UNDERSTANDING THE APPLICATIONS OF GAME THEORY IN BLOCKCHAIN TECHNOLOGY

Yashwanth Alapati
NetID: ya2351

***Abstract*—Blockchain technology has emerged popular in the past few decades. There has been abundant work carried out in the technical aspects of blockchain, however the game theoretic research work has been less extensive . This paper focuses on the applications of Game Theory, a fundamental concept of the technology. We start with an explanation of Block Chain Technology followed by understanding some fundamental aspects of Game Theory. Then, we look at some use cases that are the intersection of Game Theory and BlockChain Technology. This paper sheds light on an often less explored mathematical field in the domain of Blockchain technology and serves as an introductory material. Primary focus is on the network attacks. As Game Theory is a broad area in mathematics, various aspects can be integrated to design different protocols and mechanisms underlying the technology.**

Keywords—Game Theory, Blockchain, Distributed protocols, Consensus Mechanism, Security

I. INTRODUCTION

Blockchain technology became popular with the paper [1] by Satoshi Nakomoto where the technology acts as a ledger for transactions in cryptocurrency. Since then the technology has been widely adopted to build a plethora of currencies. There have been numerous applications of the technology in other domains as well such as Supply chain management [5], Internet of Things, Sports. The adoption into other industries will continue in the future as well. Blockchain technology involves a participation of consensus nodes in the network. These nodes indulge to grow their own functionality. Some nodes might be malicious and can launch network attacks to disrupt the network. To counter such attacks the technology uses consensus protocols such as Byzantine fault tolerance [2]. But, such consensus protocols need a centralized entity which makes it difficult for adoption in a decentralized network with many systems. Probabilistic models such as Markov Decision Process(MDP) as an optimization technique to prevent malicious activities [2]. MDP functions as a tool for decision making in situations involving randomness.These approaches do not take into account the interaction among nodes [4]. Game Theory has been applied to deal with such issues. With game theory based mechanisms, nodes will be able to predict mining behaviors [4]. It is possible to develop incentive mechanisms which discourage nodes from misbehaving [4]. This paper discusses major issues mentioned in the survey paper in the domain of networks and their security. For thorough analysis refer [4].

The later aspects in this paper are as follows. Section II discusses the foundations of blockchain tehcnology and the architecture. Section III describes the foundations of game theory. Section IV highlights the intersection of game theory and blockchain technology with an onverview and focuses on network security issues in blockchain. Section V discusses the benefits and limitations of pursuing research effort in this domain. Section VI summarizes with a review. Section VII is Acknowledgement and Section VIII mentions the References used in the paper.

II. FOUNDATIONS OF BLOCKCHAIN TECHNOLOGY

Blockchain is a revolutionary technology characterized by a continuous sequence of blocks, each containing a record of transactions. This decentralized and distributed ledger system ensures transparency, security, and immutability. Each block in the chain is linked to the previous one through cryptographic hashes, forming a tamper-resistant and interconnected structure. This design allows for a transparent and verifiable history of transactions, making blockchain particularly valuable in industries such as finance, supply chain, and healthcare. The continuous nature of the blockchain ensures that once information is recorded, it becomes a permanent and integral part of the chain, creating a trustless and efficient system for various applications. Fig.1 [10]provides a description of the structure of a blockchain.

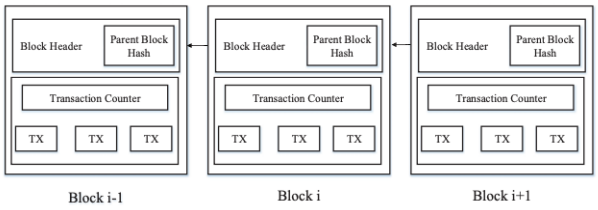

Fig. 1. Sample picture of Blockchain

The block structure is a fundamental aspect of blockchain technology, providing the framework for its decentralized and secure nature. Each block typically includes a block header, timestamp, a nonce (a random number used in the mining process), and the cryptographic hash of the previous block, ensuring the integrity and chronological order of the entire chain. The block structure, with its transparent and interconnected design, plays a crucial role in preventing tampering and providing a reliable ledger for various applications, ranging from cryptocurrencies to smart contracts and beyond. This inherent structure contributes to the security, transparency, and

trustworthiness that define the essence of blockchain technology. Fig2 [10] provides a high level overview of the individual blockstructure in a blockchain. A block also contains a merkle tree which is a data strucutre comprised of cryptographic hashes.

