Impact Factor (SJIF): 5.301

International Journal of Advance Research in Engineering, Science & Technology

e-ISSN: 2393-9877, p-ISSN: 2394-2444

Volume 5, Issue 4, April-2018

Enhanced Blockchain Based CryptoCurrency Exchange

Rekha Shinde[1], Vaidehi Kanekar[2], Snehal Huljute[3], Amruta Suryawanshi[4], Prof. Poonam Thorat[5]

[1]Computer Department, P K Technical Campus,Chakan

[2]Computer Department, P K Technical Campus,Chakan

[3] Computer Department, P K Technical Campus,Chakan

[4] Computer Department, P K Technical Campus,Chakan

[5]Assistant Professor, Computer Department, P K Technical Campus,Chakan

Abstract --- Blockchain is a decentralized record used to safely trade computerized cash, perform arrangements and exchanges. Every individual from the system approaches the most recent duplicate of encoded record so they can approve another exchange. Blockchain record is an accumulation of all Bitcoin ex- changes executed previously. Fundamentally, it's a conveyed database which keeps up a ceaselessly developing sealed information structure pieces which holds groups of individual exchanges. The finished pieces are included a straight and sequential request. Each square contains a timestamp and data connect which focuses to a past piece. Bitcoin is distributed authorization less system which enables each client to associate with the system and send new exchange to check and make new pieces. Satoshi Nakamoto depicted plan of Bitcoin computerized money in his examination paper presented on cryptography listserv in 2008. Nakamoto's recommendation has tackled long pending issue of cryptographers and established the framework stone for advanced cash. This paper clarifies the idea, qualities, need of Blockchain and how Bitcoin functions. It endeavours to features part of Blockchain in moulding the fate of managing an account, budgetary establishments and reception of Internet of Things(IoT).

Keywords- Blockchain, distributed systems, internet of things, cryptocurrency

I. INTRODUCTION

Cryptocurrency could be a type of digital cash that's designed to be secure and, in several cases, anonymous. It is a currency related to the net that uses cryptography, the method of changing clean data into associate virtually uncrackable code, to trace purchases and transfers.Cryptography was born out of the necessity for secure communication within the Second war. it's evolved within the digital era with parts of mathematical theory and applied science to become the way to secure communications, data and cash on-line. Cryptocurrencies use reorganized technology to let users can do secure payments and store cash while its not necessary to use their name or bear a bank. They run on a distributed public ledger referred to as blockchain, that could be a record of all transactions updated and control by currency holders. the protection of cryptocurrencies is 2 half. the primary half comes from the issue find hash set intersections, a task done by miners. The second and a lot of seemingly of the 2 cases could be a 51% attack. during this situation, a manual laborer who has the mining power of over fifty-one of the network, will take charge of the worldwide blockchain ledger and generate another block-chain. Even at this time the wrongdoer is proscribed to what he will do. The wrongdoer might reverse his own transactions or block alternative transactions.

Cryptocurrencies are less prone to seizure by enforcement or having group action holds placed on them from acquirers like PayPal. All cryptocurrencies square measure pseudo-anonymous, and a few coins have acquisitions options to make true namelessness. Blockchain could facilitate solve many complicated issues associated with securing the integrity and trait of fast, distributed, complicated energy transactions and information exchanges. During a move towards grid resilience, blockchain commoditizes trust and permits machine-driven good contracts to support auditable multiparty transactions supported predefined rules between distributed energy suppliers and customers. Blockchain primarily based good contracts conjointly facilitate take away the requirement to move with third-parties, facilitating the adoption and substantiation of distributed energy transactions and exchanges, each energy flows additionally as monetary transactions. this could facilitate scale back transactive energy prices and increase the safety and property of distributed energy resource (DER) integration, serving to get rid of barriers to a lot of redistributed and resilient grid. A cryptocurrency constructed to work as a medium of exchange using cryptography to secure the transactions, to control the creation of additional units, and to check the transfer of assets. Cryptocurrencies are classified as a subset of digital currencies and are also classified as a subset of alternative currencies and virtual currencies.

II. RELATED WORK

1 Security of the blockchain. : Related work for that design smart contract applications for cryptocurrencies, we depend on the decentralized blockchain to be secure. Therefore, we are considering the blockchains consensus protocol provides security when an attacker does not wield a large fraction of the computational power. Present cryptocurrencies are available in the market designed with heuristic security. researchers have identified attacks on various parts in the the system ,then efforts to understand the security of blockchain consensus have begun.

2. Minimizing on-chain costs. cryptocurrencies including Bitcoin and Ethereum collect transaction fees that roughly correlate with the cost of execution.in our system every miner will execute the smart contract programs while verifying each transaction, , we are designing our protocols to minimize on-chain costs by performing most of the heavy-weight computation off-chain.

