Darkpool - the digital asset exchange

Abstract

The market capitalization and trading volume of cryptocurrencies is growing rapidly every month. With institutional investors arriving into the cryptocurrency market, the development of alternative trading systems is critical for trading large blocks of cryptographic assets while maintaining minimal price slippage and market impact.

We live in a world of finance. Monetary incentives and market movements influence our daily decisions and define human lives in general. Under capitalism, the financial industry has become global expressing economic relations between people and institutions. Nowadays, existing wealth distribution mechanisms are inefficient and the economic environment is unstable. A lack of trust become inevitable and we are moving into the new era of decentralized finance (DeFi). Borderless, accessible and transparent interactions between participants without counterparties to transform old and inefficient financial instruments is the new paradigm of the trustless economy.

We introduce Darkpool, the first decentralized dark pool protocol bridging broad digital assets to DeFi. With interoperability in mind and solid team cross-chain expertise Darkpool blockchain will bring new markets to the Cosmos ecosystem providing users with the liquidity and the necessary fundamentals for DeFi applications and services. Trades are placed on a hidden order book and are matched through an engine built on a multi-party computation protocol. This provides order execution without exposing market sensitive information such as price and volume at a certain position, which would provide an advantage to other traders. Darkpool removes the need for a trusted intermediary to operate a dark pool and provides crypto-economic incentives through a protocol token for governance; enabling the development of a secure, decentralized, scalable dark pool protocol capable of handling billions in trading volume daily.

Introduction

The advent of blockchain technologies has enabled the development of an entirely new class of assets backed by cryptographic verification. Bitcoin (BTC) and Ethereum (ETH) are two blockchain-based cryptocurrencies which, as of eclipse the aggregate market capitalization of all other cryptocurrencies.

In November 2017, the volumes for BTC and ETH trades exceeded USD $181B (not including over-thecounter and trades executed on private forums). This statistic, coupled with the announcements of Bitcoin futures markets from CME Group and NASDAQ, signals interest from institutional investors looking to gain exposure to digital cryptographic assets. With institutions and HNWIs looking to deploy vast amounts of wealth into cryptocurrencies, we must develop the underlying infrastructure to support such volumes.

At a fundamental level, dark pools are private exchanges where financial assets and instruments are traded and matched by an engine running on a hidden order book. These exchanges are primarily created to serve institutional or HNW retail investors who require a system where significant volumes of assets can be block traded with minimal price slippage. Dark pools are estimated to represent approximately 15% of all trading volume of all US stock trades [6]. Extrapolating this statistic for BTC and ETH volumes, a dark pool for such has the potential to execute USD $27.2B of orders monthly. We introduce the Darkpool Protocol which facilitates the exchange of Ethereum, ERC20 and Bitcoin cryptocurrencies through a decentralized dark pool. This is enabled through research within subfields of cryptography such as secure multi-party computation, which allow us to develop a matching engine to run on the distributed hidden order book. We facilitate cross-chain trades through atomic swaps and implement proper economic incentives to ensure these trades are executed thoroughly. Compared to a centralized dark pool or exchange, the Darkpool Protocol removes the risk of asset theft, confiscation or possibility of interference from a malicious exchange operator. This leads to greater trust between institutional investors placing block orders and dark pool exchanges leveraging the Darkpool protocol. Additionally, the Darkpool Protocol is available universally and is highly transparent with regards to how the underlying protocol operates.

The Inception of 5G

5G, the fifth-generation mobile network, is hundreds of times faster than 4G. As the media industry that is very depending on technology, 5G is exerting a profound impact in the big data industry whether it is the construction of a modern communication network with a high starting point for radio and television for the transformation of the film and television chain, or the promotion of the integration of traditional blockchain multi-node technologies.

Due to the three characteristics of 5G technology: ultra-high speed, ultra-large connections and ultra-low latency, with the advent of 5G era, the production mode and reception mode of blockchain trading data transmission will change accordingly. The restriction and limitation of network speed will also be reduced gradually. Decentralized exchange will benefit directly from this and become the form of basic life consumption from people. Therefore that will become the main force of data transmission. Decentralized exchange will also benefit from 5G and face in a new round of outbreak.

