International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 07 Issue: 04 | Apr 2020 www.irjet.net p-ISSN: 2395-0072

A Detailed Study on Cryptocurrency

Prabha M[1], Priya R[2], Varsha D[3], Preethi S[4]

[1]*Assistant Professor, Department of IT*
[2,3,4]*UG Students, Department of IT, Velammal College of Engineering and Technology, Madurai.*

Abstract- *Cryptocurrency has now emerged as an important asset in financial and business applications. They rely on a secure backbone technology called Blockchain Technology which allows storing all the transactions made in a secure distributed ledger, a data structure which is done by the process called mining. Cryptocurrency lacks a central authority as they were designed as peer-to-peer systems making it largely decentralized. In this paper, we survey various cryptocurrencies and their underlying technology architecture along with different aspects of the challenges and attacks they face.*

Keywords- Cryptocurrency, Blockchain Technology, Mining, Peer-to-peer network.

1. INTRODUCTION

Cryptocurrencies are digital assets where cryptography is used to create and distribute currency through peer-to-peer networks [1]. Since the development of Bitcoin in 2009 by Satoshi Nakamoto, the first-ever cryptocurrency, it has become an important component of the international financial market after ten years of development [2]. The cryptocurrency market has grown to a total market capitalization of 209 billion USD [3].

2. HISTORY

Currency types of payment were made as early as 22000 BC. In the era of digitalization, it's just being converted into a digital format called cryptocurrency run by a secure technology [4]. Earlier around 2008 there were several theories on cryptocurrencies but around 2009, a group of people or an anonymous person named Satoshi Nakamoto developed the first-ever cryptocurrency, called the Bitcoin. Initially it's value was nothing, later in 2010 it was just approximately 0.003 USD.

In 2011, coins slowly started emerging namely: Litecoin, Namecoin, Peercoin, Ripple, NEM, Stellar, Etherum, and Tether, etc. Since then there have been around 2,502 coins to date with new coins coming into existence every now and then.

3. OVERVIEW AND KEY CONCEPTS

Cryptocurrencies are based on a technology which was originally built for the same, known as the Blockchain Technology.

Blockchain is basically an endless chain of blocks that stores all the transactions processed in a public ledger. It works in a decentralized environment involving several core technologies such as digital signature, cryptographic hash and distributed consensus algorithms. Blockchain has many key characteristics like transparency, immutability and auditability [5].

Mining plays a vital role in cryptocurrency by performing various important processes such as storing all the previous transactions in blocks and providing certain verification processes like the proof-of-work and proof-of-stake.

A malicious user may create multiple nodes and try to validate an invalid transaction. To prevent this, miners are required to solve resource-intensive tasks. Resource intensiveness makes it expensive for a malicious user to create enough false identities to outnumber benign users and validate an invalid transaction.

The resource-intensive task can be any of the following:

- ***Proof of Work*** - which is an easily verifiable result of a resource-intensive task that confirms that the task has been performed.
- ***Proof of Stake*** - which requires the miner to show how much currency the miner owns in the system.
- ***Proof of Retrievability -*** which requires the miner to show that the data he was given to the store is intact and can be recovered at will [1].

Proof-of-work is the dynamic construction of a blockchain that can be seen as a sequential composition of it. The analysis relies critically on generic properties of cryptographic hash functions, modeled as a random oracle (RO) and only given oracle access [6]. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work which forms a record that cannot be changed without redoing the proof-of-work,

it forms a long chain called the ***proof-of-sequence*** [7].

The ***Proof-of-Stake*** model uses a different model to confirm transactions and reach consensus by using a cryptographic algorithm.

4. ARCHITECTURE

The Blockchain is the fundamental technology underlying various applications globally. The technology helps establish a disintermediary transaction system without mutual trust and centralized control over the individual nodes based on techniques such as data encryption, time-stamping, distributed consensus algorithms and economic incentive mechanisms [8].

The first block contains the first transactions of a given cryptocurrency. The hash of the first block is passed forward to the miner, which uses it and generates a nonce to create a hash for the second block. Likewise, the hash of the third block contains the hashes of the first and second block and so on. A strict chronological chain or link is created from the genesis block to the current block through the inclusion of hashes. There is a single, unique path from the most recent block to that first block. This relationship makes it extremely difficult for an attacker to tamper with the information in a block, because all subsequent blocks would have to be regenerated, which would be detected because the final hash wouldn't match.

