
# GemBites Technical Whitepaper

Collection of Proof of Concepts, mathematical logic, smart contract structures, technologies and game logic

GemBites Development Team  4-30-2021

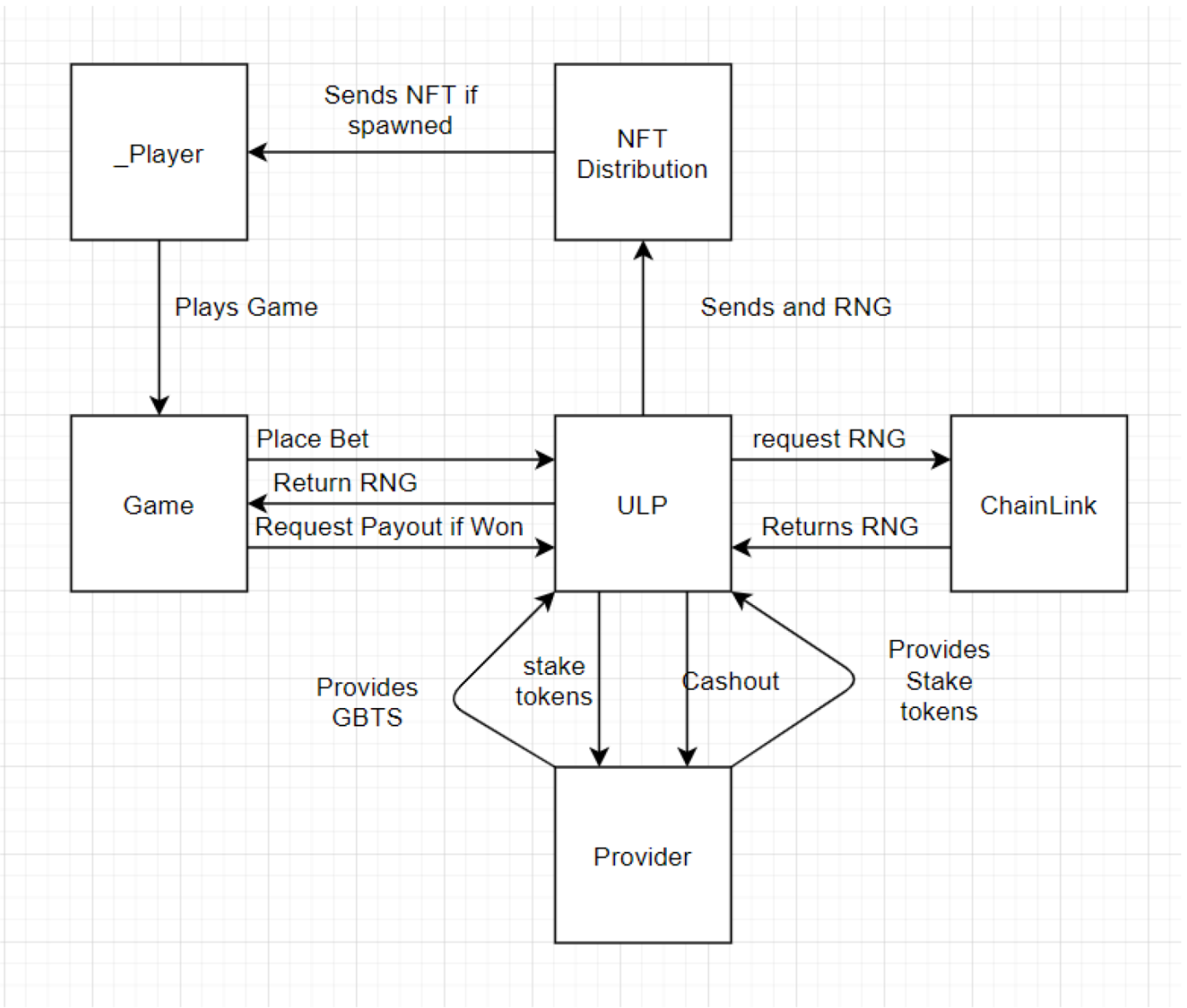
# Overview



GemBites is a decentralized, provably fair blockchain casino that utilizes a Unified Liquidity Pool structure to facilitate gambling

