International Advance Journal of Engineering Research (IAJER)
*Volume 07, Issue 10 (**October - 2024**), PP 01-09*
ISSN: 2360-819X
www.iajer.com

Research Paper **Open Access**

Blockchain in Cloud Computing

Ishaan Hemrajani
USA

ABSTRACT:- In recent years we have discovered blockchain technology can be applied to other areas that are different from financial technology where it was originally intended. The study dives into the effect of blockchain's implementation in cloud computing specifically to determine if there is a profit incentive for companies to implement blockchain technology into their cloud computing systems. Past studies have determined the implementation of blockchain would result in more secure cloud computing networks, however, they did not do the cost analysis. The study found there is a profit when companies implement blockchain into cloud computing, however, the amount of profit varies based on the contract companies choose to implement. Future companies should do their own research on the topic to check the security trade-off between different contracts and scalability concerns. Since there is a cost-incentive other companies would follow-on, however, this is not accounting for the strain that would be applied to the decentralized network which could be a potential scalability problem. Thus, we conclude there is a net positive effect for companies profit when blockchain is applied to cloud computing companies infrastructure, this is different from other sectors such as supply chain where the opposite was deemed to be true.

I. LITERATURE REVIEW

The blockchain can solve security when authenticating data sources (A Blockchain-Based Decentralized Public Key Infrastructure for Information-Centric Networks). It can be applied to most public infrastructure (Blockchains as Infrastructure and Semicommons). The blockchain was originally intended for finance only, but recently has been noticed as a more secure implementation method in other sectors, however, there are still concerns regarding scalability. We can notice the implementation of blockchain into the supply chain however, there is current literature regarding implementation into the supply chain, and the blockchain was deemed very hard to scale, which is the purpose of this research paper. Due to the recent implementation into other industries, it has been rumored blockchain will be implemented in most sectors. Specifically, in the paper we will be delving into the implementation of blockchain into cloud computing. Cloud computing is the delivery of computing services over the cloud (Cloud Computing Security using Blockchain) Cloud computing systems right now have flaws (Cloud Computing Security using Blockchain), and blockchain may be a potential solution through better authentication frameworks and irreversible transaction history (A Blockchain-Based Decentralized Public Key Infrastructure for Information-Centric Networks). Many major companies use cloud computing services through AWS and Google services, examples are Netflix and Pinterest. Cloud computing right now has multiple security flaws, and recent news wants to move to more secure alternatives. For example, Netflix wants to limit logins to one household, one of the best ways to achieve this mechanism is with a blockchain implementation. Blockchain would be able to track every login without any way of erasing previous mechanisms, this prevents workarounds such as VPN's from avoiding detection systems and enforcing rules. Additionally, blockchain is not just beneficial on the user level -- switching to a blockchain system would aid in the securitization of the backend of cloud computing networks. Hacks into big companies are becoming increasingly common and blockchain would serve as a record of attacks and as a security barrier. Although blockchain would not actually increase encryption, it could deter cyber attacks because they become more traceable.This study is designed to help demonstrate how blockchain systems affect cloud computing. The study uses three key metrics - security, scalability, and efficiency. Security is a paramount reason why blockchain is being explored as an implementation mechanism for cloud computing, blockchain is able to track every node and is uneditable. Previous studies have deemed blockchain's implementation into cloud computing to be successful at increasing security levels. One of the general drawbacks to a blockchain implementation in cloud computing is scalability. The past reasons why blockchain has failed in other industries is the problems with scalability. Currently, no studies using game-theoretical analysis and cryptanalysis have been conducted to analyze the security and efficiency with regard to scalability of the implementation of blockchain into cloud computing. This will likely be a future direction after determining if implementation is profitable. If we deem

