi coin is also a hyped cryptocurrency which is waiting for launch. This paper will highlight the prediction of the value of PI coin based on the bitcoin timeline.

Keywords: Blockchain, Cryptocurrency, Bitcoin, Pi Network, Value

INTRODUCTION

In the present era many cryptocurrencies are coming based on block chains. Bitcoin is a famous cryptocurrency. Bitcoin has many obstacles, but still the valuation of Bitcoin has been so high and the amount of value of bitcoin has Up and down and we all know that. But bitcoin is not so much available to people so far and people have to suffer a lot to generate bitcoin. For this reason, pi networks or pi coins created by a few people who have passed out of Stamford or have done their PhD. And the basic purpose of creating it is to make the cryptocurrency available to people. Already its mining is going on. Although the market is not yet available. But based on everything's perspective, based on bitcoin's currency rate in futures, based on how large the pie network can be, paper is being prepared.

CRYPTO CURRENCY'S AVAILABILITY FOR COMMON PEOPLE

There was a small crave to utilize cryptocurrency. On a scale of 10, the number juggling implies an aim to utilize them was a 3. When respondents were addressed approximately their eagerly to utilize cryptocurrencies within the close future, the score hopped to an normal of 4, which is amazingly near to the tipping point between utilizing and not utilizing cryptocurrencies (5). The standard deviations were huge (the coefficient of variety was 1.08 for the purposeful to utilize and 0.83 for anticipated utilize). Given the scattering in deliberate to utilize, it was exceedingly prescribed that an illustrative demonstrate be created to get it bitcoin acknowledgment patterns.

Digital currency has recently become a vast sector and people are adapting day by day. But in many terms, people are still not used to it. And also 78% of people don't have full trust in it. Also, bitcoin or other currencies like bitcoin are not mining-able in their easy devices. It's also made people less dependable on crypto currency. But if there is any friendly and easy usable crypto currency cam changes people's perspective.

BITCOIN

A.   The Fundamentals of Bitcoin

Bitcoin creator Satoshi Nakamoto illustrated an arrangement to the challenges of execution and ease of use in his now-famous work. Experienced by advanced cash, especially the issue of double-spending the issue [12]. While Nakamoto's exact identity remains a mystery, Speculations abound, but what is certain is that he stayed in office until 2010. He was involved on the Bitcoin project for a while, then he took a step back and [7] the project was given to the community for future development.

He proposed a system based on peer-to-peer distributed timestamps. A server that generates the computational proof of concept Transactions are listed in chronological sequence [12]. An electronic device, a chain of digital signatures is characterized as a coin. Each transaction is unique. Is defined as a collection of prior hashes that have been digitally signed. Transaction and the next owner's public key the personal the private key used to sign the transaction, while the public key is used to verify it is demonstrated in Fig. 1 [12], this was utilized to verify the transaction. The public key is stored in the wallet and can be used. Software, hardware, or the internet.
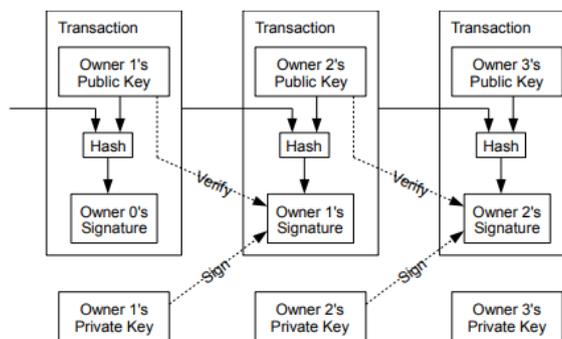

Figure 1. A coin piece with hashed exchanges into a Merkle tree

The Bitcoin record can be a state move system that comprises a state that appears the ownership status of all existing bitcoins and a state move work, which takes the shape of a trade. The state move work returns an advanced state [13]. Within the occasion that the sender has adequate bitcoins to conduct a trade, this technique produces state changes for the sender and beneficiary; something else, it produces a goof.

