The Back Room DAO

Polygon's First Truly Decentralized Casino

Boris Radulov
@VAPORGRIPS
sc20br@leeds.ac.uk

José Betancourt
@tridentity_
jose.betancourt@yale.edu

Nikolay Mitev
@T_SYMMETRY
nikolay.mitev@yale.edu

March 23, 2022

DISCLAIMER

This article does not constitute investment advice and should not be construed as solicitation. It is not guaranteed to be up to date but is accurate at the published date.

Contents

1 Introduction

The following outlines a proposal for "The Back Room," an Polygon-based DAO that facilitates online casino-style gaming in a trustless and decentralized manner. This paper outlines the technical details of how multiplayer games can be executed through cryptographic proofs, a comprehensive smart contract, and a single class of tokens used for both governance and betting.

2 Trustless Multiplayer Gaming

2.1 The Impossible Trinity

The principal issue in playing a fair game of poker is solving the seemingly impossible trinity of verifiability, privacy, and trustlessness. Most online casinos sacrifice trustlessness by relying on a centralized dealer to originate randomness and ensure the platform is secure. This, of course, opens the door for exploitation and tampering as these solutions are never open source. On the other hand, a primitive blockchain solution could host casino-style gaming by utilizing smart contracts to handle the actual gameplay. This sacrifices the secrecy of players' hands as it would be infeasible to secure private data on a traditionally public blockchain. Furthermore, such a solution would make games beholden to block times and other potential slowdowns unrelated to the casino. Verifiability can also be compromised with weak solutions that attempt to use unreliable or exploitable sources of randomness. For example, some Polygon smart contracts use the SHA256 hash of a block parameter as a source of randomness, meaning that randomness seeds are both slow (one per block) and can be rigged if the validator has placed bets on the current game. One can argue that this is by design, as the EVM aims to be a deterministic state machine. Thus, to find the solution to the trilemma and to guarantee true randomness, we must go off-chain.

In this endeavor, The Back Room utilizes cryptography to shuffle and deal a deck of cards in a secure, decentralized manner, as put forth by Philippe Golle [2]. A generalized version of this off-chain approach can be used to play any card game and even other non-card-based casino style games. This process of verifying only finished game states and updated player balances with the on-chain smart contract will be known as Proof of Result (PoR). It functions as follows.

2.2 Our Solution

We assume the following player agreements:

1. The players all agree to the game parameters such as deck size, potential outcomes, etc.

2. The players all agree to some homomorphic encryption scheme to be used in the game.

3. The players utilize a peer-to-peer protocol such as libp2p [3] to establish communication between one another.

4. Any player can communicate with another player in a way that is invisible to the other participants. (The Back Room uses a different approach compared to Golle: asymmetric encryption with the public/private key pairs related to players' Polygon wallets.)

If all those agreements are satisfied, the game can proceed as follows:

1. The players come together, establish communication, and perform Pederson DKG [5] to generate the parameters of a homomorphic encryption scheme such as El Gamal [1].

2. The players then use peer-to-peer communication to play rounds of the chosen casino-style game in a trustless manner as outlined by Golle. The pre-agreed homomorphic encryption scheme allows for the secure decentralized generation of new random cards on the fly for players to use in the game.

3. For each round, players store a non-malleable cryptographic commitment to the current game state by hashing the state and appending it to a Merkle Tree used for verification [4].

4. At the end of the game, each player will have an identical Merkle Tree which can be used as a proof for the result of the game.

5. The Merkle Tree's root hash along with the player's public key is then used as a PRNG to generate a sequence of states which need to be provided along with the Merkle Tree root as a proof.

6. This Proof of Result, along with the outcome of the game, is sent to a smart contract for verification. All players attempt to send said proof to the smart contract but only one is necessary to verify.

2.3 Proof Of Result

In summary, Proof of Result allows actual gaming to happen off-chain with only the outcome and a corresponding proof being appended to the Polygon blockchain. This decimates gas fees and allows for multiple games to be played per block. The nature of this gameplay algorithm also guarantees that the proofs submitted are not only valid but non-conflicting between players. Proof of Result means that results can be validated without the need for individual game states. This means that players can fold without revealing their cards, as is sometimes preferred.

The ERC-20 token, CHIPS, is used to handle betting and the redistribution of funds. The players' buy-ins will act as their wallets during the game meaning that their larger balances and locked amounts are insulated and secured. Following the conclusion of the game, wallets are updated according to PoR and deposited back into their accounts.

In Proof of Result, the CHIPS a player has bid are stored as collateral within the pot. Upon detected fraud or lack of response from any player, the other players may choose to forfeit the table as a security precaution. Since the shared encryption is resilient to a number of players leaving the table, the remaining group may choose to continue in cases where they either believe the mistake is due to network disconnection or for anti-collusion assurances. If they chose to end the hand, they commit the state of the last valid played hand as if the game has ended there. Since placing a bet requires a cryptographic commitment from the bettor, remaining players can prove that someone has bet even if they leave the table mid-hand.

Because players have competing interests yet can verify game results independently, shuffling is verifiably random and players can even prove the cards they received were not tampered.

3 Democratized Gaming

The Back Room is not only player controlled, but player owned. In fact, what is most exciting about CHIPS, the cryptocurrency, is that its multipurpose design enables it to be used in governance as well. This means that there is only one class of tokens so that ownership is truly of the players, and not by a higher level of managers. Every bet you place represents stake in the DAO you collectively own.