3. Smart contracts. Other cryptocurrencies, which guarantee authenticity but not privacy, other smart contract implementations rely on trusted servers for security . Our work therefore comes closest to realizing the original vision of parties interacting with a reliable virtual computer that executes programs involving money and data.

4. The blockchains expressive power is further upgraded by the fact that blockchains naturally demonstrate a clock that increments whenever a new block is mined. The existence of such a trusted clock is crucial for attaining financial fairness in protocols.

CRYPTOCURRENCY ARCHITECTURE:

We are having the various cryptocurrencies available around us,all of them having the same implementation design. cryptocurrency implementation has following parts:

- Network Protocol
- Consensus Protocol
- Transaction Protocol
- Internal State

A. *Network Protocol*

P2P network is the important part of a cryptocurrency, and that important part is following some network protocol. It is quite simple usually. For example, p2p network of a cryptocurency could be implemented with asynchronous exchange of the following messages:

- M1: Serialized unconfirmed transaction
- M2: Serialized block
- M3: Blockchain quality score request(e.g. height for the Bitcoin, cumulative difficulty for the NXT).
- M4: Blockchain quality score response
- M5: Get known peers request
- M6: Get known peers response
- M7: Request a block for a certain height

B. *Consensus Protocol*

The problem is canonical chain shared by majority,what will be the right kind of history an user can trust on. Consensus protocol aims to solve the problem.

A node follow rules to determine canonical chain like these:

1. Every block in a chain must be valid as well as its signature
2. Each and every child block must have a valid reference to its parent block with first block having reference to a genesis block which is constant for an each node
3. Every block must be created by a entity having a authority to produce it
4. If any chain having the maximum score then it will be considered as canonical. If any chains having the same score first seen or a randomly one could be chosen

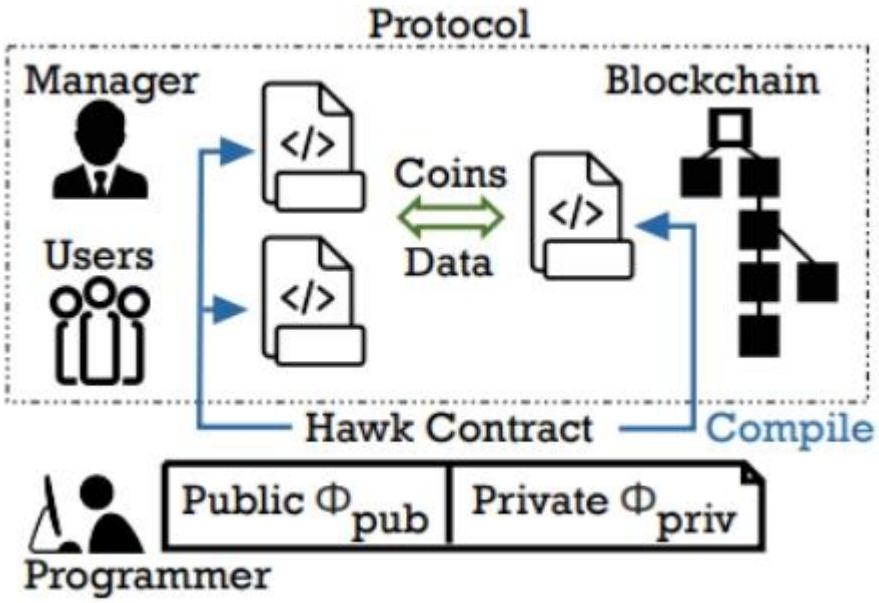
C. *Transaction Protocol*

A block stores the transactions. A transaction is the state modifier. In simplest case it modifies balance sheet. As there's no central entity, each node need to have the same state as others. So each node executes all the transactions coming within blocks, and validity rules must be same for each network participant.

D. ***Internal State***

In Bitcoin node a can store no any state at all or use different formats for it, e.g. UTXO list or some indexes in addition. In contrast, Ethereum has state hash stored into each block, so each node must comply with state representation interface given in the Yellow Paper to check block validity.

IV. PROPOSED SYSTEM



If we take out all clatter throughout the cryptocurrencies and lower simply define it, we would find that its simply resrained entries in database and unless we satisfy certain conditions its not possible to change those entries. It would look ordinary, but, trust it or not: thts how currency can be defined.

If we consider the money on our bank account, its nothing than the number of records in bank`s database which can be modified only in certain conditions.

We can even consider the physical notes and coins, they are just the restricted records in public physical database that can only be manipulated until we satisfy that thenotes or coins are physically owned by us. Hence, Money is all about verified record in specific kind of database of transactons, accounts, balances.