blockchain to be profitable, then we assume other actors will follow-on, hence blockchain would be considered a scalable solution in cloud computing. Game theoretical analysis, which is one of the methods that analyzes a "players" motivations in a game. The game in this situation is the implementation of blockchain into cloud computing. The method of game theoretical analysis will be effective at testing security, as it analyzes why and how hackers could take advantage of the implementation of a blockchain system. However, we would analyze this differently in order to determine the profitability of blockchain into cloud computing. First, the method will set up a game for the way cloud computing is right now, and then compare the new motivations once blockchain is implemented into cloud computing. It accounts for differences in transactional costs and variance between different contracts to determine different costs associated with the different contracts which can be used to implement blockchain. The second method is using code in order to determine specific costs of the implementation of blockchain. The code accounts for Blockchain is meant to be unalterable, but in order to implement it into cloud computing there may need to be alterations made for a corporate setting. Cryptanalysis in the past has allowed us to analyze specifically what blockchain would track e.g logins, accounts, etc. This was done in previous studies and is what we are using as a baseline for our conclusions regarding security in blockchain, as previous studies have concluded that adding blockchain would make cloud computing environments more secure. Blockchain will significantly aid the security and efficiency of cloud computing, but there may be scalability drawbacks. In order to analyze scalability drawbacks. Cryptography aids the process of cryptanalysis through proper records in order for the analysis to not solely be based on random metrics but rather based on real statistics. Using secondary sources, we can notice the security increase as a result of the implementation of blockchain, specifically using Ayana Aspembitova and Michael Bentleys's study which explores the security of DeFi implementation in systems. In the study, they explore common attacks which occur in financial systems which implement DeFi. They also explore the efficiency increases which happen as a result of decentralized implementation. This literature on the topic of blockchain has established that implementation would be very beneficial for security and it comes down to profitability to determine whether blockchain should be implemented. Other literature we will use specifically to base our methodology off of will be Justine and others utilization of the method of game-theoretical analysis to analyze usable security and privacy in banking. The results were the common misconception regarding the idea we cannot combine usability, security, and privacy is untrue. The author provides a theoretical framework to solve the compromises in usability for security and privacy, he shows that it is possible to maintain security, usability, and privacy using game-theoretical analysis which analyzes all the options the "player" has. This will be similar to what we will be doing, except in cloud computing. We are also setting up "players" as computers in order to determine decisions companies will make and assuming profitability through contract variability costs. In order to combine blockchain into cloud computing there will be a security question, we are assuming blockchain will aid security due to Yannan Li and others in "Decentralized Public Key Infrastructures atop Blockchain" a study into the security concerns of public infrastructure; they find that blockchain is a good way of solving the security deficit which exists within public infrastructure. However the depth of the paper will not be limited to scalability and security, the paper will also analyze the efficiency spillover effect of the implementation of blockchain into cloud computing because if we deem blockchain to be profitable then other companies will follow. Literature regarding the implementation of blockchain into other sectors suggests blockchain will lead to an increase in efficiency (Decentralized Public Key Infrastructures atop Blockchain). Our hypothesis is it will be the same for blockchain when implemented in cloud computing. Using past studies as a basis, it is likely blockchains implementation into cloud computing is beneficial for security and efficiency. The effects are far from limited to efficiency, as currently the majority of infrastructure should implement blockchain for the security of applications (Decentralized Public Key Infrastructures atop Blockchain). However, there are conflicting views on the topic as some hackers specifically target applications with blockchain due to the low governance associated with it (Oracles in Decentralized Finance: Attack Costs, Profits and Mitigation Measures). Our paper helps establish a clear view on what the implementation of blockchain truly entails in general infrastructures as well since there are conflicting views on the topic. Although the paper discusses the negative effects of blockchain on security, most are outdated and now the general consensus is that blockchain implementation creates more secure networks because every transaction is traceable. There is no such thing as disappearing in a system with blockchain because transactions cannot be deleted, this creates increased security because there is no such thing as tampering and there is a constant log of what is going through the network. Efficiency, scalability, and security are combined in the paper where the vast opportunity through profitability associated with blockchain in cloud computing are explored. Regarding all the ideas the paper will be exploring, we will be asking the question, is the implementation of blockchain into cloud computing profitable and how is this based upon scalability, efficiency, and security? The study will attempt to fill the gaps which exist in the field which is the profitability of blockchains implementation in cloud computing. Current studies conclude that blockchain would be secure in cloud computing, so we will use the following as an assumption in order to build upon how profitable implementation would be. The implementation of blockchain into cloud computing has not been

explored in depth and this paper serves as a baseline for future research. Creation of infrastructure and research are not accounted for in the costs of implementation and should be studied in future studies.