B. Transactions of Bitcoin

Each exchange contains a hash esteem that speaks to an exchange recognizable proof as well as a collection of inputs and yields. Within the whole blockchain, each exchange yield may be utilized once as an input [7]. Endeavouring to reference the same yield twice comes about in a double-spending problem, which is disallowed within the organisation. It's named an unspent exchange yield (UTXO) in case the transaction's yield hasn't been referenced already, and it's called went through exchange yield (STO) in the event that it has (STXO). An exchange can have up to two yields and different inputs. Different inputs can be utilized to total lesser amounts of coins being sent, with yields being either a sum transmitted to the other party or later returned to the sender [12].

All exchanges and proprietorships within the Bitcoin arrange are recorded on the dispersed record. This P2P network's hubs each store a duplicate of the record [13]. In case a client wishes to transmit a certain amount of coins to another, he can do so by freely pronouncing the exchange, and the organizer will at that point confirm its precision. Be that as it may, a client might attempt to divert the framework by sending a few exchanges of the same cash to other clients (double-spending issue). Furthermore, a single user can create several instances to validate his original purpose and so launch a Sybil assault.

C. Blockchain and proof-of-work

Within the Bitcoin arrangement, these circumstances are maintained a strategic distance from (or at least relieved) by requiring a proof-of-work from each hub that affirms the exchange. To confirm that they are veritable individuals of the organization, the hubs must do a few complex calculations. The framework will remain steady and all true-blue exchanges will occur as long as the overall computational control of the legitimate hubs surpasses the computational control of the assailant [7], [12].

A hash is characterized by a collection of exchanges, as well as the going a few times as of late block's hash and a nonce. A timestamp server makes a hash of a chunk and disseminates it, appearing up that the information contained inside the piece must have existed at the smaller than expected of hashing. The timestamp server must guarantee that the block's timestamp is more basic than the going a few times as of late, and is less than two hours lost. As seen in Fig. 2 [12], these hashes shape a chain, which is suggested as a blockchain. The capacity to require after exchanges back to any point in time may be a fundamental highlight of the blockchain.
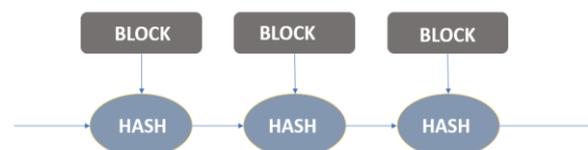

Figure 2. The blockchain conspire

Bitcoin utilizes a proof-of-work hashing calculation comparable to Hash cash [14] and is based on the SHA-256 hash work [15]. The proof-of-work is performed by increasing a nonce within the piece until a value is produced with the desired number of zero bits at the block's hash's starting. It is incomprehensible to switch it without re-trying the calculations. In case it is altered by a pernicious aggressor, all consequent pieces will have off base hashes. The rule is that the longest chain with lion's

share agreement within the arrange is the correct one, hence in the event that an aggressor needs to adjust a block, he'll require sufficient handling control to outflank the larger part of fair hubs, coming about in a race problem.