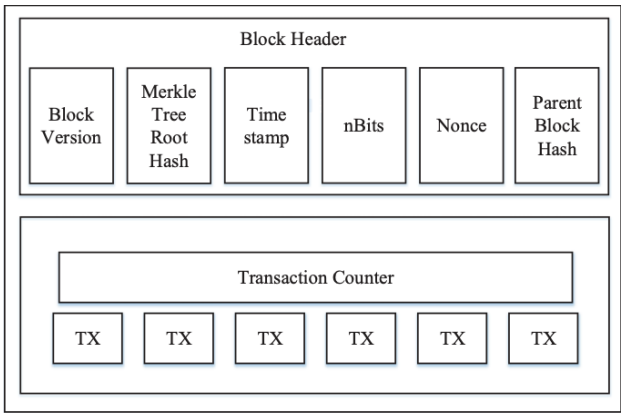

Fig. 2. Structure of a Block

The **Merkle tree** is a fundamental data structure used in blockchain technology and cryptographic systems.It is named after its inventor Ralph Merkle. It is a binary tree structure where each leaf node represents a data block, and each non-leaf (internal) node is a hash of its children. The process is repeated until a single root hash, known as the Merkle root, is obtained. This hierarchical structure allows for efficient and secure verification of the integrity of large datasets. Merkle

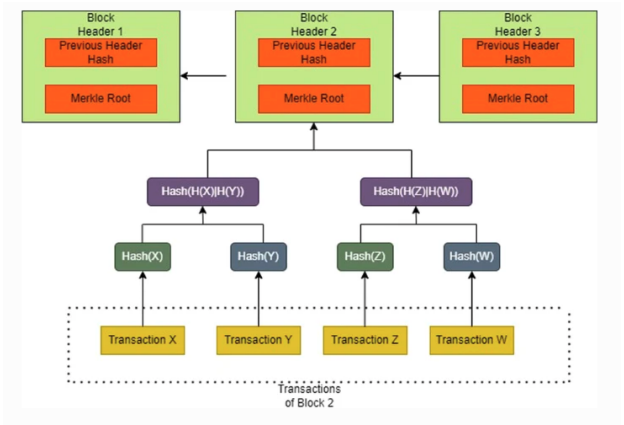

Fig. 3. Merkle tree

trees summarize and efficiently represent the transactions within a block. The Merkle root is then included in the block's header. This has several advantages, including the ability to efficiently verify the presence of a transaction within a block and detect any tampering or corruption within the block.It takes logarithmic search time to find a transaction as opposed to using a linked list to store the transaction details. This makes merkle tree faster and efficient data strcuture. If any piece of data in a block is altered, the corresponding hash in the Merkle tree changes, affecting the root hash and signaling potential foul play. Fig3 [3] provides a description of the usage of Merkle tree in blockchain. Merkle trees find their usecase in wide domain of technologies such as IPFS, Apache Wave protocol etc. [9]

CONSENSUS MECHANISMS:

Consensus mechanisms are the backbone of blockchain networks, ensuring agreement among distributed nodes on the state of the ledger. [6]They play a crucial role in validating transactions and creating new blocks.

- **Non-Byzantine Based Consensus Algorithm:** Non-Byzantine consensus algorithms, like Practical Byzantine Fault Tolerance (PBFT) or Raft, ensure agreement among nodes in a network even when some nodes may fail or behave erroneously, without assuming malicious intent [3].

- **Byzantine Based Consensus Algorithm:** Byzantine consensus algorithms, such as the Byzantine Fault Tolerance (BFT) family, are designed to handle nodes that may exhibit malicious behavior within a network, ensuring consensus despite potential Byzantine faults or intentional disruptions [3].

- **DAG-Based Consensus:** DAG (Directed Acyclic Graph) based consensus, replace the linear block structure of traditional blockchains with a graph, allowing for parallel processing of transactions and potentially enhancing scalability [3].

