DECENTRALIZED ELECTRONIC VOTING SYSTEM

Digital Assignment 3

Submitted by

Name	***Registration no.***
Abuzar Bagewadi	*19BCE0773*
Shreyas Chaudhry	*19BCE0774*
Daksh Paleria	*19BCE0779*
Harshit Mishra	*19BCE0799*
Alokam Nikhitha	*19BCE2555*
Anika Gupta	*19BCI0273*
Aiswarya Satish	*19BCI0265*

CSE1901
Technical Answers for Real World Problems (TARP)

Under the guidance of
Prof. Ushus Elizebeth Zachariah

VIT®
Vellore Institute of Technology
(Deemed to be University under section 3 of UGC Act, 1956)

SCHOOL OF COMPUTER SCIENCE AND ENGINEERING

Literature Review:

S. No.	Paper and Author	Summary	Inference
1.	A systematic Review of Challenges and Opportunities of blockchain for e-voting (09-Aug-2020) Ruhi Tas, Omer Ozgur Tanriover	This paper studies the up-to-date state of blockchain-based voting research along with associated possible challenges while aiming to forecast future directions. The methodology applied is a systematic review approach. Following an introduction to the basic structure and features of the blockchain in relation to e-voting, this paper provides a conceptual description of the desired blockchain-based e-voting application.	It is determined from the publications examined that voting systems enabled by blockchain might offer alternative solutions to conventional electronic voting. The five following categories were used to group the most important current issues: general, integrity, coin-based, privacy, and consensus. This research led to the conclusion that several issues with the current election systems can be resolved by blockchain technologies. On the other side, the issues with blockchain applications that are commonly highlighted are privacy protection and transaction speed. For

			blockchain-based e-voting to be sustainable, remote participation security and scalability should be improved. Due to these misgivings, it was determined that frameworks needed improvements in order to be employed in voting systems.
2.	**Success Implementation of E-Voting Technology in Various Countries: A Review** (30-Jan-2020) Slamet Risnanto, Yahaya Bin Abd Rahim and Nanna Suryana Herman	A technology created for voting is called electronic voting, or e-voting. It has been extensively adopted to employ electronic voting in the general election. In this study, countries that have effectively implemented electronic voting are presented, analysed, and conclusions are drawn from the analysis. In order to prevent future deployment of e-voting technology from failing, this article also lists the nations that have successfully adopted it as examples for nations that will do so in the future.	This study's conclusion is that there are other factors at play in the adoption of electronic voting. In order for other nations who aim to implement e-voting in the future to benefit from the success of these countries, many other elements that contribute to the successful implementation of e-voting in a country are no less significant.
3.	**E-Voting System Based on Blockchain**	Any democracy must have an open voting process that satisfies the needs of the populace in order to	It is recommended that trust in electronic voting methods be

	Technology: A Survey (01-Jul-2021) Sarah Al-Maaitah, Mohammad Qatawneh, Abdullah Quzmar	give the appropriate individual the power. Additionally, there are numerous problems with the current traditional voting systems, including a lack of security and transparency. This survey paper explores the potential for using BC technology in electronic voting systems to enhance the voting process by addressing concerns of trust, privacy, and security. This study attempts to assess various blockchain-based distributed electronic voting system implementations. Others have been put into practise in the actual world, while others have merely been draught papers. A blockchain-based electronic voting technology enhances security and privacy while further reducing costs.	leveraged to cut down on election fraud. This study reveals that BC technology is most chosen to address this issue and provide assistance in this situation by monitoring each step and ensuring that the entire process is. Additionally, the majority of the connected works failed to inspire management and maintenance of the blockchain. Gaps Identified: Various limitations were found based on the research done. These limitations included: the scale of the implementation is applied on the small scale, the need to improve the Synchronization, latency, and performance, improvement of cryptography methods and also they do not support complex

