International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2018 IJSRCSEIT | Volume 3 | Issue 3 | ISSN : 2456-3307

Smart Contract Management Using Blockchain Technology

Chandrashekhar Singh Rajawat, Prof. Hemant Gupta
P.G. Student, Madhya Pradesh, India CSE, LNCTS (RIT), Indore, Madhya Pradesh
Assistant Professor, Madhya Pradesh, India CSE, LNCTS (RIT), Indore, Madhya Pradesh

ABSTRACT

Recent interest around blockchains and Emerging smart contract systems over blockchain technology which allows mutually distrustful parties to transact safely without trusted third parties provided requirements good fit for the Smart Contracts sector. In the event of contractual breaches or cancellations, the decentralized blockchain ensures that honest parties get their just compensation. Blockchains permit us to have a distributed peer-to-peer network wherever non-trusting members can interact with each other without depending on an intermediary and be able to verify the transaction. All transactions, together with the flow of cash are exposed on the blockchain. A smart contract is used to

1) Facilitates for sharing of services and resources managing to the creation of a marketplace of services between devices and

2) permits us to automate in an exceedingly cryptographically verifiable manner many existing, long workflows My conclusion is that the smart contract over blockchain combination is powerful and can cause vital transformations across many industries, making new ways for new business models and innovative distributed applications.

Keywords : Blockchain, Cryptographically, Smart Contracts Sector

I. INTRODUCTION

Blockchains have recently attracted the interest of investors across a wide spectrum of businesses from finance, healthcare, utilities, real estate and the government sector.

The reason for this eruption of interest is that with blockchain, applications that could previously run only through a trusted intermediary, can now operate in a decentralized fashion, without the need for a central authority, and achieve the same functionality with the same amount of certainty, which was not possible before.

Blockchain empower trustless networks, because the parties can transactions between parties while in current systems are usually conducted in a centralized form, which requires the involvement of a trusted third party like bank. However, this often means potential security issues and high transaction fees.

Blockchain technology can tackle these issues by allowing untrusted entities to interact with each other in a distributed manner without the involvement of a trusted third party.

Blockchain is a truly a distributed database that records all transactions that have ever occurred in a network. Blockchain was originally introduced for Bitcoin a peer-to-peer digital payment system, but then evolved to be used for developing a wide range of decentralized applications. An enthralling application that can be deployed on top of blockchain is smart contracts.

What is a Smart Contract?

A smart contract is executable code that runs on the blockchain to facilitate, execute and enforce the terms of an agreement between untrusted parties. It helps act like an expert evidence of as a system that releases digital assets to all or some of the once the pre-defined rules have been met.

Compared to traditional contracts, smart contracts do not rely on a trusted third party to operate, resulting in low transaction costs. There are different blockchain platforms that can be exploit to develop smart contracts, but Ethereum is the most common one.

Smart contracts can be applied to different applications for example smart properties, e-commerce and music rights management. Smart contracts –self-executing scripts that reside on the blockchain– integrate these concepts and allow for proper, distributed, heavily computerized workflows. Blockchains and smart contracts bring a multitude of advantages to the table, but they also come with a sack of disadvantages. This document explains a detailed description of how blockchains and smart contracts work, to identify the pros and cons and highlight the methods of the blockchains and smart contract can be organized.

The structure of this paper is as follows. Next section discusses background information about smart contracts over blockchain technologies and how smart contracts Works. In another section I will show how Smart Contract and blockchains can be used together, and highlight existing smart contract-on-the-blockchain applications

Smart Contract Blockchains

User-defined assets could be represented with the help of a smart contract on a smart contract blockchain. The contract could store the mapping of the addresses of current holders of the asset to the corresponding balances. These balances could be updated with the help of messages sent to the contract encoding asset transfer or issuance. The contract could use the conventional authorization scheme of the underlying blockchain in order to check transfer and issuance permissions, or could specify new rules for asset transactions. Ethereum is an example of an independent stat smart contract blockchain. Rootstock is a conceptual smart contract blockchain pegged to Bitcoin.

How Blockchains work

A blockchain is a distributed data structure that is replicated and shared among the members of a network. It was introduced with Bitcoin to solve the double-spending problem. As a result of how the nodes on the Bitcoin network (the so-called miners) append validated, mutually agreed-upon transactions to it, the Bitcoin blockchain houses the authoritative ledger of transactions that establishes who owns what. In this section general background information about blockchain and smart contracts technologies is depicted.