When two blocks are created at the same time a ***fork*** occurs. The block created first according to the timestamp in the block header is accepted in the chain and subsequent blocks link to the accepted block [1].

Block structure - The Blockchain comprises a sequence of blocks, which stores the information of all the transactions, similar to a public ledger. These blocks are linked to each other via a reference hash that belongs to the previous block known as the parent block. The starting block is called the genesis block, which does not have any parent block. A block consists of the block header and the block body. The block header includes metadata such as block version, parent block hash, Merkle tree root hash, timestamp, n Bits, and nonce. The block body is composed of a transaction counter and transactions. The transaction counter refers to how many transactions follow, and transactions represent the list of recorded transactions in the block. The maximum number of transactions that a block can contain depends on the block size and the size of each transaction. Blockchain uses an asymmetric cryptography mechanism to validate the authentication of transactions. A digital signature based on asymmetric cryptography is used in an untrustworthy environment such as the blockchain network. In this process, each participant in the network owns a private key and public key pair. The private key is used for signing or encrypting the transaction while the public key is distributed throughout the network and is visible to everyone, which helps to decrypt the following transaction [5].

5. SMART CONTRACTS

In 1974, Nick Szabo introduced the concept of a smart contract. He defined it as a "computerized transaction protocol". Smart contracts translate contractual clauses into coded and embed them into hardware and software. This structure makes them self-enforceable in order to minimize the need for trusted intermediaries between transacting parties. Blockchain technology, which provides characteristics of immutability, irreversibility, decentralization and persistence, has made smart contracts achievable.

Smart contract platforms need to provide three properties: they need to be deterministic, isolated and terminable.

Deterministic - they need to produce the same result each time they run. Several conditions that affect deterministic behavior in a program are

- If it relies on an external state or relies on dynamic or non-deterministic function calls, such as those that depend on hardware timer values, random values or dynamic values.
- If it operates in a way that is sensitive to timing, for example if multiple processors are writing to the same data at the same time, the precise order in which each processor writes its data affects the result.
- If a hardware error causes the program's state of change unexpectedly.

Isolation- is the second for a smart contract. A smart can be uploaded by anyone, which introduces a risk since any single contract may contain viruses and bugs. If the contract is not isolated, this could impact the entire blockchain ecosystem. Therefore, contracts need to be isolated in a sandbox to save the entire ecosystem from any negative effects that one contract could introduce.

Termination- is also essential in smart contracts since by definition a smart contract must be capable of completing within a specified time limit. There are three primary methods to guarantee termination in smart contract programs.

- *Turing incompleteness* - to avoid entering an endless loop, a Turing incomplete blockchain will have limited functionality and may not be capable of making jumps and loops.
- *Steps and Fee Meters*- a program can keep track of the

steps it has taken and then terminates once a step count has reached. With a fee meter, contracts are executed with a prepaid amount. Every instruction execution requires a specified fee. If the fee spent exceeds the prepaid allocated amount, the contract is subsequently terminated.

- *Timers*- a predetermined timer is maintained so if the contract execution exceeds the time limit then it is externally aborted.

Smart contracts, due to their self- executing, self-enforcing nature provide great potential to disrupt numerous industries. However as currently implemented they are not without considerable risks and challenges. The results of these risks and challenges can be observed in a number of bugs, scams and errors that have occurred since their inception in mid-2015 [10].

6. CHALLENGES

As an emerging technology, Blockchain is facing multiple challenges and problems. These challenges can be broadly classified under various factors. A major flaw detected in the proof-of-work system was the 51% attack. If a single entity occupies more than half of the total mining hash-rate, then that entity would be able to manipulate the Blockchain at will. An attacker who controls more than 50% of the network's computing power can for the time that they are in control, exclude and modify the ordering of transactions. This allows the successful attacker to perform the following operations:

- Reverse transactions that they send
- Prevent some or all transactions from validation
- Prevent some or all other generators from getting any generations.

While this is theoretically possible, it would require the attacker to have access to immense resources. Acquiring such resources would be expensive and the overall expense might well exceed the potential profit. However, to address this threat proof-of-stake was introduced.

