International Journal of Research in Engineering and Science (IJRES)
ISSN (Online): 2320-9364, ISSN (Print): 2320-9356
www.ijres.org Volume 12 Issue 2 ǁ February 2024 ǁ PP. 77-83

An analysis of blockchain technology

Alaka Rout
College of Engineering Bhubaneswar, Biju Pattnaik University of Technology, Odisha, India

Abstract— *In this paper, we will discuss blockchain technologies. Blockchain engineers are in high demand regardless of the blockchain they are developing on. Protocols such as Aave, Yearn Finance, and Synthetix have significant monetary value locked in them, allowing people to engage in decentralized finance (DeFi) and make censorship-resistant actions. Some of these procedures are less than one year old. Blockchain and solidity applications are fostering a world of more trust and accountability, with smart contract engineering talents becoming the most sought-after in the world.*

Keywords—*Blockchain; technologies; decentralized; finance; solidity*

Date of Submission: 04-02-2024 Date of acceptance: 16-02-2024

I. INTRODUCTION

Bitcoin [15] was among the first protocols to utilize blockchain technology [16]. Satoshi Nakamoto, the pseudonymous creator of Bitcoin, issued the whitepaper [15]. It described how bitcoin can be used to conduct peer-to-peer transactions in a decentralized network. This network is cryptographically secure and allows users to engage in censorship-resistant finance in a decentralized manner. A few years later, in 2015, a man named Vitalik Buterin published a white paper [3] outlining a new protocol called Ethereum that used the same blockchain technology but added an extra functionality. Other co-founders took this blockchain technology and applied it in ways that allow anyone to create completely decentralized applications [4], decentralize organizations [12], develop smart contracts [14],[5], and enter into agreements without a third-party mediator or centralized governing agency.

Their idea was to take the same pieces that made bit coin and add smart contracts to it. Technically this wasn't a new idea.In1994 a man named Nick Zabo proposed a technology called smart contracts. Asmart contract is a self-executing set of instructions. It is executed without a third party intermediary. They are placed on a block chain. Smart contracts are similar to regular traditional contracts that people make between each other but instead of writing these contracts down on pen and paper or typing that on the computer it's entirely written in code. The terms of the agreement are written in code and automatically executed by the decentralized blockchain network. Bitcoin also have smart contracts however they're not turing complete. They don't have the full range of capabilities as a turing complete application like Ethereum. This is an intentional move by the Bitcoin developers as they view the Bitcoin network as an asset whereas Ethereum developers viewed the Ethereum network asan asset and also autility for the building of smart contracts.

This paper consists of six sections. In section II we present smart contracts. Section III describes features of block chain smart contracts. Section IV gives details on the Ethereum wallet. In section V we give two block chain consensus mechanisms, proof of work and proof of stake.The conclusion is given in section VI.

II. SMARTCONTRACTS

Smart contracts are revolutionary technologies, but they actually come with a fatal flaw. This is known as the oracle problem. Blockchains are deterministic systems and everything that happens in these smart contracts and on this blockchain happens in a little sandbox. If you want smart contracts to actually be digital superior agreements, then they need some way to interact with the real world and get real data which is external to or outside the block chain computation. Oracles come into play in such circumstances. Oracles are devices that bring data into a block chain or execute some type of external computation. At first view this seems like the perfect solution.Well this may not quite be the case. Our block chains and smart contracts are decentralized applications and in order for them to stay decentralized that means they would also need to get their data and external computation in a decentralized manner. Thus, your on-chain logic will be decentralized on the blockchain, but you'll also need your off-chain data and external computation decentralized as well. Combining these on-chain logic settlement layers and these off-chain data and external computation builds what's called hybrid smart contracts. A large majority of applications today are hybrid smart contracts.

The protocol Chain link [17]is a decentralized modular oracle network that allows you to bring data into your smart contracts and do external computation. These hybrid smart contracts can have on-chain

settlement and interact with the real world in some meaningful way. Chain link is an incredibly powerful oracle network because it allows us toget data, get randomness, do some type of upkeep or really customize our smart contracts and elevate them to perform other tasks. A hybrid smart contract is a smart contract with an off chain component. A decentralized application isusually a combination of several smart contracts. Solidity is a smart contract programming language. You can write a singular smart with Solidity [6] and deploy on a blockchain such as Ethereum. Non-fungible token (NFTs) [8] and decentralized autonomous organizations (DAOs) [20] have taken the Ethereum vision to a new level.