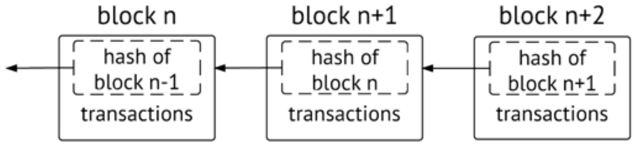

Figure 1. Each block in the chain carries a list of a transactions and a hash to the previous block.

Think of the blockchain as a log whose records are batched into time stamped blocks. Each block is identified by its cryptographic hash. Each block references the hash of the block that came before it. This establishes a link between the blocks, thus creating a *chain* of blocks, or *blockchain*

Any node with access to this ordered, back-linked list of blocks can read it and figure out what is the world state of the data that is being exchanged on the network. We get a better understanding of how a blockchain works,

1) Users interact with the blockchain via a pair of private/public keys. They use their private key to sign their own transactions, and they are addressable on the network via their public key. The use of asymmetric cryptography brings authentication, integrity, and nonrepudiation into the network. Every signed transaction is broadcasted by a user's node to its one-hop peers.

2) The neighboring peers make sure this incoming transaction is valid before relaying it any further; invalid transactions are discarded. Eventually this transaction is spread across the entire network.

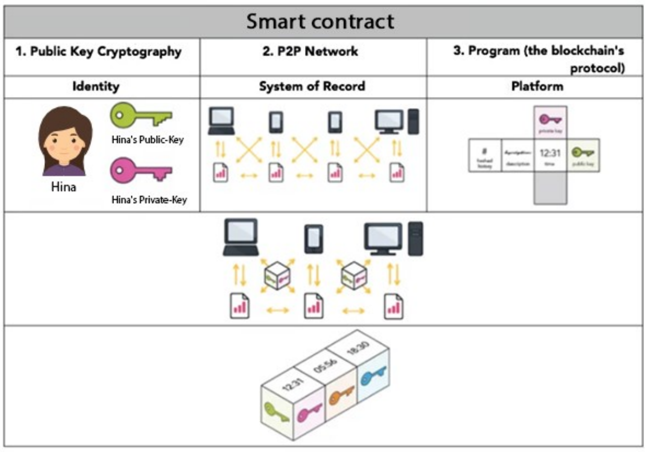

Figure 2. How smart Contract Work.

3) The transactions that have been collected and validated by the network using the process above during an agreed-upon time interval, are ordered and packaged into a time stamped candidate block. This is a process called *mining*. The mining node broadcasts this block back to the network.

4) The nodes verify that the suggested block (a) contains valid transactions, and (b) references via hash the correct previous block on their chain. If that is the case, they add the block to their chain, and apply the transactions it contains to update their world view. If that is not the case, the proposed block is discarded. This marks the end of a round.

USES of BLOCKCHAINS

Naturally, different categories of user would have differing requirements as to the operation of a blockchain. The requirements would also depend on the nature of Smart Contract recorded on the blockchain. For example, legality concerns for digital securities would be higher than for other assets, and the entry barrier for these types of digital assets is expected to be quite high.
In general, Smart Contract fall into one of two categories:

Institutional assets, which are characterized by institutionalized transaction processors and the legal requirements taking precedence of ease of entry and global reach. Smart Contract that represent securities would generally fall into this type.

Peer-to-peer contract, with the underdeveloped or non-existent market of dedicated transaction processors and a strong requirement of easy entry and global reach of technology. This type of smart contract would include in-application assets, business-to-consumer assets (e.g., discounts, gift cards), content subscription assets, etc.

In the case of smart contract, the categorization is unclear. There are institutional registries for certain types of contract, however for most property, centralized ownership registries do not and, arguably, should not exist.

Regulatory requirements for institutional assets could necessitate the use of private or strictly regulated public permissioned blockchains, which would be maintained by existing transaction processors. In this case, blockchain technology could provide an innovative application deployment model built-in audit trails and, possibly, more third-party participation (e.g., in the form of independent authentication services). In contrast,peer-to-peer assets could productively use public blockchains because they cover the requirements of easy entry and global reach, while the cost of operation would be low for asset issuers and application developers.

