Tangram: A Peer-to-Peer Electronic Cash System

Matthew Hellyer

1 March 2025

Abstract

Tangram is a novel dynamic *Pure Proof-of-Stake (PPoS)* blockchain protocol that achieves high-efficiency, decentralized agreement on transactions. By employing *Verifiable Random Functions (VRFs)* to select block proposers and voting committees, Tangram ensures fair participation while reducing network congestion and energy consumption. A multi-phase voting system supports rapid finality and prevents forks, while advanced privacy-preserving technologies—namely *MLSAG, RingCT, Bulletproofs, and Dandelion++*—enhance both confidentiality and Sybil resistance. A dedicated *relay participant* mechanism fortifies network liveness under adverse conditions. This paper provides an in-depth exploration of Tangram's consensus mechanism, privacy features, security model, and its improvements over existing protocols, including Algorand and Ethereum 2.0.

1 Introduction

1.1 Motivation

Blockchain technology has revolutionized data and value transfer by enabling decentralized, trust-minimized systems. Yet, widespread adoption still faces major hurdles. *Proof-of-Work (PoW)* systems, while foundational, consume excessive energy and often yield slow transaction finality. Traditional *Proof-of-Stake (PoS)* frameworks can suffer from centralization risks, long-range attacks, and liveness issues, especially if participation drops below required thresholds.

Tangram addresses these challenges through a dynamic **Pure Proof-of-Stake (PPoS)** approach that balances efficiency, security, and decentralization. The protocol is built on several key innovations:

- *VRF-Driven Committee Selection:* Uses a transparent and tamper-resistant VRF to randomly select block proposers and committees, limiting collusion and centralization.
- *Multi-Phase Voting:* Accelerates finality while mitigating forks through distinct phases of block approval.

- *Relay Participant System:* Guarantees continuous block production even if the proposer-selection process stalls or fails.
- *Privacy-Preserving Tools:* Integrates *MLSAG, RingCT, Bulletproofs, and Dandelion++* to enhance transaction confidentiality and inhibit Sybil attacks.

By solving critical inefficiencies in existing protocols, Tangram aspires to offer a **scalable, resilient, and privacy-centric** network with short finalization times and robust decentralization guarantees.

2 Key Components of Tangram Consensus

2.1 Verifiable Random Function (VRF) Selection

Tangram employs **Verifiable Random Functions (VRFs)** to provide an unbiased, unpredictable, and private method of selecting both proposers and voting committees. VRFs generate a pseudorandom output along with a proof that any observer can verify, ensuring honest randomness without revealing the private key.

1. *Setup:* Let $\mathcal{G}$ be a cyclic group of prime order q with generator g. Each participant i possesses a key pair (sk_i, pk_i), with $pk_i = g^{sk_i}$.
2. *Evaluation:* In round r, the seed Q_r feeds into the VRF:

   $$\beta = H(Q_r)^{sk_i},$$

   where $H(\cdot)$ is a cryptographic hash function (mapping into $\mathcal{G}$). The signer also produces a zero-knowledge proof π showing that β was computed correctly.
3. *Verification:* Any node can verify β using the proof π and the public key pk_i. The verification confirms that β was derived from sk_i without revealing sk_i.
4. *Threshold Check:* A stake-based threshold T_s determines selection:

   $$\beta < T_s \quad \Longrightarrow \quad \text{Participant } i \text{ is selected as proposer or committee member.}$$

   Participants with higher stakes have greater probability of meeting the threshold, aligning economic incentives with network security.

2.2 Multi-Phase Voting Process

Tangram's multi-phase voting process minimizes fork risk and delivers fast block finality:

- **Phase 1: Block Proposal** A single proposer (selected via VRF) broadcasts a candidate block to the network.
- **Phase 2: Soft Vote** A randomly chosen committee checks the block's validity (transaction correctness, signatures, etc.). Each committee member issues a "soft vote" either approving or rejecting the block.

- **Phase 3: Certify Vote** A different committee (also VRF-selected) finalizes the block. If a supermajority of soft votes is detected, committee members broadcast a certify vote in favor of including the block in the chain.
- **Phase 4: Binary Agreement (Fallback)** If a block fails to achieve supermajority approval, Tangram invokes *Binary Byzantine Agreement (BBA)*. The BBA ensures that all honest nodes converge on a single, globally accepted chain—resolving any potential conflicts.