Some notable technical features are –

- The use of Polygon (ex. Matic) sidechain to provide gasless transactions with instant settlement
- The use of Chainlink Verifiable Random Function (VRF) to provide True RNG to games
- The use of a unique pool-share based Unified Liquidity System to provide a base infrastructure to build games on
- Using previously stated Liquidity System to allow anyone to become the house, and gain from house edge
- A distribution system to give users of the platform a fair chance to win unique NFTs. The same NFT distribution system will be used to further incentivize the house stakers



# Table of contents

The Unified Liquidity Pool (ULP) is the backbone of the GemBites betting platform. It simulates a traditional casino house by pooling funds from multiple users in order to finance bets and gain from edge. The ULP will contain anti-rug mechanisms such as a 3% entry/exit fee, in order to prevent bad actors from removing liquidity from the pool in the event of unfavorable bets found in the mempool. The ULP acts as a central contract with which other contracts will interact with in order to perform various functions such as requesting RNG, financing bets and facilitating NFT distribution.

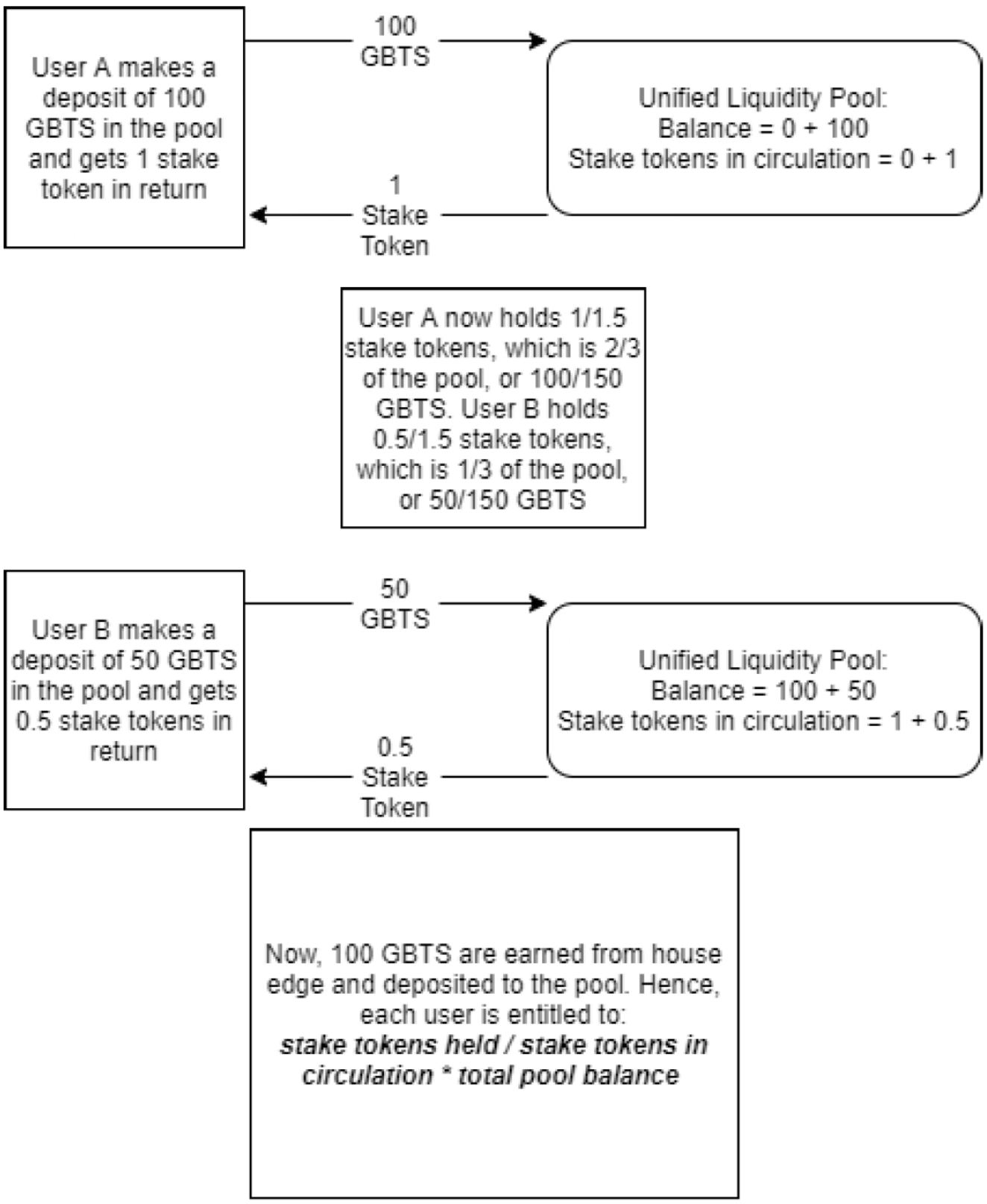
## Proof of Concept(s) for the Unified Liquidity Pool System:

