CryptoBet

Bulgaria's First Truly Decentralized Casino

Boris Radulov
@VAPORGRIPS
sc20br@leeds.ac.uk

Nikolay Mitev
@T_SYMMETRY
nikolay.mitev@yale.edu

José Betancourt
@tridentity_
jose.betancourt@yale.edu

July 15, 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 “CryptoBet,” a Polygon-based DAO that facilitates online gaming in a trustless and decentralized manner. This paper outlines the features, structure, and advantages of decentralization for both playing and governance.

2 Structure of the DAO

2.1 Owned by the Players

CryptoBet will be structured as a Decentralized Autonomous Organization (DAO), which will allow players to collectively govern, engage with, and share the profits of the organization. You can learn more about DAOs here.

To become an owner of CryptoBet, the player simply has to purchase the platform-native token called CryptoBet token (CBT) and then lock it for a certain period of time in exchange of governance tokens (or gCBTs). These governance tokens give the players access to special features of the DAO since now they are members of the community of owners. These special features include:

- Passive Yield derived from the profitability of the DAO
- Cashback on multiple of the games in the platform
- Additional bonuses, rewards in crypto, discounts, and better rates
- Access to the owners' collection of limited edition NFTs
- Access to exclusive events, poker tournaments, parties, and more

2.2 Passive Yields and Governance

CBTs are one-to-one convertible to gCBTs. The number of gCBTs a player owns proportional to the total number of CBTs determines their stake in the DAO as well as the percentage of the total profit which they are entitled to.

These profits will be regularly paid out to the gCBT holders and will be based on the pre-fixed yield rate and the profitability of the platform.

2.3 Innovative gaming

By structuring CryptoBet as a DAO and utilizing the capabilities of blockchain technologies, we can build a new generation of iGaming platforms which allow users to immerse in the gaming experience, freely express their opinions, and structurally participate in the project while sharing its profits.

This movement towards democratized gaming can change the entire structure of the iGaming industry by opening many doors for collaboration and creativity. As this organizational model distributes the profits among a wide number of contributors, it further decentralizes the rewarding model because the beneficiaries of a given project are the people using it.

Therefore, with CryptoBet and similar decentralized organizations, the players can participate in projects they enjoy and profit while doing so, which brings us one step closer to the transition towards a better, more transparent, and truly fair gaming experience.

3 Trustless Multiplayer Gaming

3.1 The Problem with Generating Randomness

The principal issue in decentralized gaming is solving the seemingly impossible trinity of verifiability, privacy, and trustlessness. Most iGaming platforms sacrifice trustlessness by relying on a centralized entity 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 iGaming by utilizing smart contracts to handle the actual gameplay. This sacrifices the secrecy of players' information 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 platform. 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 easily compromised.

In this endeavor, CryptoBet utilizes cryptography to generate both public and private random numbers in a secure, decentralized manner, as put forth by Philippe Golle [2]. A generalized version of this approach can be used to play any single or multi-party game. This process of encrypted, provable, and consensus-based communication between the participants in the system will be known as Dynamic User Entropy (DUE). It functions as follows.

3.2 Our Solution

We assume the following player agreements:

1. The players all agree to the game parameters such as initial conditions, 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. (CryptoBet 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 players can run a fully decentralized game 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 game in a trustless manner as outlined by Golle. The pre-agreed homomorphic encryption scheme allows for the secure decentralized generation of new random values on the fly for players to use in the game.

3. The players locally generate a random number in the range supported by the game. They encrypt it using El Gamal and send a non-malleable commitment to all other participants.

4. After the commitments have been verified, the cyphertexts are revealed and players compute the aggregate encryption by homomorphically multiplying the cyphertexts.

5. In the case where the randomness is meant to be a publicly accessed value such as a face-up card or a roulette spin result, the players all reveal their seed values. All other participants verify the correctness of the precommited encryptions. Then they sum the seeds, encrypt them using El Gamal, and compare the result with the homomorphic aggregate value of the original cyphertexts.

6. In the case where the randomness is meant to be privately accessed, a variation of zero-knowledge proofs is used. All participants send their seeds to the player who is meant to receive the randomness. He sums the seeds and gets a random value. Utilizing a variation of the classical Schnorr signature, the receiver proofs that the derived value is unique and that he has performed all operations correctly.

7. 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].

8. 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.

