# SAAGE: DECENTRALIZED SPORTS BETTING PROTOCOL

Lightning Labs[a)]

(Dated: 18 June 2021)

We present Synthetic Asset and Gaming Exchange (Saage), a decentralized (and trustless) sports betting protocol powered by Saage token using Cosmos SDK. Saage's design enables bettors to place wagers on a given sporting event or participate as the book maker by receiving bets as a decentralized and autonomous house (DAO)[a] that pays or collects from bettors. Saage leverages the scaling capacity, blockchain interoperability and minimal gas fees of the Cosmos SDK infrastructure to provide a seamless and real-time wagering experience. Cosmos-based Proof of Stake consensus mechanism is used for the validation of the Saage network. Odds data from Saage-listed sporting events is onboarded on-chain using a customized Oracle, which is used for odds display and finality in bets settlement.

Keywords: Sports betting, Decentralized, DAO

## I. INTRODUCTION

The global sports betting market as reported in[?] is projected to grow by $ 130 billion during 2020-2024, projected at a 10% CAGR during the forecast period. It is a market that suffers from geographic isolation due to regulatory constraints, centralized operations that are inherently flawed, and lack of access and payment transparency. Yet, this market as an asset-class is unparalleled on a risk adjusted return on capital and diversification.

From a bettor's perspective, centralization within existing sports betting systems gives an unnecessary informational advantage to the system operators. These platforms require bettors to organize through a trusted third-party for settlement of the bets, with wait times of up to 2 weeks for settlement of those payments. These entities are compromised by their own business interests and goals, to the detriment of the bettor.

In particular, the need to trust a third-party authority (**house**) and the accumulation of power that follows, leads to: (a) Vulnerability to odds manipulation, non-payment, or delayed payment; (b) Exploitation of identity and betting pattern data collected from bettors; (c) Total and irrecoverable loss of funds due to assets being frozen.

For the first time in human history, users of sports betting platforms can act in whatever capacity they think will generate the best return. Users can themselves become the house, one that takes wagers and pays odds real time, based on a transparent and fair oracle, and is ultimately governed by the users themselves. Alternatively, bettors can act as traditional bettors, making wagers with Saage's Blockchain based betting, which provides trustless and instant finality in bets settlement, removing need for a trusted third-party.

We summarize our contributions below:

1. Saage enables the transfer of control over the sports betting industry from centralized entities to a community of users who value a fair, trustless and decentralized betting system. Saage eliminates the need for a centralized house by implementing a decentralized autonomous organization (DAO) to decide on the rules and the rewards of the protocol, which is implemented on-chain using Cosmos-SDK.
2. Saage's on-chain, automated code-driven model prevents any single point of authority from controlling the publishing of odds, settlement risks from a given outcome of events, or the payout from the result.
3. Saage token powers the Saage ecosystem by providing economic incentives to secure the network. Saage token:
   (a) is a settlement asset;
   (b) provides security for driving economic behavior;
   (c) enables governance on-chain;
   (d) and is a medium of exchange for the ecosystem.
4. Saage DAO is designed to be a two-layered fund with: (1) a *Staking pool* that is responsible for providing instant liquidity and finality to all bets; and (2) an *Insurance fund* that is responsible for paying-out all winning bets.[?] .
   (a) The DAO design transforms the traditional, centralized discretionary authority into a fully-automated, on-chain, decentralized, community-driven fund using an Oracle and a decentralized voting mechanism (DVM)[?] .
   (b) An Incentive Pendulum design is used by Saage DAO to allocate the assets and the rewards between the SP and the IF for all live bets on the platform. ,

[a)] In this paper we will refer to the Saage DAO as the bookmaker

(c) The DAO utilizes DVM for on-chain governance voting to reduce token supply from DAO when over capitalized through buy-back mechanism.

(d) Saage DAO will offer collateralized borrowing of Saage tokens leveraging Cosmos IBC to facilitate Saage adoption.

The rest of the paper is organized as follows. Section II explains the importance of the Saage token. Section III explains the design and implementation of the Saage DAO. Section IV explains the modular Saage architecture: (1) the Blockchain layer; (2) Communication layer; and (3) Applications layer; and how the interaction between the various layers are designed to drive value and utility of the Saage token.

## II. SAAGE TOKEN

Saage is the native token that secures and operates the Saage ecosystem. The Saage token release schedule is determined at genesis and published publicly Saage token generates utility and value in the following categories.