II. METHOD

The focus of the paper is to identify profitability of blockchain through examining costs by analyzing efficiency, scalability, and security effects of implementation of blockchain into cloud computing. We employ a quantitative research design approach through the format of analyzing profitability. We use a quantitative method to analyze company behavior using game theory in order to zoom into security and we use the Stackelberg game model to assess scalability. We also conduct interviews with companies to determine efficiency of the implementation of blockchain into cloud computing. The reasoning for the following set up is the fact that blockchain security is reliant on behavior, hence analyzing and set up a "game" is the best way to measure security, a qualitative approach is representative of this. Specifically we utilize a quantitative method of game theoretical analysis, a Stackelberg game model which are integrated into the code of our model by finding revenue per blockchain computation. The qualitative approach has the independent variable of blockchain with the dependent variables of security and scalability depending on the method used. We use company behavior using game theory in order to zoom into other companies revenue per blockchain computation and use the Stackelberg game model to assess weather companies will follow on, which there will be an incentive to do so if the model is profitable - thus filling the gap by finding the implications on profitability of the implementation of blockchain into cloud computing. Right now literature discusses hypotheticals regarding blockchain without substantial hands-on research (A Blockchain-Based Authentication and Authorization Scheme for Distributed Mobile Cloud Computing Services). The Stackelberg game model analyzes the number of firms which follow a firm leader (Blockchain in Supply Chain Collaboration: A Quantitative Study), this helps determine scalability in the study. Regarding the independent variable, blockchain is a digital decentralized network aimed at staying away from authority. In order to measure the effect on efficiency we interview corporate employees. The ethical considerations are numbers may be flawed or outdated in the future which means future studies might not be properly based on money considerartions. The second method of game theoretical analysis is used by creating a "game" (Game Theoretical Analysis of Usable Security and Privacy).The research method analyzes the profitability effects of implementing blockchain in cloud computing. In order to do this we learned how to set up a "game" by reviewing literature on human behavior when blockchain is implemented and used the "game" to analyze the security of blockchain. In order to analyze scalability we set up the Stackelberg game model, then used the model to analyze scalability of blockchain in cloud computing - measured by how many companies would follow implementation. The study method uses outcomes which we predict using pre-existing studies on contract variation to determine the cost of business continuation, contract variation is what is accounted for to determine transaction costs as well as tradeoff with profitability. If contracts were to increase in price or become more volatile over time then these numbers from our method and past studies would change, this study accounts for previous analysis on contract volatility and predicted prices of transactions on the blockchain.

III. Results

Researching the effects of the implementation of blockchain in cloud computing resulted in multiple different conclusions. Blockchain's implementation on cloud computing would have different profitability margins based upon which company implemented it, although this may be true, the conclusion is implementing blockchain in cloud computing would be scalable as other companies would adopt similar techniques to compete, and it would be more profitable. The findings prove blockchain in cloud computing would be similar to implementation in other sectors and is projected to be profitable for companies in planning. However, models upon how to implement blockchain must be properly researched as the data finds costs and benefits vary based on which contracts are used. Our study used previous analysis on transaction variation to determine costs and benefits of the implementation of blockchain into cloud computing, this can change over time if contracts become more volatile so costs and benefits are subject to change.

