**Decentralized Secure Collaborations (DeSC): Litepaper**

**Zubayr Khalid & Co.**

**Abstract: *This paper introduces the DeSC (Decentralized Secure Collaboration) framework, designed to manage decentralized collaborations through smart contracts. The system enables initiators to secure investments via the Investor Smart Contract, which utilizes multi-signature wallets for fund management. Collaborations are formalized through the Initiator and Acceptor Smart Contracts. The framework's core concept is atomicity, breaking collaborations into discrete levels reviewed by randomly selected moderators. These moderators vote on the collaboration's progress and may initiate a Motion for No Confidence (MNC) if issues arise, impacting their Soulbound Token (SBT) credits. Privacy is ensured through encrypted off-chain communication, combining decentralization, security, and scalability to manage complex collaborations and minimize risks.***

**INTRODUCTION:**

Decentralized Secure Collaboration (DeSC) is an application designed to facilitate secure collaborations between untrusted parties, going beyond the traditional asset-transfer model found in escrow services. It addresses various scenarios where verification of task completion or agreement is essential:

a) **Freelancing Services**: An example is a freelance web designer hired by a coffee shop. Here, the focus is on verifying the completion of the task rather than asset transfer.

b) **Contract-Based Jobs**: Companies may hire employees for specific tasks where it’s necessary to verify both job completion and payment fulfillment.

c) **Influencer Marketing**: Companies collaborating with social media influencers can use DeSC to ensure transparency and prevent scams, especially prevalent in crypto marketing.

d) **Crowdfunding**: DeSC can verify progress at different stages of a crowdfunding campaign by dividing it into atomic levels, enabling adjustments in target goals based on project development and market conditions.

This platform ensures collaboration integrity across diverse use cases.

Definitions:

Since DeSC is more than import-export trading, we can't rely on the concepts of ‘buyer’ and ‘seller’. So in this subsection, we will redefine our entities and we will use these names for the rest of the paper.

a) **Initiator**: Instead of a buyer we have an initiator. An initiator is an entity that initiates a collaboration.

b) **Acceptor**: Instead of a seller we have an acceptor. An acceptor is an entity that accepts the collaboration request from an initiator.

c) **Moderator Universe**: It is the set of all the moderators available in DeSC.

d) **Moderator Set**: It is the set that will monitor a particular collaboration. The moderator set is a subset of the moderator universe.

e) **Investor Set**: The investor set includes entities that can provide grants to the initiator for a collaboration.

f) **Collaboration**: It is the whole campaign between the initiator and the acceptor.

g) **Atomicity**: It is the property of dividing a collaboration into atomic levels.

In DeSC, the initiator starts a collaboration and, if needed, interacts with the **Investor smart contract** to arrange deals with investors. If no investment is necessary, the initiator moves forward by calling the **Collaboration smart contract**. Once the acceptor joins, both parties divide the collaboration into atomic stages and assign a **Moderator set** for each, using the **Moderator smart contract**. These stages ensure that each part of the collaboration is verified independently, or the entire collaboration can be managed by a single moderator set.

Atomic stages are verified by their assigned moderator sets before moving to the next, and moderators participate automatically without waiting for a dispute call. Each moderator set is only aware of its specific stage, ensuring privacy. Identities of the parties and moderators are kept hidden unless voluntarily revealed using zero-knowledge proofs.

