**Fall 2023 ISEC 885 : Project Overview Report: Research on Asynchronous Consensus Protocols**

**Introduction:**

The Idea Concept Paper will identify and focus a research direction in the field of Asynchronous Consensus and Permissionless Systems. Specifically, the research will incorporate the Aleph protocol (Gągol et al., 2019) as the basis of the consensus protocol targeted for improvement to enhance its efficiency and scalability by reducing communication complexity. The paper will address a performance problem with Alephs communication complexity and propose an improvement based on the evaluation and integration of published improved Reliable Broadcast Communications (RBC), replacing Aleph’s merkle tree based RBC with one based on RSA accumulators (Hussein & Al-Gailani, 2022).

The Aleph protocol is important because it is credited to being one of the first asynchronous consensus protocols to operate in a permissionless setting by removing the need of Distributed Key Generation (DKG) and operating without a trusted dealer (Guo et al., 2022). However, performance is throttled by the use of merkle tree based RBC, which becomes resource intensive as the network scales. This is because merkle trees provide cryptographic proofs of data integrity, but require significant computational resources for construction and verification leading to increased latency and reduced throughput in blockchain systems. (Hussein & Al-Gailani, 2022).

To address these issues, this research proposes replacing Aleph's merkle tree based RBC with a more efficient system based on RSA accumulators. RSA accumulators offer a cryptographic alternative that can significantly reduce communication and computational complexity (Reddy, 2021). By integrating RSA accumulator based RBC, the protocol aims to decrease communication complexity, leading to an enhanced performance.

**Objective:**

The objcitve of this research is to reduce the communication complexity of the Aleph protocol by implementing an improved RBC protocol using RSA accumulators instead of merkle trees and conducting comprehensive simulations with comparative analyses to obtain quantifiable metrics to support this claim.

As stated in the F.1 Lemma of Aleph, implementing RSA accumulators to replace merkle trees in the RBC protocol can significantly improve scalability. The reason being that RSA accumulators provide a cryptographic method for aggregating multiple values into a single, fixed-size accumulator (Reddy, 2021). Research has also supported that RSA accumulators allow for more efficient verification and communication processes in blockchain networks compared to the logarithmic and quadratic complexity of merkle trees (Hussein & Al-Gailani, 2022). This is important because RSA accumulators offer efficient aggregation of multiple values into fixed-size accumulators, allowing the protocol to achieve more streamlined verification and communication processes.

The simulations and comparative analyses will involve replicating similar development environments and benchmarking methodologies used in previous asynchronous consensus research like HBFT, BEAT, DUMBO, and the Asynchronous Byzantine Fault Tolerance (ABFT) protocols to ensure consistent and reliable performance data (Miller et al., 2016, Knudsen et al., 2021, Duan et al., 2018, and Guo, Lu, Tang, Xu, & Zhang, 2020).

The goal will be to obtain quantifiable metrics to support the claim of a reduction in communication complexity of Aleph by reducing the computational and communication overhead of the ch-RBC with RSA accumulators. Thereby improving the overall scalability and communication complexity of the Aleph protocol.

Current Level of Completion:

Currently in the research proposal stage.

Milestones and Deliverables: The project will progress through the following milestones and deliverables:

* Problem identification and definition
* Concrete problem direction, need, and goal
* Literature review completion
* Experimental setup exploration and validation
* Quantitative assessment and performance analysis

Current Accomplishments:

* Initiated literature review and identified key problems within Asynchronous Consensus.

Scheduled Completions:

* Literature review completion by [Q4 2023]
* Finalization of concrete problem direction, need, and goal by [Q1 2024]
* Proposal of Idea Concept Paper [Q2 2024]
* Formal Idea Concept Paper [Q3 2024]
* Aleph setup exploration and validation by [Q4 2024]
* Aleph RSA accumulator setup exploration and validation by [Q2 2025]
* Quantitative assessment and performance analysis by [Q32025]
* Dissertation [Q4 2025]

Missed Targets: There are currently no missed targets as the project is still in its early stages.

Issues and Changes

Open Issues:

None at this time.

Open Change Requests:

None at this time.

