
CRYPTOACES

Table of Contents

Introduction

The online community of card games is on a rapid growth curve - be it Poker, Blackjack, Rummy and so many more. This multi-billion-dollar community is thriving and has given rise to many players who now play professionally. At the same time, it also attracts an ever-growing number of recreational players, daily, which is only expected to grow further.

While the current generation of online card games are great for general gameplay experience, they fail to ensure two key tenets of the game that would elevate the overall experience multi-fold: fairness and security. There have been multiple instances of rigging in online card games and most online platforms that host the most popular card games fail to always ensure security of player funds and winnings. Some of these examples are discussed in detail in the following sections.

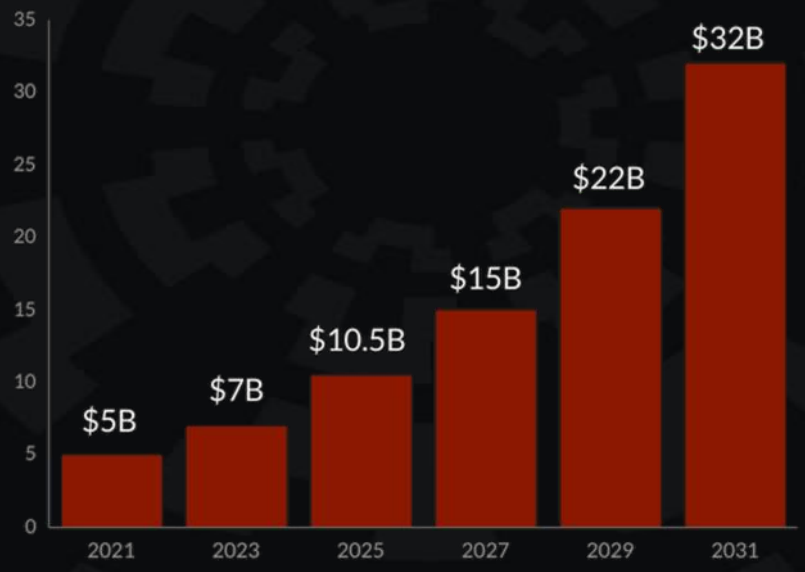
In the context of these challenges, CryptoAces aims to bring fairness and transparency to online card games by hosting them on a fully secure decentralised blockchain network. We are building a core underlying decentralised network where all you have got to do is simply plug-in and play. Our unique peer-to-peer cryptographic shuffling protocol among the players on the table provides full transparency and ensures that the game is always fair.

We want to create a seamless and safe online experience for all card players where they can have fun without constantly worrying about game rigging, deposit risk, and high rake fees.

Market Analysis

The global online gambling market is anticipated to be valued at more than $ 92.9 billion in 2023. The current size of the market is almost $ 59 billion, meaning the size is forecast to double in the upcoming years. Online gambling consists of playing casino games, card games like poker, and sports betting via the internet. Out of the total share, Poker alone is estimated to be somewhere in the range of 10-15% of the total online gambling market and is projected to grow at a 20.5% CAGR.

With the global leaders in the online poker industry reporting more than $1 billion in revenue from the game in 2018, online poker is certainly a big business. The COVID-19 pandemic has also resulted in a massive increase in online poker traffic. Many operators reported traffic of double or more the previous volume, depending on the time of day.



Current Problems with Online Card Games

There have been multiple instances where existing platforms have used player behaviour data (enhanced using third-party tools) to engineer outcomes that are best for the platform's revenue stream. Worse still, platform employees with admin account access can view all the other players' cards on the table and easily rig the game. Recreational players are especially at higher risk to such malicious practices. At times, even professional players have fallen victims to various frauds. Players have often faced issues with timely fund withdrawal and in some cases, indefinite lock-up of funds. And to top it all, all platforms charge high rake fees which keep on accruing the longer you play and thus, players end up burning a hole in their pockets.

It is impossible to determine with absolute certainty what really goes behind the scenes of large, centralized online platforms that double up as gaming arenas. Many critics question whether the operators of such games might be engaging in fraud themselves. Internet discussion forums are rife with allegations of non-random card dealing, possibly to favour house-employed players or bots, or to give multiple good hands thus increasing the bets and the rake, or simply to prevent new players from losing so quickly that they become discouraged. Many players claim to see many "bad beats" with large hands pitted against others all too often at a rate that seems to be a lot more common than in live games. There is enough anecdotal evidence to support such claims.