CHIPS generated from yield or from the original ICO are in playing mode by default. CHIPS can be transacted, exchanged, or used in betting, functioning both like cryptocurrencies and poker chips. When a vote occurs, users may lock their CHIPS in exchange for one-to-one convertible gCHIPS that are then used in governance. New releases, updates, and decisions are then passed by a majority agreement of the gCHIPS in circulation.

The reason the token must be converted is because some wallets may become inactive, or temporarily unavailable, rendering the outstanding supply incomplete. Because CHIPS can only be locked for finite time intervals, gCHIP holders are assured to be active members of the community.

A player-owned casino has several interesting implications. Namely, it means that certain rules ensuring the long-term success of the casino are abolished. The most popular of these facets is the rake, where the house collects 5-10% of every winning pot. The typical profits from this are now able to be directed back towards the players. The rake is thus abolished and instead a reverse rake is implemented, meaning that the odds now lie with the players and that poker is no longer gambling.

4 Tokenomics

There are two sources of yield: reverse rake and passive locking.

4.1 CHIPS

The ERC-20 token, CHIPS, will be first introduced in a few rounds within the ICO. From therein, CHIPS will only be produced from predetermined yields or through an agreement of a majority of the token holders.

4.2 Reverse Rake

The reverse rake is the first source of yield. While most casinos decide to cut a pot by 5-10% for their own profit, The Back Room will match all pots with a 570% APY. This "reverse rake" takes the form of a jackpot that periodically doubles the size of the winning pot, with The Back Room taking no rake for all other games. The more often a user plays and wins, the higher their expected APY. With The Back Room, the players enjoy a positive-sum-game where the house is not expected to win.

4.3 Passive Locking

Passive locking allows tokenholders to exchange their CHIPS for gCHIPS for predetermined amounts of time for extremely high, fixed-rate APYs [1].

Say a user held 1000 CHIPS and wished to lock 200 for 6 months that they would not use to gamble. The 200 CHIPS are then placed in a vault in The Back Room and 200 gCHIPS are given as a receipt back to the user. Every month and at the conclusion of the locking period, the holder of the gCHIPS is awarded their proportionate yield, or 7.08 CHIPS. The 200 CHIPS can be exchanged back for gCHIPS after the locking period ends, or if the user decides to terminate the agreement early, for a 25% early withdrawal penalty.

While a user locks CHIPS, the corresponding gCHIPS can be used in governance to vote on new releases, additional games, and other updates. Because CHIPS are one-to-one exchangeable with gCHIPS, the users of The Back Room are also its owners. There is no separate class of tokens.

		Amount of Tokens Locked			
Time Period		1-2000	2001-10000	10001-100000	100000+
	2 Weeks	90%	81%	69%	30%
	1 Month	100%	89.5%	75,5%	40%
	2 Months	110%	98%	82%	50%
	4 Months	120%	106.5%	88.5%	60%
	6 Months	**130%**	115%	95%	70%

Table 1: Passive Locking yield for different token amounts and time periods.

[1] Yields are approximate and subject to change

This model is sustainable because the high yield environment will only persist for early adopters who quickly see and unlock its value. Starting yields, as displayed in the table above, will begin to taper as the circulating supply begins to approach the token cap of 100,000,000,000. Additionally, transaction fees will help maintain a deflationary ecosystem.

It should be noted that all yields are approximate, but not arbitrary. They derive from the system as follows:

- M - Supply Multiplier
- X - Circulating supply
- S - Token Cap
- P - Payout
- V - Vault
- T - Table
- K - Capital
- Y - Yield

A tapering effect is defined as:

$$M = (1 - \frac{X}{S})$$

So that the total payout is:

$$P_V + P_T = K_V \cdot M \cdot e^2$$

The payout within the vault (locking tokens) will then be:

$$P_V = \frac{(1 - \frac{P_{V_{i-1}}}{P_{V_{i-1}} + P_{T_{i-1}}})^2}{K_V \cdot M \cdot e^2}$$

Which means the average vault yield is:

$$Y_V = \frac{P_V}{K_V}$$

Thus, the payout from the table (reverse rake) is:

$$P_T = K_V \cdot M \cdot e^2 - P_V$$

This means that the average yield from the table is:

$$Y_T = \frac{P_T}{X - K_V}$$

5 Conclusion

The Back Room DAO brings rakeless gaming to the masses by ending the centralized casino monopoly. Our commitment is to security and transparency, so we designed a game where you're the dealer. Even more, you own The Back Room and share its value. This time, it's you making the decisions, and it's you winning.

References

[1] Elgamal, T. "A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms." IEEE Transactions on Information Theory, vol. 31, no. 4, July 1985, pp. 469–472., https://doi.org/10.1109/tit.1985.1057074.

[2] Golle, P. "Dealing Cards in Poker Games." International Conference on Information Technology: Coding and Computing (ITCC'05) - Volume II, 2005, https://doi.org/10.1109/itcc.2005.119.

[3] Protocol Labs. "A Modular Network Stack." libp2p, Protocol Labs, 2022, https://libp2p.io/.

[4] Merkle, Ralph. Method of Providing Digital Signatures. 5 Jan. 1982.

[5] Pedersen, Torben Pryds. "Non-Interactive and Information-Theoretic Secure Verifiable Secret Sharing." Advances in Cryptology — CRYPTO '91, 991AD, pp. 129–140., https://doi.org/10.1007/3-540-46766-1_9.