Cryptocurrencies are also vulnerable to various attacks so far. One such attack is the ***Sybil Attack*** in which the user takes on multiple identities. Here attackers populate the network with spurious clients controlled by them. Then they use them to gain a disproportionately large influence to the point where the number of malicious nodes is greater than the number of legitimate nodes. The attackers can disconnect legitimate nodes from the network by Denial of Service by not relaying transaction information and selectively relay transaction information, exposing the victim to double spending [1].

Pool Hopping attack- M. Rosenfeld introduced a pool hopping attack, in which an adversary exploits information about the number of transmitted shares in the mining pool to carry out selfish mining (i.e., the process of mining bitcoins where a set of miners collude to augment their revenue). Under this threat model, the attacker attempts to execute a continual and uninterrupted analysis over the number of shares transmitted by contiguous miner nodes to their pool manager for the purpose of exploring a new transaction block. The promise here is that rewards are distributed according to the transmitted shares. Therefore, if a huge amount of shares is transmitted and do not have any new transaction block, the attacker will eventually get a relatively small portion of the reward. Hence, it could be more beneficial for an attacker to turn into another mining pool or even mine distinctly. Conversely, a selfish miner could complicate with another pool to gain a reward from this connivance pool and attack another pool.

Bribery attack- J. Bonneau details an attack model called the bribery, in which an adversary can acquire most of the processing resources for a fixed period of time through bribery. In particular, J. Bonneau describes three methods to insert bribery into the Bitcoin network. (1) Negative-Fee Mining Pool where an adversary creates a pool through paying a higher return, (2) Out-of-Band Payment where an attacker pays the owner with processing resources and directly makes these tricked owners mine transactions' blocks appointed by the attacker, and (3) In-Band Payment through a forking operation where an adversary tries to bribe via Bitcoin itself (by originating a fork that has a bribe in the form of free money for any miner node taking over the fork). If an adversary possesses most of the hashing power, they might establish various types of attacks, including, but not limited to, DDoS and double-spending. Furthermore, miner nodes accepting bribes will acquire only a short-lived profit, which could be undermined by the losses under the existence of Goldfinger and DDoS attacks, or even through an exchange rate-based crash.

Security Issues - The Open Web Application Security Project (OWASP) mobile application provides a collection of the most common security issues.

- **Improper Platform Usage:** The mobile platform such as Apple iOS and Android provides a suite of host operating system services. Improper implementation of these services can lead to known security threats. The host system has published guidelines for implementation, violation of these guidelines is the most common way of inflicting a known threat. For example, using App Local Storage instead of iOS Keychain in iOS applications to store sensitive data. App local storage may expose the information to other components of the application whereas the data stored in Keychain is secured from

unauthorized access by the operating system.

- **Insecure Data Storage:** This category includes unintentional data leakage and insecure information storage. Data stored in local SQL databases and Log files may be prone to threat if the adversary gains access to the device. Storing sensitive data to external storage is considered insecure and can be exploited. Unlike the insecure storage media, the unintentional data leakage may be hard to detect. The data leakage may exist due to vulnerabilities present in frameworks, hardware or due to rooted devices. Applications without proper checks for data leakage can suffer from known exploitable vulnerabilities.

- **Insecure Communication:** Mobile applications often communicate with various services on the internet. This communication at times may involve the transmission of sensitive information such as user credentials. Bad actors might exploit vulnerabilities present in communication to intercept sensitive information. This category includes threats induced by improper implementation of SSL for network communication.

- **Insecure Authentication Applications:** dealing with sensitive information such as personal or financial data should implement proper user authentication. This category of threat includes issues related to session management and user identification. One example of insecure authentication is the case where the application permits the device to execute a backend API service request without an access token.

- **Insufficient Cryptography Applications:** that leverage encryption often uses cryptographic functions. There are two types of threats that can exploit insufficient cryptography. The first one is using a vulnerability in the implementation of the encryption/decryption process to gain access to sensitive information. The second threat occurs due to the usage of a broken cryptographic function.

- **Insecure Authorization:** During authorization, the application should verify if the authenticated user has permission to perform a given operation. Failure to do so may leave the application and back-end vulnerable. If an application allows the user to perform API calls without proper authorization, a rogue user may compromise the security of the application.