Next Phase Schedule (Start and Completion Targets):

Finalization of concrete problem direction, need, and goal by [Q1 2024]

* Start Date: [January 2024]
* Completion Target: [April 2024]

Summary: The summary of this research is on enhancing the field of asynchronous permissionless systems by improving the Aleph protocol using RSA accumulators. The research will replicate the Aleph protocol and the integrate RSA accumulators into it a replacement for the existing Merkle Tree-based Reliable Broadcast Communications (RBC), aiming to reduce communication complexity, decrease network latency, and improve overall protocol performance. By establishing a robust baseline and comparing it with new research incorporating RSA accumulators, this research seeks to make significant contributions to the field of asynchronous permissionless systems and enhance the scalability and efficiency of the Aleph protocol.

**References**

Abraham, I., Jovanovic, P., Maller, M., Meiklejohn, S., Stern, G., & Tomescu, A. (2021). Reaching consensus for asynchronous distributed key generation. In *Proceedings of the 2021 ACM Symposium on Principles of Distributed Computing* (pp. 363–373).

Baird, L., & Luykx, A. (2020). The Hashgraph Protocol: Efficient Asynchronous BFT for High-Throughput Distributed Ledgers. *International Conference on Omni-layer Intelligent Systems* (pp. 1-7).<https://doi.org/10.1109/COINS49042.2020.9191430>

Boldyreva, A. (2002). Threshold signatures, multisignatures and blind signatures based on the gap-diffie-hellman-group signature scheme. In *Public key cryptography–PKC 2003* (pp. 31–46). Springer.

Das, S., Xiang, Z., & Ren, L. (2020). Asynchronous data dissemination and its applications. In *Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security*.

Djari, A., Anceaume, E., & Tucci-Piergiovanni, S. (2022). An extensive agent-based simulation study of sycomore++, a DAG-based permissionless ledger. In *Proceedings of the 37th ACM/SIGAPP Symposium on Applied Computing* (pp. 334–336). Association for Computing Machinery.<https://doi-org.ezproxylocal.library.nova.edu/10.1145/3477314.3507245>

Duan, S., Reiter, M., & Zhang, H. (2018). Beat: Asynchronous BFT Made Practical. In *ACM SIGSAC Conference on Computer and Communications Security* (pp. 2028–2041).<https://doi.org/10.1145/3243734.3243812>

Fischer, M. J., Lynch, N. A., & Paterson, M. S. (1982). Impossibility of distributed consensus with one faulty process (Technical Report No. MIT/LCS/TR-728). Massachusetts Institute of Technology, Laboratory for Computer Science, Cambridge.

Gągol, A., Leśniak, D., Straszak, D., & Świętek, M. (2019). Aleph: Efficient atomic broadcast in asynchronous networks with Byzantine nodes. In *Proceedings of the 1st ACM Conference on Advances in Financial Technologies (AFT '19)* (pp. 214–228). Association for Computing Machinery.<https://doi.org/10.1145/3318041.3355467>

Gao, Y., Lu, Y., Lu, Z., Tang, Q., Xu, J., & Zhang, Z. (2022). Dumbo-NG: Fast Asynchronous BFT Consensus with Throughput-Oblivious Latency. In *Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security (CCS '22)* (p. 1187–1201). Association for Computing Machinery.<https://doi.org/10.1145/3548606.3559379>

[Gencer, A. E., Basu, S., Eyal, I., van Renesse, R., & Sirer, E. G. (2018). Decentralization in Bitcoin and Ethereum Networks. In *Proceedings of the 22nd International Conference on Financial Cryptography and Data Security* (pp. 439-457). Springer. https://doi.org/10.1007/978-3-662-58387-6\_25](https://doi.org/10.1007/978-3-662-58387-6_25)

Gennaro, R., Jarecki, S., Krawczyk, H., & Rabin, T. (2003). Secure Applications of Pedersen’s Distributed Key Generation Protocol. In *Topics in Cryptology - CT-RSA 2003, The Cryptographers’ Track at the RSA Conference 2003, San Francisco, CA, USA, April 13-17, 2003, Proceedings* (pp. 373–390).<https://doi.org/10.1007/3-540-36563-X_26>

