CrushCrypto

Layer 2 Blockchain Scaling Solutions – State Channels

Educational Series

November 6, 2018

What does “layer 2" mean?

- Layer 2 is a term used to describe developments for blockchain technology that are being built on top of the existing “layer 1” infrastructure. It is also referred to as “off-chain” solutions.
- Layer 2 scaling solutions are needed because public blockchains (“layer 1” protocols) currently do not provide enough scalability for mainstream usage. For example, Bitcoin can handle 5 transactions per second while Ethereum can handle 10-15, yet Visa processes thousands of transactions per second on average with a maximum capacity of around 24,000.

What does “layer 2" mean? (continued)

- Upgrading existing blockchains to handle this level of transaction throughput on-chain while maintaining the current level of security and decentralization is very difficult. Layer 2 solutions are addressing this issue by moving some computations off-chain for reasons such as enabling privacy, saving computing resources, obtaining lower latency, and so on.
- Utilizing layer 2 scaling solutions, the original blockchain will still be the ultimate judge when there are disputes. The benefit to this is that it frees up processing resources, allowing for network scalability while still allowing users to benefit from the security and decentralization of blockchain technology.

What is a state channel?

- Two main types of layer 2 scaling solutions are state channels and side chains.
- A state channel is a two-way interaction channel between users. Here's a simple example: Two users each place a deposit to open a channel, then they perform a series of transactions with each other. When the session is over, the two parties close the channel and settle the net amount owed to each other.
- Notice that only the transactions concerning the opening and closing of channel is recorded on the blockchain; the transactions happening between the two parties while the channel is open is conducted off the blockchain. The state channel can be closed at any time, with the blockchain set in place as a mediator for disagreements.

Application-specific state channels

- Application-specific state channels are a type of state channel specific to a certain application, allowing for people to engage in turn-based systems off-chain and resolve bets based on the outcome on-chain.
- These are typically used for games, where users can each place a bet, take turns off-chain, and then finally resolve the outcome for distributing funds to the winner on-chain after the players finish the game(s).
- In app-specific state channels, the “judge” that decides outcomes is a smart contract that has rules of the game coded in and holds the funds. The two users must sign off on each off-chain move to agree on the state of the game.
- The rules coded into the smart contract must account for the situation where one user is being non-cooperative and refusing to sign off on the state of the game.

Application-specific state channels (continued)

- For example, a rule could be “If a player does not respond to a dispute within 2 minutes, reward all funds to the disputing player”. One example of a dispute case could be a losing player refusing to sign off on the final move of the game, effectively claiming they haven’t lost yet.
- The winner would submit the second to last move of the game as the most recent state that both parties agreed on, and the burden would be on the loser to submit the next agreed upon state. This could only be the final winning move – they would either sign off on this state and lose, or the dispute 2-minute time limit would run out.
- Either way, the winner gets all the funds held in the smart contract. This is one example of a state channel handling a non-cooperative party, but there are also other methods to settle the dispute.

Generalized state channels

- Generalized state channels allow for the use of the same state channel for multiple different purposes. This is separate from application-specific state channels, where a state channel is used for one distinct application.
- Instead of requiring each application developer to build a whole new state channel architecture, they can install new functionality in an existing channel for use with any application or set of applications.
- Just like app-specific state channels, a multi-signature wallet is used as a state deposit holder for generalized state channels. The difference, however, is that this is the only on-chain component that must be deployed for each extra application users want to “install” in a generalized state channel.

Lightning Network

- Currently the largest and most famous Layer 2 scaling solution for the Bitcoin blockchain. First proposed in 2015 that has since been updated.
- Makes use of bi-directional payment channels. However, instead of opening a new channel every time two parties want to conduct transactions, it allows for people to route their payments through payment channels that already exist.
- The Bitcoin blockchain is used as an arbiter, allowing for these off-chain transactions to occur with the confidence of on-chain enforceability. In the event of non-cooperation between users, the blockchain is resolves disputes in a deterministic way.