This tree is utilized to hash the trades interior a chunk [16], [17]. A Merkle tree may be a parallel tree with a sweeping number of leaf hubs, each of which highlights a root that's a hash of its relative. A Bitcoin piece is depicted in Figure 4 as a Merkle tree of trade hashes. Since any botch inside the tree will show up up wherever along the chain, the Merkle tree is fundamental for long-term upkeep [13]. More often than not done to free up capacity on the centers, which is required to hold the blockchain. The Bitcoin blockchain is as of presently 144.8 GB in assess [18]. The orchestrate arranges of all hashes in a tree but the root hash contained inside the piece header after the trades have been combined into a piece and this square has been asserted. Bitcoin displayed Improved Portion Affirmation (SPV), which needs centers to store a copy of the piece headers of the longest chain [12], rather than a add up to record of trades.
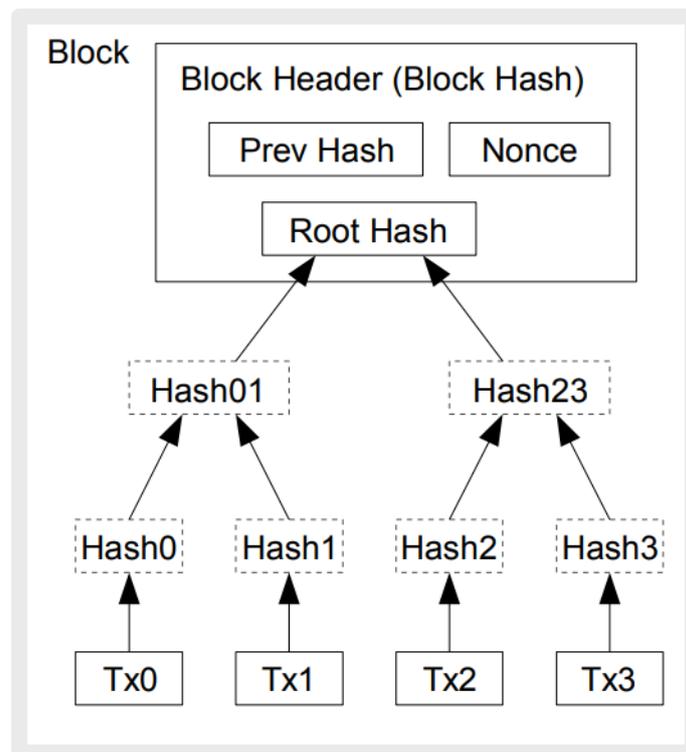

Figure 3. A Bitcoin block with hashed transactions into a Merkle tree

D. Bitcoin mining and the Bitcoin network

The primary exchange in a piece creates a modern cash that has a place to the block's creator [12]. Since there's no central specialist issuing cash, this invigorates hubs to confirm exchanges and puts money into circulation. A Coinbase exchange is the title for this sort of exchange. The hubs have a motivating force to keep legitimate with this technique. The Bitcoin arrangement is planned to create one piece each 10 minutes [13]. Since the handling capacity of the computer develops over time, the blocks term is kept moderately consistent by continuously expanding the complexity of creating unused pieces.

Modern exchanges are broadcast to all hubs at the beginning of the Bitcoin arrangement. Each hub compiles exchanges into a block and looks for proof-of-work, after which it broadcasts its blocks to the rest of the organization. The network's hubs respect a piece as true blue as it were in the event that all of the exchanges inside it are adjusted and have not, however, been gone through. In case the organizer acknowledges the piece, the chain is preceded by creating other blocks and adding the hash of the already added blocks [12].

Aside from the motivating force for making squares, hubs are compensated with bitcoin and for approving exchanges. Mining [7] is the method of making unused squares to the blockchain. The Starting square remunerate was set at 50 coins (50 BTC), after each 210,000 squares the prize would be cut in half. The beginning square is the primary square on the blockchain, and it is utilized to supply the organizer with the primary 50 BTC. The piece era motivating force will proceed to be divided until it falls underneath one Satoshi, which is the littlest unit of Bitcoin and rises to 10-8 BTC [7].

Considering the nature of distributed decentralized systems, there are times when various nodes broadcast the same block practically simultaneously, but with likely distinct sets of transactions. This is referred to as a fork, and it results in the network's inconsistency. Essentially, there are multiple chains that stem from various blocks. This problem is overcome by ensuring that the network always follows the longest chain. Gradually, the network will agree on the proper path for the blockchain, and the chains created as a consequence of a fork will become invalid [7].

E. The issue of Bitcoin's scalability

Bitcoin has versatility concerns due to its 1MB piece estimate. With this piece estimate, the greatest number of exchanges that will be bolstered is less than seven exchanges per moment (tps) [19]. Visa, on the other hand, came to 47,000 exchanges per moment over the 2013 occasions and presently midpoints hundreds of millions each day [20]. To accomplish such a pace on the Bitcoin, with a 1MB square estimate and an exchange measure of 300 bytes, a throughput of 8GB per Bitcoin square each ten minutes would be required, coming in nearly 400TB of information each year [19]. This would intensely concentrate the Bitcoin organization, permitting as it were those hubs with expansive capacity capabilities to take an interest, which is the polar inverse of what Bitcoin and blockchain were outlined for.