The decentralized exchange industry is currently in at the dawn time of development. With the acceleration of increasing growth in defected centralized exchange, the loss of assets raised by those deceptive promotions for the traditional exchange. However, decentralized exchange are played well in data transparency on trading safety yet it requires large amount of bandwidth to support the usability, 5G technology is giving right at the good use case to opening this DEX era.

In the mean time, the BPOS industry has become an ocean market for high-quality investors moving into the DEX, and among which the best have made incredible profits in a short time with the fair trading mechanism. Over the growth of trending financial technology will benefit the participants and among which the best have made unimaginable huge profits in a short time.

Elementary Components

- Decentralized hidden order book
  - A decentralized, hidden order book.
- Decentralized order matching
  - Matching orders without knowing the underlying details
- Atomic swap infrastructure
  - The ability to swap between Bitcoin, Ethereum and Ethereum-based tokens without trust.
- Protocol token
  - The DAP token

Motivation

- Infrastructure for block orders
- Cross-chain trades
- Trustless, equitable access to dark pools
- Centralization risk

Darkpool Protocol

How the Darkpool Protocol works

The primary technical goal of the Darkpool Protocol is to enable a decentralized network of nodes to

match orders, without knowing anything about the orders. While it might seem like this is impossible, it can be achieved by applying cryptographic techniques that have been thoroughly researched over that last 30 years; modifying them to be suitable for the world of decentralized computation.

The Darkpool Protocol uses the BPOS [1] to break down orders into a large number of order fragments, and distributes them throughout the network. Orders cannot be reconstructed unless a majority of the order fragments are recombined. To prevent this from happening, the Darkpool Protocol defines in the native chain mechanism called the Registrar that organizes nodes into a network topology that makes it unreasonably difficult for an adversary to acquire the enough of the order fragments to reconstruct an order. As long as traders respect the network topology defined by the Registrar, their orders will be safe. If they fail to do so, only their own orders are at risk of exposure. Using order fragments from two different orders, a node can cooperate with other nodes that hold other order fragments for the same two orders to perform a decentralized computation that will determine if the two orders match. The decentralized computation does not expose the order fragments, and performs a random scaling of the final output [2][3]. This prevents nodes from reconstructing the original orders, and prevents them from using the output to infer anything about the orders. A Zero knowledge proof is used to verify the integrity of the computation, without revealing any information. These proofs are simple and efficient, allowing them to be performed by an public chain called the bonds [3]. After two orders have been matched, an atomic swap is initiated between the two traders over the Darkpool Hub Network, a decentralized peer-to-peer network. Using standard asymmetric encryption primitives, the details of the atomic swap are kept secure.

System Properties

The Darkpool Protocol provides the following properties:

1. The identity of the traders is secure within the Dark Pool. The underlying cryptocurrency that is being traded may provide different limitations for privacy.
2. Traders do not have to remain connected to the network while their orders are being matched. Once an order is placed, nodes will run the matching computation until a match is found, or the order is expired (either manually, or by passing a deadline designated by the trader).
3. An order is secure until it is matched. After being matched, some details of the order are revealed to the matching parties. This is the natural limit of security for an order, since both parties know what they submitted, and both parties need to know when a match has occurred. Note that information disclosed in these cases does not provide any informational advantage to either party.
4. The total liquidity of the Darkpool cannot be reasonably estimated by any participant.

Assumptions

The Darkpool Protocol is built on the following assumptions:
I. There exists a trusted third-party that will always perform computations honestly, but has limited computational power (i.e. 21 supernode consensus).
II. Participants act rationally and will not participate if there is no financial incentive to do so, and will attempt to maximize their own profit. In this way, we do not assume that a participant will act honestly if they can maximize their profit by acting maliciously.