The initial prototype of the liquidity system used a mapping based system, where the user's share of GemBites in the pool would be stored in a map. It is a simple, easy to understand system with not much complex math/logic. However, this system had one large flaw when implemented in a blockchain environment. If / When the amount of stakers were in large amounts, it would be very gas intensive to iterate through each user and deduct/add tokens. This made the system (eventually) expensive and non-scalable.

The current system that we plan on using uses a pool-share based infinite minting system. It follows the basic ideas behind the Uniswap Liquidity Provider tokens by allowing users to exchange their GemBites for staked GemBites tokens (sGBTS), which will represent their percentage share of the pool. This system is highly scalable as it does not require constant reiteration of maps. Moreover it simplifies the staking process by allowing users to mint/redeem sGBTS any time. Example:

# Unified Liquidity Pool

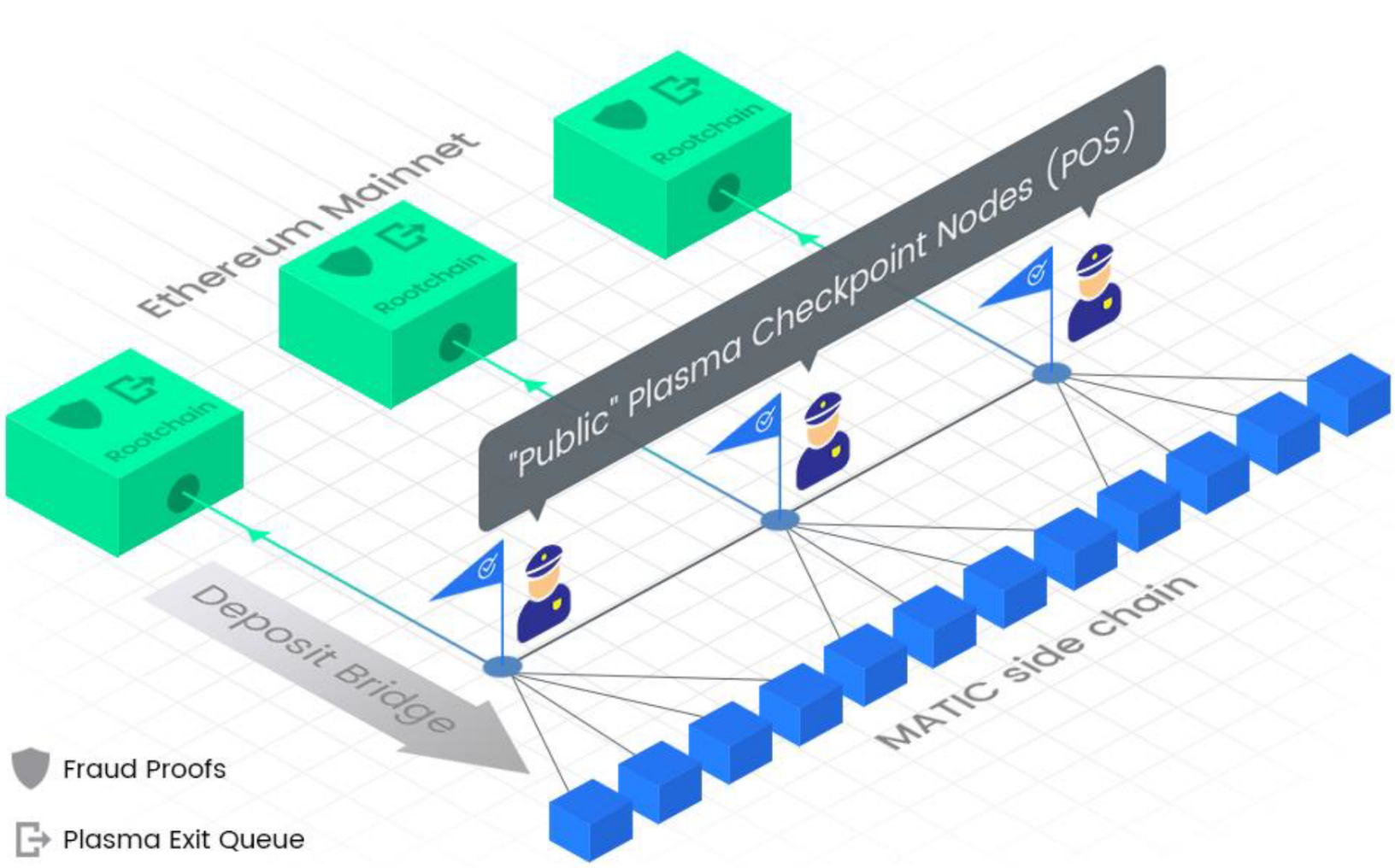




# Polygon (ex. Matic) Sidechain



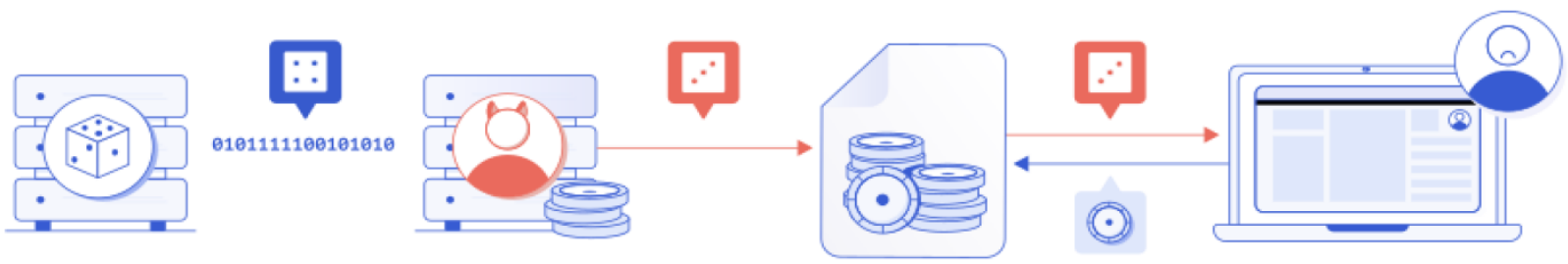
Polygon is a highly scalable sidechain powered by Plasma PoS validator nodes. It is built to be natively interoperable with Ethereum based blockchains. It has a high throughput, scaling upto 65,000 transactions per second. This scalability allows it to keep gas fees low. The main highlight of Polygon is its ability to bridge to different blockchains. By building GemBite's base infrastructure on Polygon, we have the freedom to create cross-chain betting pools that can be bridged to blockchains such as Polkadot, Smart Chain and Ethereum