9. 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.

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

In case of a single player game, the same approach can be easily adapted to a two-sided communication between a player and a smart contract. No matter what the seed generated by the contract is, as long as there are two parties in this system (the player being one of them), the randomness generated is verifiable and unexploitable.

3.3 Dynamic User Entropy

In summary, DUE allows for an instant, trustless, and secure way of generating random values. The nature of this gameplay algorithm also guarantees that the proofs submitted are not only valid but non-conflicting between players. DUE means that results can be validated without the need for individual game states. This means that players can leave the game without revealing their data and without disrupting the security of the process.

The ERC-20 token, CBT, 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 DUE and deposited back into their accounts.

In DUE, the CBTs a player has bid are stored as collateral within the smart contract. Upon detected fraud or lack of response from any player, the other players may choose to forfeit the game as a security precaution. Since the shared encryption is resilient to a number of players leaving, 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 round, 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 game in the middle of the generation process.

Following the process outlined above, players can easily mathematically prove that the numbers they received were truly random.

4 Democratized Gaming

CryptoBet is not only player controlled, but player owned. In fact, what is most exciting about CBTs, 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.

CBTs generated from yield or from the original ICO are in playing mode by default. CBTs can be transacted, exchanged, or used in betting, functioning both like cryptocurrencies and poker chips. When a vote occurs, users may lock their tokens in exchange for one-to-one convertible gCBTs that are then used in governance. New releases, updates, and decisions are then passed by a majority agreement of the gCBTs 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 CBTs can only be locked for finite time intervals, gCBT 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 platform 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 can be implemented in games like poker, meaning that the odds now lie with the players.

5 Tokenomics

5.1 Pre-Sale Period

In order to raise funds to improve and fully develop the platform, CryptoBet will hold a pre-sale period which will allow early adopters to buy up to 7% of the ICO. Buyers of these first CBTs will get a preferential lower price and will also become members of the Owners Lounge: a community of early adopters who will additionally get access to premium NFTs, special events, increased rates, etc.

5.2 ICO

When the platform is fully operational, CryptoBet will start its Initial Coin Offering period. The ICO will let players buy tokens which can then be used in games. The ICO will aim to sell 15% of the total CBT supply which will enable the platform to start generating the first yields.

5.3 Reserves

The funds raised during the ICO will be stored in the smart contract and will be used by the DAO to further develop CryptoBet and back the token. This budget will be managed by the community of players and will facilitate the growth of the collective venture.

5.4 Passive Locking

Passive locking allows tokenholders to exchange their CBTs for gCBTs for predetermined amounts of time for fixed-rate APYs [1].

[1] Yields are approximate and subject to minor changes

Say a user held 1000 CBTs and wished to lock 200 for 6 months. The 200 tokens are then placed in a vault in CryptoBet and 200 gCBTs are given as a receipt back to the user. Every month and at the conclusion of the locking period, the holder of the gCBTs is awarded their proportionate yield, or 3.3 CBTs. The 200 CBTs can be exchanged back for gCBTs after the locking period ends, or if the user decides to terminate the agreement early, for a 20% early withdrawal penalty.

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

Amount of Tokens Locked	**APY**
2 Weeks	2%
1 Month	5%
3 Months	10%
6 Months	20%
12 Months	**30%**

Table 1: Passive Locking yield for different time periods.

This model is sustainable because the 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. 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 - Tapering multiplier
- X - Circulating supply
- S - Token cap
- Pv - Payout to vault
- R - Daily rake
- ar - Average rake (past 30 days)
- Yv - Yield to a wallet
- Kv - Capital locked in vault
- ΔKv - Change in capital locked in vault

A tapering effect is defined as:

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

So that the total payout is:

$$P_V = a \cdot (1 + \Delta K_V) \cdot e^M$$

Thus, the yields offered to the players are:

$$Y_V(time) = \frac{P_V(time)}{K_V(time)}$$

Which lets us approximate the inflationary effects of these emissions:

$$CPI = ar \cdot (1 + K_V) \cdot e^M - ar$$

The aforementioned rate is accounted for in the model which mathematically preserves the token stability.

6 Conclusion

CryptoBet brings fair and decentralized gaming to the Bulgarian market. Our commitment is to security and transparency, so we designed a game where the randomness is generated by the players in a trustless manner. Even more, the very same players own CryptoBet 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.