1. Saage token is the settlement and medium of exchange for the Saage ecosystem.
2. Saage token is the reward asset for Stakers and Bettors.
3. Saage token is used for validating the transactions associated with on-chain bet placement and voting needed by DVM.
4. Saage token is used to guarantee payouts by the Insurance Fund (IF).
5. Saage token is needed to participate in on-chain governance (voting on the staking parameters, voting using DVM, change in governance, deciding on fees and rewards in the system).

## III. SAAGE DAO

Saage DAO acts as a bookmaker for any Saage-listed sporting event guaranteeing payout to the betters. Staking pool (SP) in the DAO provides liquidity to the Saage betting system, while the Insurance Fund (IF) acts as the DAO's payout fund. Saage DAO's design enables 24x7 sports betting, guaranteeing full transparency in the settlement and the payment of bets of any size. Reserves in the DAO use an incentive pendulum for the optimal allocation of the assets as well as rewards between the SP and IF.

### III.A. Incentive Pendulum

The objective of the design is to prevent the protocol from becoming **inefficient**, (majority of assets in SP and not enough funds in the IF for payout to encourage bettors) or **unsafe** (majority of assets in the IF, increasing bankruptcy risk). The on-chain redistribution of the assets and the rewards between the SP and the IF is automated. The DAO receives inflation rewards and fees generated from betting activity, on-chain governance, odds listing, and on-chain data verification services. When a user bets on any Saage-listed sports event, the bet amount is locked in the IF. The IF is a reserve fund created and seeded at genesis in the DAO to guarantee winning payouts and profit from the bettors' losses.

| Scenario | SP Assets | IF Assets | Ξ | SP Rewards | IF Rewards |
|---|---|---|---|---|---|
| Optimal | 65% | 35% | 3 | 65% | 35% |
| Unsafe | 50% | 50% | - | 0 | 100% |
| Inefficient | 100% | 0 | 1 | 100% | 0 |

TABLE I Incentive Pendulum: Allocation of the capital between the SP and the IF.

At Genesis, the assets in the DAO are divided between the SP and the IF, where the IF is seeded at genesis, and the SP are contingent on user validation and delegation. The IF profit split generated through wagering is calculated as (Ξ) where $\Xi = \frac{SP+IF}{SP-IF}$ ; $SP =$ SP assets, $IF =$ IF assets. The DAO uses the inverse of the Ξ to distribute the funds between SP and IF. The incentive pendulum monitors the distribution of the assets and rewards between the SP and the IF to make Saage operate and allocate between the following states. Table(I) provides the split between SF and IF at genesis.

(a) **Optimal** This is the desired state, where SP has 65% of the assets and the IF has 35% of the assets. In such a situation, the system income is distributed as follows: 33% for the IF and 67% for the SP. (b) **Unsafe** The system may become unsafe where SP has 50% of the assets and the IF has 50% of the assets. In such a situation, the system income is distributed as follows: 100% for the IF and 0% for the SP. This is a scenario where the stakers have no incentive to validate the block-chain and the inflation rewards (C) can not be properly tied to restore the balance, returning the system to the optimal state.? .

The unsafe scenario needs to be explained in further detail to completely understand the design of the DAO; the balances of Saage in the Insurance Fund is a function of the betting activity and bankruptcy risk, explained in detail in III.B. At Genesis, IF will be initialized with a percentage of the Saage tokens. Saage tokens will be utilized to update the weighted capital allocation policy between the SP and IF periodically through on-chain governance (proposal and voting-based governance mechanism).

(c) **Inefficient** The system can also become inefficient, where SP has 100% of the assets and the IF has 0% of the assets. In such a situation, the system income is distributed as follows: 0% for the IF and 100% for the SP. This situation would result in payouts for adverse bet

settlements coming from balances in the SP. The expectation is that the Saage DAO would be performing such that capital and rewards will be re-allocated between SP and IF to pursue maximum yield, balancing the imbalance. The Saage incentive pendulum will help maintain the protocol at near-optimal states. Ultimately Saage stakers can vote to re-capitalize the Insurance Fund.