- **Hybrid Consensus:** [3]Hybrid consensus mechanisms combine different approaches, often integrating both Proof of Work (PoW) and Proof of Stake (PoS) elements, aiming to leverage the strengths of each to achieve a balance between security, decentralization, and efficiency in blockchain networks [3].

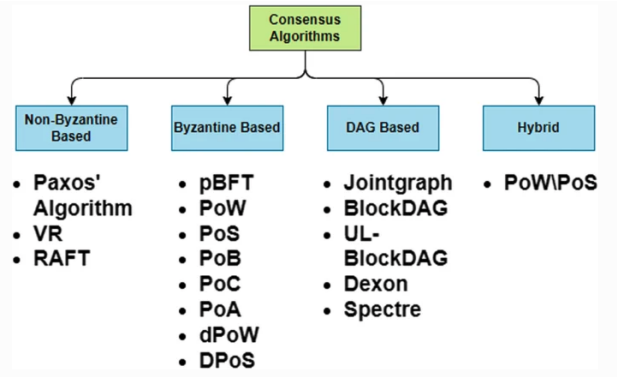

Fig. 4. A variety of consensus algorithms

Fig.4 [3] provides an overview of the different consensus algorithms with examples. Fig.5 provides a comparison between them. [10]

Property	PoW	PoS	PBFT	DPOS	Ripple	Tendermint
Node identity management	open	open	permissioned	open	open	permissioned
Energy saving	no	partial	yes	partial	yes	yes
Tolerated power of adversary	< 25% computing power	< 51% stake	< 33.3% faulty replicas	< 51% validators	< 20% faulty nodes in UNL	< 33.3% byzantine voting power
Example	Bitcoin [2]	Peercoin [21]	Hyperledger Fabric [18]	Bitshares [22]	Ripple [23]	Tendermint [24]

Fig. 5. Consensus algorithms- Comparison

III. Foundations of Game Theory

Game theory, a branch of applied mathematics and economics, provides a conceptual framework for analyzing interactions and decision-making in strategic situations. [7] [8].It explores the rational choices of individuals or entities, known as players, in scenarios where the outcome of each participant's decision depends on the choices of others. Game theory is particularly relevant in situations where interdependence and conflicting interests exist, such as in economics, political science, biology, and even everyday social interactions. Central to game theory is the concept of a game, which comprises players, strategies, and payoffs. [7] [8] Players make decisions based on their assessments of the likely actions and reactions of others, seeking to maximize their own outcomes. Whether used to understand economic markets, international relations, or evolutionary dynamics, game theory provides valuable insights into the dynamics of strategic decision-making and has become an indispensable tool in various fields of study. Let's have a look at some of the most common types of games in Game Theory.

Cooperative/Non-cooperative game theory: In cooperative game theory, participants collaborate to achieve mutual benefits by forming coalitions and making joint decisions. The focus is on how players can achieve optimal outcomes through cooperation, considering the value of binding agreements and the distribution of gains. On the other hand, non-cooperative game theory examines situations where participants act independently, making decisions based on self-interest and without formal agreements. It emphasizes strategic interactions and analyzes the optimal choices individuals make when faced with competitive scenarios. Both cooperative and non-cooperative game theory provide valuable insights into understanding and predicting behavior in diverse decision-making situations, from business negotiations to international relations.

Symmetric/ Asymmetric game theory: Symmetric game theory focuses on situations where players in a game have identical strategies, payoffs, and information. In such games, each participant faces the same set of choices and outcomes, leading to a balanced and often simpler analysis. [7] [8]Examples of symmetric games include the classic Prisoner's Dilemma, where two suspects face identical decisions regarding cooperation and betrayal. In contrast, asymmetric game theory deals with situations where players possess different strategies, payoffs, or information. These games acknowledge the inherent disparities among participants, leading to varied decision-making processes and outcomes. [7] [8]Asymmetric games introduce complexities, as players may have unique advantages, disadvantages, or goals. Examples include games where one participant has more information than others or scenarios with varying abilities among players. Analyzing asymmetric games requires a more nuanced approach, often involving considerations of strategic moves, information asymmetry, and the development of mixed strategies to account for the diverse characteristics of the players involved. Fig.6 provides an example as mentioned in [8]