Transfering Digital Assents on Blockchain

Blockchain technology allows the efficient, direct transfer of digital assets between parties. For our purposes, we'll first define "digital assets" very broadly as any binary content that someone can own, or that represents content that someone can own. For instance, a music file is a digital asset, as are text files, photos, videos, computer programs and the like.

blockchain can be used to generate digital "tokens" that actually represent some or all of the underlying asset; these are sometimes called "asset-backed" tokens (not to be confused with "intrinsic" tokens like Bitcoins themselves that are built into a blockchain system as incentives—essentially the coin of the realm for that ecosystem). Such a digital asset token would be encrypted and would require the owner's private key to be transferred. These tokens act as an IOU; present the token to the party holding the underlying asset, and you can claim your share.

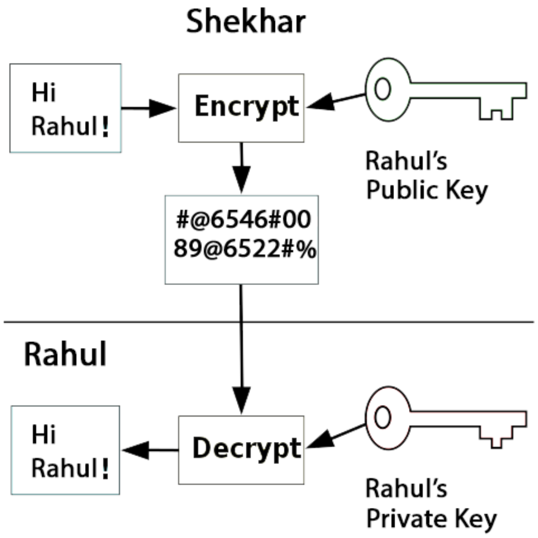

Figure 3. Basic flow of communication between two entities over blockchain

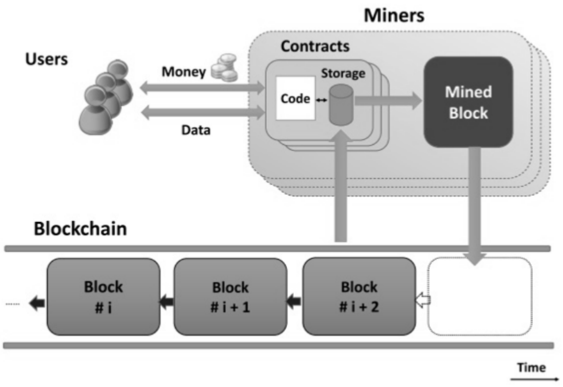

Figure 4. Basic flow of miners in blockchain Model.

II. CONCLUSION

Blockchains could be one of transformative technologies for digital asset management, serving as a specialized platform as a service (PaaS) with significant growth potential. Blockchains could provide for unprecedented levels of counterfeit resistance, openness, transparency, and auditability. Blockchain technology could allow decoupling tasks associated with asset management and transaction processing, therefore providing an attractive alternative to existing centralized asset management platforms for small and medium-sized businesses, third-party application developers and end customers. Internal, algorithmically enforced properties of blockchains and their increased auditability could prove attractive for regulatory bodies.

Blockchains give us resilient, truly distributed peer-to-peer systems and the ability to interact with peers in a trustless, auditable manner. Smart contracts allow us to automate complex multi-step processes.

III. REFERENCES

[1]. Profr3cev.com/blog/2016/6/2/ethereum-platform-review
[2]. etherscan.io/chart/gaslimit
[3]. ethgasstation.info/
[4]. greentechmedia.com/articles/read/the-energy-blockchain-could-bitcoin-be-catalyst-forthe-distributed-grid

[5]. blog.ethereum.org/2015/08/07/on-public-and-private-blockchains.

[6]. rstmonday.org/ojs/index.php/fm/article/view/548/4691

[7]. A Peer-to-Peer Electronic Cash System.

[8]. https://docs.erisindustries.com/blockchains/

[9]. https://www.coindesk.com/information/how-does-blockchain-technology-work/

[10]. http://www.truthcoin.info/blog/wise-contracts/

[11]. https://www.ccn.com/smart-contracts-12-use-cases-for-business-and-beyond/

[12]. https://solidity.readthedocs.io/en/v0.3.1/solidity-in-depth.html

[13]. https://blockgeeks.com/guides/smart-contracts/

[14]. https://medium.com/crypto-currently/build-your-first-smart-contract-fc36a8ff50ca

[15]. https://hackernoon.com/advantages-and-disadvantages-of-smart-contracts-in-financial-blockchain-systems-3a443145ae1c

[16]. http://searchcompliance.techtarget.com/definition/smart-contract