### III.B. Design of IF

The Insurance Fund monitors the odds of being bankrupt and provides liquidity to guarantee full payment to winning bettors in all scenarios. The IF is initialized with a certain amount of Saage tokens[?] equivalent to dollar amount: Saage is in optimal state: if the IF start with bankroll $\mathcal{W}_0$, and accepts bets which are a fixed fraction $f$ of $\mathcal{W}_0$ each time; with odds $d$ ¿ 0[?] , with winning probability $p$ at each bet and losing probability $q = 1 - p$. If $\mathcal{X}_1, X_2, \dots X_n$ be variables that indicate whether you win or lose in each of $n$ bets, where $X_i = 1$ if a win, 0 if a loss; for $i = 1, 2, \dots, n$. Using compounding at each trial, expected wealth for the IF would be $E[\mathcal{W}_n]$ after $n$ bets is

$$\begin{aligned} E[\mathcal{W}_n] &= \mathcal{W}_0 E\left[\prod_{i=1}^{i=n}(1+fd)^{X_i}(1-f)^{1-X_i}\right] \\ &= \mathcal{W}_0 E[\ (1+fd)^{\sum_i X_i}(1-f)^{n-\sum_i X_i}] \\ &= \mathcal{W}_0 \sum_{i=1}^{i=n}\binom{n}{k}(1+fd)^k(1-f)^{n-k}p^k(1-p)^{n-k} \\ &= \mathcal{W}_0((1+fd)p+(1-f)(1-p))^n \\ &= \mathcal{W}_0(1+(pd-q)f)^n, \end{aligned} \tag{1}$$

For the calculation we use binomial probabilities with $k$ successes in $n$ trials for sports betting related events. From (1), we conclude that the optimal betting fraction is $f = 1$ if $pd - q$ ¿ 0, or 0 otherwise. To calculate the growth rate $G_f$ of the IF for an i.i.d. $\pm 1$ sequence $X_i$ with $P[X_i = 1] = p$, we have to assume a generalized version of the wealth $\mathcal{W}$; for $d > 0$; the compounded value of your gains after $k$ bets, given initial wealth $\mathcal{W}_0$, is

$$\mathcal{W}(k; f, X) = \mathcal{W}_0(1+fd)^{\sum_{i=1}^{i=k} X_i}(1-f)^{k-\sum_{i=1}^{i=k} X_i}, \quad k \geq 1 \tag{2}$$

$$\begin{aligned} G_f &= \lim_{n\to\infty}\frac{1}{n}\log(\mathcal{W}(n; f, \mathcal{X})/\mathcal{W}_0) \\ &= \lim_{n\to\infty}\frac{1}{n}\log((1+fd)^{\sum_{i=1}^{i=n} X_i}(1-f)^{k-\sum_{i=1}^{i=n} X_i} \end{aligned} \tag{3}$$

Using the strong law of large numbers, it can be shown that (3) converges to $\log((1+fd)^p(1-f)^{1-p})$ and this expression is maximized for

$$f = \begin{cases} p - q/d, & p - q/d > 0, \\ 0, & p - q/d \leq 0. \end{cases} \tag{4}$$

For the IF, the best strategy which compounds the wealth is accept bets a fraction $f = p - q/d$ at each turn when $p - q/d$ ¿ 0 and $f = 0$ when $p - q/d \leq 0$. Anything greater than the critical fraction $f_c$ for the IF would make IF go broke. When faced with a betting situation in which the probability of winning at each turn varies with random probability $P$, then the optimal fraction is $f = p - q/d$ with $p = E[P]$ and $q = 1 - p$.

Besides monitoring the odds for betting on-chain, IF employs two threshold levels for balancing the reserve: **baseline cap (lower threshold)** and **max line cap (upper threshold)**. Baseline threshold occurs when IF is on a losing streak, with the bettors taking advantage of the excessive imbalance in the odds of the Saage-listed sporting events. During such events IF reserve is significantly reduced. The IF enters a protective mode, balances the decision-making ability of the on-chain analytics to stop accepting bets. The Insurance Fund will wait for the odds imbalance to improve and actively tries to off-load the one-sided risk it has accumulated. The system automatically adjusts the Profit and Loss distribution policy if the baseline threshold is met. This ensures that IF will guarantee winner payouts in the case of unfavorable events.

When IF reserve exceeds the max line cap, Saage on-chain governance[?] will be used to implement policies to permanently burn the excess amount from the reserve. Initially the parameters deciding the token buy-back schedule is given in Appendix (B).

