Outline of Business Models	Key Risks
Staking is the process by which participants of a blockchain network contribute to the Proof-of-Stake ("**PoS**") consensus mechanism. In PoS systems, network participants ("**Validators**") create and validate new blocks on the blockchain in return for block rewards and transaction fees ("**Rewards**") paid in the network's native tokens. Validators pledge or stake a certain amount of the network's native VA to the blockchain network. The probability of a Validator being chosen to create a new block often correlates with the amount of staked VAs, although many PoS systems have more complex selection algorithms that consider additional factors. Validator nodes in PoS systems allow other network participants ("**Delegators**") to contribute their VAs to the Validator's stake. When a Validator successfully creates and validates a new block of transactions, the Rewards are typically shared between the Validator and their Delegators, in proportion to each Delegator's contribution to the total stake. Where the Delegator individually is unable to raise the minimum stake to run a Validator node, it may seek to group its VAs with the contributions of other Delegators by participating in staking pools operated by third parties ("**Pool Operators**"). **Staking Models:** the FSRA understands that different staking models have emerged, including the following: (a) Solo staking: The participant, often called a 'Solo-Staker', directly operates the staking infrastructure and uses only its own resources (VAs and technical infrastructure) to meet the minimum requirements of the blockchain network. A Solo-Staker sets up and maintains their own Validator node using either local or cloud-based staking infrastructure. Once properly configured and identifiable onchain, this Validator node is where the Solo-Staker stakes its VAs. The participant retains direct control over their staked VAs at all times, as well as complete responsibility for the operation and security of their Validator node. (b) Staking-as-a-Service ("**SaaS**"): SaaS is an option for participants who want to operate as Validators but do not wish to maintain their own hardware and software. In this model, the participant employs a technology service provider to oversee the setup, operation and maintenance of the staking infrastructure. The participant uses its own VAs to meet the minimum assets requirements for the network. While maintaining direct control over its staked VAs, the participant relies on the SaaS provider to perform the technical aspects of Validator duties, such as node operation and software updates. This model allows for active participation in network validation while outsourcing the technical complexities. (c) Pooled staking: Pooled staking is a solution that allows multiple users to combine their VAs to meet the minimum staking requirements on a PoS blockchain network. This model enables participants who may not have enough assets to stake independently, or who prefer not to manage their own staking infrastructure, to participate in the network's consensus mechanism and earn Rewards. A staking Pool Operator is responsible	**Validator-related risks** (a) *Poor Validator performance*: The Rewards earned by stakers depend on the performance and reliability of the Validator they are delegating to. If the Validator experiences downtime, fails to validate transactions properly, or engages in malicious behaviour, it can negatively impact the stakers' Rewards. (b) *Slashing penalties*: Validators can be penalised / slashed for misbehaviour, such as being offline for an extended period, submitting contradictory attestations, or attempting to validate conflicting transactions (double-signing). (c) *Non-compliant block building*: Staking with Validators who process transactions linked to illicit finance or sanctioned entities poses compliance and reputational risks for Delegators. (d) *Validator software / hardware risks*: Validators rely on the proper functioning of their staking software and hardware. Bugs, misconfigurations, or hardware failures can result in missed Rewards or potential penalties. **Delegator-related risks** (a) *Smart contract risk*: Staking through smart contracts operated by staking pools introduces the risk of smart contract vulnerabilities or bugs. If the smart contract code contains errors or is exploited, stakers may lose their staked tokens or Rewards. (b) *Liquidity risk*: Staking involves locking up the staked VAs, which cannot be used until the Delegator choses to withdraw their tokens. Should the Delegator need to access their tokens during the lock-up period, they may be unable to do so or may face penalties for early withdrawal. If the price of the staked VAs falls sharply during the lock-up period, the Delegator will not be able to withdraw their investment. (c) *LST over issuance or under collateralization*: Liquid staking pools that issue more LSTs than they hold in VA staking deposits expose stakers to the risk of not being able to redeem their LSTs for the full value in VAs staked. LST over-issuance can lead to liquidity stress, declining LST value, and loss of confidence in the staking ecosystem.

Outline of Business Models	Key Risks
for setting up, operating, and maintaining the staking infrastructure. The Pool Operator collects the pooled VAs from users and manages the allocation of these resources across multiple Validators. This process involves deciding which Validators to deploy the pooled VAs to. The Pool Operator may choose to run the staking infrastructure in-house or outsource it to a SaaS provider. The Pool Operator is responsible for securely managing the pooled VAs and distributing the earned Rewards proportionally among the pool users based on their individual contributions. In this model, pool participants relinquish direct control of their staked VAs to the Pool Operator for the duration of the staking period. In a particular model of pooled staking known as liquid staking, when the participant contributes their VAs to a staking pool, they receive another token ("**Liquid Staking Token**" or "**LST**") in return. LSTs are fungible tokens, that represent a share of staked assets in a staking pool, and that allow a pool participant to maintain liquidity while still earning staking Rewards. To withdraw staked tokens and obtain the Rewards earned, the pool participant is required to provide the corresponding LSTs at the time of redemption. Because LSTs are fungible and can be traded, their value tracks the underlying staked tokens and Rewards earned. LSTs may be traded, used as collateral, or employed in various DeFi applications. (d) Centralised VA exchanges, dealing intermediaries or custodians: Centralised VA exchanges, dealing intermediaries or custodians ("**Centralised Intermediaries**") offer one of the most accessible options for participants who wish to earn Rewards passively but lack the knowledge or ability to do so independently. The Centralised Intermediary may take on the responsibility of setting up, operating, and maintaining the staking infrastructure, or delegate these tasks to a SaaS provider. The Rewards are paid out proportionately to clients based on their staked amounts. Similar to pooled staking, participants must transfer control of their assets to the Centralised Intermediary.	(d) *Loss of the Delegator address private key*: Losing or compromising the Delegator address private key can result in the permanent loss of staked assets and associated Rewards. **Network-level risks** (a) *Blockchain bugs or exploits*: Bugs or vulnerabilities at the network level can pose significant risks to the entire blockchain ecosystem. If a critical bug is discovered and exploited, it can lead to severe consequences, such as double-spending, loss of funds, or a complete network shutdown. (b) *Validator selection risks*: Stake grinding and Sybil attacks are examples of threats that target the Validator selection process. In such cases, other Validators on the network are disadvantaged by the actions of the malicious Validator, and the Rewards earned by bona fide Delegators are adversely impacted. (c) *Blockchain network takeover*: Instead of exploiting a bug on the blockchain network, or attacking the Validator selection, the attacker may attempt to gain control over the blockchain network, for example by using "long-range" attacks and / or "51%" attacks.