- **Poor Code Quality:** This category involves bad programming practices that may result in vulnerabilities such as buffer overflow. These code-level mistakes may result in the attacker exploiting business logic to bypass security provisions.

- **Code Tampering Mobile applications:** work in an environment that is not administered by the developers of the application. This allows attackers to tamper with the code of the application to insert a backdoor or to change API calls to gain sensitive information. Attackers can modify the source code and re-sign the application before distributing it to end-users.

- **Reverse Engineering:** This category involves the generation of an abstract view of the functionality of the application. This view may allow the attacker to determine the application logic in place including the deduction of source code, libraries, and other assets in use. After determining the application logic, the attacker can find vulnerabilities to exploit in the design or flow of information.

- **Extraneous Functionality:** During the development process, the developers often use back doors for testing. This back door may involve bypassing two-step authentication during testing. Failure to remove such back doors can leave the application vulnerable[3].

Performance and Scalability- There is a concern regarding whether it could meet up with the increasing demand coming from different business and government-based sectors, especially regarding performance and scalability. Recently, researchers are working to address the scalability issues regarding the number of replicas in the network as well the performance concern, such as throughput (number of transactions per second) and latency (required time for adding a block of transactions in the blockchain). Increasing the number of replicas can have a detrimental effect on the throughput and latency because the network needs to deal with the increased amount of message exchange and processing. Although protocols such as PoW can ensure scalability, it is suffering from low throughput and high latency. This bottleneck occurs due to the resource wasted for solving the cryptographic puzzle to publish a block and append it to the chain. For example, Bitcoin is a PoW-based protocol that can scale a large number of replicas. In contrast, it provides low throughput considering only 6-10 transactions per second and is capable of generating a block with an average of 10 minutes. Another drawback of this consensus procedure, is that it is CPU intensive and hence, causes high consumption of electricity.

Privacy- Blockchain is considered to provide safety and privacy to the sensitive personal data as users can make transactions with generated addresses instead of using a real identity. However, some researchers suggested that Blockchain might be vulnerable in terms of transactional privacy as the public key for initiating a transaction is visible to the network peers. Although it is claimed that a peer can be anonymous in the Blockchain network, some

recent studies on the Bitcoin platform have shown that the transaction history can be linked to reveal members' true identity. In addition, Biryukov et al. proposed a method to link peers' pseudonyms to IP addresses while they are behind the firewalls or network address translation (NAT). He also mentioned that peers can be uniquely identified through its connected set of nodes. The main reason behind blockchains vulnerability to information leakage is because the details and balances of all public keys are visible to everyone in the network. Therefore, the privacy and security requirements should be defined at the initial stage of Blockchain applications.

Interoperability- From Deloitte's 2018 report, it can be observed that many industries are currently interested in adopting blockchain technology. However, there is no standard protocol that will allow them to collaborate and integrate with each other. This situation is called a lack of interoperability and has a detrimental impact on the growth of the blockchain industry. For this reason, instead of offering different practical solutions to a variety of business models, cryptocurrency is still the main platform for blockchain technology. Although the lack of interoperability grants freedom to the blockchain developers to code in different programming platforms, all these networks are isolated and can not interact with each other. Standardization is required for the collaboration of enterprises on application development to share blockchain-based solutions as well as integrate with existing systems.

Energy consumption- The proof-of-work (PoW) algorithm has enabled bitcoin to perform transactions among peers in a trustless distributed decentralized environment. However, while doing this work, miner computers are consuming a huge amount of electrical energy. To provide insights about this highly unsustainable nature of the PoW algorithm, the bitcoin energy consumption index was created. The incentive mechanism motivates people around the world to mine Bitcoin. The mining process provides a solid stream of revenue that attracts individuals to run power-hungry devices to gain a chunk of it. As a result, the total energy consumption rate of the Bitcoin network reached a new high along with the value of the cryptocurrency. Based on a report published by the International Energy Agency, the overall consumption of the Bitcoin network is higher than a number of countries. Bitcoin is not only responsible for the consumption of a massive amount of energy but also contributes to an extreme carbon footprint. The coal-fired power plants in China are providing fuel for the bitcoins network. Nature Climate Change (October 2018) even suggested that Bitcoin mining alone could push global warming above 2 C within less than three decades.

