JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

BLOCKCHAIN SMART CONTRACTS – A FUTURISTIC PARADIGM

Dr. Nisha Tanwar[1] and Dr. Archana Golwalkar[2]

[1]Asstistant Professor, Department of Computer Science & Application, Bhupal Nobles' University, Udaipur, Rajasthan, India
[2]Head, NCA. NSS, Udaipur, Rajasthan, India

ABSTRACT

As an outcome of fast-paced development in the field of information and communication technology, witnessed in the last two decades, depicted a progressive experience that has broken the geographical borders and brought the world closer never as before and empowered netizens.

The concept of Bitcoin (a digital currency) which was put forth in the white paper under the pseudonym "Satoshi Nakamoto" in 2008 has evolved largely with an immense increase in its value around 30050 USD in June 2022 from the value of 1 USD in 2011. Crypto currencies as a tool for digital transactions in a decentralized system are extremely attractive and gaining popularity worldwide, despite posing challenges in the developmental stages based on the blockchain data structure offering advantages on time, money, effort, and more.

Decentralized application is also known as "dApps" or "dapps". These digital applications run on a peer-to-peer (P2P) blockchain network of computers instead of dependent on a single computer. To complete the transaction between two anonymous parties without the need to rely on a central authority DApps use smart contracts.

On this backdrop, the present review-based study provides an insight into Smart Contracts which will soon become a standard for digital deals on the internet.

Keywords: *IoT, Blockchain economic system, Crypto currency, Crypto economics, Smart Contracts, DApps*

Introduction

A crypto currency is a digital or virtual or electronic currency, which is an alternative form of payment. The crypto currency attains security with cryptography techniques, which makes it almost impossible to copied or double-spend. Cryptography is very old technique, dedicated to securing, protecting messages (ensuring confidentiality, authenticity, and integrity). It insures to prevent theunauthorized access of information. There are numerous types of cryptography algorithms.

There is an array of accessible crypto currencies like Bitcoin (BTC), Ethereum (ETH), Tether (USDT), USD Coin (USDC), Binance Coin (BNB), Binance USD (BUSD), Cardano (ADA), Ripple (XRP), Solana (SOL), Dogecoin (DOGE), Polkadot (DOT), TRON (TRX), Avalanche (AVAX), ShibaInu (SHIB), Litecoin (LTC) and many more.

Blockchain

Blockchain is a secure, transparent technology for storage and transmission which operates without a central control device that can be used to transfer data from point A to point B. It is a distributed database that manages a

list of records mechanically protected against tampering or modification by storage in nodes through its decentralized timeline.

A blockchain, as a database, contains the history of all the exchanges between its users since its creation. It is shared by its several users, without intermediaries, which permits each one to check the validity of the channel. The fact to share is based on a consensus, and historically to arrive at this type of consensus we used "proof of work". This method uses energy as a means of verification that the "miner" has done a good job.

The blockchain protocol, consequently, uses a cryptographic system based on a decentralized system of proofs: the resolution of the proof requires high computing power, provided by the miners. In order not to be falsifiable, a blockchain requires that no hostile operator at any time have more than half the computing power of the chain. A blockchain is referred public if each participant can read it and use it to carry out transactions but also if everyone can participate in the process of creating the consensus. There is therefore no central register, nor a trustworthy third party.

The governance of public channels, resulting from the open source movement and cipher punk, is simple: "Code is Law". In this system, the nodes of the network validate the choices discussed and initiated by the developers by deciding whether to integrate the proposed modifications. This operation is based on "**cryptoeconomics**", the combination of economic incentives and verification mechanisms using cryptography. Based on a community, or alternative, approach to the economy, this system has demonstrated its strength and resilience (Sharma et. al. (2020)).

The blockchain economic system conventions will be persistent by the smart contracts, each and every time stimulatory transactions are applied independently. The blockchain economy has shaped to a novel organizational structure called the decentralized autonomous organizations (DAO). Blockchain is the basis for the Decentralized Autonomous Organizations (DAOs) which provide novel stages of crowd coordination by eradicating trust and fault problems.

Blockchain can **enable** authentication and authorization without using any trusted authority. With its exclusive advantages and applications, the blockchain paradigm is being promoted more rapidly than usual. The adoption and adaptation are on the progressive side. Enterprises are rolling out newer blockchain use cases to make it more visible and viable. Therefore, there are a few blockchain types (Aggarwal and Kumar, 2021).

Blockchain is classified into three major categories

Public blockchain: All records are broadcasted and all the members and everyone are involved in the procedure of confirming and validating the transactions in the public blockchain system.

Private blockchain: Private blockchain is also referred to as a centralized network, as only one organization controls complete process and only the members of the organization are involved in the procedure of concluding to consensus (Guegan, (2017)).

Consortium blockchain: This blockchain system is monitored and regulated by several bodies and is moderately decentralized as few pre-selected groups of nodes would be selected to contribute to the decision-making process.