			applications, also the number of nodes as if we increase them the time will be increased.
4.	**Preparatory Component for Adoption E-Voting** (01-Oct-2019) Slamet Risnanto	Democracy-based nations often conduct general elections. The traditional general election method is very dangerous, has caused controversy in the past, and is relatively expensive. Many nations strive to use electronic voting technology in national elections. India and Brazil, two sizable democracies, were successful in implementing electronic voting; other unsuccessful nations included England and the Netherlands. This study suggests a thorough research, assessment, and development plan for the preparation of e-voting deployment so that there won't be any challenges and it will be successful in the future	E-voting technology appears to address issues with traditional elections. However, nations who are serious about implementing electronic voting make various preparations in addition to those related to technology. This study makes a complete research, evaluation, and development proposal in support of the implementation readiness of electronic voting.
5.	**A Survey on Anonymity and Privacy in Bitcoin-like Digital Cash Systems** (26-Mar-2018)	The paper explains how bitcoin has become the most widely known distributed, peer-to-peer payment network without existence of central authority and what different flaws are in the	Bitcoin like architecture, if used plainly, cannot guarantee anonymity which has to be the most important part of any voting system

	Merve Can Kus Khalilov, Albert Levi	architecture of bitcoin. It explains how bitcoin is not completely anonymous but pseudo-anonymous. The paper also deals about describing how different transactions on careful study can be attributed to revelation of the identity of a person on this distributed chain and hence there is still various loop-holes when it comes to anonymity and privacy on blockchain as network.	around any democracy in the world. Although, bitcoin protocols provide huge applications all in fields of smart contracts and more as anonymity is kind of a bane when it comes to keeping civil laws intact.
6.	**Exploring Ethereum's Blockchain Anonymity Using smart contract code attribution** (27-Feb-2020) Shlomi Linoy, Natalia Stakhanova, Alina Matyukhina	The paper deals about explaining various architecture of blockchains and how are users identified, added and removed from a blockchain and the concepts of public keys and private keys along with asymmetric key encryption protocols. It again deals with how a blockchain network is not completely anonymous and is more of pseudo-anonymous. They deal with analysing how public addresses can be linked back to the users. In this work, they proposed a leverage *"stylometry"* approach to explore the extent to which a deployed smart contract's source code can	It can again be interpreted that the architecture of Ethereum is not full-proof anonymous. But we can use the concept of stylometry, heuristics and refinements to identify the weaknesses in a smart contract and correct them out. There experimental results stood at an accuracy of 93.5% on preliminary basis and hence their proposed model can be used as a benchmark to any prototype.

		contribute to the affiliation of account addresses.	
7.	**Blockchain-based RBAC for User Authentication with Anonymity** (24-Sep-2019) YongJoo Lee, Keon Myung Lee	The paper proposes an integration of two different models, RBAC and P2P networks. RBAC stands for Role-Based Access Control and P2P stands for peer-to-peer networks. RBAC is a very popular means of ensuring authentication in fields of security and P2P is widely used a distributed architecture which primarily deals with decentralization of resources and ledgers. They have used an architecture that has payment based on cryptocurrency for a smart contract. So, their proposed model allows user to be identified as individuals at the same time. Users are authorized to the role to which they belonged. They defined a list that can manage role of user units called CRL, and linked this to personal authentication by using Roll Pass (RP). To provide this simple and powerful authentication based on RBAC.	Their proposed architecture is a bit different from how we want our smart-contract to be, but it has got all the essence of what we need (except the anonymity). We can use their authentication services to ensure that votes are coming in from valid sources and there is no multiple voting by same source. This can provide a big break-through in ensuring free and fair conduct of any e-election.
8.	**Anonymity on blockchain based**	According to the paper, the transactions of most	The paper proposed an architecture to

	e-cash protocols – A survey (01-May-2021) Nitish Andola, Raghav, Vijay Kumar Yadav, S. Venkatesan, Sekhar Verma	of the blockchain framework-based cryptocurrencies are publicly available, thereby accessible to all users by design. However, the anonymity of blockchain transactions is necessary for acceptance of such frameworks. There is a need to preserve the privacy of the identities of the blockchain members and the transaction. They have listed the concepts of mixings and pooling to preserve one's identity in the ledger and make sure the transactions are not traceable. The paper also provides a comprehensive study of the threats and attacks that aim to deanonymize the e-cash protocols. They also redefined anonymity on the blockchain and categorized the anonymity – provisioning methods and protocols with their outcomes.	ensure the anonymity of any user in our smart-contract. They were, mixers and pools. Use of pools in our scenario is not possible as it will make it obvious for each voter's vote to their pool and hence mixers can come to rescue. Mixers will have to be set-up by the election committee itself and it can be done similar to polling booth set-up for each ward. In fact, here we can use mixers at whole new levels by ensuring even wards are not traceable using random allocation of wards to each mixer based on any mathematical function.
9.	BlendMAS: A BLockchain-Enabled Decentralized Microservices Architecture for Smart Public Safety	The authors in the paper have discussed how a centralized authority has all the control over Smart Public Safety (SPS) which was essentially developed using the Internet of Things (IoT) but since the system has entirely relied	The authors have proposed how smart contracts are capable enough to handle complex services to make sure that the main gist of the safety program remains