A few methodologies have been proposed in arrange to viably address this issue. As a result, there have been a number of Bitcoin delicate and difficult forks. Any adjustment that's in reverse consistent, i.e., permitting ancient program to distinguish naturally delivered squares as authentic, is alluded to as a delicate fork. A difficult fork, on the other hand, could be a arrange computer program overhaul that presents a modern run the show, taking off the ancient program incapable to distinguish unused squares [21].

F. Lightning and SegWit

One of the recommended arrangements to the Bitcoin versatility issue is SegWit (Isolated Witness), which addresses the issue of exchange flexibility. This issue emerges since the exchange signature does not cover all of the information within the exchange, making it simple for a pernicious hub on the arrange to change the exchange and nullify its hash [22].

SegWit permits for a most extreme piece estimate of 4MB and the expansion of a moment layer on best of the display organize [23]. It confines signature information from other exchange information, making the Lightning organize a second-layer convention less demanding to actualize. On the 24th of Admirable 2017, it was actuated on square 481,824 [24].

On the Bitcoin organize, the Lightning arrangement is the "following enormous thing." Its objective is to make micropayments simpler by utilizing an organization of micropayment channels. A micropayment channel is an assertion between two parties to delay informing a exchange to the arrange until after the exchange has been completed. Both parties may guarantee their current adjust on the blockchain, but they pick to put off broadcasting exchange data to the organize [19]. Block stream carried out a successful Lightning network experiment in January 2018 [25].

G. BTC Gold and Cache

As Bitcoin's ubiquity developed, the arrange couldn't keep up with the volume of exchanges, in this way affirmations took days [26]. On Eminent 1st, 2017, a difficult fork of Bitcoin Cache (BCH) happened at piece 478,558. At the time of the fork, those who possessed Bitcoin moreover claimed the Bitcoin Cache. The square estimate was expanded to 8MB, which brought about in speedier affirmation times.

Bitcoin Gold (BTG) is a hard fork of Bitcoin that occurred on the 24th of October, 2017 [27] on block 491,407 [28]. As with Bitcoin Cache, anybody who had Bitcoin before the fork became a Bitcoin Gold owner. The reason for this divide is because Bitcoin was originally mined with ASIC devices rather than CPUs. Bitcoin Gold's authors attempted to remedy this by switching the proof-of-work algorithm from SHA-256 to Equihash [28]. This technique uses a lot of memory and is best suited for mining on graphics processors. In Bitcoin [27], the mining difficulty is modified every time a new block is mined, rather than every 2016 blocks..

IV. PI NETWORK

A. Pi Introduction

Pi was made with the objective of re-democratizing get to to cryptocurrencies by permitting anybody to mine them utilizing promptly accessible innovation, such as a smartphone.[32]

The extend fulfills this by utilizing a variation of the Combined Byzantine Understanding (FBA), which was created by the Stellar blockchain's researchers. The FBA includes a diverse methodology than confirmation of work and the various varieties on confirmation of stake, which depend on one mineworker or validator getting to be the "pioneer" by displaying a square for agreement.[32]

Instead of choosing a pioneer, this agreement depends on hubs picking up ascension on a particular piece through an arrangement of votes conducted through message trade. Byzantine Blame Resistance (BFT), which is actualized in a few blockchains such as Swell, Hyperledger Fabric, and Zilliqa, may be a well-known shape of a calculation that employs such a method to accomplish an agreement. In any case, one evaluate of BFT agreement models, in common is that they have a point of centralization since the framework engineer chooses the voting majority at beginning.[32]

Pi employs an additional layer of FBA to avoid centralization by allowing each node to set its own "quorum slices" in a decentralized manner.[32] Rather than relying on a central authority, this feature allows nodes to decide for themselves whether or not to trust other nodes. [32]