Insider cheating can also occur when a person with trusted access to the system (e.g., an employee of the poker room) uses their position to play poker themselves with an unfair advantage. This could be done without the knowledge of the site managers. Perhaps the first known major case came to light in October 2007, when Absolute Poker acknowledged that its integrity had been breached by an employee, who had been able to play at high stakes while viewing his opponents' hidden "hole" cards. The cheating was first brought to light by the efforts of

players, whose saved histories of play showed the employee was playing as only someone who could see their opponents' cards could. In 2008, UltimateBet became embroiled in a similar scandal, with former employees accused of using a software backdoor to see opponents' cards. UltimateBet confirmed the allegations on May 29, 2008.

Our Value Proposition

We at CryptoAces love poker and see it as a game that should reward skill. Our mission is to provide a fair, safe and secure decentralized platform to play online poker. In due course of time, we will extend gameplay accessibility to other online card games too.

Our first aim is to build a customizable plug-and-play interface built on a decentralized online network that is easily accessible to developers and third-party operators. We aim to support anyone who wishes to provide a fair platform to play online card games, through our core underlying technology that will live on the blockchain.

We also aim to provide the lowest gas fees on the blockchain network, using our optimized smart contracts. We know that it is not feasible to support a game as complex as poker on the blockchain if there are multiple transactions with high gas fees involved. Therefore, we have our best minds working on this, who have come up with a state-of-the-art solution. Our smart contracts also ensure that all players always have full control over their funds on the platform. They also govern the autonomous pay-out distribution based on game outcomes.

We have also developed proprietary P2P cryptographic shuffling protocol between players seated at the table and compute the consensus between them

through Byzantine Fault Tolerant mechanism. This ensures that all gameplay on our platform is fair and completely secure.

Technical Details

CryptoAces aims to create a decentralized online card game network with trust, transparency and accountability. We will start by supporting Texas Hold'Em Poker on our platform and utilize the Polygon blockchain network to achieve our goals. We aim to employ peer-to-peer networking, user-owned identity, and cryptographically secured cards, to present an improved playing experience at a lower cost to players.

User Flow

Initially, we only plan to release our web application. We will also have a mobile application, which will be a Web View App. Once the user reaches our website, he can use an already created BlockPass identity, or create a new one. Afterwards, depending on the validity of the identity to participate on our platform (there will be age, and jurisdiction limitations to keep our platform fully legal), the user can access the rest of our platform.

The user will have access to the lobby, which will show all publicly available games, or can create a private game (support for private games to be added later) and invite other players. The user can join either a public or private game by sending CryptoAces (CACE) tokens to the table address of the game they want to join. The smart contract sits on the Polygon blockchain and acts as an escrow account while the game is in progress. Each game is represented by a table contract that contains the custom parameters of that game.

The peers at the table form a P2P subnet and use a Mental Poker protocol that requires each individual peer to shuffle and encrypt the deck of cards. When a

tournament is completed, or a player leaves a cash table, the table contract auto-executes, and the player(s) is(are) paid their winnings (if due).

Mental Poker

Mental Poker is the common name for a set of cryptographic problems that concerns playing a fair game over distance without the need for a trusted third party. The term is also applied to the theories surrounding these problems and their possible solutions. In poker, this translates to: "How can we make sure no player is stacking the deck or peeking at other players' cards when we are shuffling the deck ourselves?". In a physical card game, this would be relatively simple if the players were sitting face to face and observing each other, at least the possibility of conventional cheating can be ruled out. However, if the players are not sitting at the same location but instead are at widely separate locations and pass the entire deck between them (using the postal mail, for instance), this suddenly becomes very difficult. And for electronic card games, such as online poker, where the mechanics of the game are hidden from the user, this is impossible unless the method used is such that it cannot allow any party to cheat by manipulating or inappropriately observing the electronic "deck".

Several protocols for ding this have been suggested, the first by the creators of the RSA-encryption protocol - Adi Shamir, Ron Rivest, and Len Adleman. We will give one possible algorithm for shuffling cards without the use of a trusted third party, using a commutative encryption scheme. A commutative scheme means that if some data is encrypted more than once, the order in which one decrypts this data will not matter.

Example: Alice has a plaintext message. She encrypts this, producing a garbled ciphertext which she gives then to Bob. Bob encrypts the ciphertext again, using the same scheme as Alice, but with another key. When decrypting this double encrypted message, if the encryption scheme is commutative, it will not matter who decrypts first.

