Blockchain & Web3 in Carbon Credits

Ms. Dhruvi Kayastha[1], Mr. Mukesh Parmar[2], Mr. Prakash Patel[3]
[1,2,3] *Computer Engineering, Gandhinagar University, Gandhinagar, India.*

***Abstract*—Blockchain technology has garnered much attention from a wide range of stakeholders including carbon credit trading companies, financial institutions, technology developers, start-ups, national governments, and the academic community. This technology offers the potential for transparent, secure, and tamper-proof systems that can enable innovative business solutions, particularly when combined with smart contracts. In this paper, we provide a comprehensive overview of the fundamental principles behind blockchain technology and then delve into blockchain solutions for the Carbon credit industry, and provide a systematic review of the literature and current business cases related to this topic.**

1. INTRODUCTION

Climate change and global warming are major challenges facing the world in the 21st century. The Kyoto Protocol, an international treaty signed in 1997, proposed a market-based solution to reduce greenhouse gas emissions by establishing a system of carbon trading. Under this system, emissions of carbon dioxide and other greenhouse gases are treated as a commodity that can be bought and sold. The goal of carbon trading is to incentivize countries and businesses to reduce their emissions by creating a financial cost for emitting these gases. By creating a market for emissions, the hope is that the most cost-effective methods for reducing emissions will be adopted, leading to overall reductions in greenhouse gases.

Greenhouse gas emissions from human activities have already warmed the Earth's temperature more than 1°C (That's almost 2°F!). Reducing atmospheric carbon dioxide (CO2) levels is critically important to reverse the climate change that's already happening. We need to not only reduce emissions but to remove existing emissions from the atmosphere. The challenge with carbon marketplaces today is that they're project-based. They connect individual buyers with individual 'suppliers' of carbon assets, on a one-by-one basis. This model isn't going to scale carbon removal 1,000x. To accomplish that, carbon markets will have to look more like commodities markets. Atmospheric carbon dioxide is a commodity like oil or gold. There's a lot of it. Work is required to bring it to market. And society places a value on it. There's no reason the carbon market can't reach the commodity market scale.

Blockchain technology has the potential to revolutionize the carbon credits market by providing a secure and transparent platform for the creation, tracking, and trading of carbon credits. Some notable use cases for blockchain in the carbon credits market include the Verification and tracking of carbon offset projects: Blockchain can be used to verify and track the reduction of greenhouse gas emissions through carbon offset projects, such as reforestation or clean energy projects. This can help ensure that carbon credits are being issued for verifiable emissions reductions and can prevent the creation of fraudulent credits.

Trading and exchange of carbon credits: Blockchain can facilitate the efficient and transparent trading of carbon credits by providing a secure and immutable record of transactions. This can make it easier for buyers and sellers to find each other and can help increase liquidity in the carbon credits market.

Integration with other sustainability efforts: Blockchain can be used to integrate carbon credits with other sustainability efforts, such as water conservation or waste reduction. This can help create a more holistic approach to sustainability and can enable the creation of multi-benefit credits that can be traded on the same platform.

Overall, the use of blockchain in the carbon credits market has the potential to increase the efficiency, transparency, and credibility of this market, which can help drive the transition to a low-carbon economy.

2. BLOCKCHAIN TECHNOLOGY CONCEPTUAL BACKGROUND

Blockchain technology is a decentralized, distributed ledger technology (DLT) that securely stores digital transactions without the need for a central authority. It is a shared, distributed ledger that can be used to record transactions between parties transparently and securely.

One of the key benefits of blockchain technology is its ability to facilitate the automated execution of smart contracts in peer-to-peer (P2P) networks. Smart contracts are self-executing contracts with the terms of the agreement between buyer and seller being directly written into lines of code. When certain conditions are met, the contract is automatically executed.