Pi's consensus process uses very little energy since the communications involved in voting are relatively low, especially when compared to proof of work.[32]

B. Pi Mining

By downloading the Pi Organize app to their smartphone, clients can lock in in Pi mining. They can at that point take portion within the Pi agreement in one of four ways:

Pioneers are app clients that fair affirm their nearness each time they log in. Their commitment is to form Pi Organize more freely accessible. They can as of now as it were send and get Test-Pi on the Pi Testnet utilizing their Pi wallets. [32]

Contributors are clients who donate and keep an up-to-date list of pioneers they know and believe. Supporters are eventually helping within the improvement of the worldwide belief chart required for Pi's agreement.[32]

Ambassadors are Pi network users who introduce others to it.

Nodes are pioneers and contributors who also run the Pi node software on a desktop or laptop computer. Pi Nodes perform the heavy lifting of running the consensus algorithm of the blockchain and will use the trust graph aggregated from the trusted pioneers provided by mobile contributors

Participants can play more than one role. Each day, they receive a newly minted Pi based on their participation and contribution. [32]

The current value of Pi is stated as zero. The team behind Pi believes that value can be realized through the creation of utilities of the cryptocurrency where people use Pi to transact goods and services at scale globally. These goods and services will ultimately back the value of Pi.

C. PI KYC & SECURITY

Pi contains a KYC method in put to ensure the network's judgment. To be able to move Pi into the Pi Mininet blockchain, clients must give a duplicate of their ID. This stops individuals from mishandling the framework by making a few accounts, running bots or ranches, and so on. Pi is additionally on its way to be one of the primary and biggest confirmed systems.[32]

The KYC strategy and information are as of now secured by a trusted third-party merchant. Concurring to its protection approach, the company promises to keep client information secure and not to offer or something else abuse

D. A Streamlined Presentation to Stellar Agreement Convention

Pi lives the other sort of assention calculations and is based on the Stellar Assention Tradition (SCP) and an calculation called Bound together Byzantine Understanding (FBA). In spite of the fact that such calculations don't squander vitality, they do require the trade of a few arrange messages in arrange for the hubs to "concur" on what the following piece ought to be. Based on the cryptographic signature

and exchange history, each hub can freely choose whether an exchange is veritable or not, such as specialist to create the exchange and twofold investing. To come to an understanding on which exchanges to record in a square and the grouping in which these exchanges[32] and pieces ought to be recorded, a arrange of computers must communicate with one another and vote many times. Instinctively, signals from diverse computers within the arrange showing which square is the following would see like usually: known as Byzantine Blame Resilience (BFT).A few of today's most prevalent blockchains, such as NEO and Swell, are built on BFT forms.

One of the foremost common reactions of BFT is that it contains a centralization point: since voting is included, the set of hubs taking an interest within the voting "majority" is chosen centrally by the system's inventor at the begin. Rather than having a single centrally decided majority, FBA permits each hub to set up the possess "majority cuts," which at that point make different quorums. Unused hubs can connect the arrange in a decentralized way: they demonstrate which hubs they believe and influence other hubs to accept them without having to induce any central authority.[32]

FBA has a few appearances, one of which is SCP. SCP hubs secure the shared record by vouching for other hubs within the network as dependable, instead of squandering vitality like Bitcoin's proof of work agreement component. Each hub within the network creates a majority cut, which is made up of other hubs within the arrangement that they believe. Quorums are developed based on the majority cuts of its individuals, and validators will as it were acknowledge modern exchanges in the event that and as it were in the event that a division of the hubs in their quorums agree. As validators construct their quorums over the arrangement, these quorums aid nodes in coming to agreement on exchanges whereas guaranteeing security. This specialized outline of SCP might assist you learn more approximately the Stellar Agreement Protocol.[32]

E. Pi's Adjustments to Stellar Agreement Convention (SCP)

SCP is the establishment for Pi's agreement calculation. SCP has been formally approved [Mazieres 2015] and is presently in utilize interior the Stellar Organize. Not at all like the Stellar Organize, which essentially comprises of endeavours and organizations (e.g., IBM) as hubs, Pi looks for to permit individuals' gadgets, counting as versatile phones, tablets, and desktops, to contribute on the convention level and be paid. The taking after is an outline of how Pi employments SCP to empower person mining.