	(02-Jan-2020) Ronghua Xu, Seyed Yahya Nikouei, Yu Chen, Erik Blasch, Alexander Aved	on one single central authority it can result as a single point of failure and then eventually bottleneck the entire purpose of the system which is to provide the safety to the users. The paper discusses how a permissioned blockchain network can be used to remove the central authority from the scenario and create a decentralized, trust less network for the system.	intact. The paper was able to enlighten us on how the blockchain can be used to keep the anonymity of the user and also provide a high level of security to the users.
10.	**Beyond bitcoin: an early overview on smart contract** (05-Apr-2017) Pierluigi Cuccuru	Bitcoin was the very first and most successful blockchain that helped in paving the path for decentralization, and trust less networks. But as they say one has to keep moving forward with more new advancements, this is essentially an overview of what the author has discussed in this paper. The authors have mentioned how the technology of decentralization can be added to other applications/domains like finance, and gaming. The authors have discussed how we can look forward by taking all the necessary learnings from bitcoin and then scaling them to	The authors have proposed an early look into the world of smart contracts by relating the existing system with the blockchain one, and how the application can contact the attributes that are on the chain. They have discussed the possibilities of writing a few lines of code which will be eventually named smart contracts that will help the developers in securing the data, and automate the process at the same time.

		develop much better applications by taking the advantage of the network's security.	
11.	**An Overview of Smart Contract: Architecture, Applications, and Future Trends** (21-Oct-2018) Shuai Wang; Yong Yuan; Xiao Wang; Juanjuan Li; Rui Qin; Fei-Yue Wang	The paper is discussing the developments that we have achieved in the world of blockchain by introducing the world to smart contracts which are essentially chunks of code that can be automated, and live on the chain which behaves as a public ledger. Before the introduction of smart contract, blockchains was majorly considered as a medium of paying money and as a medium of processing the transaction in a very safe, secured manner without the ill politics a central authority would play to favor a certain personality. Smart contracts just leveraged on these points which can now be followed by writing a few instructions that will behave accordingly.	The authors have proposed how smart contracts can be used in the most efficient way possible as for every other action one is supposed to pay a specific amount of gas as money to make sure that the transaction goes through, the researchers have put up more emphasis on writing gas efficient contracts which eventually will help in saving more energy by the miner in order to process the transaction and add it into a block in the network.
12.	**Smart Contract: Attacks and Protections** (10-Feb-2020)	Based on the attack reasoning and targeting consensus protocols, defects in the smart contract, malware running in the operating system, and fraudulent users, they grouped blockchain	They have disclosed in this research that this technology is not without flaws and threats. We developed an attack classification based on the attack vector

	Sarwar Sayeed, Hector Marco-Gisbert, Tom Caira	exploitation approaches into four groups in this article. They then concentrated on smart contract vulnerabilities, examining the seven most common attack methods to establish the true impact on smart contract technology. They discovered that even when the ten most extensively used tools for detecting smart contract flaws were utilised, they still contained known vulnerabilities, offering a dangerously misleading impression of security. They finished the report with a discussion of recommendations and future research directions to move forward toward a secure smart contract solution.	to focus on vulnerabilities in smart contract programming. We discovered that not all vulnerabilities were spotted after reviewing ten security tools to determine their efficiency in detecting vulnerabilities. This provides a hazardous false sense of security that attackers can exploit. According to their study, creating a viable solution to secure smart contracts remains a problem, and future work will include developing ways to detect and mitigate the primary security issues revealed in this paper.
13.	**Smart Contract Development: Challenges and Opportunities** (01-Oct-2021)	They conducted exploratory research in this article to investigate the present status and prospective issues developers face while implementing smart contracts on blockchains, with a focus on Ethereum. They eventually did their	This study specifically focused on the Ethereum platform to explore the difficulties that developers are having when creating these smart contracts. According to the