According to Bitcoin energy consumption index :

• Bitcoin's current estimated annual electricity consumption: 51.92 TWh

• Annualized estimated global mining costs:

$2,595,834,583

• Bitcoin's electricity consumption as a percentage of the world's electricity consumption: 0.23%

• Carbon footprint per transaction: 274.29 kg of CO2 another way to demonstrate the unsustainable nature of a blockchain application is to compare its energy consumption with other payment systems such as VISA. This company has consumed 674,922 Gigajoules of energy for processing 111.2 billion transactions in 2017. Approximately 17,000 US households could use this amount of energy. However, a blockchain application such as bitcoin is more energy-intensive per transaction than VISA. It is possible to argue that blockchain has eliminated the need for intermediary costs; however, the cost is too high to bear. The solution for this issue might be redesigning the infrastructure of blockchain or simply using an alternative consensus algorithm such as PoS, where selected miners will verify the block without any competition. Hence, it will consume less energy.

7. FUTURE DIRECTIONS

The future of blockchain technology is about to take over the world just because of solutions and not because of the availability of conventional technology offered. In a word, socio-economic is emerging on the number of growing innovation technologies. In such a case, digital economics accepts the challenge within taking an approach by increasing the number of developers, scientists and IT specialists growing all around the world. But in some cases like bitcoin future halving of some cryptocurrency new miners' reward will become narrow of their profit range. Otherwise, new miners can gain profit if the opportunities continue through the existing market [4].

Blockchain technology allows companies to create a digital trail of records of their innovations and can generate a certificate upon registering the new inventions, proofs-of-concept and designs that could prove the integrity, existence, and ownership of any IP asset. By using the unique cryptographic layer, all notarized data such as trade secrets or copyright claims could remain private and secured.

It is also believed that big data analytics could be well combined with blockchain, especially in data management and data analytics. For data management, blockchain could be utilized to store data in a secured and distributed manner. Moreover, the immutability feature of blockchain

could ensure the authenticity of the data. For instance, patient health records stored in the distributed ledger would be difficult to tamper and no one can steal that information without the consent of the owner. Transactions on the blockchain could be used for data analytics. In this process, it is possible to determine the potential partners' trading patterns and behaviors in the blockchain network.

Likewise, various smart contract developing platforms are emerging. A smart contract in blockchain could be used in different application areas, such as IoT-based platforms and banking services. The research on smart contracts can be separated into two types; development and evaluation.

Smart contract platform development could be performed under development. Ethereum is providing the infrastructure to deploy many smart-contract based solutions, such as car auctions, online trading, and so on. Evaluation refers to performance and code analysis. It has been proven that even a small bug in developing smart contracts could cause a disastrous impact. The precise example could be the DAO attack, where over 60 million dollars were stolen due to the recursive call bug. Therefore, it is very important to analyze the attacks on the smart contract. On the other hand, the performance of the smart contract could become an important research topic. As blockchain technology is acquiring immense attention from the public and private sectors, more smart contract-based applications would be put into use [5].

8. APPLICATIONS

- INTERNET OF THINGS:

The significant increase in IoT devices in recent years leads to exposing insecure big data. The privacy and security of the data produced by IoT devices are the major challenges in this field. Exploiting blockchain technology has been investigated by many researchers to address these issues. Samaniego and Deters introduce blockchain as a service for IoT systems. They discuss that blockchain and smart contracts can be applied for the configuration of IoT devices, recording data capture from sensors, and micro-payments. Panarello et al. represent a survey to analyze the research related to the blockchain and IoT context.

- HEALTHCARE:

Current healthcare systems suffer from various problems such as scattered data, difficult access, data consistency, interoperability and privacy concerns. In general, most of the studies aim to solve these issues by proposing an architecture design or implementing a system based on blockchain and smart contracts. The main focus of these studies is the management of users' identity, access control and sharing medical data using different available blockchain platforms such as Ethereum and Hyperledger. Also, blockchain key benefits for different healthcare applications such as record management, insurance claim process, clinical research or creating a healthcare data ledger. In this review paper, we chose studies with the focus on smart contracts or at least the smart contract design has been presented in the architecture. Healthcare applications based on blockchain and smart contracts.