Decentralized Autonomous Organizations (DAO)

The term DAO stands for "decentralized autonomous organization" and can be described as an open-source blockchain protocol governed by a set of rules, created by its elected members, which automatically execute certain actions without the requirement for intermediaries. The concept of a DAO was first coined by BitShares, Steemit, and EOS (Block.one) founder Dan Larimer in 2015, and further amended by Ethereum's Vitalik Buterin in 2016.

The DAO's rules are implanted into computer code, which executes by itself based on the behavior of the protocol. There is no requirement to interpret these program rules as they are implemented automatically on the basis of specified conditions occurrence. Both the program rules and subsequent actions are recognized on a transparent and secure blockchain ledger, which cannot be altered with thanks to an immutable timestamp and the distribution of the information to the network participants.

A DAO supports to keep a network safe and optimized without the requirement of manual intermediation by its members. Participants are not indebted by a legal contract, but incentivized by rewards in the form of native asset tokens that motivate them to work towards a unified goal. A DAO supports to speed up network decision-making and actions and extremely lowers management costs because no third parties are required, (Singh and Kim, 2019) .

DAOs and Security

The rules that control a DAO can be complex and tough to change after they come into effect, as any alterations would be unavoidable on the writing of new code and network approval by consensus.

This incompetence to react hastily to code bugs does leave a DAO open to hacker attacks that could abuse security flaws and drain the crypto currency's funds (Vermaak (2021)).

Significance of DAOs

DAOs, don't need to trust anyone else in the group, just the DAO's code, which is 100% transparent and verifiable by anyone. This brings up so many new opportunities for global collaboration and coordination. A comparison -

A traditional organization	**DAO**
Usually hierarchical.	As DAO is usually flat, and fully democratized.
Depending on structure, changes can be required from a sole party, or voting may be offered.	Voting needed by members for any changes to be implemented.
If voting allowed, votes are matched, internally, and outcome of voting must be handled manually.	Votes matched, and outcome implemented automatically without trusted intermediary.
Requires human handling, or centrally controlled automation, likely to manipulation.	Services are handled automatically in a decentralized mode.

Smart Contract is the backbone of a DAO. The contract expresses the rules of the organization and grips the group's treasury. Once the contract is live, no one can change the rules except by a vote. It will fail if anyone tries to do something that's not covered by the rules and logic in the code. Since the treasury is well-defined by the smart contract too that means no one can spend the money without the group's approval either. Without the need of a central authority in the DAOs, the group creates decisions jointly, and payments are automatically approved when votes pass.

Centralized and decentralized applications

A decentralized app (also known as a dApp or dapp) activates on a blockchain or peer-to-peer network of computers. It enables users to engage in the transactions directly with one another in contrast to relying on a central authority. A dApp user will pay the developer an amount of crypto currency to download and use the program's source code. The source code is known as a SMART CONTRACT that allows users to complete transactions without revealing personal information. DApps—which are frequently built on the Ethereum platform—can be developed for a range of purposes including gaming, finance, and social media (George W. and Al-Ansari T. (2023)).

DApp vs DAO

Although the two concepts are generated by two different groups of people, they are used interchangeably at times. The key difference is the word “Autonomous”. DAO can be considered as one type of DApp, the fully autonomous DApp. DApp is not necessarily DAO.

Examples of operational DAOs include DASH, a crypto currency accomplished by its users, MakerDAO, software that retains a stable coin, and Augur, a prediction market platform.

In the perspective of cryptocurrencies, dApps run on a blockchain network in a public, decentralized environment, open-source, and are free from control and intervention by any single authority. For example, a developer can concept a Twitter-like dApp and put it on a blockchain where any user can publish messages. No one including the app creators can delete the messages once posted.

Smart Contracts

American cryptographer and computer scientist Nick Szabo hosted the term "smart contract" in 1996 as a graduate student at the University of Washington.

A smart contract is a self-executing digital agreement that permits two or more parties to exchange money, shares, property, or anything of value in a transparent, conflict-free way while avoiding the need for a third party.

Examples of smart contract applications consist of financial purposes like trading, lending, investing, and borrowing. They can be used for applications in gaming, real estate, and healthcare; and they can even be used to configure entire corporate structures.

Smart contracts are basically programs stored on a blockchain that run when predetermined conditions are fulfilled, they are used to automate the execution of an agreement such that all the participants can be immediately certain of the outcome, avoiding time loss or an intermediary's involvement. They can also automate a working, triggering the subsequent action when conditions are fulfilled.

Ordinarily, a complex transaction involves significant money, may involve a lawyer or a notary, and have them set up a third party account, pay them, and wait while the work is on and ensure the contract terms are satisfied. Only after the lawyer has done the work to ensure everything is executed correctly, documents/goods/money, etc will be received by the second party.

With smart contracts, the processing is simplified, by dropping a crypto currency into the vending machine (i.e. ledger), whatever may be the contract for, to the party's account. The smart contract performs all the work to decide whether the conditions of the order were satisfied. Smart contracts both define the rules and penalties around an agreement in the same way that a traditional contract does and also automatically enforce those obligations.