Algorithm

The algorithm for shuffling cards using commutative encryption:

- Alice and Bob agree on a certain "deck" of cards. In practice, this means they agree on a set of numbers or other data such that each element of the set represents a card.
- Alice picks an encryption key A and uses this to encrypt each card of the deck.
- Alice shuffles the cards.
- Alice passes the encrypted and shuffled deck to Bob. With the encryption in place, Bob cannot know which card is which.
- Bob picks an encryption key B and uses this to encrypt each card of the encrypted and shuffled deck.
- Bob shuffles the deck.
- Bob passes the double encrypted and shuffled deck back to Alice.
- Alice decrypts each card using her key A. This still leaves Bob's encryption in place though so she cannot know which card is which.
- Alice picks one encryption key for each card (A1, A2, etc) and encrypts them individually.
- Alice passes the deck to Bob.
- Bob decrypts each card using his key B. This still leaves Alice's individual encryption in place though so he cannot know which card is which.
- Bob picks one encryption key for each card (B1, B2, etc) and encrypts them individually.
- Bob passes the deck back to Alice.
- Alice publishes the deck for playing.

During the game, Alice and Bob will pick cards from the deck, identified in which order they are placed in the shuffled deck. When either player wants to see their cards, they will request the corresponding keys from the other player. That player, upon checking that the requesting player is indeed entitled to look

at the cards, passes the individual keys for those cards to the other player. The check is to ensure that the player does not try to request keys for cards that do not belong to that player.

P2P Off-Chain Interaction

A programmable blockchain technology like Polygon network allows a definitive and immutable data store for things that might otherwise be handled by a single server, like managing the players at a particular table. Our web app can interact with smart contracts on the blockchain, which allows for trustless, distributed management of player funds and table stakes, and provides an immutable record of these interactions. However, the blockchain cannot simply be used as a replacement for a server for all aspects of the game, partly because data and instructions sent by a client take at best a few seconds to propagate across the chain, making it impractical to use it to manage game events at a finer granularity than at the hand level.

Game events occurring at a higher rate, like betting, must be managed by the client software itself, or more properly, by the software that manages the peer-to-peer subnet consisting of the clients playing at a particular table. The use of digital signatures allows each client to verify that messages received have been sent by the claimed sender, preventing forgery. Fault tolerant consensus formation techniques are used to ensure that at each step in the process of gameplay, every client agrees with every other client as to exactly what has happened. In addition to catching errors and hardware failures, Byzantine faults (intentionally bad data) are also detected.

At the end of each hand, this consensus data - digitally signed by every client - is passed to the blockchain for processing, and the clients themselves move on to the next hand. Disagreements among clients or peers at the table are resolved by Arbiters.

Arbiter System

We have developed the Arbiter System to combat collusion and cheating on our platform. Arbiters are non-playing referees that are randomly assigned to poker tables. They provide security and protection to players on the CryptoAces network and receive fees in exchange.

They perform three core functions:

- **Dispute resolution** –
  In the rare instance that two peers at a table disagree as to the state of the table at the end of a hand or a game, an Arbiter resolves the dispute in real-time and awards the pot to the winner.

- **Data Feed** –
  Each Arbiter submits each action of every hand to IPFS so hand histories can be stored. This data can be used to enable essential services such as collusion detection, bot detection, and multi-accounting identification.

- **Partial Storage of Player Encryption Keys** –
  The "Dropped Player Problem" of Mental Poker occurs when a player drops out of a hand prior to its completion. This is problematic, as all the players must share encryption keys for community cards to be revealed, and for a hand to be completed. Using Shamir's Secret Sharing, each player's keys can be encrypted and split amongst all the players, plus the Arbiter. If the player drops out for any reason, the Arbiter can request the pieces from each player and decrypt the assembled pieces so that the hand can be completed.

To act as an Arbiter, a user will have to stake CACE tokens on the Arbiter registry and have the Arbiter section of our Web App running in his or her browser.

NFTs

Players on our platform will have the opportunity to win and collect NFTs based on several different activities that they perform on the platform. CryptoAces will use NFTs primarily as a method to enhance a player's experience on the platform.

Some examples of how an NFT can be earned on the platform are:

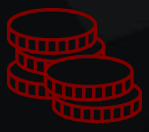
- **Volume Play** –
  Players can earn increasing tiers of NFT based on the number of games played on the platform.
- **Collective Value** –
  NFTs can be awarded depending on the total value of bets placed on the platform
- **Leaderboard** –
  Depending on how much a player won, different NFTs can be awarded
- **Podium Finishes** –
  Special tournaments will be organised with NFTs as some of the prizes.

The NFTs earned from the above categories can be used in several ways.

- Airdrops - Initial winners of our NFTs can be airdropped the CACE tokens directly to their wallets
- Rake bonuses - Play with discounted or zero rake for a certain duration
- Special Tournament Access - Certain special tournaments can be organised exclusively for NFT owners.