Website: https://lightning.network

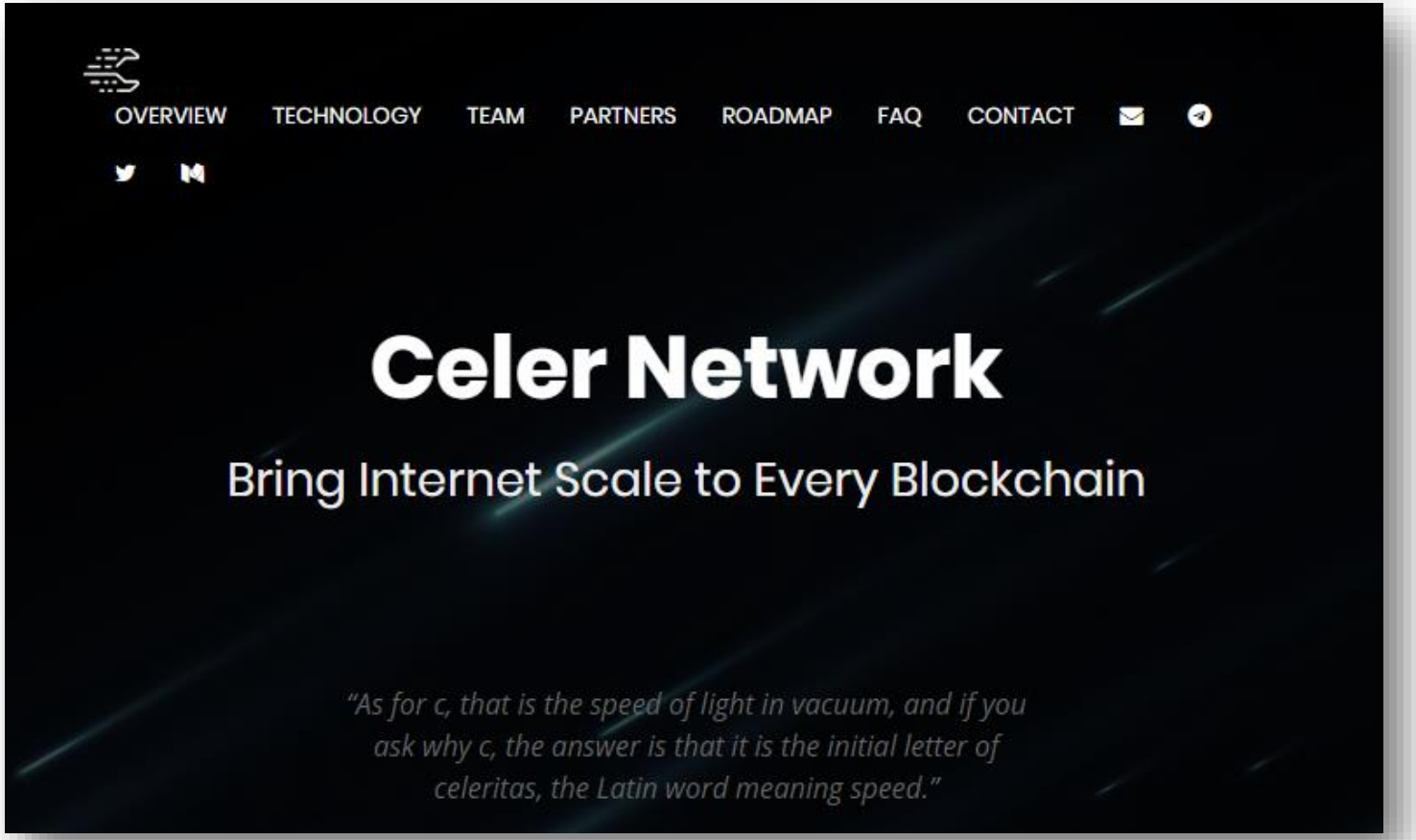
Raiden Network

- An off-chain scaling solution for the Ethereum blockchain.
- By utilizing payment channel technology, it facilitates token transfers without the need for global consensus by using digitally signed and hash-locked transfers called balance proofs.
- A Raiden balance proof is a binding agreement enforced by the Ethereum blockchain.
- Two people do not have to create a payment channel every time they transact. Instead, there must be at least one route through a network of channels that connects the two parties.