Adversarial Assumptions

The Darkpool Protocol makes the following adversarial assumptions:
I. Adversaries cannot corrupt the trusted third-party defined previously by Assumption (II). Concretely, an adversary cannot subvert the correctness of computations done by the Darkpool network. All platforms built on Darkpool need to make this adversarial assumption.
II. Adversaries have limited financial, and computational, powers. Limited financial powers are a reasonable assumption to make in the real world, and computational powers are naturally limited by financial powers.
III.Computationally hard problems used to construct cryptographic primitives are sufficiently secure. This assumption is made by all blockchains that utilize any form of cryptography, including Bitcoin and Ethereum.

Security Model

Defining a security model allows us to analyze the security guarantees provided by the Darkpool Protocol. The Darkpool Protocol makes use of the real vs. ideal paradigm; analyzing the security of a real world decentralized protocol with respect to some non-existent ideal world in which there is a trusted, and incorruptible, third-party that can be used to handle all sensitive information and perform all sensitive computations (this is not the same as Ethereum, since all transactions and data on Ethereum is publicly available). The security of the Darkpool Protocol can be demonstrated by showing that any possible attack in the real world is also possible in the ideal world. Since the ideal world is trivial to define, the real protocol is secure by implication. This approach to security analysis is typical for decentralized computation protocols in which there are active and passive adversaries. The ideal Darkpool Protocol contains a trusted, and incorruptible, third-party T. Traders submit their orders to T, and T guarantees to never reveal the details of these orders. T constantly attempts to match orders that have been submitted, and when a match is found T informs the respective traders. The traders each submit their cryptocurrencies to T, and if they both do so, T swaps the cryptocurrencies and gives them back to the traders. This completes the trade. The real Darkpool Protocol is considered secure if, and

only if, all attacks on the real protocol are also possible on the ideal protocol. From the definition of the ideal Darkpool Protocol it is clear that such an equivalence is sufficient.

The Darkpool Protocol is able to guarantee that, unless the majority of nodes in the network are active adversaries, it is as secure as the ideal world protocol. If 50% of nodes are active adversaries, and they are enjoying the attackers best-case scenario, they are able to reconstruct all orders. However, the Darkpool Protocol ensures that such a best-case scenario is impossible to achieve in the real world. In the typical case, 50% of nodes becoming active adversaries would only allow the adversaries to reconstruct 50% of the orders. A more detailed explanation is given in “Attacks and Defenses”.

Decentralized Order Matching

Order matching is the process through which nodes match orders against each other without being able to observe the details of the order. To achieve this, traders first breakup their order into a set of order fragments. Note that these fragments do not individually represent a fraction of the order’s value, they simply represent the separation of sensitive data regarding the underlying order. On its own an order fragment reveals nothing about the underlying order, but when at least half of the order fragments for an order are combined, the order can be reconstructed (see “Attacks and Defenses” for details about protecting against this). Each node performs an order matching computation on order fragments from multiple different orders and combines the results with the results from nodes (who are using different fragments). The fragments are constructed in such a way that, after the computations are applied, the resulting fragments can be combined to reveal, not the underlying orders, but the result of the order matching computations for the underlying orders.
This has several nice properties. For one, only half of the order fragments are needed to reconstruct an order. Nodes are incentivized to avoid collusion (and adversaries have a difficult time subverting this system, see “Attacks and Defenses”). This means that if half of the nodes accidentally die, or leave the network halfway through an order matching computation, the network can still finish the computation.

This makes it highly resilient to DDoS attacks, and expected failures.

Order fragments are constructed in such a way that the order matching computations can use any function, applied over a polynomial, and can be involve two or more underlying orders. This allows for very flexible order matching computations. Nodes can match orders based on exact price points, partially match orders (when only some of an order can be matched due to the currently available liquidity), match triplets (or more) of orders to increase liquidity (e.g. the

triplet BTC-to-ETH and DOLLAR-to-DAP and DAP-to-DOLLAR, where no match can be found with only pairs). Assuming the existence of a decentralized, consensus-based, data stream for National Best Bid and Offer (NBBO) data, the order matching computations can even involve orders without an explicit price point.