- BUSINESS PROCESS MANAGEMENT (BPM):

The main unsolved issue in the collaborative business process in organizations is the lack of trust, and similar to many other applications using blockchain has been considered as a solution to address this issue without relying on any central authority. Investigating blockchain potential in the domain of BPM applications, the challenges for applying this technology and the advantages that it brings for us.

Weber implemented three cases for integrating blockchain in BPM by introducing a method to transform the collaborative business process to a factory contract and then run its instances as a smart contract. In continuation they represent an optimized resource usage approach to minimize the cost in terms of Gas for executing smart contracts that are responsible for executing business process instances as well as increasing throughput.

- VOTING:

Blockchain can help to create a secure and privacy-preserving voting system. Generally, voting systems suffer from trust issues and the chance of cheating and leakage is remarkable in centralized voting systems. presents a voting system based on smart contracts.

McCorry et al presents a privacy-preserving boardroom voting system using smart contacts and Zero-knowledge proof protocol. The implementation is based on Solidity smart contracts and Ethereum public blockchain. The two main smart contracts are "voting contract" and "cryptography contract". The voting contract implements the voting protocol and verifies zero-knowledge proofs. The cryptography contract is responsible for generating two types of zero-knowledge proofs for the voters: Schnorr proof and one-out-of-two proof.

Shah also proposes a voting system, which integrates client-server architecture with blockchain. The four main components of the proposed system include User or front-end interface, Authentication server, Arbitration Server, and private Blockchain. The smart contract is responsible for verifying the votes based on the type of the election

(interim or non-interim) and adding the vote as a new record on the Blockchain [11].

9. CONCLUSION

This paper studied cryptocurrencies from their origin of making along with its underlying Blockchain Technology architecture and involving all the concepts regarding cryptocurrencies and its stature. The transaction protocol called the smart contract for excluding the intervention of any third-party involvement. We looked into all the various challenges and attacks met by the cryptocurrencies. Blockchain technology and cryptocurrencies have a long way to go as they are still in the development process. Hence a future predicament was reformed based on their current status. The cryptocurrencies and blockchain have tremendous usage as they can be widely used in any field and further in future this is about to get intensified.

10. REFERENCES

[1] Ujan Mukhopadhyay, Anthony Skjellum, Oluwakemi Hambolu, Jon Oakley, Lu Yu, and Richard Brooks, "A Brief Survey of Cryptocurrency Systems".

[2] Jiaqi Liang, Linjing Li, Weiyun Chen and Daniel Zeng, "Towards an Understanding of Cryptocurrency: A Comparative Analysis of Cryptocurrency, Foreign Exchange, and Stock".

[3] Ashish Rajendra Sai, Jim Buckley and Andrew Le Gear, "Privacy and Security analysis of cryptocurrency mobile applications".

[4] Mohammad Rabiul Islam, Prof Dr. Imad Fakhri Al-Shaikhli, Dr. Rizal Mohd Nor and Kabir Sardar Mohammad, "Cryptocurrency vs Fiat Currency: Architecture, Algorithm, Cashflow & Ledger Technology on Emerging Economy" Subtitle: The Influential facts of Cryptocurrency and Fiat Currency.

[5] Ahmed Afif Monrat, Olov Schelen and Karl Andersson, "A Survey of Blockchain from the Perspectives of Applications, Challenges and Opportunities", DOI 10.1109/ACCESS.2019.2936094, IEEE Access.

[6] Alexandru Cojocaru, Juan Garay, Aggelos Kiayias, Fang Song and Petros WalldeN, "The Bitcoin Backbone Protocol Against Quantum Adversaries".

[7] SatoshiNakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System".

[8] Yong Yuan and Fei-Yue Wang, "Blockchain and Cryptocurrencies: Model, Techniques, and Applications".

[9] Mohamed Rahouti, Kaiqi, Xiong and Nasir Ghani, "Bitcoin Concepts, Threats, and Machine-Learning Security Solutions", DOI 10.1109/ACCESS.2018.2874539, IEEE Access.

[10] Christopher G.Harris, "The Risk and Challenges of Implementing Ethereum Smart Contracts ", University of Northern Colorado Greeley, CO 80639 USA.

[11] S. Rouhani and R. Deters, "Security, Performance, and Applications of Smart Contracts: A Systematic Survey ", DOI 10.1109/ACCESS.2019.2911031, IEEE Access.