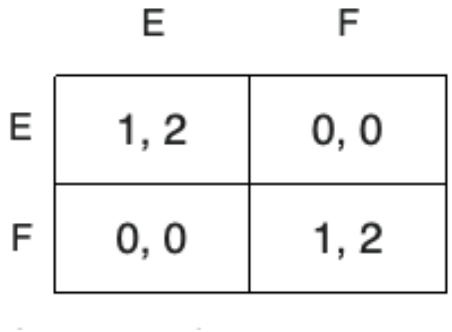

Fig. 6. Example of an Asymmetric game

Zero-sum/non-zero sum game theory: A zero-sum game is a concept in game theory where the total amount of wealth, utility, or value in a given interaction remains constant, meaning any gain by one participant must be offset by an equivalent loss by another. In other words, the participants' interests are directly opposed, and what one player gains, the other loses. The term "zero-sum" reflects the idea that the sum of the players' gains and losses totals to zero. Common examples include competitive sports, where the victory of one team corresponds to the defeat of the other, or certain economic scenarios where wealth is redistributed rather than created. [8] Zero-sum games highlight the inherent conflict of interest among participants and serve as a contrast to non-zero-sum games, where cooperation can lead to mutually beneficial outcomes. Fig.7 provides an example as mentioned in [8] Understanding zero-sum dynamics is crucial in analyzing competitive situations and strategic interactions where resources or benefits are fixed and finite.

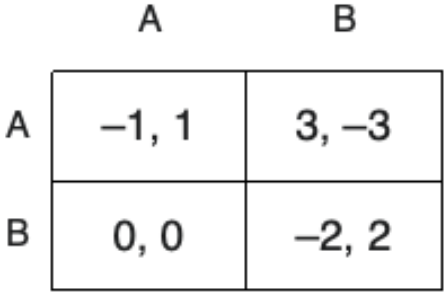

Fig. 7. zero-sum game

Simultaneous/Sequential game theory: Simultaneous and sequential games characterize the timing of players' decision-making. Simultaneous games involve participants making choices simultaneously, without knowledge of each other's decisions. Examples include classic Rock-paper scissors. [7] [8]In contrast, sequential games unfold in stages, where one player makes a move after observing the previous player's decision. This sequential structure introduces an element of anticipation and reaction, often represented in extensive form games. Chess is an illustrative example of a sequential game where players take turns making moves based on the unfolding board position. [7] [8] The distinction between simultaneous and sequential games is crucial in analyzing strategic interactions, as the timing of decisions can significantly influence the outcomes and strategies employed by rational players.Fig.8 provides an example as mentioned in [8]

	Sequential	Simultaneous
Normally denoted by	Decision trees	Payoff matrices
Prior knowledge of opponent's move?	Yes	No
Time axis?	Yes	No
Also known as	Extensive-form game Extensive game	Strategy game Strategic game

Fig. 8. sequantial/simultaneous game

Bayesian game: A Bayesian game is an extension of traditional game theory that incorporates the concept of incomplete information, where players have uncertainty about some key parameters. In Bayesian games, players hold beliefs about the probability distribution of the other players' types or characteristics, which may affect their strategies and decisions. Fig.9 provides an example of bayesian game between two players. Unlike classical game theory, where players have complete information, Bayesian games allow for modeling situations where participants have private information or different perceptions of the game's parameters. [8]

	2 wishes to meet 1	
	B	S
B	2,1	0,0
S	0,0	1,2

	2 wishes to avoid 1	
	B	S
B	2,0	0,2
S	0,1	1,0

Fig. 9. Bayesian game

Stackelberg Game: [4] In Stackelberg games, named after the German economist Heinrich Stackelberg, the players have a hierarchical structure, with one player, the leader, making decisions first, and the other player, the follower, making decisions in response. The leader's strategy is known to the follower when making their decisions. This type of game is prevalent in various real-world scenarios, such as business competition, where one firm may set prices or production levels, and others respond. Stackelberg games are analyzed using mathematical models to determine optimal strategies for both the leader and the follower. This hierarchical structure introduces an element of strategic advantage for the leader, who can anticipate and exploit the reactions of the follower, leading to different outcomes compared to simultaneous decision-making scenarios.Fig.10 provides an example as mentioned in [4]