Winning and Losing

Nodes race to discover order matches. Any match that is found must be registered so that other nodes can see which orders have been closed. The associated traders are notified, and none of the matched orders can be involved in future matches. This is done on the Darkpool network, under Assumption (1). If two orders do not match, they continue to be used in future matching games. If an order cannot be matched before it expires, the associated fee is refunded. The nodes that combine their outputs to register a match are rewarded a fee, to incentivize their honest participation in the order matching game (see “Incentive Layer”). This also incentivizes them to match as many orders as quickly as possible, since this correlates to a higher reward over time. The Darkpool Protocol also includes an Atomic Swapping protocol that is initiated between traders that have had their orders matched. Nodes facilitate passing messages (and where possible, setting up a direct P2P connection between traders) that executes the order. Note that traders cannot be bound to execute on the orders, due to the limited way in which blockchains can communicate (see “Attacks and Defenses” for information about placing false orders). However, using trader bonds, traders can be heavily incentivized to faithfully execute orders.

At no point during order matching, or even after orders have matched, are Darkpool Protocol nodes capable of revealing the details of an order. Even if a malicious adversary is capable of performing a 51% attack, the order fragments are distributed in such a way that the adversary is only able to reconstruct 50% of the orders (the higher attack percentage they achieve, the higher the rate of order reconstruction).

DAP Tokens

Under Assumption (II), computational nodes must be incentivized to perform the order matching computations. It is unlikely that participants will be willing to run order matching nodes if they have no financial incentive to do so, especially when running and maintaining order matching nodes is not free. The DAP token is introduced to provide this incentivization. It is also used to pay bonds to the Registrar, allowing traders and order matching nodes to participate in the Darkpool.

Order Fees

Fees provide a decentralized mechanism for the users of the system (i.e. traders) to remunerate those that are providing the computational power (i.e. nodes) necessary to fulfill the needs of the users. This is necessary under Assumption (II). Traders pay an order fee, in DAP, when submitting an order. If the order expires before it is matched, the order fee is refunded to the trader. Any node that participates in the decentralized computation for an order that has been matched receives a share of the order fee (the shares are calculated by evenly splitting the order fee amongst all of the participating nodes). The order fee is variable, and under Assumption (II), orders with higher order fees will be favored by the order matching nodes. However, nodes have no incentive to ignore an order, especially since they do not know the identity of the trader, nor the details of the order. The only information available to the node is the amount of DAP that they will receive for successfully matching this order. Note, all order matches will actually result in two payouts to each participating node, one from each side of the match.

Bonds

Orders are secured by breaking them down into several order fragments that are distributed throughout the network. An adversary attempting to reconstruct orders could join the network with a large number of nodes in the hope that they will receive the majority of the order fragments (we will see later that this is
not actually feasible). Similarly, an adversary could submit a large number of false orders (that they do not intend to execute on) in an attempt to probe the legitimate orders. To prevent this class of Sybil attacks, and provide a simple identity mechanism, traders and nodes must submit a bond in DAP before they are allowed to access the network. This bond is associated with a single identity in the Registrar smart contract and the registration status can be queried by anyone. The bond is refunded in full when the trader or node leaves the network. Traders are free to submit a flexible bond, with higher amounts allowing a higher number of parallel open orders (the larger the financial bond, the harder it is to perform a Sybil attack, and so more orders can be submitted safely).

Nodes must submit a bond in DAP higher than some globally defined threshold (this threshold can be set as needed, to keep the bond requirement above a sufficiently large financial commitment). Since this threshold is dynamic, nodes can alter the bond amount however they choose but will not be able to participate unless their bond is above the threshold. During verification, the Challenger and the Provers (usually the trader and a group of order matching nodes, respectively) put their bond on the line. If the Challenger is correct, the Prover that is unable to provide evidence of a truthful computation loses their bond. Likewise, if all Provers are correct, the Challenger loses their bond. In this way, the DAP bond also acts as a disincentive to attempt to cheat.

Attacks and Defenses

Order Reconstruction

The security of an order maintained as long as n/2 of its n order fragments are not discovered by an adversary. If an adversary does acquire n/2 (or more) order fragments, the original order can be reconstructed. As such, it is important to understand the defenses in place against such an attack.