There are four parts Pi clients can play, as Pi mineworkers. To be specific:

● Pioneer. A client of the Pi flexible app who is fundamentally certifying that they are not a "robot" on an each day preface. This client endorses their closeness each time they sign in to the app. They can in addition open the app to inquire trades (e.g., make an instalment in Pi to another Pioneer)

● Contributor. A client of the Pi versatile app who is contributing by giving a list of pioneers he or she knows and trusts. In total, Pi supporters will construct a worldwide belief chart.

● Ambassador. A client of the Pi versatile app who is presenting other clients into the Pi network.

● Node. A client who may be a pioneer, a donor utilizing the Pi convenient app, and in addition running the Pi center computer program on their desktop or convenient workstation computer. The Pi center computer program is the program that runs the center SCP calculation, taking beneath thought the conviction chart information given by the Supporters.

A client can play more than one of the over parts. All parts are crucial; thus all parts are compensated with as of late stamped Pi on a day by day introduction as long as they took an interest and contributed in the midst of that given day. Inside the free definition of a "miner" being a client who gets as of late stamped cash as a compensation for commitments, all four parts are considered to be Pi diggers. We characterize "mining" more broadly than its routine meaning compared to executing affirmation of work understanding calculations as in Bitcoin.

To begin with, we ought to emphasize that the Pi Node computer program has not been discharged however. So this segment is advertised more as a building plan and as a way to request comments from the specialized community. This program will be completely open source and it'll too intensely depend on stellar-core which is additionally open source computer program, accessible here. This implies that anybody within the community will be able to study, comment and propose advancements on it. Underneath are the Pi proposed changes to SCP to empower mining by personal gadgets.[32]

V. COMPARISON OF AUDIENCE AND VALUE RAISING

COMPARISON TABLE
THIS TABLE CONTAINS THE BITCOIN AUDIENCE AND VALUE CHART.[30],[31].

S. N.	Bitcoin Timeline After Value Rising			
	Time	Exact Period	Description	User (Million)
01	138 days	Jan 2, 2017 -> May 20, 2017	$1,000 to $2,000	11.68-14.19
02	23 days	May 20, 2017 -> June 11, 2017	$2,000 to $3,000	14.19-14.86
03	63 days	June 11, 2017 -> Aug 13, 2017	$3,000 to $4,000	14.86-16.46
04	61 days	Aug 13, 2017 -> Oct 12, 2017	$4,000 to $5,000	16.46-18.06
05	10 days	Oct 12, 2017 -> Oct 21, 2017	$5,000 to $6,000	18.06-18.09
06	13 days	Oct 21, 2017 -> Nov 2, 2017	$6,000 to $7,000	18.09-19.34
07	17 days	Nov 2, 2017 -> Nov 19, 2017	$7,000 to $8,000	19.34-19.38
08	7 days	Nov 19, 2017 -> Nov 26, 2017	$8,000 to $9,000	19.38-19.42
09	5 years	Apr 12,2022	$9,000 to $10,000	81

COMPARISON TABLE

THIS TABLE CONTAINS THE PI NETWORK AUDIENCE AND VALUE CHART.[33]

S. N.	Bitcoin Timeline After Value Rising			
	Time	Exact Period	Description	User
01	45days	Mar 14, 2019 -> April 30, 2019	$0	1000
02	23 days	May 23, 2019 -> Oct 30, 2017	$0	10000
03	63 days	Mar 31, 2020 -> May 01, 2020	$0	1million
04	61 days	Dec 08, 2020	$0	10 million
05	10 days	Sep 24,2021	$0	25 million
06	240 days	Apr 12,2022	$0	29 million