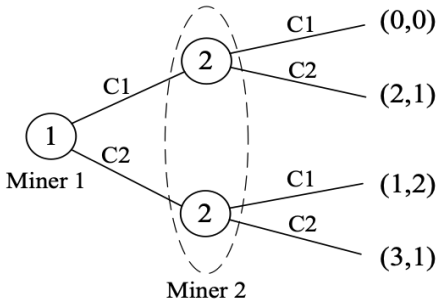

Fig. 10. extensive form game

Stochastic Game: Stochastic games extend traditional game theory models to incorporate elements of uncertainty and randomness. [4] In stochastic games, players make decisions in a dynamic environment where the outcomes are influenced by random events or chance. Unlike deterministic games, where the consequences of actions are fixed, stochastic games involve probabilistic transitions between states. [4] This model is particularly useful for representing scenarios with incomplete information, evolving dynamics, or random elements. Stochastic games find applications in various fields, including finance, biology, and decentralized decision-making processes. [4] Analyzing stochastic games involves considering the probabilities associated with different actions and outcomes, requiring more sophisticated mathematical tools, such as Markov decision processes, to determine optimal strategies in the face of uncertainty

The diverse branches of game theory offer a rich toolkit for understanding and analyzing strategic interactions across a wide spectrum of disciplines. In the following section we will focus on the applications of game theory in the domain of Blockchain Technology. We will provide an overview and quickly focus primarily on the network aspects and the solutions to these problems using Game theory. We will contrast with the solutions offered by MDP as well, to provide the reader with a comparison as to why game theory is a better solution than the former.

IV. Intersection of Game Theory and Blockchain Technology

The prominent application is in consensus mechanisms, where nodes must agree on the state of the blockchain. Byzantine Fault Tolerance (BFT) algorithms, inspired by game theory principles, ensure consensus even in the presence of malicious actors. Additionally, incentive mechanisms for blockchain participants, such as Proof of Work (PoW) and Proof of Stake (PoS), are designed using game-theoretic principles to encourage honest participation and discourage malicious behavior.

Furthermore, tokenomics, the study of the economic incentives and mechanics of blockchain tokens, heavily relies on game theory to design systems that align the interests of various stakeholders. Decentralized finance (DeFi) applications, which operate on blockchain platforms, frequently employ game-theoretic models to create robust and secure financial ecosystems.

In essence, game theory provides a theoretical foundation for understanding and designing the incentives, mechanisms, and interactions within blockchain systems, contributing to the development and sustainability of decentralized networks. While there are many different areas that can be modelled using game theory, we will focus primarily on the network aspects of the blockchain technology.

Selfish Mining Attack: In the realm of blockchain and game theory, the selfish mining attack is a strategic maneuver where a miner seeks to gain an unfair advantage by selectively revealing mined blocks. While MDP can be used to model the issue, it doesn't take into account the interactin among multiple players.The authors in [4] utilize a non-cooperative game to understand the interaction among the pools. We can visualize the scenario discussed in the paper in Fig.11 [4]