Blockchain technology allows multiple users to make changes to the ledger simultaneously, resulting in numerous chain versions. Instead of being managed by a single, trusted center, each network member holds a copy of the record chain, and consensus is reached on the valid state of the ledger. The methodology for reaching a consensus can vary and is an area of ongoing research.

New transactions are linked to previous transactions through cryptography, which makes blockchain networks resilient and secure. Every network user can verify the validity of transactions, providing transparency and tamper-proof records.

Blockchain technology is most commonly associated with cryptocurrency applications, which have experienced a surge in popularity in recent years with a market capitalization of over $335 billion at the time of writing. While the long-term future of cryptocurrencies may be uncertain, there are many potential applications for blockchain technology beyond cryptocurrency.

2.1. Definition and overview of fundamental principles of Blockchain

A blockchain is a digital database of transactions that is shared and distributed among a network of computers. This means that the database is not stored in a single location, but is instead replicated across a network of computers. This allows multiple parties to access and verify the contents of the database. Transactions are added to the database in blocks, which are time-stamped and linked to previous blocks, forming a chain of records.

Each block contains a group of transactions that have been added to the database. These transactions are time-stamped to ensure the chronological order of events. The blocks are also linked to previous blocks through the use of cryptographic techniques, creating a chain of records that can be traced back to the beginning of the blockchain.

The purpose of a blockchain is to enable a network of computers to reach a consensus on the state of the database without the need for a central authority.

In traditional systems, a central point of authority such as a bank is responsible for maintaining the records of the database and ensuring that transactions are valid. However, in a blockchain, the network of computers reaches consensus on the state of the database through the use of distributed consensus algorithms. This allows the network to operate without the need for a central authority.

In traditional systems, a central point of authority such as a central bank acts as an intermediary to store and maintain the records of the database. This central authority is responsible for verifying transactions and ensuring that the database is accurate and up to date. However, this centralization introduces intermediary costs and requires users to trust a third party to operate the system. By using a distributed network of computers to validate transactions and maintain the integrity of the database, blockchains can eliminate the need for intermediaries and provide a high level of transparency.

In a blockchain, the network of computers is responsible for verifying transactions and maintaining the accuracy of the database. This eliminates the need for intermediaries and allows for a higher level of transparency, as all users of the network can access and verify the contents of the database.

The process of validation and database synchronization varies among different types of blockchains but generally involves a distributed voting

process to reach a consensus on the valid state of the database. To reach a consensus on the state of the database, the network of computers must agree on which transactions are valid and should be added to the database. This process, known as distributed consensus, can take various forms depending on the specific blockchain in question but generally involves some form of the distributed voting process to determine the valid state of the database.

2.2. Two important paradigms: Bitcoin and Ethereum

Bitcoin is the first cryptocurrency, introduced in 2009 in a white paper by an anonymous individual or group known as Nakamoto.

Bitcoin is a digital currency that was created to serve as a decentralized, electronic cash system. It was first proposed in a white paper released by an anonymous individual or group known as Nakamoto.

It is a decentralized digital currency that uses peer-to-peer communication and cryptography to secure transactions.

Bitcoin is decentralized, meaning that it is not controlled by any central authority such as a bank or government. Instead, it relies on a network of computers to process and secure transactions. Peer-to-peer communication is used to facilitate the exchange of information between parties, and cryptography is used to ensure the security of the transaction.

Each user has a digital wallet, which is accessed using a private key and is identified by a public key.

To use Bitcoin, users must have a digital wallet to store their coins. This wallet is accessed using a private key, which is known only to the user and is used to prove ownership of the wallet. The wallet is also identified by a public key, which is a unique code that is used to identify the user and receive transactions.

Before a Bitcoin transaction can take place, the parties involved must exchange public addresses. To send or receive a Bitcoin transaction, the parties involved must exchange their public addresses. This allows the sender to know where to send the coins and the receiver to know where to look for them. The sender creates a transaction, which includes the number of coins being traded and the addresses of the parties involved. When a user wants to send a Bitcoin transaction, they create a message that includes the number of coins being traded and the addresses of the parties involved.