Nodes in the Darkpool are partitioned into n disjoint sets, where each order share is randomly distributed to at most two nodes in any one set. To model an attack on this topology, we assume that the adversary has full control over which nodes to corrupt (the Darkpool Protocol enforces that nodes are actually randomly distributed amongst the disjoint sets, meaning that this assumption provides the adversary with more power than they have in reality).

The ideal attack scenario would be where an adversary corrupts all of the nodes in n/2 sets, guaranteeing that n/2 order fragments will be acquired for every single order. Assuming an approximately uniform size of each pool, the adversary must control 50% of the network. Note that it is impossible for an adversary to control in which set their nodes will be registered, making this type of attack impossible.

Realistically, when controlling 50% of the network, the adversary is most likely to control 50% of the nodes in all of the n disjoint sets. At this level of control, an adversary has a 0.5 probability of successfully acquiring each order fragment but must successfully acquire n/2 order fragments to know the order. We can model this as a binomial distribution.

Let X be the number of successfully acquired order fragments, p be the probability of acquiring any one order fragment, and n be the number of attempts that the adversary has for any one order fragment.

$$X \sim B(n, 0.5)$$

Because *X* is binomially distributed with a 0.5 probability of success. It follows that,

$$= 1 - \sum_{i=0}^{n/2} C_k^n \, p^i (1-p)^{n-i}$$

$Pr(X \geq n/2) = 1 - Pr(X < n/2)$

This formulation relies on n, the number of disjoint sets, which is directly proportional to the number of nodes in the Darkpool.

$$\lim_{n \to \infty} 1 - \sum_{i=0}^{n/2} C_k^n \, p^i (1-p)^{n-i}$$

$$= 0.5$$

As the number of nodes in the Darkpool grows, the probability that an adversary is able to reconstruct a single order approaches 0.5. This implies that an adversary that somehow manages to corrupt 50% of the network only manages to discover 50% of the orders.

False Orders

When two orders are matched, both of the matching parties learn that there exists some corresponding order in the Darkpool (otherwise a match would not have occurred). An adversary can take advantage of this in an attempt to gain insight into the liquidity of the Darkpool.

Assume that there are n legitimate orders in the dark pool when there is no adversary. To simplify the analysis we also assume, in the favor of the adversary, that the adversary knows the maximum price point of orders in the dark pool (realistically, this is impossible and the adversary would have to make several guesses).
If we assume that none of the legitimate orders have matches, the adversary needs to submit n false orders (at the maximum price point) to discover all orders. Compared to the fees paid by the rest of the network, the adversary needs to match 100% of the financial commitments to order fees made by the network. By Assumption (II) this is not realistic, and becomes more and more difficult as the Darkpool is used.

Now we assume that each of the n legitimate orders has exactly one legitimate match, and an attacker has a way of distributing their order fragments in such a way that their false orders are instead matched with a p=50% probability. Again, this assumption is in favor of the adversary, since they cannot actually know how to perform such a distribution.

For a binomial distribution with corresponding probability of success , the probability of exactly successes given trials is given as

$$\frac{n!}{k!(n-k)!}p^k(1-p)^{n-k}$$

For example, if n=100 and p=0.5, then the probability is approximately 54%. This shows that only with a substantial commitment to order fees compared to the network as a whole, along with many favorable assumptions, is an adversary able to gain insight into the liquidity of the dark pool.
This analysis does not take into account that there is a limited number of orders that can be submitted by any one trader. To submit a large quantity of false orders a trader would also need to stake a large amount of financial power into bond registrations.

Future versions will also discuss methods by which traders must forfeit their bond if they do not execute on false orders. Taking these three parts of the analysis into account: the high amount of order fees required to gain insight into the dark pool, the high amount of bond required to submit that many orders, and the high amount of bond sacrificed when false orders are not executed, Adversarial Assumption (II) prevents adversaries from being able to expose the liquidity of the dark pool by submitting false orders.

Sybil Attacks

In the Darkpool Protocol, defending against order reconstruction attacks (and false order attacks) requires associating an identity with a node (or trader). This opens the possibility for an adversary to forge multiple identities, known as a Sybil attack, in an attempt to subvert the network.