We also plan to come up with our own NFT marketplace, where these NFTs minted by CryptoAces can be purchased, sold, or traded.

Token Uses



In Game Currency:

The token will be used by players to get access to chips to stake on poker tables, and their winnings will also be cashed out in terms of this token.

Special Tournaments:

Tokens shall be required for access to special tournaments, whereby the participant must spend a prescribed amount of tokens to participate.

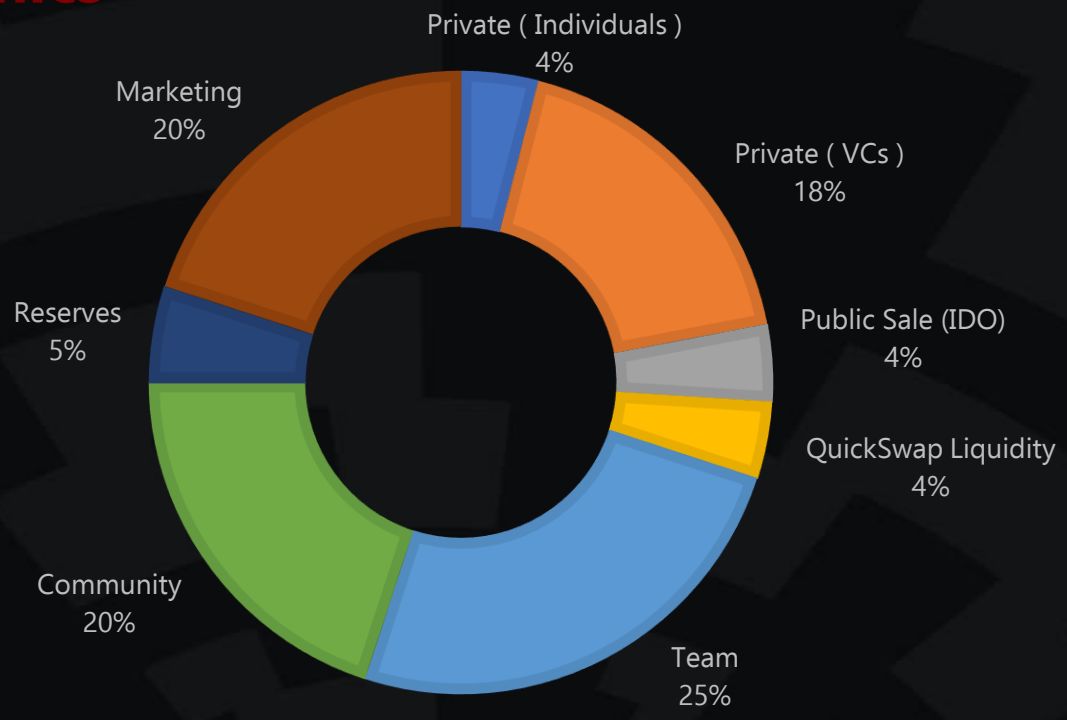
Arbiter Registry:

The user can stake his tokens to the arbiter registry which enables him/her to validate hands on the network in exchange of earning fees.

NFTs

Our unique NFTs, which can be acquired by playing on the platform, can be traded using the CACE tokens on our exclusive NFT marketplace.

Tokenomics



Price per token ($)

Private (Individuals/VCs)	0.008
Public Sale (IDO)	0.010
QuickSwap Listing	0.012

Vesting Schedule

Private (Individuals)	7.5% at TGE. 1 month cliff, then daily vesting over 8 months
Private (VCs)	7.5% at TGE. 1 month cliff, then daily vesting over 8 months
Public Sale (IDO)	10% at TGE, 1 month cliff, then daily vesting over 8 months
Quickswap Liquidity	Liquidity Locked
Team	0% at TGE, 5-month cliff, then daily vesting over 15 months
Community	Daily vesting over 12 months
Marketing	Daily vesting over 12 months
Reserves	Emergency Funds

Total Tokens: 500 MM | Initial Circulating Supply Market Cap: $360k

Roadmap

We aim to list our token on a swapping platform by the end of Q3, 2021 together with collaborations with influencers and huge partners. The working platform for Texas Hold'em poker will be launched by Q4, 2021 together with our NFT marketplace. Next, we shall be introducing Omaha variant and/or the variant voted by the community. Then moving onto Q2, 2022, more games such as Blackjack and Pontoon will be introduced. Starting Q3, 2022, we aim to have a plan to move our platform across different chains and start scaling in that direction.