The transaction is encrypted with the receiver's public key, signed by the sender, and then transmitted to the Bitcoin network.

The transaction is encrypted using the receiver's public key to ensure that only the intended recipient can decrypt and access the coins. It is also signed by the sender to prove ownership and prevent fraud. The transaction is then broadcast to the Bitcoin network for processing. Special nodes, called miners, collect all the outgoing transactions of the past 10 minutes into a single block. Miners are special nodes in the Bitcoin network that are responsible for collecting and validating transactions. They collect all the transactions that have taken place in the past 10 minutes and group them into a single block.

These miners also validate the transaction, to include one block in the blockchain every 10 minutes on average.

In addition to collecting transactions, miners are also responsible for validating them to ensure their accuracy and prevent fraud. Once a block of transactions has been collected, the miners work to solve a complex mathematical problem to add the block to the blockchain. The goal is to include one block in the blockchain every 10 minutes on average.

Ethereum is a blockchain platform that allows users to create and run their applications, called decentralized applications (DApps), it provides a decentralized virtual machine and cloud platform for users to create their applications that run on top of blockchain architectures. These applications, called decentralized applications or DApps, can operate autonomously and without human intervention, using cryptocurrencies or tokens and storing their output in public ledgers.

DApps are open-source, meaning that their source code is available for anyone to view and modify. They operate on a network of computers and use cryptocurrencies or tokens to function. The output of DApps is stored in public ledgers, which allows for transparency and allows anyone to verify the results of the application.

Ethereum has gained widespread adoption and is currently used by over 1000 projects. It is also frequently used by startups for initial coin offerings (ICOs), a process through which a company raises funding by selling a new cryptocurrency.

Bitcoin is the most well-known and established blockchain application, but Ethereum has a range of applications beyond just cryptocurrency. It is particularly well-suited for smart contracts, which are self-executing contracts with the terms of the agreement between buyer and seller being directly written into lines of code. Ethereum is also used to build DApps, as previously mentioned.

Bitcoin relies on complete decentralization to function properly. Others may not require this level of decentralization and can use alternative system architectures that are more suitable for their needs.

Ethereum is a blockchain platform that is designed to accommodate a wide range of use cases and applications, Bitcoin is specifically designed for cryptocurrency-based transactions. Bitcoin is designed to be a store of value and a medium of exchange, and it is often referred to as "digital gold." While Ethereum is also used as a digital currency.

2.3. Distributed Consensus Algorithms

Many different algorithms can be used to reach consensus in a blockchain network. These algorithms determine how transactions are validated and how new blocks are added to the chain. The choice of algorithm can have a significant impact on key characteristics of the network, such as scalability, transaction speed, and security.

One key aspect of a consensus algorithm is how it handles the generation and acceptance of new blocks. In a blockchain system, a node may propose a new block that contains several transactions. The proposed block is then subjected to a consensus process, in which other nodes in the network decide whether to accept it. If the block is accepted, it becomes part of the blockchain and is linked to previous blocks through cryptographic means. Over time, the block becomes increasingly difficult to reverse, and it becomes a permanent part of the blockchain. While it is theoretically possible for a block to be reversed as part of a fork, the likelihood of this happening decreases as more blocks are added to the chain.

Consensus algorithms are used to ensure that the nodes in a distributed system, such as a blockchain network, can reach an agreement on the state of the system. These algorithms must be able to withstand various types of failures and malicious behavior to ensure the integrity of the system. There are two main categories of consensus algorithms: lottery-based and voting-based.

Lottery-based algorithms, such as proof of work (PoW) and proof of stake (PoS), rely on randomized selection to choose the nodes that will validate transactions and create new blocks. PoW systems, used by many cryptocurrencies like Bitcoin and Ethereum, require participants to solve cryptographic puzzles in order to earn the right to validate transactions and create new blocks. In PoS systems, validators are chosen randomly or through a round-robin mechanism, but the weight of each validator's vote depends on the size of their stake in the system, such as the amount of cryptocurrency they hold. These algorithms are generally good at scaling to large numbers of nodes but may result in multiple chains that need to be consolidated before finality is reached, which can affect the speed of transactions.