The whole DeSC workflow can be categorised into these sections:  
a) Entity Registration and Entity Rating using SBT (SoulBound Tokens)

b) Initiation and Acceptance of Collaboration

c) Investor Set and Investments (optional)

d) Moderator Universe, Moderator Set, providing Atomicity and Dispute Resolution

**DEFINITIONS:**

**a) Entity Registration and Entity Rating using SBT (SoulBound Tokens):**

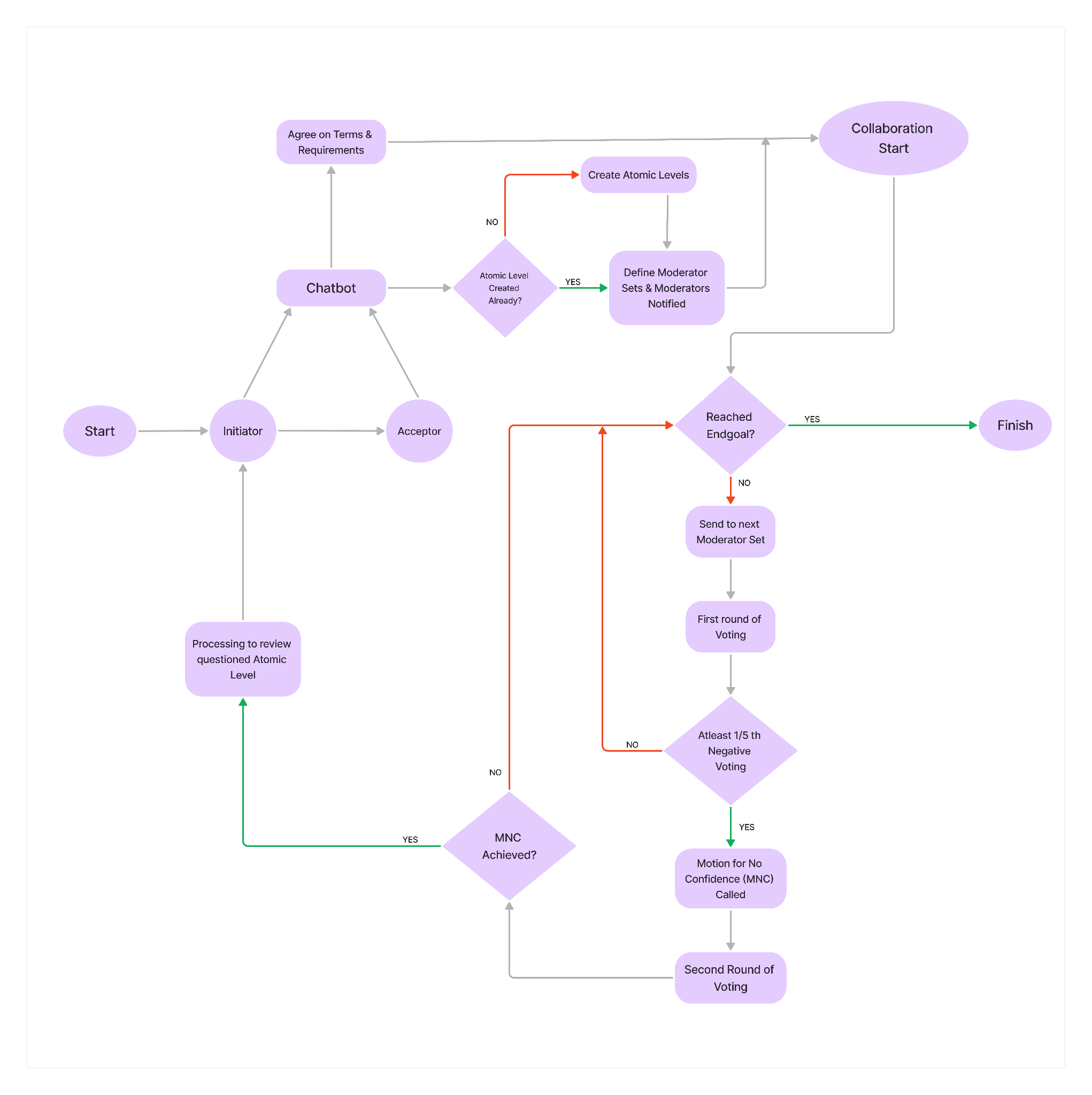
In DeSC, user registration involves generating a private key, public key, and user address using ECDSA[1] and SHA512 algorithms. The user’s public key is linked to their Soulbound Token (SBT) [2] rating, and identity verification in disputes is handled through Zero Knowledge Proofs (ZKP) [3], ensuring privacy. A smart contract called **SBTRegistry** stores and manages the SBT ratings, linking them to users' public keys. Collaborations are registered through the **CollaborationRegistry** contract, which validates ratings via digital signatures, using nonces to prevent replay attacks. ZKP enables users to prove ownership of their identity without revealing private keys.