Once you learn the core basics of smart contract development on the Ethereum platform, the skills translate to these other chains as well. Learning a specific tool or chain is useful because most of them work together pretty seamlessly. There are a few exceptions to this rule and there are some smart contract platforms aka block chains that don't use Solidity. However, learning the fundamental skills will translate to every single other block chain and Ethereum is by far the most popular and most used smart contract block chain or smart contract protocol. These three terms are usedinterchangeably: blockchain, smart contract platform, smart contract protocol. Similarly, Chainlink is the most popularand powerful decentralized oracle network and is going to be the one that we're going to focus on. Chain link is also blockchain and smart contract platform agnostic meaning it'll work on Ethereum, Avalanche [19], Polygon, Polkadot [9] or any blockchain or smart contract platform.

This para graph gives a quick summary of what was discussed so far. Bitcoin was the first application to take the blockchain technology into a meaningful concept. Bitcoin is like digital gold where owners are able to make transactions between users. Ethereum takes this blockchain technology one step further. You can also build smart contract or decentralized applications, decentralized autonomous organizations and more for example you can code with smart contracts which can then access external data and external computation outside the blockchain using what's called oracles. Chainlink is the most powerful decentralized oracle network and allows us to build hybrid smart contracts which is a combination of decentralized on-chain logic settlement layer and any decentralized external off-chain data or computation hybrid smart contracts. A lot of questions can come up now likewhat makes bitcoin so interesting or what makes it like a digital gold and how are these smart contracts going to add any valueto therealworld.Beforewe getinto thenitty-gritty of how these blockchains and how these smart contracts actually work from a low level let's go high level and talk about some of the features and massive advantages that blockchains and smart contracts have over our traditional environments.

III. FEATURESOFBLOCKCHAINSMART CONTRACTS

Thefirstfeaturethatthesehaveistheyaredecentralized.It has a massive benefit blockchains are decentralized meaning there's no centralized source thatcontrolstheblockchain.The individuals that make up blockchain are known as node operatorsandtheyaretheindependentindividualsrunningthe software that connects the whole blockchain together. It's all these different independent individuals that make the blockchain decentralized. Let us look at an example. GameStop shares were no longer allowed to be bought because a centralized entity didn't want them to be bought anymore. They flipped a switch and nobody could buy that stock anymore. Essentially having a single entity controlling the entire financial market with the power to make these choices forus can be dangerous. How ever, Block chain is here to solve this. There's a narrative called the 'Bankless' narrative where users can actually live in a world where they don'thave a bank. Banks while good in theirownrighthave a history of doing some uncanny things. They also have the power to potentially freeze your funds, not letting you withdraw or move assets. They can do this as they are a centralized entity. They can flip as witch and control how you interact with your money every day. Being free of these centralized entities have this much power and this much control over your life has widespread positive ramifications transparency and flexibility. Everything that's done on a blockchain and all the rules that are made can be seen by everyone. There's no backdoor deals and there's no shady happenings. Everything that happens on chain can be seen by you. Thismeansthat there's no special information that a few have. Everyone has to play by the same rules and everyone can see exactly what those rules are.

Additionally, this doesn't mean that everything you do is tracked. The blockchain is pseudo-anonymous so you can create different accounts and you can interact with it in many different ways. Speed and efficiency is another advantage. Have you ever tried to make a withdrawal from the bank and it took three to five days. All the bank is doing is adding and subtracting numbers, basic first grade math. Why does it take so long? On the other hand block chains are verified by a decentralized collective. The settlement or withdrawal period in this case is substantially faster and depending on the block chain that you're using it can be from 10 minutes all the way down to just a couple of seconds. In the stock trading or hedge fund world it can actually take up to a week for you to buy or sell of a stock. You have to go through security and immutability. Block chains are immutable which means they can't be changed and because of this it means that they can't be tampered with or corrupted in any way shape or form. This allows us to have massive security on our data and on our transactions. If your computer goes down and your backup computers go down in the regular world your data is gone. If all your data

is on those two computers, you can be in dire straits. However, on a Block chain if several nodesgo down it doesn't matter because as long as one node and the entire system is running the data is safe and secure. There are thousands or hundreds of thousands of nodes running these block chain software meaning that everything that happens is recorded and is immutable and won't change. Hacking the block chain is nearly impossible and substantially harder than hacking a centralized entity. This is also much more secure in the asset sense as well instead of having gold in a vault or contract written on a piece of paper or on your computer you have an asset that is locked on the block chain forever. All you need to do to access it is have a private key or mnemonic which is essentially a password so you don't have to carry your gold around or carry your contracts around with you. It is always on the Blockchain.