2.3 Byzantine Binary Agreement (BBA) Protocol

Tangram uses BBA to ensure consensus finality even in the presence of adversarial conditions. This process prevents deadlock by using a stepwise approach where nodes attempt to reach agreement on a binary decision. If a supermajority consensus is not reached, the protocol ensures eventual agreement through a **common coin flip** mechanism. This guarantees that even if an adversary disrupts consensus rounds, honest participants will still converge on the same decision over multiple iterations. The protocol operates in three steps:

1. *Common Input:* Each node starts with a bit $b_i \in \{0, 1\}$, indicating support (1) or rejection (0) of a given block.
2. *Coin-Fixed-to-0 (Step 1):* If at least $2t + 1$ participants (where t is the maximum tolerated number of Byzantine nodes) vote 0, the network finalizes 0.
3. *Coin-Fixed-to-1 (Step 2):* Similarly, if at least $2t + 1$ participants vote 1, the network finalizes 1.
4. *Common Coin Flip (Step 3):* If neither bit reaches the threshold, the protocol triggers a "common coin," computed from participants VRF outputs σ_r on the current round r:

   $$c_i = H(\sigma_r) \mod 2.$$

   This shared randomness forces a decisive outcome in subsequent rounds, countering adversarial attempts to stall finalization.

3 Sybil Resistance and Privacy Enhancements

3.1 Sybil Resistance and Stake-Based Selection

By weighting committee selection by stake, Tangram raises the economic cost of Sybil attacks. Splitting a stake across multiple identities offers no net advantage, as the selection probability remains proportional to the total stake held.

3.2 Privacy-Preserving Transaction Propagation (Dandelion++)

Tangram leverages **Dandelion++** to obfuscate transaction origins:

- *Stem Phase:* A transaction initially travels along a small set of nodes before public dissemination.
- *Fluff Phase:* After the stem phase, the transaction is "fluffed" to the entire network, making it extremely difficult to pinpoint the original sender.

3.3 MLSAG, RingCT, and Bulletproofs

Tangram extends transaction privacy by combining **Multi-Layered Linkable Spontaneous Anonymous Group (MLSAG) signatures**, **Ring Confidential Transactions (RingCT)**, and **Bulletproofs**. These techniques work together to preserve input/output anonymity, conceal transaction amounts, and ensure correct balances—all without leaking sensitive information on-chain.

3.3.1 MLSAG Signatures

MLSAG signatures allow the signer to prove ownership of exactly one public key within a ring of n public keys, without revealing which key is actually theirs.

- *Setup:* A ring of public keys $\{P_1, P_2, \ldots, P_n\}$ is formed. The real signer controls one secret key x corresponding to one P_i.
- *Challenge-Response Construction:* The signer picks random scalars $\alpha_1, \ldots, \alpha_n$ and computes intermediate values that obfuscate which key is associated with the secret key. A cyclic chain of challenges $\{c_i\}$ and responses $\{r_i\}$ ensures only one key in the ring corresponds to the real signature.
- *Linkability & Verification:* A *Key Image* ($\text{KeyImage} = x \cdot H(P_i)$) links multiple uses of the same secret key without identifying which public key is being used. Verifiers confirm the signature is valid for exactly one key in the ring but cannot determine which key it is.

3.3.2 Ring Confidential Transactions (RingCT)

RingCT conceals transaction **amounts**:

- *Pedersen Commitments:* Outputs are recorded as commitments $C = rG + vH$, where v is the amount and r is a random blinding factor. Pedersen commitments allow public verification that transactions balance without revealing actual amounts.
- *Ring Structure:* Input addresses are masked by mixing the real input with decoy inputs in a ring, reinforcing anonymity.
- *Zero-Knowledge Proof of Balance:* The spender shows (in zero knowledge) that total input equals total output plus fees, preserving confidentiality of the amounts.

3.3.3 Bulletproofs

Bulletproofs are short, non-interactive zero-knowledge proofs that confirm an amount lies within a valid range (e.g., 0 to $2^{64} - 1$) without revealing the actual value.

- *Range Commitment:* A Pedersen commitment C is proved to represent a value v within a known range using a Bulletproof.
- *Inner-Product Argument:* Bulletproofs leverage an inner-product argument to show each bit of v is either 0 or 1, all in zero knowledge.
- *Efficiency:* Bulletproofs require only a few hundred bytes per proof, substantially smaller than older range proofs, minimizing on-chain overhead.

3.4 Dual-Key Stealth Address Protocol

Tangram implements dual-key stealth addresses to protect both sender and receiver privacy. Each transaction is directed to a unique one-time address, preventing address reuse and thwarting attempts to link on-chain addresses to specific identities.