	Weiqin Zou, David Lo, Pavneet Singh Kochhar, Xuan-Bach Dinh Le, Xin Xia, Yang Feng, Zhenyu Chen, Baowen Xu	investigation in two parts. During the first round, we conducted semi-structured interviews with 20 GitHub engineers and industry experts working on smart contracts. To confirm the findings from the interviews, they conducted a survey of 232 practitioners in the second phase.	survey results, smart contract development is still in its early stages. For example, there is no widely accepted method for securing smart contract code, the current development toolchain is inadequate, development and runtime platforms (such as programming languages, virtual machines), and online learning resources and community support are scarce. Gaps identified: The results indicate some specific and practical directions that researchers and practitioners should pursue in the future (e.g., automated smart contract patching, Solidity compiler testing, source-code level gas optimization, automated Solidity library construction, etc.). Development

			of smart contracts would be made easier with progress in these directions.
14.	**A systematic literature review of blockchain and smart contract development: Techniques, tools, and open challenges** (01-Apr-2021) Anna Vacca, Andrea Di Sorbo, Corrado A. Visaggio, Gerardo Canfora	They investigated 96 publications (published between 2016 and 2020) proposing solutions to software engineering-specific difficulties connected to the creation, testing, and security evaluation of blockchain-oriented software in this work. They specifically analyse education articles (published in international journals and conferences) on six topics: smart contract testing, smart contract code analysis, smart contract metrics, smart contract security, Dapp performance, and blockchain applications. Beyond a comprehensive analysis of the methodologies, tools, and approaches offered in the literature to handle the concerns raised by the creation of blockchain-based software, they highlighted outstanding challenges that require future research for each of the six afore mentioned themes.	According to the analysis conducted, it is seen that, the examination of the literature is solely focused on particular topics, including security or blockchain applications. Software engineering best practises can, however, enhance this technology. Based on these motivations, a review of the literature was conducted in the area of software engineering to gain a better understanding of the methods, procedures, and tools designed specifically to address the problems associated with the creation of blockchain-based software and to pinpoint any unresolved issues.

15.	**A Blockchain-Based Smart Contract System for Healthcare Management** (03-Jan-2020) Asma Khatoon	In application sectors like the financial sector, supply chain management, food industry, energy sector, internet of things, and healthcare, blockchain is developing to be a secure and dependable platform for secure data sharing. In this essay, we examine current research and blockchain-based applications for the healthcare sector. Additionally, for better data management, this paper also suggests a number of workflows for the healthcare sector using blockchain technology. The Ethereum blockchain platform has been used to develop and implement a variety of medical processes, including complicated surgical and clinical trial procedures. Accessing and controlling a sizable amount of medical data are also included. The cost of this system has been estimated as part of a feasibility study that has been extensively reported in this article. This cost is related with the deployment of the workflows of the medical	The proposed solution employs blockchain technology to provide a decentralised, iterative, scalable, safe, and accessible healthcare ecosystem. This would provide patients complete control over the privacy of their medical data while enabling them to freely and securely exchange their medical records with physicians, hospitals, research institutions, and other stakeholders. Numerous problems with the current healthcare system, such as data siloing, legacy network incongruity, challenges with collecting unstructured data, unreasonably high administrative expenses, a lack of data security, and unresolved privacy issues, will be resolved as a result.

		smart contract system for healthcare management.	
16.	**A conceptual framework for blockchain smart contract adoption to manage real estate deals in smart cities** (01-Feb-2021) Fahim Ullah, Fadi Al-Turjman	Blockchain-based smart contracts are upending the smart city's real estate market. The current study examines the body of research on blockchain smart contracts for smart real estate and offers a conceptual framework for their application in smart cities. The material published between 2000 and 2020 is investigated and analysed using a systematic review methodology. Ten essential elements of blockchain smart contracts are identified in the literature and categorised into six tiers for use in smart real estate. To demonstrate the development of a smart contract that may be used for blockchain smart contracts in real estate, the decentralised application and its interactions with the Ethereum Virtual Machine (EVM) are described. For the real estate owners and users who are parties to a smart contract, a thorough design and interaction mechanism are emphasised. Along	Based on the systematic, thorough literature research, a conceptual framework for implementing blockchain smart contracts for smart real estate management in smart cities is proposed. For handling smart real estate deals and transactions, the 10 highlighted aspects are connected to and exhibited as six levels of blockchain. These include the application layer, trust layer, network layer, transaction layer, blockchain layer, and security and administration layer. A DApps and its interactions with the EVM have been shown, which demonstrate how a smart contract is created and distributed to the important parties—users and owners. For the buyers and