Smart contracts in particular remove a massive conflict of interest in the traditional world. When we engage with users or individuals, they don't always have our best interests at heart. A lot of them are usually self-motivated in some sense. However, when we make an agreement with them this agreement can have a massive conflict of interest with the user who's supposed to execute that agreement. Let's take insurance for example. If I pay an insurance provider 100 a month and in the event that i get hit by a car we've made an agreement or a contract that they're going to pay my medical bills. However, they have this massive conflict of interest. Insurance companies aren't in the business of giving out money. They're in the business of making money so even thoughthey'vesignedthisagreementwhenthiseventoccurs they still don't want to pay this money out to me and if they can find a loophole in the contract they will because that is whattheyaremotivatedtodo.Thisisnativeintheagreements that we make today. Another party is the one who decides whetherornotthey'regoingtoexecutetheiragreementgiving execution power to that party who may not want to execute the contract. This has often led to frustration. You can sue themandgothroughthecourtprocessbutnowyou'rewasting allthistimeandmoneygoingthrough this longprocesstoget something that you should have originally gotten in the first place. This leads us to one of the biggest value of smart contracts. Smart contracts allow us to engage in trustless and trust minimized agreements. We currently live in a world of brand-based agreements. If I engage in some agreement and don't like the service that I'm provided with my alternative to thisis togo totoanotherbrandforan alternative service.The alternative brand is going to make the exact same set of promisesto me and then I have to trust them. Smart contracts allow us to move from this brand based agreements to math- based agreements. These math-based agreements we don't even have to trust that they're going to do the right thing. Hence, the name trustless as one plus one is always going to equal two. In a math world whatever the code determines is the input and output that's exactly what's going to happen every single time. There is exact replication of state as in a Turing machine.

Two major pieces of smart contracts are freedom and trustless. All these pieces allow us to live in a world that's more accountable more trusting more friendly. It allows us to work in an environment and a universe where things work seamlessly. It allows us the freedom to engage with other people. This happens because there's no centralized controlling body influencing every action that we make. All the rules are the same and nobody's getting special treatment. This brings out this new world of economic opportunity. As ourlivesbecomemoreandmoredigitalwe'reconstantlybeing bombarded with centralized services that want us to use their interfacesotheycanprofitonhowweinteractandforceusor push us to making the decisions that they're motivated for us. To make smart contracts decentralized applications and blockchain allows us to be free of these parties and live in an environment that's truly free and trustless.

Let's do a quick summary of what we just discussed. Blockchains are decentralized meaning that they are not controlled by a single centralized entity itis run by a network of independent users. Blockchains are transparent meaning that everything that happens on a blockchain everybody else can see and everybody else can work with and see that everyone's playing by the same rules. Blockchains are quick and efficient especially when it comes to monetary policy settlement. Blockchains are fast and easy immutability. Blockchains can't be changed or tampered with or corrupted andareincrediblysecure.Smartcontractsremovethemassive conflict of interest traditional agreements. Smart contracts allowustomoveawayfrompoliticalbrand-basedagreements to secure math-based agreements. Smartcontractsallowusto engage in trustless and trust minimized agreements. Smart contracts are a set of instructions which when placed on a blockchain are self-executing pieces of code not run by any centralizedintermediary.Inaddition,smartcontractsare typically paired with some type of oracle to get some information about the real world. When smart contracts are paired with an oracle they're called hybrid smart contracts. Chainlink is a secure decentralized modular oracle network used to bring data into your smart contracts and also make sometypeofexternalcomputation.Decentralizedautonomous organizations are organizations that live online and live in thesesmartcontracts.They'resimilartoaregularorganization inthetraditionalworldhowevertheyhavepeoplewhomaybe hold governance tokens to make voting decisions, or they do alltheirgovernanceon chain,onthisdecentralized settlement layer giving us the freedom to engage with each other as we please.