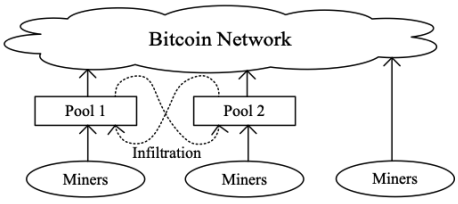

Fig. 11. PBWH attack

Selfish Mining Attack	[35]	Non-cooperative game	Mining pools	Infiltrate other pools to launch BWH attack	Determination of the infiltration rate	Mining rewards minus cost	Nash equilibrium
	[55]	Splitting game	One miner and pools	Distribute mining power for selfish mining	Determination of the power distribution	Mining rewards minus cost	Mixed strategy Nash equilibrium
	[56]	Mean-payoff game	Mining pools	Migrate to other pools to launch PBWH attack	Determination of the migration rate	Mean-payoff	Mean-payoff objective
	[50]	Stochastic game	Miners	Block withholding (BWH) attack	Selection between honest mining and selfish mining	Social welfare	Zero-Determinant strategy
	[57]	Non-cooperative game	Miners	Selfish propagation attack	Selection of identity duplication and transactions relaying	Mining rewards	Nash equilibrium
	[33]	Non-cooperative game	Miners	Fork chain	Selection of fork to mine	Transaction fees	Nash equilibrium
	[58]	Non-cooperative game	Miners	Delay submitting shares	Decision of the proper time to submit shares	Mining rewards	Nash equilibrium
	[28]	Non-cooperative game	Miners	Select or create a chain to mine	Selection of the chain to mine	Mining rewards	Nash equilibrium

Fig. 12. selfish mining attack

This is similar to the problem we discussed before- the prisoner's dilemma. [4] discusses the solution in detail.

Majority Attack: A majority attack, or 51 percent attack, is a significant threat to blockchain security wherein a malicious actor gains control of over half the network's computational power. Game theory plays a pivotal role in evaluating the strategic considerations of such an attack and devising preventive measures. The attacker's incentive lies in the ability to rewrite transaction history, enabling double-spending and undermining the trust in the blockchain. [4] discusses in detail a game theoretic solution to the majority attack problem.

majority Attack	[28]	Stochastic game	Miners	BWH attack	Decision of the proper time to release the block	Mining rewards	Nash equilibrium
	[59]	Non-cooperative game	Miners	Post smart contract transaction of mining on private chain	Selection between working on smart contract transaction and honestly mining	Transaction fees and mining rewards	Nash equilibrium
	[51]	Stochastic game	Miners	Compete to fork chain	Selection of adding the block to the chain	Mining rewards minus cost	Nash equilibrium
	[60]	Non-cooperative game	Attacking and defending miners	Issue whale transaction to attract miners mine on the private chain	Determination of the threshold of attack cost and block selection	Mining reward minus cost	Nash equilibrium
	[61]	Sequential game	Attacking and defending miners	Buy stake to launch majority attack	Determine the cost of attack and selling selection	Function of profit and interest	Nash equilibrium
	[28]	Non-cooperative game	Attacking and defending miners	Goldfinger attack	Decision of forming cartel and determination of the tax paid to the attacker	Profits minus cost	Nash equilibrium
	[43]	Stackelberg game	Blockchain users and miners	Form cartel to launch majority attack	Setting transaction fee and selection of recruiting miners	Profits minus cost	Stackelberg equilibrium

Fig. 13. majority attack

DOS Attack: In the context of blockchain and game theory, a Denial-of-Service (DOS) attack involves flooding the network with malicious traffic to disrupt its normal operation. Game theory helps understand the strategic motivations behind DOS attacks and devising resilient protocols. By exploiting vulnerabilities in the network, attackers can hinder transaction processing and compromise the availability of blockchain services. [4] Game-theoretic models we discussed already like the non-cooperative game theory can be adopted to analayze intreaction between the pools. [4] provides a thorough description of the problem.

DoS Attack	[62]	Non-cooperative game	Mining pools	DDoS attack	Selection of launching attack or not	Profits minus cost	Nash equilibrium
	[63]	Sequential game	Mining pools	DDoS attack	Chosen of the attack level	Profits minus cost	Nash equilibrium
	[64]	Repeated game	Mining pools	DDoS attack under a reputation-based scheme	Selection of launching attack or not	Profits associate with the loss of reputation	Nash equilibrium
	[65]	Non-cooperative game	One server and devices	DDoS attack in edge network	Selection between executing or sending request and launching attack	Profits minus cost	Nash equilibrium

Fig. 14. Denial Of Service attack

V. Benefits and Limitations

In this section we will discuss the advantages and disadvantages of pursuing game theoretic solutions to problems in the domain of blockchian technology.

[6] LLM has been prompted with some scenarios and case specific prompts to get an overall idea about the limitations that game theory could have in respect of Blockchain Technology.