Website: https://raiden.network

Celer Network

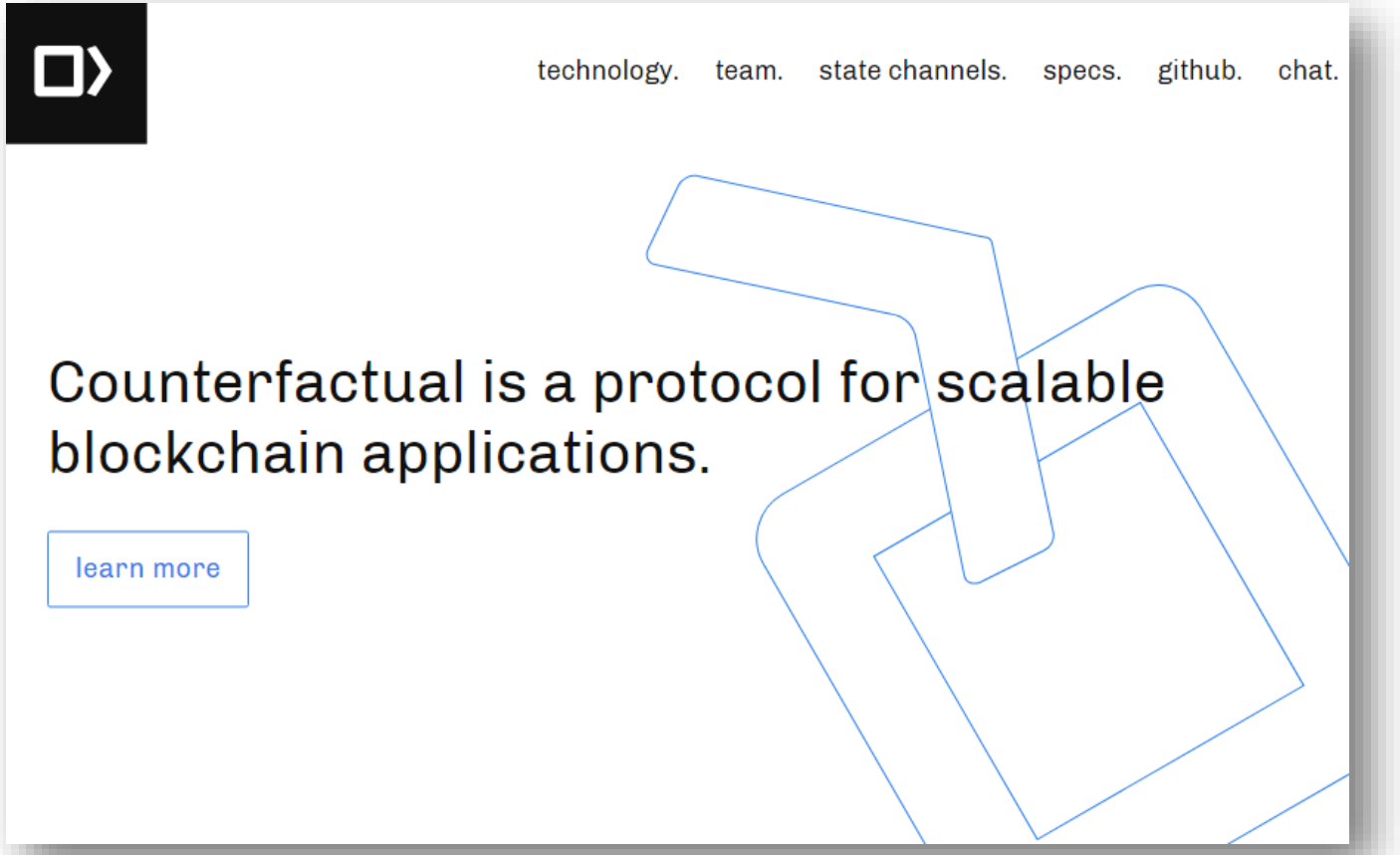
- The project is building a technology architecture that aims to bring internet scale to existing and future blockchains.
- The main part of the project is a generalized state channel that promises to be more optimal and efficient than other state channel projects. Celer Network is blockchain agnostic.