VI. PREDICTED FUTURE VALUE OF PI ON BASIS OF BITCOIN:

In 2017, Cryptocurrency was not a popular subject, and people were not habituated to cryptocurrency. In that era, few people stored or mined bitcoin. At that time, the bitcoin price was around 2.3 dollars. Bitcoin crossed 100 USD in April 2017. Bitcoin launched in 2010. After 7 years bitcoin crossed 100 dollars. Mar 4 market cap was 25 billion and this crossed 100 billion on October 20, 2017. In 2022, the bitcoin price is 40,000 (+-) USD. In 2010, cryptocurrency was not too popular, and also there was not much technology for common people to use cryptocurrency. Bitcoin gained users in 10 years. In comparison to Bitcoin, the Pi coin has a better opportunity to gain a huge value after launch. The pi coin has already gained 29 million users. And also their mechanism is much more user-friendly. Bitcoin needs to be mined by a full price machine or computer. On the other hand, Pi coins are mined on regular use phones. The predicted Market of PI Coin is 10,411,808,510,386,988.00 $ and Pi Leader's org didn't declare any limitation till now. This can be used as regular currency in the near future. And the pool tools are too simple and also easy for regular people. All the aspects and sides of this can be predicted that Pi Coin can create a huge impact on cryptocurrency.

VII. POSSIBLE OUTCOME OF PI NETWORK

Bitcoin is the most valuable and high price cryptocurrency. And its value is getting higher day by day. But this type of cryptocurrency is not user-friendly. On the other hand, the Pi coin is the most user-friendly crypto-currency. Though Pi is not launched yet, 29 million people are mining and its circle is getting bigger day by day. If we check the comparison analysis, the PI coin can gain a vast value in the future.

VIII.   POSSIBLE WORST OUTCOME:

There are some possible worst outcomes, if the PI coin does not manage to launch on time people will lose hope and it can create a bad impact on market cap and market value. And the last worst outcome is Pi community authority will not be able to launch the coin and face a disastrous failure.

IX.   CONCLUSIONS

Although Bitcoin is now a very good and well-known cryptocurrency, the Pie Network will work to make it available and accessible to people of all different levels of humanity. In this paper, we have mentioned the Bitcoin key, the Pie network key and the predictions about the future value of the Pie network in the Bitcoin perspective.

In the comparison of the situation, Bitcoin passed a hard path and established a higher value. And PI network already has achieved 29 million users and is still gaining more audience. Till now Pi has mined 889,865,486 coins. This can be predicted that Pi can establish a user-friendly cryptocurrency.

References

[1] A Review on Blockchain Technology and Blockchain Projects Fostering Open Science,available at: https://www.frontiersin.org/articles/10.3389/fbloc.2019.00016/full

[2] CVEM: A Cross-chain Value Exchange Mechanism,available at: https://dl.acm.org/doi/abs/10.1145/3291064.3291073#sec-comments

[3] A Perspective on Blockchain Smart Contracts Reducing Uncertainty and Complexity in Value Exchange,available at: https://ieeexplore.ieee.org/abstract/document/8038512

[4] Strengthening the Blockchain-Based Internet of Value with Trust,available at: https://ieeexplore.ieee.org/abstract/document/8423014

[5] Securing Data With Blockchain and AI,available at: https://ieeexplore.ieee.org/abstract/document/8733072

[6] When Bitcoin encounters information in an online forum: Using text mining to analyse user opinions and predict value fluctuation,available at: https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0177630

[7] F. Tschorsch and B. Scheuermann, "Bitcoin and beyond: a technical survey on decentralized digital currencies," IEEE Communications Surveys & Tutorials, vol. 18, no. 3, pp. 2084-2123, March 2016

[8] V. Vishnumurthy, S. Chandrakumar, and E. G. Sirer, "KARMA: A secure economic framework for peer-to-peer resource sharing," 1st Workshop on Economics of Peer-To-Peer Systems, 2003

[9] N. Szabo, "Secure property titles with owner authority," 1998, available at: http://nakamotoinstitute.org/secure-property-titles/

[10] D. Malkhi and M. Reiter, "Byzantine quorum systems," Distributed Computing, vol. 11, no. 4, pp. 203-213, 1998