		with a step-by-step process for establishing and terminating smart contracts, a list of functions for initiating, generating, altering, or terminating a smart contract is provided. The results of the current study may lead to a more engaging, intuitive, and visually appealing contractual procedure for users, while increasing business and sales for owners, Prop-tech firms, and real estate agents.	users of smart contracts, a thorough design and interaction mechanism is emphasised.
17.	**Decentralized Finance: On Blockchain- and Smart Contract-Based Financial Markets** (14-May-2021) Fabian Schär	Decentralized finance (DeFi) refers to a financial infrastructure that is constructed on top of the Ethereum blockchain. DeFi creates protocols using smart contracts to duplicate present financial services in a more open, interoperable, and transparent manner. This article discusses the DeFi ecosystem's prospects and possible hazards. To evaluate the implicit architecture and the many DeFi building elements, such as token standards, decentralized exchanges, decentralized debt markets, blockchain derivatives, and on-chain asset management	DeFi opens up new possibilities and has the ability to build a completely open, transparent, and irreversible financial infrastructure. Because DeFi is made up of several highly interoperable protocols and apps, anybody can verify all transactions, and data is easily accessible for users and researchers to evaluate. DeFi has sparked a flood of creativity. On the one hand, developers are

		protocols, a multi-layered framework is suggested.	creating trust less copies of standard financial products utilizing smart contracts and the decentralized settlement layer. They are, on the other hand, developing totally new financial products that would not be possible without the underlying public blockchain. Atomic swaps, autonomous liquidity pools, decentralized stablecoins, and flash loans are just a few of the numerous examples that demonstrate this ecosystem's enormous potential.
18.	**Secure Digital Voting System based on Blockchain Technology** (01-Jan-2018) Kashif Mehboob Khan, Junaid	The paper investigates the key issues such as voter anonymity, vote confidentiality and end-to-end verification. These challenges form the foundation of an efficient voting system preserving the integrity of the voting process. In this paper, the authors present our efforts to explore the use	This paper deals with voter anonymity and confidentiality by generating a hash for each vote such that it can't be traced back to the voter's details. They use a multichain blockchain platform to maintain the

	Arshad, Muhammad Mubashir Khan	of the blockchain technology to seek solutions to these challenges. In particular, their system is based on the Prêt à Voter approach (Ryan, 2008) and uses an open source blockchain platform, Multichain (Multichain, 2017) as the underlying technology to develop our system. In their system, in order to protect the anonymity and integrity of a vote, the system generates strong cryptographic hash for each vote transaction based on information specific to a voter.	ledger of voter details and votes.
19.	**E-Voting with Blockchain: An E-Voting Protocol with Decentralisation and Voter Privacy** (03-Jul-2018) Freya Sheer Hardwick, Apostolos Gioulis, Raja Naeem Akram, Konstantinos Markantonakis	In this paper, the authors propose a potential new e-voting protocol that utilises the blockchain as a transparent ballot box. The protocol has been designed to adhere to fundamental e-voting properties as well as offer a degree of decentralisation and allow for the voter to change/update their vote (within the permissible voting period). This paper highlights the pros and cons of using blockchain for such a proposal from a practical point view in both	The proposed voting protocol utilises the blockchain to store the cast ballots, therefore in this context the blockchain acts as a transparent ballot box. The main reason for using the blockchain in an e-voting protocol is to take advantage of the fact that it enables a group of people to maintain a public database, that is owned, updated, and

		development/deployment and usage contexts. Concluding the paper is a potential roadmap for blockchain technology to be able to support complex applications.	maintained by every user, but controlled by no one. Since the protocol is based on the blockchain, it will be realised as a network of peers. Each voter will be a peer i.e., a node in a network of equals. Every voter will be responsible for making sure that fraudulent votes are rejected, hence that consensus is maintained according to the election rules. The blockchain also has the additional advantage of being increasingly well-known and well-trusted to operate as intended.
20.	**E-voting using block chain Technology.** (01-May-2019) Pallavi Shejwal, Aditya Gaikwad, Mayur Jadhav, Nikhil Nanaware,	The authors claim that block chain technology mostly works the same as the block chain technology contained in the E-voting system and focuses on database recording. The nodes involved in Block chain that have been used by Bitcoin are independently random and not counted. However, in this e-voting	A nation with less voting percentage will struggle to develop as choosing a right leader for the nation is very essential. Their proposed system designed to provide a secure data and a trustworthy E-voting amongst the people of the