Website: https://www.celer.network

Counterfactual

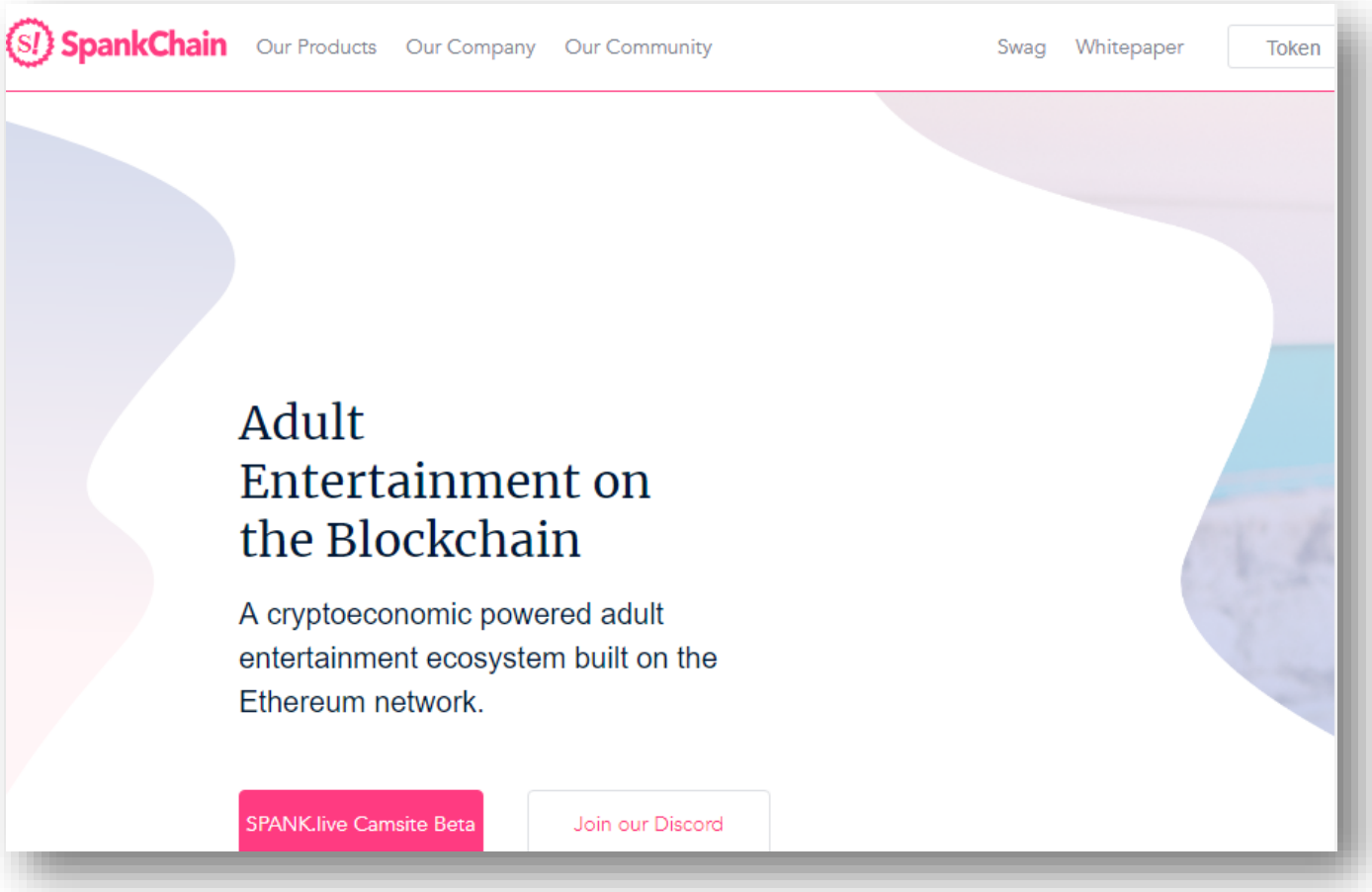
- An open-source initiative to make secure off-chain applications easy to build on Ethereum.
- The project is working on generalized state channels on Ethereum. They are focused on internally progressing the framework to an abstraction that makes developing “channelized” applications easy and intuitive.