IV. ETHEREUMWALLET

Let's now get an Ethereum wallet and make our first transactiononaliveBlockchain.We'regoingtomakeourfirst interactionwiththeEthereumblockchain.We'regoingtoneed an Ethereum wallet. We will use MetaMask because it's one of the most popular wallets and one of the easiest to use. We're going to download it. It works for chrome Firefox and manyotherbrowsers.Itwouldbeanextensioninthetopright hand of your browser. Thus, we can easily see at any time whatwehaveinourwallet.ThiswillstoreallofourEthereum based currencies. Hit create wallet or if you already have a walletyoucanactuallyimportit.Wewillcreateourpassword and make sure that this is really secure. We're going to use fake money.

Ifyouloseaccesstoyourprivatekeysyouwillloseaccess toyourwalletandyouwillloseaccesstoallyourfunds.We're going to go ahead and hit confirm. We can use a tool like Etherscan [1] to view different addresses. If you create multiple different accounts each account has a unique identifier. The mnemonic (password) however is associated withallaccounts.Ifyouloseyourprivatekeyyouloseaccess tooneaccountbutifyou loseyourmnemonicyou loseaccess to all your accounts. Back up your mnemonic since it has access to everything. In MetaMask [13] we can see Ethereum Mainnetandwhenweclickitweactuallyseeabunchofother networks.Whenyoubuyether andwhenyouworkwithether you're working on the Ethereum Mainnet. When you interact with smart contracts you're also going to be working on the Mainnet. However, may want to test our applications or do some type of integration tests. There are Testnets [10] which are networks that resemble. They do not with real money and it's just for testing your applications. Thus, a Testnet blockchain is a blockchain where the currency doesn't have any real value but it resembles and acts exactly like another blockchain for example the Ethereum Mainnet.

Etherscan is what's known as a block explorer. Block explorers [21] are applications that allow us to see details of transactionsthathappenonablockchain.Whenweworkwith smart contracts, we will also see them in a transaction in Etherscan.Weseeauniquetransactionhash.Thishashorthis uniqueidentifieruniquelyidentifiesthistransactionasthekey ofthistransaction.Ifitisasuccessfultransaction,youwillsee the block number. We have these transaction fees and gas price limits. Gas refers to the fee paid to node operators for successfully including a transaction in a blockchain. Anytime you want to change the state of blockchain whether this is sendingsomeEthereumormakinganytypeoftransactionyou actually have to pay a little bit of ether or a little bit of that native blockchain token to actually execute that transaction. Wheneverwedosomethingontheblockchainitcostsgasand if we do something that would take a lot of energy for the blockchain to do it will cost more gas.

WhenImakea transaction, anodehastodecidewhy they wanttoincludemytransactionintotheblockandiftherearea ton of people looking to make these transactions then the nodes are going to be highly incentivized to pick the transactions that are going to give them a high price. The gas pricesofEthereumfluctuatewithhowmuchpeopleuseitand the gas prices of all these blockchains fluctuate with how much people use it. You can view your transactions in MetaMask and Etherscan.

V. BLOCKCHAINCONSENSUS

Bitcoin and Ethereum have thousands and thousands of nodes. Each blockchain keeps a full list of every transaction andinteractionthathappenedonthatblockchain.Blockchains are have an immutability trait where nothing can be changed or corrupted. In essence we can think of a blockchain as a decentralized database and with Ethereum it has an extra additional feature where it also can do computation in a decentralizedmanner.Proofofwork[7]andproofofstake

[18] fall under this umbrella of consensus. Consensus is defined as the mechanism used to reach an agreement on the stateorasinglevalueontheblockchain.Aconsensusprotocol in a blockchain or decentralized system can be broken down into two pieces a chain selection algorithm and a civil resistancemechanism.Theminingpieceispartoftheproofof workalgorithmandisknownasacivilresistancemechanism. Ethereum and Bitcoin currently use proof of work. Proof of work is known as a civil resistance mechanism because it defines a way to figure out who is the block author, which nodeisgoingtobethenode,whodidthework,andtheauthor of that block. All the other nodes can verify that it's accurate. Civil resistance is a blockchain's ability to defend against userscreatingalargenumberofpseudo-anonymousidentities to gain a disproportionately advantageous influence. It's basically a way for a blockchain to defend against somebody makingabunchoffakeblockchainssothattheycangetmore and more rewards. Two types of the civil resistance mechanisms are proof of work and proof of stake. Proof of work is silver resistant because a single node has to go through a very computationally expensive process called mining. No matter how many pseudo-anonymous

accounts you make each one still has to undergo this very computationally expensive activity of finding the answer to the proof-of-work problem or the proof-of-work riddle. The riddlecanbeasimpleasfindinganouncebuteachblockchain might change the riddle work or change the problem to be a littlebitdifferent.Infactsomeoftheseblockchainsmakethis riddleintentionallyhardorintentionallyeasytochangewhat's called the block time. The block time is how long it takes between blocks being published and it's proportional to how hard these algorithms are. These problems can change depending on how long they want the block time to be. If the system wants the block time to be very long they just make the problem very hard. If they want to be very short then the problem is made a lot easier.