VI . METHODOLOGY

A major context is presented by cryptocurrencies alongwith a large prospective for research. To encapsulate and classify recent literature survey on cryptocurrencies, considerable literature survey was taken (see vom Brocke et al. 2009 and Webster and Watson 2002). Firstly, I restricted the scope to the keywords “cryptocurrency”, “cryptocurrencies”, “crypto and currency”, “crypto and currencies” and “bitcoin” to get a inclusive overview about the literature on cryptocurrencies. The keyword “Bitcoin” was also added as Bitcoin is currently the most used cryptocurrency we are focusing on our literature review on decentralized currency based on cryptography. I did not restrict the timeframe of the search, but did not expect to find much prior to 2008. we are not excluding the crryptocurrencies from the literature review.The search terms were applied to AIS Senior Scholars' Basket of Journals (Members of the Senior Scholars Consortium 2011),along with the extremely ranked Information Systems conferences AMCIS,ECIS, ICIS and HICSS, in order to see if Bitcoin and cryptocurrencies were being discussed and, if so, Cryptocurrencies and BitcoinTwenty-first Americas Conference on Information Systems, Puerto Rico, 2015 which concepts were under discussion. Based on the results of a full text search for each journal and conference, only one paper was found. Hence we further expanded our research work to incorporate digital databases and some libraries ACM, IEEE, AIS. In total, 50 papers were found in these databases. Duplicates were removed from the result set. The confirmed literature was then examined by reading the full text and 41 papers from the databases were identified as relevant, in that they explicitly addressed the concepts of cryptocurrencies or Bitcoin. Other papers that only mentioned about cryptocurrencies or Bitcoin were not considered further.

A. Algorithm

Scrypt is the quicker and more simple algorithm of the two, and as new digital currencies are being introduced, more of them are favoring it over SHA-256. Scrypt is much easier to run on an already-existing CPU, and tends to use up less energy than using SHA-256; as a result, it's favored by most individual miners. In comparison to SHA-256, Scrypt's hash rates for successful coin mining generally range in the kilohashes per second (KH/s) or megahashes per second (MH/s) areas of difficulty, which can be achieved with regular computers without the need of ASICs or other hardware. Some argue this simpler system is more susceptible to security issues, since fast transaction turnaround times can mean the system is taking a less thorough look at the data. Its advocates point out, however, that hasn't as of yet presented a real-world problem.

Over time, hash difficulties for the more popular currencies that use the SHA-256 mining algorithm such as Bitcoin are expected to rise; this may very well restrict the mining of such currencies to mining pools or individual miners who can devote hardware, energy and time to the process. As as result, it's expected that digital currencies which use Scrypt will see a comparable rise in popularity, based upon the ease of mining alone.

VII. CONCLUSION

In this paper we are providing framework which is capable to provide a partial fledged formal model for decentralized blockchains as embodied by Bitcoin, Ethereum, and many other popular decentralized cryptocurrencies. With Security in Digital Currency.

.

VIII. REFERENCES

[1] J. Kelly and A. Williams. (2016). Forty Big Banks Test Blockchain-BasedBond Trading System. [Online]. Available:http://www.nytimes.com/reuters/2016/03/02/business/02reuters-banking- blockchain-bonds.html

[2] *"scrypt page on the Tarsnap website"*.

[3] W. Suberg. (2015). Factoms Latest Partnership Takes on US Health- care. [Online]. Available: http://cointelegraph.com/news/factoms-latest- partnership-takes-on-us-healthcare

[4] Stronger Key Derivation Via Sequential Memory-Hard Functions

[5] D. Oparah. (2016). 3 Ways That the Blockchain Will Change the Real Estate Market. [Online]. Available: http://techcrunch.com/2016/02/06/3- ways-that-blockchain-will-change-the-real-estate-market/

[6] A. Mizrahi. (2015). A Blockchain-Based Property Ownership Recording System. [Online]. Available: http://chromaway.com/papers/A-blockchain- based-property-registry.pdf

[7] M. Walport, Distributed ledger technology: beyond block chain, U.K. Government Office Sci., London, U.K., Tech. Rep., Jan. 2016. [Online]. Available: https://www.gov.uk/government/publications/ distributed-ledger-technology-blackett-review

[8] S. Nakamoto. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. [Online]. Available: https://bitcoin.org/bitcoin.pdf

[9] Double-SpendingBitcoin WiKi, accessed on Mar. 15, 2016. [Online]. Available: https://en.bitcoin.it/wiki/Double-spending

[10] Eris Industries Documentation—Blockchains, accessed on Mar. 15,2016. [Online]. Available: https://docs.erisindustries.com/explainers/blockchains/

[11] G. Greenspan. (2015). Ending the Bitcoin vs Blockchain Debate.[Online]. Available: http://www.multichain.com/blog/2015/07/bitcoin-vs-blockchain-debate/2301K. Christidis, M. Devetsiokiotis: Blockchains and Smart Contracts for the IoT

[12] A. M. Antonopoulos, Mastering Bitcoin: Unlocking Digital Cryptocurrencies, 1st ed. Sebastopol, CA, USA: O'Reilly Media, Inc., 2014.