Website: https://www.counterfactual.com

SpankChain

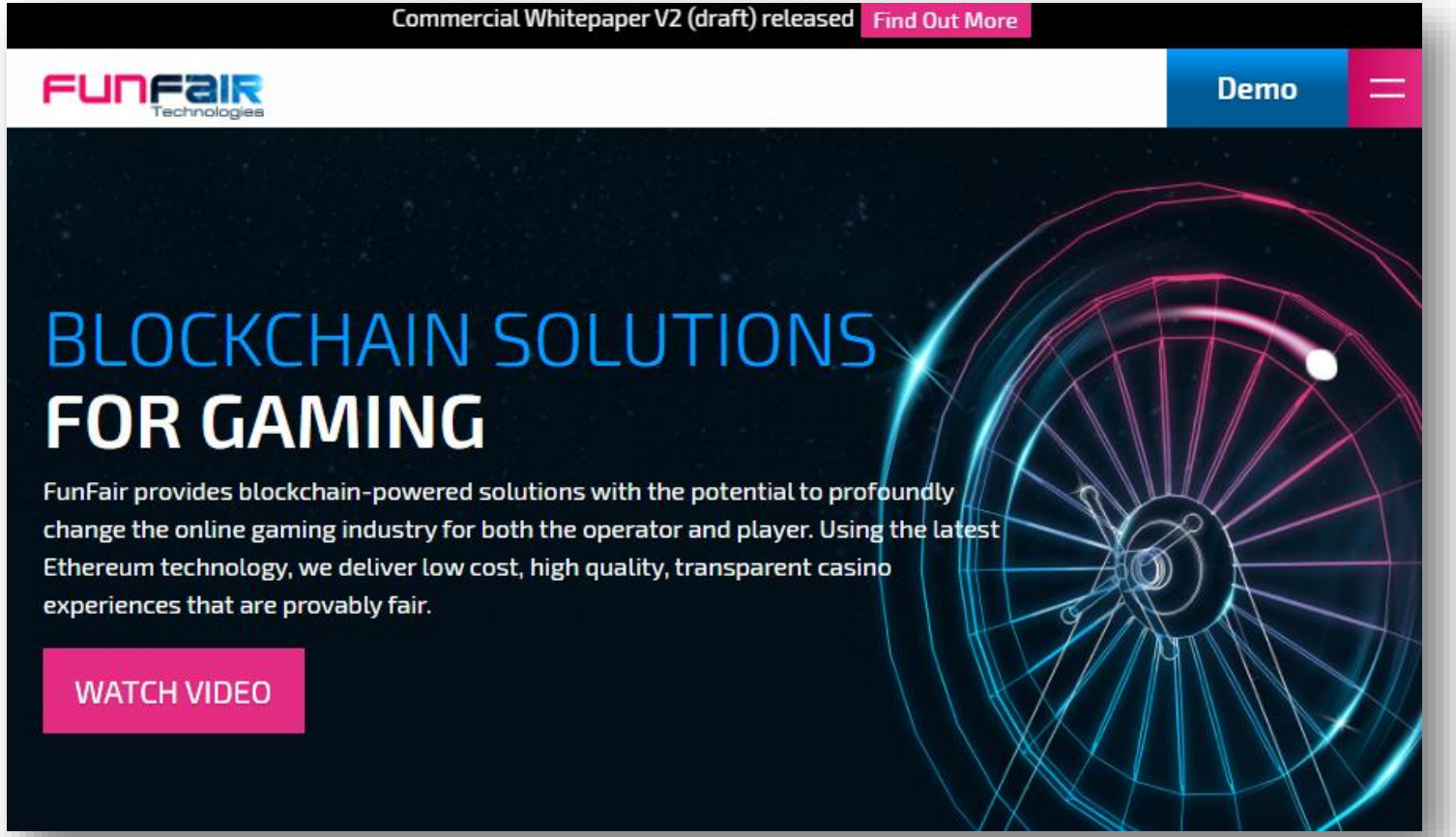
- An adult entertainment ecosystem built on the Ethereum network utilizing generalized state channels.
- Their payment channel is live on the Ethereum main-net and they conducted their token sale through a custom, single-round, blind, Dutch, state channel auction system.