Howdoweknowwhichblockchainistherealblockchain? Bitcoin and Ethereum both use a form of consensus called Nakamoto consensus. This is a combination of proof of work and the longestchainrule. The decentralizednetworkdecides that whichever blockchain has the longest chain or the most number of blocks on it is going to be the chain that they use. Thismakesalotofsensebecauseeveryadditionalblockthata chain isbehind it'sgoing to takemoreandmorecomputation. If we see confirmations is set at two it means that the block that our transaction was in has two blocks ahead of it in the longest chain. Proof of work also tells us where these transactionfeesandtheseblockrewardsgo.Transactionneeds gas to execute as a transaction fee. This transaction fee is going to the miners or the validators. In a proof of work network they're called miners and in the proof of stake network they're called Validators. All these nodes are competing against each other to find the answer to the blockchain riddle. It could be for example to find a hash that hasfivezerosat the start.Recalldependingontheblockchain implementation that riddle is going to be a little bit different, but all the nodes are trying as many combinations as possible to try to get this answer first as the firstnode to figure outthe answer to the blockchain rule is going to get the transaction fee. When a node gets paid they actually get paid in two different ways. One is going to be with a transaction fee and another piece is going to be the block reward. Thus, these nodes are competing against each other to be the first one to find this transaction, to be the first one to find the answer to this problem. They can be the ones to win both this block reward and your transaction fee. Some blockchains like Bitcoin for example have a set time when they are no longer going to give out block rewards and the miners or the nodes are only going to get paid from transaction fees. This gas fee againispaidbywhoeverinitializedthetransaction.Twotypes of attacks that can happen in these blockchain worlds. The firstonebeingtheSybilattack[23].Sybilattacksoccurswhen a single node or a single entity tries to affect the decentrality of the network by pretending to be multiple different people. This simple attack is when a user creates a whole bunch of pseudo-anonymousaccountstotrytoinfluenceanetwork.On bitcoin and Ethereum this is really difficult because the user needstodoallthisproofofworkorhaveatonofcollateralin proof of stake.
The other more prevalent attack is what's known as a 51 percent attack [22].We saw as partofour consensusprotocol these blockchains are going to agree that the longest chain is the one that they're going to go with so long as it matches up with 51 percent of the rest of the network. This means that if youhavethelongestchainandyouhavemorethan51percent of the rest of the network you can do what's called a fork in the network and bring the network onto your now longest chain. Thus, blockchains are very democratic. Whichever blockchain has the most buy-in and is the longest is the blockchainthatthewholesystemisgoingtocorroboratewhen nodes produce a new block and add to the longest chain. The other nodes will follow this longest chain that the rest of the network is agreeing with and add those blocks to their chain. Very small reorganizations are actually pretty common when a blockchainpicksa blockfrom a different longest chain puts itonandthenhastoswapitoutforanotherblockand

continue with a different blockchain. However, if a group of nodes had enough nodes or enough power they could essentially be 51 percent of the network and influence the network in whatever direction that they wanted. The 51 percent attack has happened on blockchains like Ethereum classic which is not Ethereum. This is why the bigger a blockchain is the more decentralized and the more secureitbecomes.Proofofworkisfantasticbecauseitallows us to very easily protect against these civil attacks and keep our blockchains decentralized and secure. However, it has some drawbacks as well. Proof of work costs a lot of electricitybecauseeverysinglenodeisrunningasfastasthey can to win this race to get the rewards. This has an environmental impact. Since proof of work and Nakamoto consensus a lot of other protocols have taken this idea and gone in a different direction with a different civil resistance protocol. Many of them with the intention to be a lot more environmentally friendly and the most popular one right now is proof of stake. There are some chains (Avalanche, Solana [2], Polygon, Polkadot and Terra [11]) that are already using this proof-of-stake protocol and are live and thriving. Ethereum upgrade to ETH2 will use the proof of stake algorithm. Proof of stake is a different civil resistance mechanism. Instead of solving this difficult problem proof of stake, nodes put up some collateral that indicate that they're going to behave honestly aka their stake. In the example of Ethereum 2, nodes put up some Ethereum as a stake that they're going to behave honestly in the network. If they misbehavetothenetworktheyaregoingtobeslashedorhave some of their stake removed. Obviously, this is a very

good civil resistance mechanism because if you try to create a whole bunch of anonymous accounts then each one of those accountsyouhavetoputupsomestakeandifyoumisbehave, you're going to run the risk of losing all the money that you putupascollateral.Inthissystemminersarecalledvalidators because they're no longer binding anything, they're actually just validating other nodes.