1. *Key Pairs:* Each user maintains a *view key pair* (v, V) and a *spend key pair* (s, S), where $V = vG$ and $S = sG$.
2. *Stealth Address Generation:* The sender picks a random scalar $r \in \mathbb{Z}_q$ and computes $R = rG$. The one-time destination is

   $$P = H(rV)G + S.$$

   This stealth address P is included in the transaction.
3. *Detection and Recovery:* Using v, the receiver computes $t = H(v \cdot R)$ to recover the private key $x = t + s$. Since $xG = P$, the receiver can spend funds at P without revealing their standard address.
4. *Privacy Benefits:* Each on-chain transaction uses a unique address, making it difficult to correlate transactions to the same user. Observers cannot easily determine which addresses link to a given recipient, greatly enhancing privacy.

4 Security Model: Potential Attacks and Mitigations

4.1 Sybil Attacks

Risk: Creating numerous fake identities to boost the odds of proposer/committee selection. **Mitigation:** Tangram's VRF-based selection is proportional to stake, making such attacks economically unprofitable.

4.2 Long-Range Attacks

Risk: A compromised private key might enable rewriting historic blocks if future changes to stake distributions are ignored.
Mitigation: Frequent checkpoints and consistent voting reduce the practicality of long-range attacks. Tangram also encourages continuous participation, limiting stale private keys.

4.3 Nothing-at-Stake Problem

Risk: Validators could sign multiple chains in parallel, hoping at least one yields a reward.
Mitigation: Slashing penalties and VRF-based unpredictability discourage any attempt to stake on conflicting chains.

4.4 Network Partitioning Attacks

Risk: Adversaries might isolate nodes or subnetworks, causing consensus failure.
Mitigation: The multi-phase voting structure and BBA fallback ensure agreement even under partial partitions. The relay mechanism also helps maintain liveness under adverse conditions.

4.5 Front-Running and Censorship

Risk: Malicious network participants might censor or reorder transactions for personal gain.
Mitigation: Dandelion++ hides a transaction's origin, reducing the ability to target specific senders. Moreover, the random selection of committees complicates sustained censorship.

5 Comparison with Existing Consensus Protocols

Comparison with Existing Protocols. Tangram Consensus improves upon existing PoS-based consensus mechanisms such as Algorand, Ethereum 2.0, and Cardano by integrating **MLSAG and Dandelion++ for privacy**, increasing **Sybil resistance with sortition weighted thresholds**, and enhancing **finality through multi-phase voting**. Unlike Ethereum 2.0, which relies on a complex Casper-based finality mechanism with potential reorg risks, Tangram ensures strong fork resistance through a **verifiable VRF-based selection process**. By using a multi-phase voting system and binary Byzantine agreement, Tangram minimizes forks while maintaining efficiency and decentralization. Additionally, its integration of **relay participants for liveness** helps sustain the blockchain's continuity even in adverse network conditions.

Tangram also improves upon Algorand by integrating **MLSAG and Dandelion++ for privacy**, increasing Sybil resistance using **sortition weighted thresholds**, and enhancing finality through **multi-phase voting**.

6 Future Work

Tangram's roadmap aims to further strengthen its privacy, scalability, and programmability:

- **CLASG Integration (Compact Linkable Anonymous Spontaneous Group Signatures):** Enhance privacy through more concise proof sizes and faster verification times.
- **Smart Contracts:** Introduce on-chain programmability to enable trustless, self-executing applications and DeFi-like features.
- **Relay Participant Incentives:** Refine incentives to ensure a robust relay system for block propagation, even under severe network stress.

7 References

- Ben-Sasson, E., Bentov, I., Horesh, Y., & Riabzev, M. (2018). *Scalable Transparent ARgument of Knowledge (STARKs).*
- Goldberg, I., & Boneh, D. (2022). *Dandelion++: Privacy-Preserving Transaction Propagation.*
- Rivest, R. L., Shamir, A., & Tauman, Y. (2001). *How to Leak a Secret.*
- Boneh, D., Lynn, B., & Shacham, H. (2001). *Short Signatures from the Weil Pairing.*
- Micali, S. (2016). *Algorand: A Secure and Efficient Distributed Ledger.*
- Buterin, V. (2020). *Ethereum 2.0: Serenity Design and Implementation.*
- Koblitz, N., & Menezes, A. (2015). *Elliptic Curve Cryptography and Security.*
- Shen Noether. (2015). *Ring Signature Confidential Transactions for Monero.*

Closing Remarks: Tangram's unique synthesis of *VRF-driven committee selection*, *multi-phase voting*, *robust privacy mechanisms*, and a *relay participant* fallback protocol addresses critical challenges in blockchain technology. By ensuring both **efficiency** and **anonymity**—all while maintaining robust **decentralization**—Tangram stands as a viable next-generation blockchain solution for secure, private, and scalable peer-to-peer electronic cash transactions.