ECE 8930: Blockchain Technology and Web 3.0

Homework 3

Saurabh Sharma
12/02/2023

Q1) Bitcoin also has its own scripting language. So why can't we use BTC's scripting language to implement smart contracts?
This is the case because 'Script' is a purposefully non-Turing complete language. Now let's dive deeper into what this means and why was it intentionally designed to be this way.

A Turing Complete system means a system in which a program can be written that will find an answer (although with no guarantees regarding runtime or memory). So, if somebody says "my new thing is Turing Complete" that means in principle (although often not in practice) it could be used to solve any computation problem. So to design any application, our framework or scripting language for smart contracts in our case needs to be Turing complete.

The important thing here is that there is no guarantee on runtime which can be very negative for our bitcoin use-case. If a single transaction was Turing-complete, then it would have an unknowable verification time and could be used as a DoS vector on nodes that would attempt to verify it. With any single transaction having a knowable worst-case verification time, there's no problem of a transaction's validity being unknowable.

Another reason that we don't use BTC's scripting language for smart contracts is that 'Script' doesn't have op_codes. Bitcoin's scripting language operates using a set of opcodes that define the conditions under which bitcoins can be spent. These opcodes have limitations and were primarily designed for simple transactions, not complex contract execution or computations. This again limits the complexity of Dapps we can create using BTC's script based smart contracts.

Due to these limitations, other blockchain platforms such as Ethereum were developed specifically to support more sophisticated smart contracts. Ethereum's design allows for a more expressive and flexible scripting language (Solidity) that facilitates the creation and execution of complex smart contracts, enabling developers to build decentralized applications (dApps) with diverse functionalities beyond simple transaction conditions.

To illustrate the limited complexity of BTC based smart contract dApps and Ethereum's lets consider a scenario. Suppose we want to make a simple escrow smart contract. Person A and Person B aim to set up a basic escrow smart contract to facilitate fund exchange. Person A deposits 1 BTC into the smart contract with conditions for fund release. The funds will be disbursed to Person B under two specific circumstances: first, if both Person A and Person B agree to the fund release together, and second, in case of any dispute, a specified arbitrator holds the authority to decide the recipient of the funds. This escrow scenario involves multiple conditions and requires a level of conditional logic involving multiple parties and an arbitrator that goes beyond what Bitcoin's scripting language can handle effectively.

Q2) What is the purpose of sharding? With sharding, what are sharded?

Sharding is a technique utilized in blockchain technology to alleviate scalability issues faced by traditional non-sharded blockchains. Its primary objective is to enhance the network's throughput and efficiency by dividing the blockchain into smaller, more manageable partitions known as "shards." This partitioning enables the network to process transactions and execute smart contracts in parallel across multiple shards, thereby significantly boosting the network's capacity to handle a larger number of transactions simultaneously.

The primary purpose of sharding revolves around addressing the scalability bottleneck present in many blockchain networks. By breaking down the network into smaller shards, each shard is assigned specific transactional responsibilities. Consequently, transactions are processed in a parallel and independent manner within their respective shards. This parallel processing drastically increases the overall transaction throughput of the blockchain, as opposed to a non-sharded network where all transactions are processed sequentially in a single chain.

Sharding is instrumental in reducing the computational and storage overhead on individual nodes within the network as well. Each shard only maintains a subset of the entire transaction history and state information. As a result, nodes are relieved from storing the entirety of the blockchain's data, leading to reduced storage requirements and computational load, thereby improving the overall efficiency of the network.

In a sharded blockchain, transactions and smart contracts are the primary entities that are sharded. Transactions are partitioned among different shards for processing, enabling parallel execution. Similarly, smart contracts can also be sharded, allowing each shard to handle the execution of a specific subset of smart contracts. This division of workload among shards permits concurrent execution of transactions and smart contracts, ultimately facilitating higher throughput and improved performance in the blockchain network.

Q3) What are Layer 1 and Layer 2 of Ethereum? Pick one solution of Ether's Layer 2 to describe in more details.

Layer 1 and Layer 2 solutions in Ethereum refer to different approaches to scaling the Ethereum network to handle a larger number of transactions and smart contract interactions.