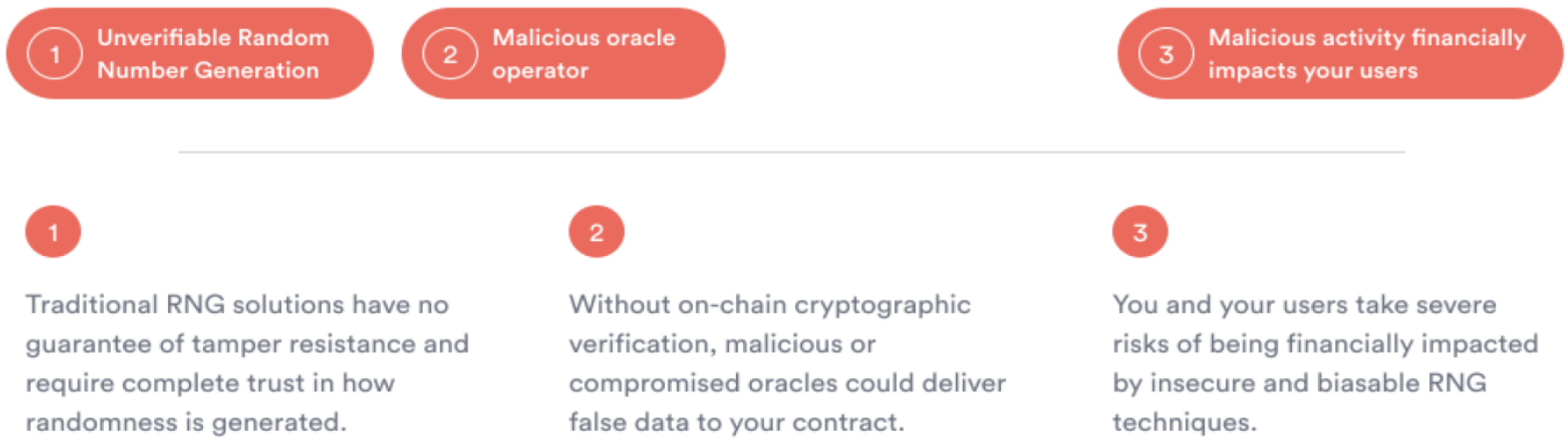


# Chainlink Verifiable Random Function (VRF)

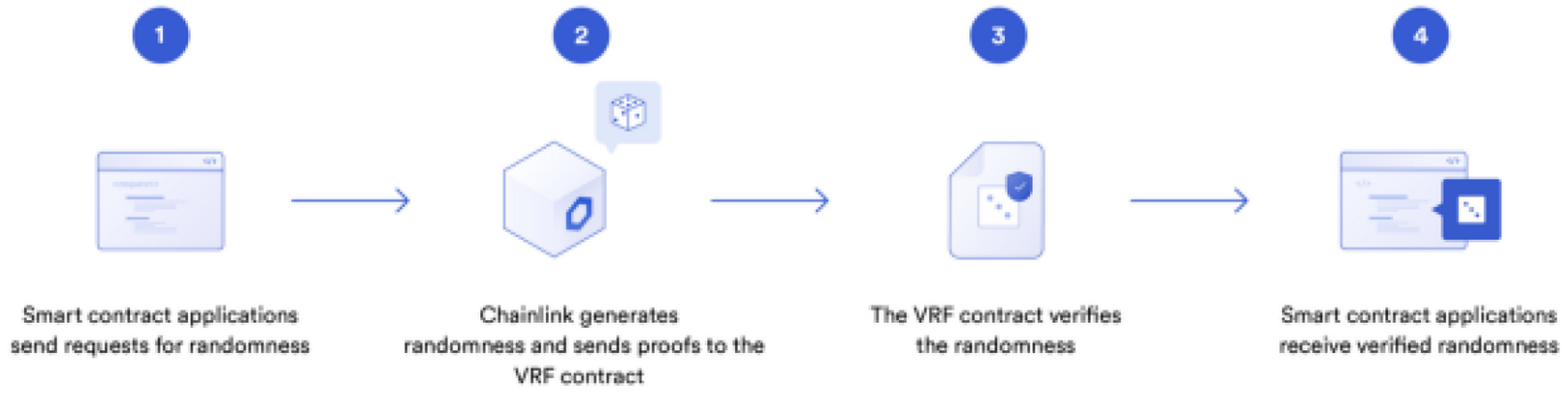


Initially, we planned to use a block-hash based random number generator, where the sha256 hash of a block was the determining factor of any played game. However, we quickly came to the realization that this method is susceptible to MEV (Maximum Extractable Value) attacks. This simply means that a validator that mines our block may simply exclude, add or reorganize transactions in order to produce a favorable block hash




Chainlink VRF solves this problem by providing verifiable, unbiased True RNG (TRNG) for an extremely low price. Off-chain generation + On-chain verification of RNG allows us to produce a truly random, tamper-proof output. Calling the VRF function returns a 77 digit, random uint256 result



# Non-Fungible tokens, their value proposition and distribution algorithms



Non-Fungible tokens (NFTs) are a form of cryptographic assets that are completely unique in nature. There can never be two identical NFTs, hence their non-fungible nature. NFTs have various purposes such as digital license ownership, art ownership and gaming. In the GemBites ecosystem, we plan on utilizing NFTs as cosmetics in-game, tradable collectibles and achievement milestones.