[11] J. Douceur, "The Sybil attack," in Proceedings of IPTPS '01 Revised Papers from the First International Workshop on Peer-to-Peer Systems, pp. 251-260, March 2002

[12] S. Nakamoto, "Bitcoin: a peer-to-peer electronic cash system," 2008, available at: https://bitcoin.org/bitcoin.pdf

[13] Ethereum Community, "A next-generation smart contract and decentralized application platform," White Paper, available at: https://github.com/ethereum/wiki/wiki/White-Paper

[14] A. Back, "Hashcash – a denial of service counter-measure," 2002, available at: http://www.hashcash.org/papers/hashcash.pdf

[15] D. Eastlake, 3rd and T. Hansen, "US Secure Hash Algorithms (SHA and SHA-based HMAC and HKDF)," RFC 6234 (Informational), May 2011, available at: http://www.ietf.org/rfc/rfc6234.txt

[16] R. Merkle, "A digital signature based on a conventional encryption function," In: Pomerance C. (eds) Advances in Cryptology —CRYPTO '87. CRYPTO 1987. Lecture Notes in Computer Science, vol 293. Springer, Berlin, Heidelberg, pp. 369-378, 1987

[17] R. Merkle, "Protocols for public key cryptosystems," in Proc. 1980 Symposium on Security and Privacy, IEEE Computer Society, pp. 122-133, April 1980

[18] Bitcoin Blockchain Size, https://charts.bitcoin.com/chart/blockchain-size

[19] J. Poon and T. Dryja, "The bitcoin lightning network: scalable off-chain instant payments,", 2016, available at: https://lightning.network/lightning-network-paper.pdf

[20] M. Trillo, "Stress test prepares VisaNet for the most wonderful time of the year," 2013, available at: https://www.visa.com/blogarchives/us/2013/10/10/stress-test-preparesvisanet-for-the-most-wonderful-time-of-the-year/index.html

[21] A. Castor, "A short guide to Bitcoin forks," March 2017, available at: https://www.coindesk.com/short-guide-bitcoin-forks-explained/

[22] Transaction malleability, available at: https://en.bitcoin.it/wiki/Transaction_malleability

[23] Coin telegraph, SegWit explained, available at: https://cointelegraph.com/explained/segwit-explained

[24] A. Hertig, "SegWit goes live: why Bitcoin's big upgrade is a blockchain game-changer," August 2017, available at: https://www.coindesk.com/50-blocks-segwit-bitcoins-coming-upgradeblockchain-game-changer/

[25] S. Sundararajan, "Blockstream launches micropayments processing system for Bitcoin apps," January 2018, available at: https://www.coindesk.com/blockstream-launches micropaymentsprocessing-system-for-bitcoin-apps/

[26] Bitcoin Cache, https://www.bitcoincash.org

[27] Bitcoin Gold Roadmap, available at: https://bitcoingold.org/wpcontent/uploads/2017/10/BitcoinGold-Roadmap.pdf

[28] A. Biryukov, D. Khovratovich, "Equihash: asymmetric proof-of work based on the generalized birthday problem," Ledger, vol. 2, pp. 1-30, April 2017

[29] V. Buterin, "Ethereum white paper: a next generation smart contract & decentralized application platform," 2013, available at: http://www.theblockchain.com/docs/Ethereum_white_papera_next_generation_smart_contract_and_decentralized_application_platform-vitalik-buterin.pdf

[30] Shamim, M. I. (2022). IT Skills Development Project and Economic Development in Bangladesh. *Academic Journal of Digital Economics and Stability*, *19*(7), 13-21.

[31] Visualizing the Journey to $10,000 Bitcoin, published by Jeff Desjardins,November 27, 2017.available at: https://www.visualcapitalist.com/visualizing-journey-10000-bitcoin/

[32] Number of Bitcoin block explorer Blockchain.com wallet users worldwide from November 2011 to April 6, 2022.available at: https://www.statista.com/statistics/647374/worldwide-blockchain-wallet-user