Unlike proof of work in which every node is racing to be the first one to find the block in proof of stake nodes are actually randomly chosen to propose the new block and then the rest of the validators will validate if that node has proposed the block honestly. It's usually very easy for other nodes to verify if a proposal or a transaction is honest. A decentralized autonomous organization that collectively chooses the random number and collectively chooses which node is going to run next is utilized keeping the block chain deterministic. Proof of work is way less computationally expensive to figure out the new block because instead of every single node on the network trying to do this only one node needs to do this and then the rest of the nodes just need to validate. It's usually considered a slightly less decentralized network due to the upfront staking costs to participate. However, the community can decide on the level of decentralization. The general consensus amongst blockchain engineers though is that proof of stake is very decentralized and secure.

Another concept that's really important in these ecosystems is scalability. When we were talking about gas prices we were saying that the gas prices can get really high if a lot of people want to send a transaction because a block only has so much block space and thenodes can only add so many nodes.Thus,whenalotofpeoplewanttouseablockchainthe gas price skyrockets. This is not very scalable because if we want to add more and more people to these blockchains it's going to cost more and more to use the blockchains. More people are going to want to get into these blocks this means that there's a ceiling to how many people can use the system because of the financial constraints that will get imposed as gas prices keep rising. Ethereum 2 is not only attacking the environmental impact of proof of work by switching to proof ofstakebuttheyarealsoimplementingthisnewmethodology called sharding. Sharding is a solution to this scalability problem. A sharded blockchainmeans that it's going to be a blockchain of blockchains. There is a main chain that's going tocoordinateeverythingamongstseveralchainsthathookinto this main chain. This means that there's more chains for people to make transactions on effectively increasing the amount of block space. Sharding can greatly increase the numberoftransactionsonablockchainlayer1.Layer1refers to any base layer blockchain implementation. Bitcoin has a layeroneasdoesEthereumandAvalanche.Alayertwoisany application thatisaddedon topof alayer one.An exampleof layer two is Chainlink. A rollup is like a sharded chain. They derive their security from the base layer like Ethereum and they bulk send their transactions onto the layer one. They solve some of the scalability issues by being another blockchain that people can make transactions. They're different from side chains because side chains derive their security from their own protocols while rollups derive their security from the base layer.

VI. CONCLUSION

Ethereum and bitcoin are now proof-of-work blockchains that use Nakamoto consensus, but Ethereum is transitioning to Ethereum 2, which will be a proof-of-stake sharded blockchain. Civil attacks are prevented thanks to standards such as proof of labor and proof of stake. 51 percent of assaults become more difficult as the blockchain grows in size. Rollups are solutions for scaling difficulties. Scalability issues exist in implementations such as Bitcoin and Ethereum, where there is not always enough block space for the desired number of transactions. This results in extremely high gas prices, which are the cost of interacting with a blockchain.

A.AuthorsandAffiliations

Koffka Khan earned his M.Sc., M.Phil., and D.Phil. degrees from the University of the West Indies. He is currently a Lecturer in Computer Science and has published multiple papers in well-known international journals and events. His research specialties include computational intelligence, routing protocols, wireless communications, information security, and adaptive streaming controllers. Wayne Goodridge is a Lecturer in the Department of Computing and Information Technology at the University of the West Indies, St. Augustine. He completed his PhD at Dalhousie University, and his research interests include computer communications and security.

REFERENCES

[1]. Baek, H., Oh, J., Kim, C.Y. and Lee, K., 2019, July. A model fordetectingcryptocurrencytransactionswithdiscerniblepurpose.In2019Eleventh International Conference on Ubiquitous and Future Networks(ICUFN) (pp. 713-717). IEEE.

[2]. Bodziony, N., Jemioło, P., Kluza, K. and Ogiela, M.R., 2021.Blockchain-Based Address Alias System. Journal of Theoretical andApplied Electronic Commerce Research, 16(5), pp.1280-1296.