Website: https://spankchain.com

FunFair

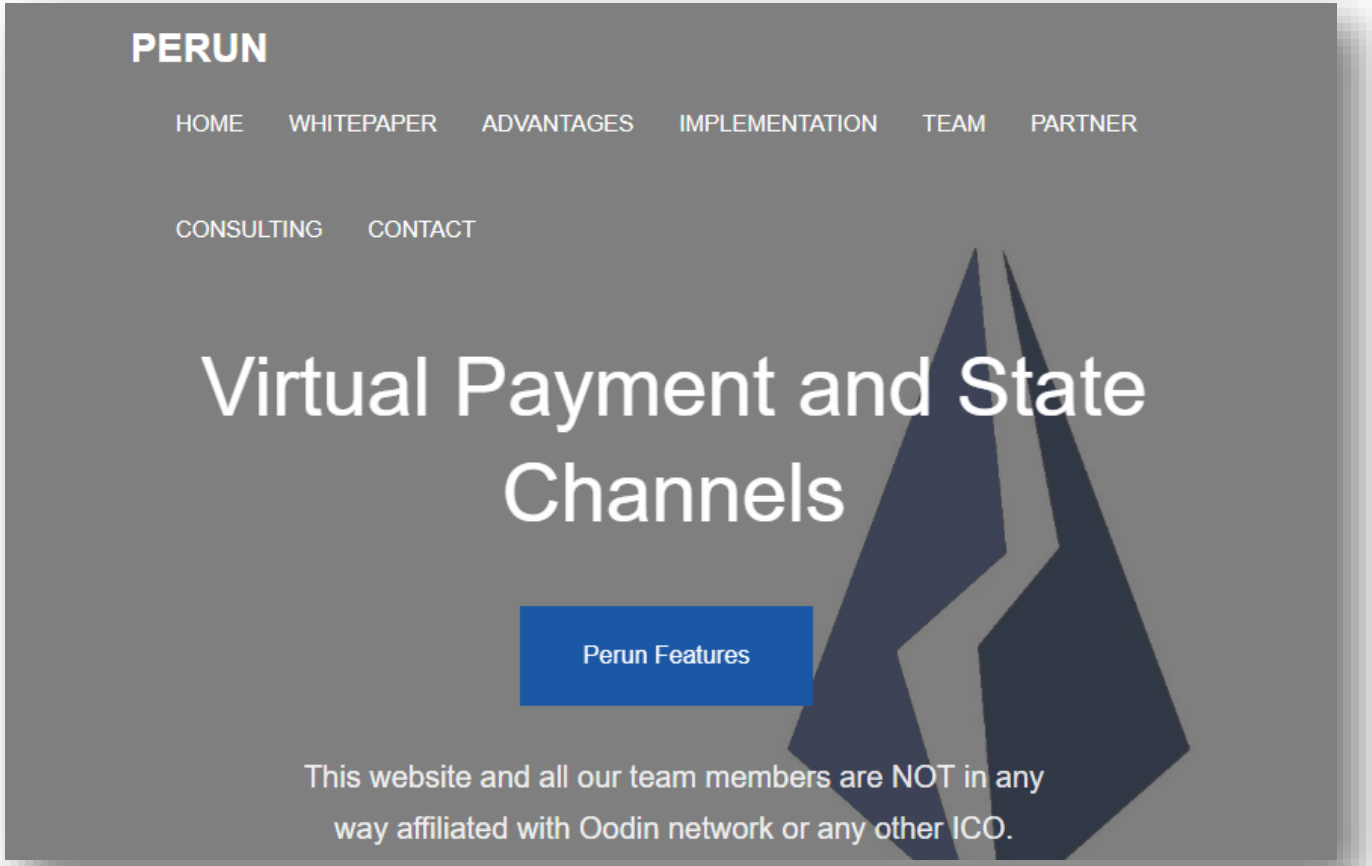
- Blockchain-powered solutions for online casino games.
- It utilizes state channels (call Fate Channel) that can produce random numbers, conduct micropayments and player interactions.



Website: https://funfair.io

Perun

- A framework supporting off-chain protocols for simple payments and generic smart contract off-chain execution.
- Perun's channels can be virtual, meaning that off-chain transactions do not require interaction with intermediaries which reduces trust, latency, and costs.



Website: https://perun.network

CrushCrypto