Figure 1: Costs of Implementation

(a) Bitcoin Costs

Transaction fee total cost in	Master hash every			
	30 min	One hour	Half day	One day
One day	$4.32	$2.16	$0.18	$0.09
One week	$30.24	$15.12	$1.26	$0.63
One month	$131.4	$65.7	$5.475	$2.738
One year	$1576.8	$788.4	$65.7	$32.85

(b) EOA Costs

Transaction fee total cost in	Master hash every			
	30 min	One hour	Half day	One day
One day	$0.288	$0.144	$0.012	$0.006
One week	$2.016	$1.008	$0.084	$0.042
One month	$8.76	$4.38	$0.365	$0.1825
One year	$105.1	$52.56	$4.38	$2.19

(c) CA (Variable Data) Costs

Transaction fee total cost in	Master hash every			
	30 min	One hour	Half day	One day
One day	$0.48	$0.24	$0.02	$0.01
One week	$3.36	$1.68	$0.14	$0.07
One month	$14.6	$7.3	$0.608	$0.304
One year	$175.2	$87.6	$7.3	$3.65

(d) CA (Log Event) Costs

Transaction fee total cost in	Master hash every			
	30 min	One hour	Half day	One day
One day	$0.24	$0.12	$0.01	$0.005
One week	$1.68	$0.84	$0.07	$0.035
One month	$7.3	$3.65	$0.3042	$0.152
One year	$87.6	$43.8	$3.65	$1.825

Data of cost of implementation based on cryptocurrency used

Model Deployment:

Figure 2: Model Code

```
import numpy as np
costs = {
   'Bitcoin': 1576.8,
   'EOA': 105.1,
   'CA_Variable': 175.2,
   'CA_Log': 87.6
}

revenue_per_bc = 200
{
   'Bitcoin': 2,
   'EOA': 2,
   'CA_Variable': 2,
   'CA_Log': 2
}

number_of_bcs = 100

csp_payoffs = {}
for key in costs:
   csp_payoffs[key] = (number_of_bcs * revenue_per_bc * revenue_multiplier[key]) - costs[key]
bc_payoffs = {key: -cost for key, cost in costs.items()}

print("CSP Payoffs: ", csp_payoffs)
print("BC Payoffs: ", bc_payoffs)
```

Model Code to calculate profits

Data from Figure 1 was utilized and placed into numpy in order to make profit predictions. The data from Figure 1 analyzes differences in costs based on type of contract, and this is determined based on the company's preferences for security for cost trade-off.

Figure 3: Model Results

```
CSP Payoffs:  {'Bitcoin': 38423.2, 'EOA': 39894.9, 'CA_Variable': 39824.8, 'CA_Log': 39912.4}
BC Payoffs:  {'Bitcoin': -1576.8, 'EOA': -105.1, 'CA_Variable': -175.2, 'CA_Log': -87.6}
```

The meaning of the following is the amount of benefits CSP's would receive from implementing each of the following blockchain technologies

Figure 3.1

```
Bitcoin: $38,423.20
EOA (Externally Owned Accounts, Ethereum): $39,894.90
CA_Variable (Smart Contract with Variable Data Storage, Ethereum): $39,824.80
CA_Log (Smart Contract with Log Event Data Storage, Ethereum): $39,912.40
```

Similarly, the following is the amount of benefits (costs in this case) BC's would receive from implementing each of the following blockchain technologies