[3]. Buterin, V., 2013. Ethereum white paper. GitHub repository, 1, pp.22-23.

[4]. Cai, W., Wang, Z., Ernst, J.B., Hong, Z., Feng, C. and Leung, V.C.,2018. Decentralized applications: The blockchain-empowered softwaresystem. IEEE Access, 6, pp.53019-53033.

[5]. Christidis, K. and Devetsikiotis, M., 2016. Blockchains and smartcontracts for the internet of things. Ieee Access, 4, pp.2292-2303.
[6]. Dannen, C., 2017. Introducing Ethereum and solidity (Vol. 318).Berkeley: Apress.
[7]. Hazari, S.S. and Mahmoud, Q.H., 2019, January. A parallel proof ofwork to improve transaction speed and scalability in blockchainsystems. In 2019 IEEE 9th Annual Computing and CommunicationWorkshop and Conference (CCWC) (pp. 0916-0921). IEEE.
[8]. Hong, S., Noh, Y. and Park, C., 2019, December. Design of ExtensibleNon-Fungible Token Model in Hyperledger Fabric. In Proceedings ofthe 3rd Workshop on Scalable and Resilient Infrastructures forDistributed Ledgers (pp. 1-2).
[9]. Kan, L., Wei, Y., Muhammad, A.H., Siyuan, W., Gao, L.C. and Kai,H., 2018, July. A multiple blockchains architecture on inter-blockchaincommunication. In 2018 IEEE International Conference on SoftwareQuality, Reliability and Security Companion (QRS-C) (pp. 139-145).IEEE.
[10]. Kera,D.R.,2020,June.SandboxesandTestnetsas"TradingZones"forBlockchain Governance. In International Congress on Blockchain andApplications (pp. 3-12). Springer, Cham.
[11]. Kereiakes, E., Do Kwon, M.D.M. and Platias, N., 2019. Terra money:Stability and adoption.
[12]. Lee, M.Y. and Edmondson, A.C., 2017. Self-managing organizations:Exploring the limits of less-hierarchical organizing. Research inorganizational behavior, 37, pp.35-58.
[13]. Lee, W.M., 2019. Using the metamask chromeextension. In BeginningEthereum Smart Contracts Programming (pp. 93-126). Apress,Berkeley,CA.
[14]. Luu, L., Chu, D.H., Olickel, H., Saxena, P. and Hobor, A., 2016,October. Making smart contracts smarter. In Proceedings of the 2016ACM SIGSAC conference on computer and communications security(pp.254-269).
[15]. Nakamoto,S.,2008.Bitcoin.Apeer-to-peerelectroniccashsystem.
[16]. Nofer, M., Gomber, P., Hinz, O. and Schiereck, D., 2017. Blockchain.Business & Information Systems Engineering, 59(3), pp.183-187.
[17]. Oates, C., 2009, September. A methodology for developing'Chainlink'converters. In 2009 13th European Conference on PowerElectronics and Applications (pp. 1-10). IEEE.
[18]. Saleh, F., 2021. Blockchain withoutwaste: Proof-of-stake. The Reviewof financial studies, 34(3), pp.1156-1190.
[19]. Tanana, D., 2019, June. Avalanche blockchain protocol for distributedcomputing security. In 2019 IEEE International Black Sea Conferenceon Communications and Networking (BlackSeaCom) (pp. 1-3). IEEE.
[20]. Wang, S., Ding, W., Li, J., Yuan, Y., Ouyang, L. and Wang, F.Y.,2019. Decentralized autonomous organizations: concept, model, andapplications. IEEE Transactions on Computational Social Systems,6(5),pp.870-878.
[21]. Werner, R., Lawrenz, S. and Rausch, A., 2020, March. Blockchainanalysis tool of a cryptocurrency. In Proceedings of the 2020 The 2ndInternational Conference on Blockchain Technology (pp. 80-84).
[22]. Yang, X., Chen, Y. and Chen, X., 2019, July. Effective scheme against51% attack on proof-of-work blockchain with history weightedinformation. In 2019 IEEE International Conference on Blockchain(Blockchain) (pp. 261-265). IEEE.
[23]. Zhang, S. and Lee, J.H., 2019. Double-spending with a sybil attack inthe bitcoin decentralized network. IEEE transactions on IndustrialInformatics, 15(10), pp.5715-5722.