Supply Chain and Logistics companies employ Smart contracts to document the transit of goods, automating payments, realtime updation of inventory, Health Care for safely recording and transferring data, Insurance companies for accelerating claims processing and payments, Retailers and Suppliers to boost trust, trade Industry for speed and proficiency, Governments for secure, tamper-free voting. Ethereum, Polkadot, Solana, Hyperledger Fabric are some of the popular smart contracts platforms

Composition of Smart Contracts

Smart contracts are verified, executed, and required by a computer program that runs on a blockchain network. When both parties tangled in the smart contract agree to its terms, the program will execute automatically. This eliminates the requirement for a third party, as the contract is verified and imposed by the blockchain network.

Because smart contracts are accomplished by code rather than people, they eliminate the possibility of human error and can automate various tasks that would traditionally involve human interaction.

Key factors of Smart Contracts comprise of

- Autonomy
- Trust
- Backup
- Safety
- Speed
- Savings
- Accuracy
- Automated

Critical issues facing Smart Contracts

Smart contracts are not flexible, meaning that if there is a problem with the contract, it can be tough or impossible to fix. Smart contracts may not be reliablealways, as they are accomplished on a blockchain network.

Smart contracts can be expensive to develop and need a high level of technical expertise.Smart contracts are not personalizedalways, meaning that they may not be appropriate for all businesses or transactions.

Conclusion

As blockchain is a decentralized system that occurs between all permitted parties, there's no requirement to pay intermediaries (Middlemen) and it saves time and conflict. To create a smart contract, a basic understanding of blockchain technology and how smart contracts work, is needed along with a working knowledge of the programming language that is used to write smart contracts, which is typically Solidity (Solidity is a statically-typed curly-braces programming language designed for developing smart contracts that run on Ethereum.)

Smart contracts are one of the causes blockchain technology could be so influential and transform our day-to-day lives; the platforms need to be faster, secure, scalable, and more affordable. They are the appliances behind the emerging decentralized finance (DeFi) industry, which refers to several applications that cut the middleman out of traditional finance.

Undoubtedly, Blockchains have their problems, but they are undeniably faster, cheaper, and more secure than traditional systems. Thus more and more smart contracts are being executed by dApps on different blockchain networks dealing with the challenges and threats which may lead to a new standard in the future, demystifying digital assets.

References

Aggarwal S. , Kumar N. (2021). *Chapter Ten - Core components of blockchain*.Advances in Computers.Elsevier.Volume 121Pages 193-209

Aggarwal, S., & Kumar, N. (2021).Core components of blockchain. In Advances in Computers (Vol. 121, pp. 193-209).Elsevier.

El Faqir, Y., Arroyo, J., & Hassan, S. (2020, August).An overview of decentralized autonomous organizations on the blockchain.In Proceedings of the 16th international symposium on open collaboration (pp. 1-8).

George W. and Al-Ansari T. (2023).*Review of Blockchain Applications in Food Supply Chains* https://www.mdpi.com/2813-5288/1/1/4*Blockchains* 2023 *1*(1), 34-57

Guegan D. (2017) *Public Blockchain versus Private blockhain.*Documents de travail du Centre d'Economie de la Sorbonne. HAL open Science. Pp 1-6

Guegan, D. (2017). Public blockchain versus private blockchain.

https://coinmarketcap.com/alexandria/article/what-is-a-dao, What Is a DAO? | Alexandria - CoinMarketCap

Konoth, R. K., Vineti, E., Moonsamy, V., Lindorfer, M., Kruegel, C., Bos, H., &Vigna, G. (2018, October). Minesweeper: An in-depth look into drive-by cryptocurrency mining and its defense. In Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security (pp. 1714-1730).

Liu, L., Zhou, S., Huang, H., &Zheng, Z. (2021). From technology to society: An overview of blockchain-based dao. IEEE Open Journal of the Computer Society.

Nakamoto, S. (2008).Bitcoin: A peer-to-peer electronic cash system. Decentralized Business Review, 21260.

Puthal, D., Malik, N., Mohanty, S. P., Kougianos, E., & Das, G. (2018). Everything you wanted to know about the blockchain: Its promise, components, processes, and problems. IEEE Consumer Electronics Magazine, 7(4), 6-14.

Sharma D. K., Pant S., Sharma M. and BrahmachariS. (2020). *Chapter 13 - Cryptocurrency Mechanisms for Blockchains: Models, Characteristics, Challenges, and Applications*Handbook of Research on Blockchain Technology. ScienceDirect, Pages 323-348

Singh M. and Kim S.(2019) Chapter Four - Blockchain technology for decentralized autonomous organizations.Advances in Computers.Elsevier.Volume 115, 2019, Pages 115-140.

Singhal, B., Dhameja, G., & Panda, P. S. (2018).Beginning Blockchain: A Beginner's guide to building Blockchain solutions.Apress.

VermaakW. (2021).*What Is a DAO?*https://coinmarketcap.com/academy/article/what-is-a-dao

Wang, S., Tang, X., Zhang, Y., & Chen, J. (2019). Auditable protocols for fair payment and physical asset delivery based on smart contracts. *Ieee Access*, *7*, 109439-109453.

What is a DAO? | Decentralized Autonomous Organization https://www.kraken.com/en-us/learn/what-is-decentralized-autonomous-organization-dao