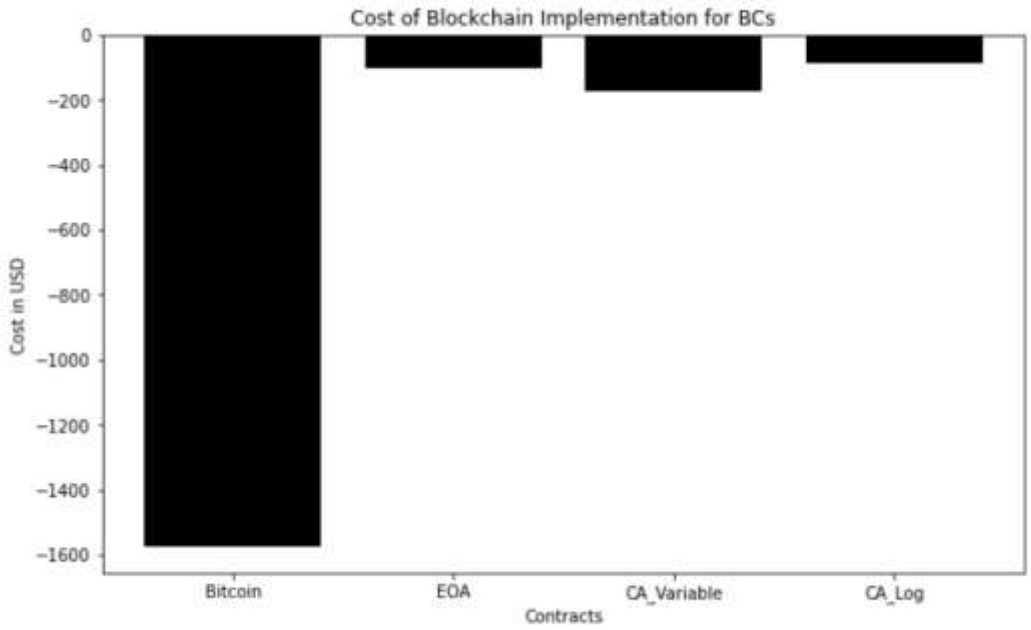
Figure 3.2

```
Bitcoin: -$1,576.80
EOA: -$105.10
CA_Variable: -$175.20
CA_Log: -$87.60
```

BC's incur costs of implementation hence the negative values.

There are various costs for implementing blockchain, and BCs will incur the majority of costs being the first companies to invest in blockchain infrastructure and integration within the cloud. However, these costs are likely to decrease over time as infrastructure becomes widely available. Starting companies' scaling spills over into lower costs for the rest of the industry. Security benefits create an incentive for companies to implement blockchain right now.