Benefits:

- Synergy: Game theory provides a powerful framework for understanding the incentives of various actors within a blockchain network. By applying game-theoretic models, researchers can design protocols that align participants' interests with the overall health and security of the network, fostering cooperation and adherence to established rules.
- Improving Security: Game theory contributes to the development of robust security mechanisms in blockchain

systems. Analyzing strategic interactions and potential attacks, researchers can design protocols that deter malicious behavior, ensuring the integrity and resilience of the decentralized network against various threats, including 51 percent attacks or selfish mining.

- Tokenomics and Incentive Structures: Understanding the economic incentives embedded in blockchain systems is crucial for their success. Game theory helps researchers model and analyze tokenomics, ensuring that the economic design of the system encourages desired behaviors, discourages malicious activities, and promotes a healthy ecosystem.

Limitations:

- Complexity and Assumptions: Game theory models often involve simplifications and assumptions about participants' rationality and information availability. In the complex and dynamic environment of blockchain, these assumptions may not always hold, leading to potential discrepancies between theoretical predictions and real-world outcomes.
- Scalability Concerns: Blockchain networks face scalability challenges, and integrating complex game-theoretic models can worsen these issues. The computational overhead associated with implementing sophisticated game theory solutions could hinder the scalability of blockchain systems.
- Human Factors: Game theory assumes rational decision-making, but human behavior is often influenced by psychological and emotional factors. Understanding and predicting the actions of participants in a blockchain network may be challenging due to the unpredictable nature of human responses to economic and strategic incentives.

VI. Conclusion

Blockchain technology has some challenges to be addressed, in terms of network security and consensus mechanisms. While the intersection of blockchain and game theory offers substantial benefits in terms of security, incentive alignment, and protocol optimization, researchers must be mindful of the limitations related to the dynamic nature of the ecosystem, scalability concerns, and the complexity of modeling human behavior. Furthering research along the intersection while looking for ways to address the limitations at the same time can help address these challenges and promote a healthy blockchain ecosystem.

VII. Acknowledgement

The Author expresses gratitude to Professor Ayesha Kiani of NYU Tandon School of Engineering, for providing an opportunity to work on this challenging project as part of the Introduction to Blockchain and Distributed Ledger Technology course.

References

[1] Nakamoto S Bitcoin. Bitcoin: A peer-to-peer electronic cash system, 2008.

[2] Miguel Castro and Barbara Liskov. Practical byzantine fault tolerance and proactive recovery. *ACM Transactions on Computer Systems (TOCS)*, 20(4):398–461, 2002.

[3] Ziad Hussein, May A Salama, and Sahar A El-Rahman. Evolution of blockchain consensus algorithms: a review on the latest milestones of blockchain consensus algorithms. *Cybersecurity*, 6(1):30, 2023.

[4] Ziyao Liu, Nguyen Cong Luong, Wenbo Wang, Dusit Niyato, Ping Wang, Ying-Chang Liang, and Dong In Kim. A survey on applications of game theory in blockchain. *arXiv preprint arXiv:1902.10865*, 2019.

[5] Rizwan Manzoor, BS Sahay, and Sujeet Kumar Singh. Blockchain technology in supply chain management: an organizational theoretic overview and research agenda. *Annals of Operations Research*, pages 1–48, 2022.

[6] OpenAI. chatgpt-large language model. 2023.

[7] John Von Neumann and Oskar Morgenstern. Theory of games and economic behavior, 2nd rev. 1947.

[8] Wikipedia. Game theory — Wikipedia, the free encyclopedia. http://en.wikipedia.org/w/index.php?title=Game%20theory&oldid=1189288630, 2023. [Online; accessed 23-December-2023].

[9] Wikipedia. Merkle tree — Wikipedia, the free encyclopedia. http://en.wikipedia.org/w/index.php?title=Merkle%20tree&oldid=1183755078, 2023. [Online; accessed 23-December-2023].

[10] Zibin Zheng, Shaoan Xie, Hongning Dai, Xiangping Chen, and Huaimin Wang. An overview of blockchain technology: Architecture, consensus, and future trends. In *2017 IEEE international congress on big data (BigData congress)*, pages 557–564. Ieee, 2017.