project4part1

April 7, 2025

1 Part I: Literature Review

1.1 *A Trustworthy Data Verification Technique for Cross-Chain Data Sharing Based on Merkle Trees*1

The authors proposed a novel technique for data verification in cross-chain data sharing based on Merkle trees, which provides an efficient and secure way to validate data in a decentralized environment. The authors describe their method as computing hashes of fixed-sized blocks from the shared data. These pairs of hashes form the binary tree structure, where the leaves are hashed into nodes and so on eventually creating the root. The root is then shared in a relay mechanism along with the corresponding data and the receiver then computes the same Merkle tree from the data. Should the roots contradict, it can be assumed the data is tainted and treated as such.

The important implication by the authors is that the relay mechanism is efficient in providing authenticity and security. Computation time of the Merkle tree is efficient when compared to using a double-layer index or EtherQL, Ethereum's data structure. This makes it ideal for decentralized sharing of data, specifically in blockchains.

1.2 *A Quantum-Resistant Photonic Hash Function*2

Researchers propose a quantum-resistant photonic hash function that demonstrates strong collision resistance, with required attempts increasing exponentially with the number of modes in the quantum hash function, thus suggesting robust resistance against birthday attacks. The proposed hash function is designed to be secure against attacks from quantum computers into the future, with strong implications for blockchain systems that are vulnerable to quantum attacks. The authors also highlight that the Gaussian boson sampling approach is easier to implement with current technology compared to other quantum hashing methods, making it feasible to implement now, and, along with exponential scalability, make sit highly cost-effective.

1.3 *Fair Client Puzzles from the Bitcoin Blockchain*3

The authors here describe a way to use hash puzzles, like those used in blockchain cryptocurrencies, to discourage denial of service (DoS) attacks. The motivation is to require some proof of work that is both non-trivial while also being reasonably achievable, and introduces a concept of fair client puzzles that can be solved independently of the client's computing capabilities. Requests require these proofs-of-concepts to elicit only honest requests of a service, where solving the puzzle makes DoS attacks computationally inefficient but still reasonable for legitimate clients. The puzzle suggested by the authors as a proof of concept supplies a message which is then encapsulated into the block through the Bitcoin public key to address generation algorithm.

1.4 References

1. Wang, R., Zhong, S., Zhou, Q., & Tu, J. (2023). A Trustworthy Data Verification Technique for Cross-Chain Data Sharing Based on Merkle Trees. *In 2023 International Conference on Distributed Computing and Electrical Circuits and Electronics (ICDCECE)* (pp. 1-6). https://doi.org/10.1109/icdcece57866.2023.10150492
2. Tomoya Hatanaka, Rikuto Fushio, Masataka Watanabe, William J. Munro, Tatsuhiko N. Ikeda, & Sho Sugiura. (2024). A Quantum-Resistant Photonic Hash Function. https://doi.org/10.48550/arxiv.2409.19932
3. Boyd, C., & Carr, C. (2016). Fair Client Puzzles from the Bitcoin Blockchain (pp. 161–177). Springer, Cham. https://doi.org/10.1007/978-3-319-40253-6_10