**b) Initiation and Acceptance of Collaboration:**

Initiators can view potential Acceptors on a dashboard that showcases profiles with key details like public keys, SBT ratings, skillsets, project history, and availability. Initiators can filter and search for suitable collaborators, initiating off-chain communication via a centralized, end-to-end encrypted chatbot once an Acceptor shows interest. This chatbot caches and displays only relevant collaborations for users while ensuring privacy through encryption. Once a collaboration is accepted, the interaction is recorded on the blockchain. **Initiator** and **Acceptor** smart contracts manage the collaboration process, with the Initiator locking funds, and the Acceptor verifying details before initiating the project, ensuring trust and transparency.

**c) Investor Set and Investments (optional):**

Initiators without sufficient funds can secure investments through an Investor smart contract before initiating collaborations. The process involves off-chain communication with investors, securing investment deals, and creating multi-signature wallets between initiators and investors to manage funds securely. Once enough funds are pooled, the collaboration can proceed, with another multisig wallet [4] created between the initiator and acceptor. Funds are transferred and authenticated through these wallets, ensuring security, transparency, and fraud prevention, with dispute resolution mechanisms in place if needed.

****

**d) Moderator Universe, Moderator Set, providing Atomicity and Dispute Resolution:**

In DeSC, moderators [5] are selected randomly from the Moderator Universe to form a Moderator Set for each collaboration. The initiator and acceptor determine the size of this set, balancing decentralization, cost, and privacy considerations. Moderators are notified through a dashboard or email, and custom invites can be sent to specific moderators if needed.

During the voting [6] phase, moderators cast Positive Votes if there are no conflicts. If conflicts arise, moderators can cast Negative Votes, and if atleast a minimum number of the moderators vote negatively, a **Motion for No Confidence (MNC)** is triggered. The system uses the MNC to escalate serious issues, ensuring thorough and fair conflict resolution. Moderators receive rewards based on their alignment with the majority, promoting careful and honest participation.

**CONCLUSION:**

The Decentralized Secure Collaboration (DeSC) framework utilizes blockchain technology to enhance transparency, security, and accountability in collaborative projects. It employs smart contracts for managing interactions and agreements, and supports a robust investment mechanism where initiators secure funding from investors before engaging with acceptors. The system features multi-signature wallets for secure fund management and dynamic moderator sets for overseeing each atomic level of collaboration. This setup ensures trust through an immutable ledger, while also protecting privacy and enabling efficient dispute resolution. The modular design and flexible moderation process contribute to a streamlined and secure collaboration experience.

**REFERENCES:**

1. **Huang, L., et al.** (2018). *"A Survey on Blockchain Security and Privacy"*  
2. **Ohlhaver, P., Weyl, E. G., Buterin, V.** (2022). *“Decentralized Society: Finding Web3’s Soul”*

3. **Ben-Sasson, E., et al.** (2014). *"Zerocash: Decentralized Anonymous Payments from Bitcoin"*

4. **K. Atallah, M. Blanton, and E. O. K. Wang** (2002). *"Secure Multi-Party Computation: An Overview"*

5. **S. R. Lichtenstein** (2016). **"***Decentralized Autonomous Organizations and Their Impact on Governance and Collaboration***"**

6. **N. Atzei, M. Bartoletti, and T. Cimino** (2017). **"***Blockchain-Based Voting Systems: A Survey***"**