	Noormohammed Shikalgar	system a block chain permission is used, for nodes to be made the opposite of the Bitcoin system and the Node in question is a place of general election because the place of elections must be registered before the commencement of implementation, it must be clear the amount and the identity. This method aims to maintain data integrity, which is protected from manipulations that should not happen in the election process.	democracy. Block chain itself has been used in the Bitcoin system known as the decentralized Bank system. By adopting block chain in the distribution of databases on e-voting systems one can reduce the cheating sources of database manipulation. This project aims to implement voting result using block chain algorithm from every place of election.
21.	Digital Voting: A Blockchain-based E-Voting System using Biohash and Smart Contract (06-Oct-2020) Syada Tasmia Alvi, Mohammed Nasir Uddin, Linta Islam	The voting method is the component for executing individuals' views to all the more likely to manage the framework. In recent years, customary votes have satisfied neither voters nor government specialists. They are not totally protected since voting forms are easy to strike. It additionally challenges elector safety and transparency. Many countries face significant difficulties in protecting security in the voting framework. To ensure the	The authors have highlighted how legitimacy of every vote is maintained while using blockchain mechanisms in elections. Also, the counting of votes without manipulation and reduced time for counting are other benefits that are going to be incorporated in our project. Also, another advantage is that votes can be

		participation and legitimacy of the voter, the integrity of the vote data, and the counting of votes without manipulation, a blockchain-based voting system using a smart contract has been proposed. This mechanism where the SC performs the authentication process of voter and plays a role in selecting a Miner in the Blockchain to reduce the computational cost. It also counts the vote immediately which reduces the time consumption of the election process. This mechanism provides the environment for the citizens to cast their votes using smart devices from anywhere.	cast from any location(remotely)
22.	**Blockchain voting: Publicly verifiable online voting protocol without trusted tallying authorities** (01-Nov-2020)	In this paper, the authors propose a new decentralized publicly verifiable online voting protocol based on blockchain technology. Their new convention utilizes another encryption system and combines a number of cryptographic techniques adapted and merged in an appropriate fashion. The	The new protocol in this paper employs a new encryption mechanism and combines a number of cryptographic techniques adapted and merged in an appropriate fashion. Each vote is to be encrypted before submission and remains

	Xuechao Yang, Xun Yi, Surya Nepal, Andrei Kelarev, Fengling Han	protocol stores all submitted votes in a blockchain database, which can be accessed by all users but is immutable. The proposed protocol also allows voters to cast their ballots by assigning different points to different candidates. Each vote is encrypted before submission and remains encrypted at all times. The additive homomorphic property of the exponential ElGamal cryptosystem enables effective processing of the ciphertexts during these procedures. Moreover, the eligibility of voters and their submissions can be verified by anyone without revealing the contents of the votes, and our proposed verification and self-tallying algorithms allow any voter to verify the correctness of the final result. The whole blockchain database is maintained by all users (voters and miners) without a need to involve a third party in verification and tallying. This paper also provides a concise security and performance analysis and confirms the feasibility of	encrypted at all time. Our project aims on using SHA-256 for encryption for all votes so that all the votes remain anonymous and cannot be traced back to its original voter in any way or form.