Voting-based algorithms, such as Practical Byzantine Fault Tolerance (PBFT), use a multi-round voting process to achieve consensus. In these systems, nodes transmit votes for blocks and eventually reach an agreement on whether to accept a block as part of the permanent chain. While voting-based algorithms can achieve finality faster than lottery-based algorithms, they may take longer to achieve consensus for a large number of nodes because of the need for multiple rounds of voting and message exchanges.

There are ongoing efforts to improve the scalability and speed of consensus algorithms, including the use of techniques like sharding, sidechains, and payment channels. Sharding involves using a subset of nodes to verify each transaction, potentially enabling parallel processing and faster transaction speeds. Sidechains are separate chains that store the data related to transactions, easing the burden on the main chain. Payment channels allow parties to transact with each

other for a set period without broadcasting each transaction to the entire network.

2.1.1. Proof of Work (PoW)

Proof of Work (PoW) is a system that is used to validate transactions and add new blocks to a blockchain. It was first implemented in the cryptocurrency, Bitcoin, as a way to prevent denial of service attacks on internet resources. In the PoW system, validators or miners compete to add a new block to the existing blockchain by solving a cryptographic puzzle. This involves generating a hash output that starts with a certain number of consecutive zeros in the most significant positions.

To do this, the miner adds a nonce, a random number that can only be used once, to the block and calculates the hash output of the block header. The block header contains information such as the hash of the previous block that has been validated and a special hash of all the transactions contained in the block (known as a Merkle tree). The goal for all miners is to achieve a hash output that is lower than a specified target. Miners have no way to predict or influence the outcome, so they can only try different nonces through a process of trial and error. This process requires a lot of computational power, which increases exponentially with the number of trailing zeros.

When a correct hash output is found, the block is returned to the Bitcoin network and accepted by other nodes if all the transactions are valid and unspent. The successful miner is then rewarded with a financial prize. Other miners then begin working on the next block. Importantly, all succeeding blocks contain hash outputs from all preceding blocks.

In the PoW system, multiple chains may be generated due to the random nature of the hash output calculation and the fact that it is performed in parallel by many miners. In this case, the network stores all the resulting chains. Eventually, the network members will abandon all chains except the longest one, which is assumed to have been produced by a network majority with the most computational power and therefore considered the most valid state of the ledger. This helps to protect the network from malicious attacks, as attackers would need to control more than 51% of the computational power in the network to successfully rewrite the history of transactions. However, security breaches can still occur due to user error, miner malfeasance, hacking, or man-in-the-middle attacks.

2.1.2. Proof of Stake (PoS)

An alternative algorithm known as proof of stake (PoS) has been proposed in response to criticisms of proof of work (PoW) systems. Rather than relying on computational work, PoS uses a random selection process where validators with more wealth have a higher probability of successful mining. This can result in faster blockchains with lower electricity consumption and a reduced risk of a 51% attack. In addition, miners are not incentivized to invest in hardware, such as ASICs, as their rewards are only based on transaction fees. PoS can utilize game-theoretical mechanism design to prevent collusion and centralization and penalize dishonest or malicious behavior.

However, PoS systems have a vulnerability known as the "nothing at stake" problem, which refers to the low cost of voting/claiming rewards for multiple chains. There are several proposed solutions, such as implementing punishment mechanisms for validators that create blocks on multiple chains or punishing validators for creating blocks on the wrong chain like PoW. PoS algorithms can be used in both public blockchains with unknown validators and private/business-oriented settings with trusted validators. Ethereum, a popular blockchain platform for developers and enterprises, plans to switch from PoW to PoS solutions.