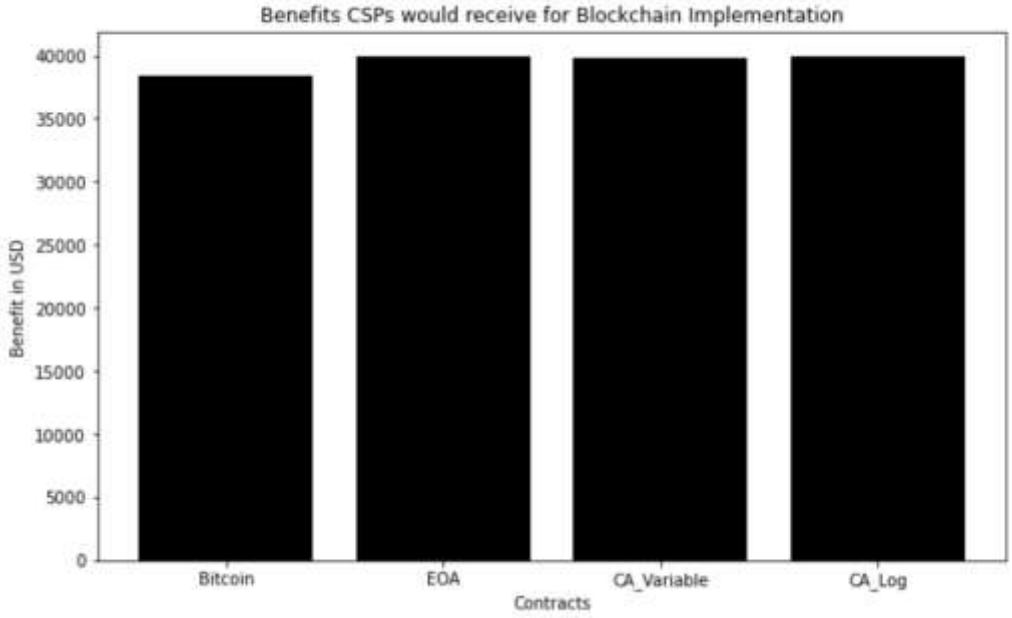
Figure 4: Implementation Costs for BCs



Cost of Implementation for BCs is significantly higher for Bitcoin Contracts

As mentioned earlier, first implementing companies will face the brunt of costs and will have to make decisions based on whether they want more security based on types of contracts. It is likely bitcoin is the most secure contract, however, it is also the most expensive in terms of costs. The study does not factor into various other research and development costs which are also likely required if the company is the leading actor. Leading actors are at a massive disadvantage in terms of cost, but will likely gain increased security first and other companies will follow-on after. Bitcoin will cost ~$1500 for transactions versus a mere ~$100 for EOA, it is clear companies will need to do proper analysis on the security trade-offs made by choosing the cheaper option. It is also not clear whether bitcoin could be the most secure option, it could turn out to be one of the cheaper contracts which would then end up being cheaper for the implementing companies without having to trade-off with security.

Figure 5: Implementation Costs for CSPs



Benefits for Implementation are similar based on contract

Implementation of Blockchain in Cloud Computing is seen to have monetary benefits with follow-on. When the key actors in the sectors were examined due to cost-benefit follow-on is expected. Blockchain is cost-effective and scalable because profitability is significant. However, types of implementation should be properly researched because different contracts have different payoffs. Additionally, different contracts may have different levels of security, so it is essential to invest in proper research before implementation. Furthermore, benefits are similar regardless so contracts come down to company discretion.

IV. DISCUSSION

After analyzing the results, it was concluded Blockchain's implementation on cloud computing would have different profitability margins based on which contracts are chosen. This is not the only thing that will vary implementation cost as the size of the company also will affect costs. There are likely other factors which were not measured by the study. The results also show it would be net profitable for companies to implement blockchain in cloud computing.

Figure 1 illustrates the transaction costs by time based on different types of contracts, however, it can be noticed some are cheaper than others. Figure 1 gives us insight into which contracts would likely be the most profitable model, as bitcoin by seconds can be viewed as having the highest number.

The numbers from figure 2 were determined by cost-security trade-off. Figure 2 showed the results in terms of companies using a comprehensive formula in order to determine revenue and profits for each company. Figure 2 finds revenue and subtracts costs in order to determine profits.

Figure 3.1 shows the results of figure 2 and when interpreted in figure 3.2 we are able to examine net costs of implementation. Bitcoin has a net cost of ~1.5K which is significantly more than the alternative contract options. It is made clear, companies will have to determine whether they want to maintain security or prioritize costs. It is likely that bitcoin is the most secure contract since it has the most robust systems, however it comes with a heavier price tag. Additionally figure 3 shows that follow-on will be cheaper meaning that the first companies to implement cloud computing into blockchain will pay more than the following companies, this is likely because companies originally implementing will have to innovate new infrastructure in order to make blockchain a plausible solution.

Figure 5 depicts the benefits of the implementation of blockchain in cloud computing. Similar to costs, there is a clear difference in benefits based on which contract is chosen. The study does not analyze consumers picking safer options however so in the long run there might end up being more benefits to choosing blockchain. Unlike costs, the difference between benefits is much more marginal between contracts. However, this does not mean that bitcoin is similar in profitability because since the costs are larger the net profit is still lower than the other contracts. Due to the benefits outweighing the costs, follow-on implementation is expected.

Computing Service Provider's or CSP's are the companies that incur both the costs and benefits. Our results do not account for the cost of the creation of infrastructure which is likely high, however, in the long run the investment into additional infrastructure would be worth the cost as there is consistent profitability over all. Although, if various studies find costs of infrastructure and research to outpace the predicted profit, then it would not be profitable for companies to implement blockchain into cloud computing.

The results conclude that benefits outweigh the costs, however, predictions are not accounting for additional research and development which will need to be conducted by the first actor. Companies may also choose less secure contracts to maximize profitability, although that would be counterintuitive to the value of implementing blockchain which is security. Blockchain is likely scalable because of the cost-benefit analysis, and this does not account for an increase in users moving to more secure platforms. It is clear that implementation of blockchain into cloud computing would be beneficial for companies and users alike due to increased security and profitability. The follow-on effect of blockchain's implementation would be concluded to be strong due to the strong profitability projected from implementation.