		the proposed blockchain online voting protocol for real-life elections. In this paper, the authors do not hide the identification of each vote (because laws in several countries require everyone to vote). In our protocol, everyone can see the sender of each vote via the blockchain database.	
23.	**Secure large-scale E-voting system based on blockchain contract using a hybrid consensus model combined with sharding** (30-Nov -2020) Yousif Abuidris, Rajesh Kumar, Ting Yang, Joseph Onginjo	In this paper, the authors have proposed a hybrid consensus model (PSC-Bchain) in which Proof of Credibility (PoC) works mutually with Proof of Stake (PoS). This led to the creation of a secure hybrid blockchain, which ensures integral security when applied to the e-voting system. They combined the mechanism of sharding with the proposed PSC-Bchain model to emphasize security and enhance the scalability and performance of the blockchain-based e-voting system. Furthermore, the paper compares attack execution on both the classical blockchain and the proposed hybrid blockchain, and also presented an attack analysis and security	The authors propose a hybrid consensus model (PSC-Bchain) in which Proof of Credibility (PoC) works mutually with Proof of Stake (PoS). This leads to creation of a secure hybrid blockchain, which ensures integral security when applied to the e-voting system. It further expands on the high concurrency handling capability and high throughput of blockchain systems. Our project is being made for large population voting and hence, high concurrency and

		analysis. Even though the latency for this method is high the throughput when the number of nodes increases in such systems.	security will have a key role to play.

Contribution of Each Member:

Abuzar Bagewadi (19BCE0773):

1) Digital Voting: A Blockchain-based E-Voting System using Biohash and Smart Contract.
2) Blockchain voting: Publicly verifiable online voting protocol without trusted tallying authorities.
3) The Application of the Blockchain Technology in Voting Systems: A Review.

Shreyas Chaudhry (19BCE0774):

1) E-Voting with Blockchain: An E-Voting Protocol with Decentralisation and Voter Privacy.
2) E-voting using block chain Technology.
3) Secure Digital Voting System based on Blockchain Technology.

Daksh Paleria (19BCE0779):

1) BlendMAS: A BLockchain-Enabled Decentralized Microservices Architecture for Smart Public Safety.
2) Beyond bitcoin: an early overview on smart contract.'
3) An Overview of Smart Contract: Architecture, Applications, and Future Trends

Harshit Mishra (19BCE0799):

1) A Survey on Anonymity and Privacy in Bitcoin-like Digital Cash Systems.
2) Exploring Ethereum's Blockchain Anonymity Using smart contract code attribution.
3) Blockchain-based RBAC for User Authentication with Anonymity.
4) Anonymity on blockchain based e-cash protocols – A survey.

Alokam Nikhitha (19BCE2555):

1) Smart Contract: Attacks and Protections.
2) Smart Contract Development: Challenges and Opportunities.
3) A systematic literature review of blockchain and smart contract development: Techniques, tools, and open challenges.

Anika Gupta (19BCI0273):

1) A systematic Review of Challenges and Opportunities of blockchain for e-voting.
2) Success Implementation of E-Voting Technology in Various Countries: A Review.
3) E-Voting System Based on Blockchain Technology: A Survey
4) Preparatory Component for Adoption E-Voting.

Aiswarya Satish (19BCI0265):

1) A Blockchain-Based Smart Contract System for Healthcare Management.
2) A conceptual framework for blockchain smart contract adoption to manage real estate deals in smart cities.
3) Decentralized Finance: On Blockchain- and Smart Contract-Based Financial Markets.

References:

[1] Taş, R. and Tanrıöver, Ö.Ö., 2020. A systematic review of challenges and opportunities of blockchain for E-voting. *Symmetry*, *12*(8), p.1328.

[2] Goretta, H. et al. (2019) 'Technology criteria analysis and e-voting adoption factors in the 2019 Indonesian presidential election', 2018 International Conference on Advanced Computer Science and Information Systems, ICACSIS 2018. IEEE, pp. 143–149. doi: 10.1109/ICACSIS.2018.8618215.

[3] S. Al-Maaitah, M. Qatawneh and A. Quzmar, "E-Voting System Based on Blockchain Technology: A Survey," 2021 International Conference on Information Technology (ICIT), 2021, pp. 200-205, doi: 10.1109/ICIT52682.2021.9491734.

[4] Risnanto, Slamet & Suryana, Nanna & rahin, yahaya. (2019). Preparatory Component For Adoption E-Voting. 10.1109/TSSA48701.2019.8985461.

[5] M. C. Kus Khalilov and A. Levi, "A Survey on Anonymity and Privacy in Bitcoin-Like Digital Cash Systems," in IEEE Communications Surveys & Tutorials, vol. 20, no. 3, pp. 2543-2585, thirdquarter 2018, doi: 10.1109/COMST.2018.2818623.