In trusted or semi-trusted environments, voting-based algorithms such as Practical Byzantine Fault Tolerance (PBFT) can also be used.

2.1.3. Practical Byzantine Fault Tolerance (PBFT)

Byzantine Fault Tolerance (BFT) is a type of algorithm used to ensure the correct functioning of distributed systems in the presence of faulty or malicious nodes. It was first introduced in a paper by Lamport et al. in 1982, which described the problem of Byzantine Generals trying to coordinate an attack on a fortress. In a distributed system, the equivalent problem is ensuring that all nodes reach a consensus on some value or action, despite the possibility of some nodes behaving erratically or maliciously.

PBFT (Practical Byzantine Fault Tolerance) is a specific type of BFT algorithm that uses voting to reach a consensus. In PBFT, validator nodes verify and sign transactions, and when a sufficient number of signatures have been collected, the transactions are considered valid and the consensus is reached. PBFT provides instant finality, as blocks that have been globally verified cannot be reversed. However, it has some limitations: it is more suited to trusted environments rather than public, permissionless ledger applications, and it requires at least 2/3 of the network to behave honestly. Additionally, as the size of the network increases, the message overhead may become significant, which can impact both speed and scalability.

There have been many variations of BFT-based protocols proposed by key developers, such as Hyperledger and Tendermint. These variations aim to address some of the limitations of PBFT and improve its performance in different contexts.

3. BLOCKCHAIN'S POTENTIAL AND NOTABLE USE CASES IN CARBON CREDITS

Blockchain technology has the potential to revolutionize the operations and business processes of carbon credit companies. It can be applied in a variety of ways, including

Billing: Blockchains, smart contracts, and smart metering can be used to automate billing for consumers and distributed generators, as well as enable carbon credit-based micropayments and pay-as-you-go solutions.

Sales and marketing: By using artificial intelligence techniques like machine learning, companies can identify consumer carbon emission patterns and offer tailored, value-added products.

Trading and markets: Blockchain-based distributed trading platforms could disrupt market operations, such as wholesale market management, commodity trading, and risk management. There are also efforts to use blockchains for green certificate trading.

Automation: Blockchains can improve the control of decentralized carbon credit trading systems enabled by peer-to-peer trading and could increase regulated trading.

Security and identity management: Blockchain can provide enhanced security and privacy, as well as protect data confidentiality and identity management.

Sharing of resources: Blockchains can be used to facilitate the sharing of resources such as EV charging infrastructure, data, and common centralized community storage.

Competition: Smart contracts could make it easier and faster to switch credit suppliers, potentially increasing competition and reducing tariffs.

Transparency: Blockchains offer immutable records and transparent processes, which can improve auditing and regulatory compliance

4. CONCLUSION

Carbon credits are a mechanism for reducing greenhouse gas emissions by investing in projects that reduce or offset them. The carbon credit market has struggled with issues of trust and verification, but there is a plan to use blockchain technology and an enhanced version of the Delegation Proof of Stake (DPoS) consensus algorithm to improve the system's performance and reliability. Artificial intelligence algorithms will also be incorporated to ensure the accuracy of carbon emission rights. Previously, carbon credits were only traded in business-to-business (B2B) markets, but they are now expanding to peer-to-peer (P2P) markets, which could potentially create a sustainable business market. Ethereum is a decentralized, open-source blockchain platform that runs smart contracts: applications that run exactly as programmed without any possibility of downtime, censorship, fraud, or third-party interference. Ethereum can be used to build decentralized applications (dApps) on its blockchain. The potential use of Ethereum in the carbon credits market is to create a decentralized platform for buying and selling carbon credits using smart contracts. This platform could facilitate the P2P trading of carbon credits and make the market more transparent and efficient. The use of smart contracts on the Ethereum platform could also help to automate the process of buying and selling

carbon credits, reducing the need for intermediaries and increasing the speed of transactions. In addition, Ethereum's blockchain could be used to track and verify the ownership and issuance of carbon credits, ensuring that they are being used accurately and appropriately. This could help to build trust in the carbon credits market and make it easier for companies and individuals to participate.