Gennaro, R., Jarecki, S., Krawczyk, H., & Rabin, T. (2007). Secure Distributed Key Generation for Discrete-Log Based Cryptosystems. *Journal of Cryptology, 20*(1), 51–83.<https://doi.org/10.1007/s00145-006-0347-3>

Guo, B., Lu, Z., Tang, Q., Xu, J., & Zhang, Z. (2020). Dumbo: Faster Asynchronous BFT Protocols. In *Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security (CCS '20)* (pp. 803–818). Association for Computing Machinery.<https://doi.org/10.1145/3372297.3417262>

Guo, B., Lu, Y., Lu, Z., Tang, Q., Xu, J., & Zhang, Z. (2022). Speeding Dumbo: Pushing Asynchronous BFT Closer to Practice. doi:10.14722/ndss.2022.24385

Hood, K., Oglio, J., Nesterenko, M., & Sharma, G. (2021). Partitionable Asynchronous Cryptocurrency Blockchain. *IEEE International Conference on Blockchain and Cryptocurrency* (pp. 1-9).<https://doi.org/10.1109/ICBC51069.2021.9461080>

Hussein, K. M., & Al-Gailani, M. F. (2022). An Efficient Bandwidth Based on the Cryptographic Technique of the RSA Accumulator in Block Chain Networks. In 2022 Fifth College of Science International Conference of Recent Trends in Information Technology (CSCTIT) (pp. 164-168). Baghdad, Iraq. doi:10.1109/CSCTIT56299.2022.10145614

Kharangate, A. (2023). Asynchronous merkle trees. arXiv. https://ar5iv.labs.arxiv.org/html/2311.17441

Kogias, E. K., Malkhi, D., & Spiegelman, A. (2020). Asynchronous Distributed Key Generation for Computationally-Secure Randomness, Consensus, and Threshold Signatures. In *Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security (CCS '20)* (pp. 1751–1767). Association for Computing Machinery.<https://doi.org/10.1145/3372297.3423364>

Knudsen, H., Li, J., Notland, J., Haro, P., & Ræder, T. (2021). High-Performance Asynchronous Byzantine Fault Tolerance Consensus Protocol. *IEEE International Conference on Blockchain* (pp. 476-483).<https://doi.org/10.1109/Blockchain53845.2021.00073>

Lauinger, J., Ernstberger, J., Regnath, E., Hamad, M., & Steinhorst, S. (2021). A-PoA: Anonymous Proof of Authorization for Decentralized Identity Management. In *2021 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)* (pp. 1-9). Sydney, Australia. doi:10.1109/ICBC51069.2021.9461082.

Miller, A., Xia, Y., Croman, K., Shi, E., & Song, D. (2016). The Honey Badger of BFT Protocols. *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security* (pp. 31–42).<https://doi.org/10.1145/2976749.2978399>

Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. Retrieved from https://bitcoin.org/bitcoin.pdf

Ramakrishna Kotla, Lorenzo Alvisi, Michael Dahlin, Allen Clement, and Edmund L. Wong. (2009). Zyzzyva: Speculative Byzantine fault tolerance. *ACM Transactions on Computer Systems (TOCS), 27*(4), 7:1–7:39.<https://doi.org/10.1145/1658357.1658358>

Reddy, B. S. (2021). securePrune: Secure block pruning in UTXO based blockchains using Accumulators. In *2021 International Conference on COMmunication Systems & NETworkS (COMSNETS)* (pp. 174-178). Bangalore, India. doi:10.1109/COMSNETS51098.2021.9352892.

Silva, P., Matos, M., & Barreto, J. (2023). NimbleChain: Speeding up Cryptocurrencies in General-purpose Permissionless Blockchains. *Distributed Ledger Technology, 2*(1), Article 8.<https://doi-org.ezproxylocal.library.nova.edu/10.1145/3573895>

Woznica, A., & Kedziora, M. (2022). Performance and scalability evaluation of a permissioned Blockchain based on the Hyperledger Fabric, Sawtooth and Iroha. *Comput. Sci. Inf. Syst., 19*, 659-678.

Zhou, Q., Huang, H., Zheng, Z., & Bian, J. (2020). Solutions to Scalability of Blockchain: A Survey. *IEEE Access*. Advance online publication.<https://doi.org/10.1109/ACCESS.2020.2967218>