[6] S. Linoy, N. Stakhanova and A. Matyukhina, "Exploring Ethereum's Blockchain Anonymity Using Smart Contract Code Attribution," 2019 15th International Conference on Network and Service Management (CNSM), 2019, pp. 1-9, doi: 10.23919/CNSM46954.2019.9012681.

https://dl.acm.org/doi/abs/10.1145/3338840.3355673

[7] Lee, Y. and Lee, K.M., 2019, September. Blockchain-based RBAC for user authentication with anonymity. In Proceedings of the Conference on Research in Adaptive and Convergent Systems (pp. 289-294).

[8] https://doi.org/10.1016/j.cosrev.2021.100394.

[9] R. Xu, S. Y. Nikouei, Y. Chen, E. Blasch and A. Aved, "BlendMAS: A Blockchain-Enabled Decentralized Microservices Architecture for Smart Public Safety," 2019 IEEE International Conference on Blockchain (Blockchain), 2019, pp. 564-571, doi: 10.1109/Blockchain.2019.00082.

[10] Pierluigi Cuccuru, Beyond bitcoin: an early overview on smart contracts, *International Journal of Law and Information Technology*, Volume 25, Issue 3, Autumn 2017, Pages 179–195

[11] S. Wang, Y. Yuan, X. Wang, J. Li, R. Qin and F. -Y. Wang, "An Overview of Smart Contract: Architecture, Applications, and Future Trends," 2018 IEEE Intelligent Vehicles Symposium (IV), 2018, pp. 108-113, doi: 10.1109/IVS.2018.8500488.

[12] S. Sayeed, H. Marco-Gisbert and T. Caira, "Smart Contract: Attacks and Protections," in IEEE Access, vol. 8, pp. 24416-24427, 2020, doi: 10.1109/ACCESS.2020.2970495.

[13] W. Zou et al., "Smart Contract Development: Challenges and Opportunities," in IEEE Transactions on Software Engineering, vol. 47, no. 10, pp. 2084-2106, 1 Oct. 2021, doi: 10.1109/TSE.2019.2942301.

[14] Vacca, A., Di Sorbo, A., Visaggio, C.A. and Canfora, G., 2021. A systematic literature review of blockchain and smart contract development: Techniques, tools, and open challenges. Journal of Systems and Software, 174, p.110891.

[15] Khatoon, A., 2020. A blockchain-based smart contract system for healthcare management. Electronics, 9(1), p.94.

[16] Ullah, F. and Al-Turjman, F., 2021. A conceptual framework for blockchain smart contract adoption to manage real estate deals in smart cities. Neural Computing and Applications, pp.1-22.

[17] Schär, F., 2021. Decentralized finance: On blockchain-and smart contract-based financial markets. FRB of St. Louis Review.

[18] Khan, K.M., Arshad, J. and Khan, M.M., 2018. Secure digital voting system based on blockchain technology. International Journal of Electronic Government Research (IJEGR), 14(1), pp.53-62.

[19] Hardwick, F.S., Gioulis, A., Akram, R.N. and Markantonakis, K., 2018, July. E-voting with blockchain: An e-voting protocol with decentralisation and voter privacy. In 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData) (pp. 1561-1567). IEEE.

[20] Shejwal, P., Gaikwad, A., Jadhav, M., Nanaware, N. and Shikalgar, N., 2020. E-voting using block chain Technology. International Journal of Scientific Development and Research (IJSDR), 4(5), pp.583-588.

[21] Alvi, S.T., Uddin, M.N. and Islam, L., 2020, August. Digital voting: A blockchain-based e-voting system using biohash and smart contract. In 2020 Third International Conference on Smart Systems and Inventive Technology (ICSSIT) (pp. 228-233). IEEE.

[22] Yang, X., Yi, X., Nepal, S., Kelarev, A. and Han, F., 2020. Blockchain voting: Publicly verifiable online voting protocol without trusted tallying authorities. Future Generation Computer Systems, 112, pp.859-874.

[23] Abuidris, Y., Kumar, R., Yang, T. and Onginjo, J., 2021. Secure large-scale E-voting system based on blockchain contract using a hybrid consensus model combined with sharding. Etri Journal, 43(2), pp.357-370.