به نام یگانه متعال
سمینار و روش تحقیق کارشناسی ارشد
دانشکده مهندسی برق و کامپیوتر
زمستان ۱۴۰۰

۱- برای بخش مقدمه هر یک از پنج مقاله زیر، چهار قدم مشخص شده را که در کلاس درس توضیح داده شدند[1]، مشخص کنید.

- مقاله اول
- مقاله دوم
- مقاله سوم
- مقاله چهارم
- مقاله پنجم

۲- در مقدمه زیر ابتدا ایرادهای موجود را مشخص کرده و سپس آن را بازنویسی کنید.

Over the past decade, there have been increasing calls for a decentralized Web3 which aims to address the disadvantages of the current centralized infrastructure, including a single point-of-failure, censorship, and data privacy.

An important aspect of a decentralized Web3 is the ability to outsource tasks to spare resources, creating network resource sharing (NRS) services. This is essential as central servers (e.g. the Cloud) should not be blindly trusted. NRS services can broadly be classified as storage, computation, or band- width sharing services. A service may also target all of these, as is the case for decentralized content delivery networks. Sharing network resources in a decentralized network isn’t a new concept, but what makes Web3 initiatives unique is their integration with blockchains to create an incentive layer. Classical peer-to-peer (P2P) systems suffered from a number of problems, rendering them useless in the long term, including, free-riding, instability due to churn, and security vulnerabilities. By providing a fair exchange for performed work in the form of cryptocurrency rewards, blockchain-based NRS services add incentives, security, and robustness.

[1] قدم اول: نشان دادن اهمیت و محوریت موضوع، قدم دوم: مرور ادبیات، قدم سوم: نشان دادن شکاف موجود، قدم چهارم: هدف تحقیق

One prominent example of a NRS service is Filecoin, a decentralized storage market. A blockchain is used as an incentive layer, allowing clients and sellers to create storage deals on a public ledger and reward the storage node accordingly. As storage on blockchain is highly inefficient, data is stored locally at storage nodes.

While the blockchain can be used to establish trust for transactions on-chain, the actual NRS service is provided off- chain and occurs directly between two parties. This means that we cannot rely solely on an honest majority of the network for security. A simple illustration is a provider node which promises a service, but is not able to complete the service. While it does not gain extra rewards, the client may experience additional negative consequences. As any node in the network is potentially malicious there is a risk with every deal.

To discern between honest and malicious parties a reputation system is needed. Generally, a reputation system is a mechanism which produces a score for nodes in a network, indicating the trust in a likely positive experience with them. The reputation system aggregates a number of metrics and follows a scoring mechanism to produce scores. A common use-case of reputation systems is in e-commerce, where trust is established between buyers and sellers using transaction feedback. However, these types of reputation systems rely on a centralized infrastructure, and are therefore unsuitable for Web3 applications.

P2P research presented a number of distributed trust and reputation systems [3], but these ultimately did not reach mass adoption due to their complexity and security vulnerabilities. While these systems used a range of metrics, both public and private, to the best of our knowledge none have incorporated blockchain data.