### III.C. Blockchain Implementation

Saage DAO performs as a SP and as an IF. The SP is implemented as a separate module using Cosmos-sdk named DAO settlement and uses the account module for the settlement of the bets. The interaction of the SP modules with other modules on Cosmos-sdk is detailed below:

1. During bet placement, the blockchain bet storage module keeper interface *AppendBet* will invoke the DAO settlement and the keeper interface *TransferBetStake*. This invokes the call to the Cosmos SDK in build bank module *SendCoinsFromAccountToModule* to transfer the fund into the Dao account. To guarantee the payout to the winning bettors account *Payout* module invokes the Bank module *SendCoinsFromModuleToAccount*. Bet storage module processes the outcome in determining the winners and invokes the payout to the winner by calling Dao settlement module Payout function, which invokes the Cosmos SDK Bank module *SendCoinsFromModuleToAccount* interface. Bet storage module updates the state of the bet using encrypted data.
2. In Phase 1, the payout would happen without using the DVM voting, subsequently in Phase 2 the payout is invoked using DVM[?] Saage oracle[?] provides

the odds to determine the outcome of the betting event.

## IV. BLOCKCHAIN LAYER

### IV.A. Saage Betting Cycle

Betting on Saage is a sequential process from the creation of betting events to the payout. We outline the full decentralization and features deployment on Saage over three phases.

1. **Betting Event Creation** In Phase1, Saage will provide odds for sports events from all the reputed third-party betting providers using a customized Oracle solution. In Phase 2, Saage token holders will be allowed to become additional providers of odds for Saage-listed sports events. In Phase 3; only odds provided by Saage token holders would be allowed for Saage listed sports events to celebrate full de-centralization and fairness in the settlement of the bets.
2. **Bet Placement** All bets are recorded on-chain in Saage, where users can place bets on listed sports events.
3. **Event Completion** Saage will fetch the event completion information from third-party providers. In Phase 2, Saage token holders can validate event completion data, progressively leading to decentralization.
4. **Data Verification Mechanism**[?] In Phase 1, winners on the Saage platform would be paid instantly, since all betting outcomes would be based on pre-match odds provided at the start of the event. In Phase 2 and 3, Saage users will get to vote to on the settlement of the outcome of the events based on voting using DVM. The voting would be based on the amount of Saage tokens and be recorded on the Saage blockchain and provide the finality regardless who the counterparties are.
5. **Bet Settlement** In Phase 1, the bet settlement would be instant due to the binary nature of the sports events listed on Saage and winners will receive their payout amount. In Phases 2-3 for complicated outcomes, the settlement of the outcome will be decided based on voting using the DVM. Saage will do the bet settlement for the betters who participated in the betting event.
6. **Betting State Management** Saage has implemented the **bet storage module** to maintain bet states and to handle bets placed by users using the cosmos sdk module.

### IV.B. How bet placement works?

Saage users can use a mobile app or the desktop version to place a bet on listed sports events.

1. The application will fetch the user's private key from the Saage in-app secure wallet (IV.D.1), sign the user's bet selection with the private key, then broadcast the transaction to the Saage node bet storage transaction endpoint[?] .
2. When the signed transaction arrives at the bet storage transaction endpoint, it will relay the message to the bet storage handlers for managing the creation of a bet object in this module.
3. The state of the bet objects is maintained in the **bet storage module** in the keeper persistent key valet store.
4. Bet storage keeper interface *AppendBet* will process this bet placement transaction message of bet placement and the key valet store will be fetched and updated by the other custom module to maintain the bet objects' state machine.
5. Saage node"s tendermint end point will receive the message, and then it will enter the consensus mechanism among other operating nodes. Once the consensus is done and the transaction is finalized, it will be delivered to the receiving node application blockchain interface (tendermint ABCI). ABCI will deliver the message to its destination bet storage module handler. This handler will verify the type of the message, and if it comes to know that it is bet message, it will call the bet storage keeper interface function *AppendBet* to create a new bet object with the relevant input parameters like the bet amount, *oddID*, the user's public address, and a unique bet id. It will then store the bet on-chain in an encrypted format. The state of each individual bet is maintained on-chain. To lock the betting amount of the placed bet, *betstorage* invoke the bet amount locking function *TransferBetStake*, which transfers the Saage tokens from bettors to the DAO.