V. CONCLUSION

The paper concludes the effect of implementation on blockchain would be follow-on because there is profit incentive. However, companies will have to make decisions regarding their own security preferences. Based on their preferences they would pick different contracts which have different profit and security levels. For the future papers on the topic, the extent of compromise on security should be researched as well as which contracts are the most secure. If the following is researched, companies will get a better understanding of which contracts to choose and how much profit they will receive. The limitations of the research conducted was investigation into the security of each contract. Additionally, we made various assumptions which should be tested in future studies such as follow-on and cost of research. Future studies should work towards specific cost analysis and how to properly implement blockchain into cloud computing such as what specific new technologies would be necessary. The paper also built upon past research addressing the security of blockchain, if future research were to deem blockchain was less secured in cloud computing then study should be redone to analyze cost-benefits for companies who implement blockchain. The conclusions of the study use the code referenced in results, which could likely be more in-depth if companies strategic decisions are studied. Additionally, the data regarding contract costs may be outdated in the future, so costs will continue to vary as prices of various contracts change -- future studies may have different results due to different contract prices at the time of the study. Additionally, the study did not account for the cost of infrastructure implementation, this would be in addition to costs of research which has not currently been researched. The costs the study accounted for were for business continuity which only occurs after proper infrastructure is implemented. In summary, future research could address additional costs and continue analysis on the security benefits associated with the implementation of blockchain in cloud computing. In order to mitigate the limitations in the study, the next researchers should work to address different variable costs which may not have been accounted for in this study, they should also delve deeper into the psychology of companies and whether others will follow-on if there is a profit incentive noticed. Future research should also look into which companies would be poised to take the first step in the development of technology for the implementation of blockchain into cloud computing.

WORKS CITED

[1]. Abramowicz, Michael. "The Very Brief History of Decentralized Blockchain Governance." Vanderbilt Journal of Entertainment & Technology Law, vol. 22, no. 2, Winter 2020, pp. 273–98. EBSCOhost, search.ebscohost.com/login.aspx?direct=true&db=asn&AN=142877357&site=ehost-live.

[2]. Aspembitova, Ayana T., and Michael A. Bentley. "Oracles in Decentralized Finance: Attack Costs, Profits and Mitigation Measures." Entropy, vol. 25, no. 1, Jan. 2023, p. 60. EBSCOhost, https://doi.org/10.3390/e25010060.

[3]. Justine, Cynara, et al. "Game Theoretical Analysis of Usable Security and Privacy." Security & Privacy, vol. 4, no. 5, Sept. 2021, pp. 1–14. EBSCOhost, https://doi.org/10.1002/spy2.55.

[4]. K. Gai, J. Guo, L. Zhu and S. Yu, "Blockchain Meets Cloud Computing: A Survey," in IEEE Communications Surveys & Tutorials, vol. 22, no. 3, pp. 2009-2030, thirdquarter 2020, doi: 10.1109/COMST.2020.2989392.

[5]. Li, Yannan, et al. "Decentralized Public Key Infrastructures atop Blockchain." IEEE Network, vol. 34, no. 6, Nov. 2020, pp. 133–39. EBSCOhost, https://doi.org/10.1109/MNET.011.2000085.

[6]. Park JH, Park JH. Blockchain Security in Cloud Computing: Use Cases, Challenges, and Solutions. Symmetry. 2017; 9(8):164. https://doi.org/10.3390/sym9080164

[7]. Shi, Jia, et al. "A Blockchain-Based Decentralized Public Key Infrastructure for Information-Centric Networks." Information (2078-2489), vol. 13, no. 5, May 2022, p. 264. EBSCOhost, https://doi.org/10.3390/info13050264.

[8]. Walker, G. A. “Money and Financial Technology (FinTech) History.” International Lawyer, vol. 56, no. 2, July 2023, pp. 227–331. EBSCOhost, search.ebscohost.com/login.aspx?direct=true&db=asn&AN=164443984&site=ehost-live.

Ishaan Hemrajani
USA