REFERENCES

[1] D. Effah, B. Chunguang, F. Appiah, B. L. Y. Agbley and M. Quayson, "Carbon Emission Monitoring and Credit Trading: The Blockchain and IOT Approach," 2021 18th International Computer Conference on Wavelet Active Media Technology and Information Processing (ICCWAMTIP), 2021, pp. 106-109, doi: 10.1109/ICCWAMTIP53232.2021.9674144.

[2] https://verra.org/npr-reporting-on-forest-carbon-credits-gets-it-wrong-in-5-ways/

[3] Junghoon Woo, Ridah Fatima, Charles J. Kibert, Richard E. Newman, Yifeng Tian, Ravi S. Srinivasan, Applying blockchain technology for building energy performance measurement, reporting, and verification (MRV) and the carbon credit market: A review of the literature,

[4] Saraji, Soheil & Borowczak, Mike. (2021). A Blockchain-based Carbon Credit Ecosystem.

[5] D. Patel, B. Britto, S. Sharma, K. Gaikwad, Y. Dusing, and M. Gupta, "Carbon Credits on Blockchain," 2020 International Conference on Innovative Trends in Information Technology (ICITIIT), 2020, pp. 1-5, doi: 10.1109/ICITIIT49094.2020.9071536.

[6] Kim, S.-K., and Huh, J.-H., (2020), Blockchain of Carbon Trading for UN Sustainable Development Goals, Sustainability, 12, 4021; doi:10.3390/su12104021

[7] Crippa, M., Guizzardi, D., Muntean, M., Schaaf, E., Solazzo, E., Monforti-Ferrario, F., Olivier, J.G.J., Vignati, E., Fossil CO2 emissions of all world countries - 2020 Report, EUR 30358 EN, Publications Office of the European Union, Luxembourg, 2020, ISBN 978-92-76-21515-8, doi:10.2760/143674, JRC121460.

[8] Franke, L.; Schletz, M.; Salomo, S. Designing a Blockchain Model for the Paris Agreement's Carbon Market Mechanism. Sustainability 2020, 12, 1068

[9] Andoni, M.; Robu, V.; Flynn, D.; Abram, S.; Geach, D.; Jenkins, D.; McCallum, P.; Peacock, A. Blockchain technology in the energy sector: A systematic review of challenges and opportunities. Renew. Sustain. Energy Rev. 2019, 100, 143–174. [CrossRef]

[10] Khaqqi, K. N., Sikorski, J. J., Hadinoto, K., & Kraft, M. (2018). Incorporating seller/buyer reputation-based system in blockchain-enabled emission trading application. Applied Energy, 209, 8–19. doi: 10.1016/j.apenergy.2017.10.070

[11] Pan, Y., Zhang, X., Wang, Y., Yan, J., Zhou, S., Li, G. & Bao, J. (2019) Application of blockchain in carbon trading, Energy Procedia.

[12] Hua, W., Sun, H., 2019. A Blockchain-Based Peer-to-Peer Trading Scheme Coupling Energy and Carbon Markets. In: SEST 2019 - 2nd International Conference on Smart Energy Systems and Technologies.

[13] Fernando, Y., Rozuar, N. H. M., & Mergeresa, F. (2021). The blockchain-enabled technology and carbon performance: Insights from early adopters. Technology in Society, 64, 101507. doi: 10.1016/j.techsoc.2020.101507

[14] Sadawi, A. A., Madani, B., Saboor, S., Ndiaye, M., & Abu-Lebdeh, G. (2021). A comprehensive hierarchical blockchain system for carbon emission trading utilizing blockchain of things and smart contracts. Technological Forecasting and Social Change, 173, 121124. doi: 10.1016/j.techfore.2021.12112