### IV.C. Communication Layer

The communication layer interfaces between the front and back end of the Saage. This layer converts and formats the odds data from Saage-listed sports events to the app and brings it on-chain. In Phase 1, Saage will list sports events with binary outcomes, so the settlement of bets would be instant. In subsequent phases, Saage will use the DVM, a community-driven, manual voting mechanism to decide on the settlement of the outcomes for the listed sports events.

### IV.D. Application Layer

Saage front end is designed to be available on iOS, Android, and desktops. The front end comes with a secure in-build wallet that supports most of the coins in the Cosmos ecosystem. The Saage application will display the upcoming sports events and the odds associated

TABLE II This is a wide table that spans the page width in `twocolumn` mode. It is formatted using the `table*` environment. It also demonstrates the use of `\multicolumn` in rows with entries that span more than one column.

| Saage | Design & Functions |
|---|---|
| Token | Settlement — Security — Governance — Medium of Exchange |
| DAO | 2-layered Fund — Incentive pendulum for rewards and asset distribution (SF + IF) |
| DVM | Voting for Governance using Saage Token |
| CDP | Lending of Saage tokens for live bets height |

with them. Saage will display a sufficient range of betting odds from reputed odds providers, stakers, and internal, analytic community-driven models for managing Saage DAO risk.

#### IV.D.1. Saage Secure Wallet

Saage has a native non-custodial wallet built using Hierarchical Deterministic wallet concept, which supports secure account creation and login functionality. Saage wallet users can check their balance, send, and withdraw Saage tokens when connected to the Saage wallet. Saage wallet is designed to make sure the mnemonics will be generated and stored in the user's device. Saage user's keys will be stored in the user device's browser extension or app cache. Saage wallet users can sign the transaction before sending it to the Saage blockchain.

## V. CONCLUSION

Saage's enables bettors to use Saage token to place wagers on a given sporting event or participate as the book maker by receiving bets as a DAO using Cosmos SDK. Table (III) lists the contributions and the innovation of a decentralized community run sports betting protocol.

## Appendix A: Appendixes

## Appendix B: Model for Token Buyback

## Appendix C: Inflation Dynamics

Saage DAO reward the stakers with an initial inflation $\mathcal{I}_0 = 50\%$ APR, and defines the time to half the inflation rate to be $\mathcal{T}_{1/2} = 3$ years. We define the relative inflation rate (token inflation + betting rebates) $i_0 = \frac{\mathcal{I}_0}{\mathcal{M}_0}$. At genesis we define, $\mathcal{I}_0 = \mathcal{M}_0$, which gives us the maximum number of tokens which that will ever be created:

$$\mathcal{I}(t) = \mathcal{I}_0 = 3^{-t/\mathcal{T}_{1/2}} = \mathcal{I}_0[\ exp(-ln3\tfrac{t}{\mathcal{T}_{1/2}})] \tag{C1}$$

The token supply can be related to the inflation at a given time $t$ as:

$$\mathcal{M}(t) = \mathcal{M}_0 + \int_0^t \mathcal{I}(t)dt = \mathcal{M}_0 + \tfrac{\mathcal{I}_0\mathcal{T}^{1/2}}{ln3}[\ 1 - 3^{\frac{t}{\mathcal{T}_{1/2}}}] \tag{C2}$$

$$\mathcal{M}_{max} = \mathcal{M}_0(1 + \tfrac{i_0\mathcal{T}_{1/2}}{ln3}) \approx 3.73\mathcal{M}_0 \tag{C3}$$

where $\mathcal{M}_0$ is initial number of tokens. $\mathcal{M}(t)$ is the current token supply with $\mathcal{M}(0) = \mathcal{M}_0$ and $dt$ can be equal to 1 day. Saage ecosystem implements a stability mechanism to adjust the inflation using $\mathcal{T}^*_{1/2} = \mathcal{T}_{1/2}/\beta$ , where $\beta$ is the mean staking parameter.

$$\mathcal{M}(t) = \mathcal{M}_0 + \int_0^t \mathcal{I}(t)dt = \mathcal{M}_0 \left( 1 + \tfrac{\mathcal{I}_0\mathcal{T}^*_{1/2}\beta}{ln3}[\ 1 - 3^{\frac{t}{\mathcal{T}_{1/2}}}] \right) \tag{C4}$$