Now you might ask, what's the point? They are technically useless. You are partially right, but truth be told, they are simply a scarce, collectible asset, each holding its own unique digital data. We plan on hosting seasonal events, each with a limited amount of unique NFTs to be distributed. These seasonal NFTs may only be obtained during its respective season, which will never occur again. Moreover, we will use this opportunity to support both established and upcoming NFT artists in the cryptoverse


AaveGotchi's unique NFT collectibles

# The working of GemBite's fully decentralized games

This is probably the part you've all been waiting for. The games. A casino is defined by the quality of its games. We at GemBites strive to create fair, fun and unique games to be played by anyone, anywhere. Let's go over some of the games that will be included in our V1 release:

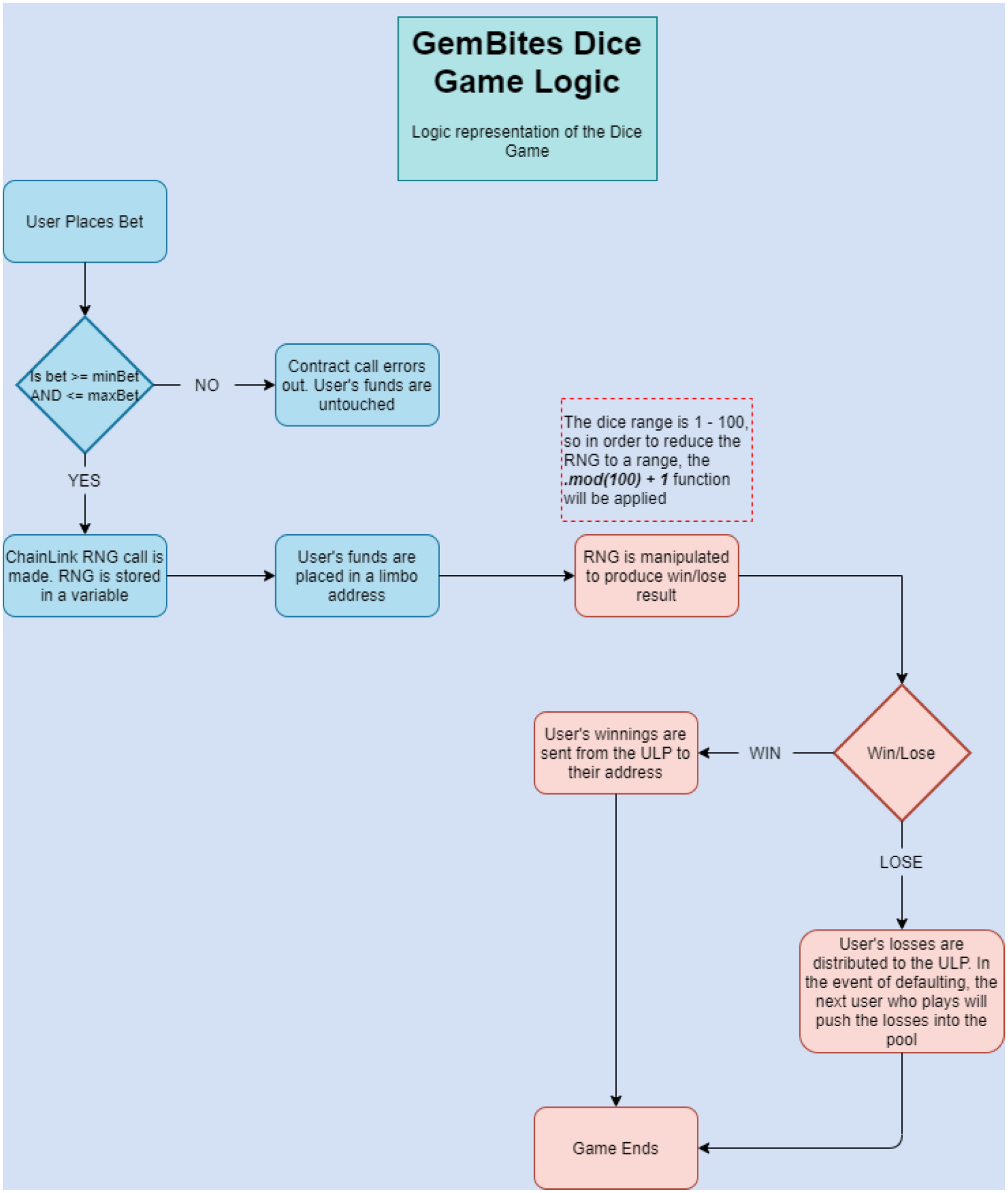
## Dice Game:

Dice is probably the simplest game on this list, and it is a bare necessity in every online casino. The game is expected to have a house edge between 2% - 2.5%. The rules are simple. A roll of a 100 sided dice is simulated. Based on the odds the player chooses, the number on the dice determines the result of the game. For example, if a played chooses 48% odds, they will multiple their bet by ~2 if they roll above 48. The algorithm works as such

**betMultiplier = (100% - 2 * houseEdge) / WinChance**

The logic flow of Dice can be seen below,

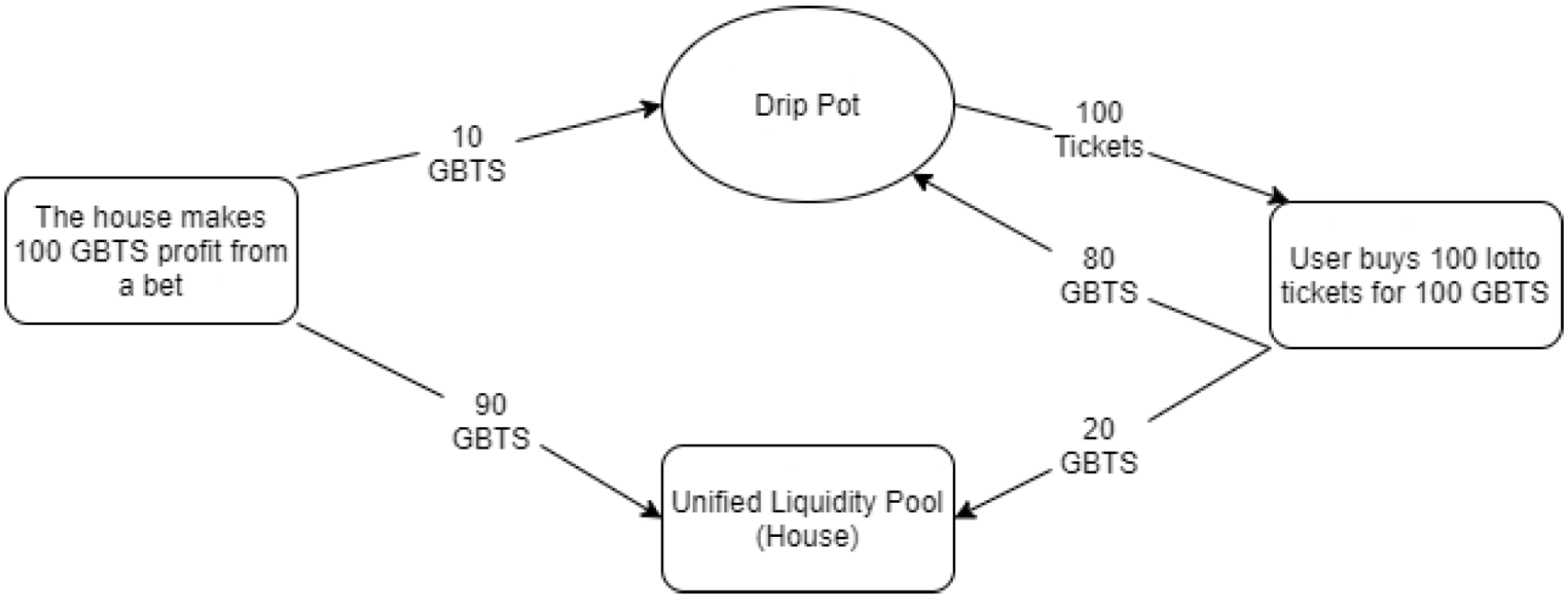
# The working of GemBite's fully decentralized games



# The Drip-Pot:



The drip-pot is a unique, passive game by GemBites that features a jackpot contract, to which a small percentage of the casino profit flows into. These drip-pots can be obtained by playing games in the casino. When you play a game, your RNG is used to determine both the outcome of your game, and roll for a chance at cracking the drip-pot. If you manage to roll a drip-pot, you will 25% of its holdings and an ultra-rare NFT that allows you to publicly display your crazy luck. Moreover, users can participate in a monthly lottery, for which tickets can be purchased at the rate of 1 TICKET / GBTS. There is a 0.2 GBTS house management fee paid per ticket to the ULP



# More Games coming soon



We have a lot in mind. We are nearly finished with the logic regarding Lucky Shot V2. This version of the Technical Whitepaper is far from complete.