Layer 1 or L1 of Ethereum refers to the base protocol layer of Ethereum. It includes the main Ethereum blockchain where transactions are processed and validated through the consensus mechanism, typically Proof of Work (PoW) in Ethereum's case (transitioning to Proof of Stake with Ethereum 2.0). Layer 1 solutions aim to improve the scalability and performance of the main blockchain itself.

Layer 2 or L2 solutions are built on top of the main Ethereum blockchain (Layer 1) and provide mechanisms to execute transactions or smart contracts off-chain or in a more scalable manner. These solutions aim to alleviate congestion on the main chain by moving some computations off-chain while maintaining security and decentralization.

Optimistic Rollup employs an off-chain execution model, processing transactions optimistically away from the Ethereum main chain. This method involves bundling transactions and conducting computations on a secondary chain known as Rollup, dedicated to storing transaction data and computation outcomes. The off-chain execution significantly enhances the scalability of Ethereum by relieving the main chain from processing each individual transaction.

Data availability remains paramount in Optimistic Rollup. To ensure a continuous connection between Layer 2 and Layer 1, a condensed form of transaction data, referred to as calldata, along with transaction results, is periodically relayed to the Ethereum main chain. This process of periodic submission safeguards the integrity of data and guarantees its availability, reinforcing the linkage between the Layer 2 off-chain computations and the Layer 1 Ethereum network.

Additionally, Optimistic Rollup incorporates a robust mechanism for fraud proofs and dispute resolution to maintain the network's security. In the event of a participant submitting fraudulent transactions, other users have the capability to present fraud proofs, providing concrete evidence of the wrongdoing, directly to the main Ethereum chain. This initiates a structured dispute resolution procedure on-chain, allowing for the verification and rectification of the fraudulent activity. Such fraud detection and resolution processes serve as critical safeguards, preserving the overall security and trustworthiness of the Optimistic Rollup system.

Optimistic Rollup significantly increases Ethereum's throughput by processing most transactions off-chain while maintaining security guarantees from the Layer 1 Ethereum blockchain. It's one of the promising Layer 2 solutions addressing Ethereum's scalability challenges without compromising on security and decentralization.

Q4) What are the most and least promising Web 3.0 applications in your opinion? Explain why.

According to my the most promising Web 3.0 application is decentralized social media as this will fundamentally implement absolute free speech which is a pretty big deal in today's world where everything is monitored.

True free speech holds significant positive implications for society. It fosters diversity of thought and innovation by allowing a wide range of opinions and perspectives to be expressed. Encouraging open dialogue and debate, it enables individuals to engage in civil discourse, leading to greater understanding and critical thinking. In democratic societies, it strengthens accountability and transparency by providing a platform for citizens to voice their opinions and hold institutions accountable. Moreover, free speech supports personal empowerment, enabling individuals, especially marginalized groups, to advocate for their rights and challenge social injustices. In academic realms, it preserves the pursuit of knowledge and academic freedom by fostering an environment where ideas can be explored without fear of censorship.

Moreover, decentralized social media ecosystems explore novel incentive models and governance structures. By leveraging blockchain and tokenization, these platforms seek to offer fairer compensation to content creators and participants. Direct interactions between creators and their audience, enabled by reduced intermediaries, can establish new reward mechanisms through microtransactions or token-based incentives. Additionally, community-driven governance models foster transparency, inclusivity, and user involvement in platform decision-making, aligning platform development with the collective interests of its users.

Least promising Web3 application is NFTs according to me. NFT or Non fungible tokens hold no real value according to me except bragging right which will fade with time. This application is fundamentally flawed according to me.

There is a lack of inherent value or ownership representation in certain NFTs, where ownership rights might not necessarily translate into tangible real-world ownership or utility beyond the digital realm. Additionally, the current hype and speculation surrounding NFTs have led to a proliferation of low-quality or plagiarized content, raising issues of authenticity, copyright infringement, and market oversaturation, which could potentially undermine the long-term value and credibility of the NFT space.

Also NFTs have a negative impact on sustainability and our environment in general. NFTs, often built on blockchains utilizing Proof of Work (PoW) consensus mechanisms, such as Ethereum, require substantial computational power, contributing to high energy consumption. This energy-intensive process has raised environmental concerns, especially regarding carbon emissions and sustainability, as the energy footprint associated with minting and trading NFTs can be significant.

Because of these reasons I personally don't believe in NFTs and I think eventually people will realise its fundamental flaw and environmental impact and won't use it.