To protect against this, all nodes and traders are required to commit a bond in order to register an identity. Under the Adversarial Assumption (2), adversaries have limited financial power, we can be sure that an adversary cannot forge a large number of identities.

For malicious nodes, the bond needs to discourage the registration of a large number of nodes and the acquisition of a sufficiently large number of order shares during the distribution of order shares (see “Order Reconstruction”). For this method to be effective, the bond must be high

enough that an adversary cannot register a large number of nodes, but small enough that honest nodes are still able to participate.

The bond amount should be globally consistent (all nodes must meet the same threshold) but dynamic, to account for fluctuations in the value of the bonded currency. For malicious traders, the bond can be used to further discourage the submission of a large number of false orders (see “False Orders”). This is done by requiring that a trader submit orders that point to their registered bond. There is a linear relationship between the bond amount, and the maximum number of orders. Therefore, a trader that submits a bond of B and is allowed M open orders could instead submit a bond of B/2 and be allowed M/2 open orders. The registration of bonds will be handled by the Ethereum network, and are incorruptible by Assumption (1).

Darkpool Terminal

We introduce a web-based decentralized application (DApp) for traders to interface with the Darkpool Protocol. This real-time terminal provides traders with the capability to place, cancel or amend orders. Users can also view the status and history of their orders, visible only to themselves.

Economics and the Dollar Reserve

When the Darkpool Association released its ideas for the operations of the Dollar Reserve, the document was intended to be a proof of concept rather than a finished roadmap for the project. Since June 2019, we have met with many different organizations, regulators, policymakers, and academics to understand key concerns and integrate actionable improvements into the economic design of the Darkpool network. These consultations and meetings around the world have been invaluable in informing our direction. In particular, the Association greatly appreciates the thorough and thoughtful research the G7 working group completed on stablecoins. The concerns raised in the report helped highlight immediate questions to be answered, as well as longer-term challenges that may emerge.

A key concern that was shared was the potential for the multi-currency Dollar Coin (DOLLAR) to interfere with monetary sovereignty and monetary policy if the network reaches significant scale in a country (i.e., DOLLAR becomes a substitute for domestic currency). While we believe this is unlikely because DOLLAR introduces foreign exchange exposure for coin holders in domestic transactions and the use of DOLLAR may be subject to restrictions, such as foreign exchange controls, we take this concern seriously.

The Darkpool network is designed to be a globally accessible and low-cost payment system — a complement to, not a replacement for, domestic currencies. The stabilization of currencies and value preservation are key efforts that are properly within the exclusive remit of the public sector. Therefore, we are augmenting the Darkpool network by including single-currency stablecoins (e.g., DOLLAR, CNY, HKD, EUR, etc.) and planning to increase the number of single-currency stablecoins over time. These will enable a range of domestic use cases by giving people and businesses the ability to transact in a stablecoin denominated in their own currency. Each single-currency stablecoin will be supported by a Reserve of cash or cash-equivalents and very short-term government securities denominated in that currency and issued by the home country of that currency. Single-currency stablecoins will only be minted and burned in response to market demand for that coin. Because of the 1:1 backing of each coin, this approach would not result in new net money creation.

What is Proof of Stake (PoS)?

If you know how Bitcoin works, you're probably familiar with Proof of Work (PoW). It's the mechanism that allows transactions to be gathered into blocks. Then, these blocks are linked together to create the blockchain. More specifically, miners compete to solve a complex mathematical puzzle, and whoever solves it first gets the right to add the next block to the blockchain.

Proof of Work has proven to be a very robust mechanism to facilitate consensus in a decentralized manner. The problem is, it involves a lot of arbitrary computation. The puzzle the miners are competing to solve serves no purpose other than keeping the network secure. One could argue, this in itself makes this excess of computation justifiable. At this point, you might be wondering: are there other ways to maintain decentralized consensus without the high computational cost?

Enter Proof of Stake. The main idea is that participants can lock coins (their "stake"), and at particular intervals, the protocol randomly assigns the right to one of them to validate the next block. Typically, the probability of being chosen is proportional to the amount of coins – the more coins locked up, the higher the chances.

Staking selection process

This way, what determines which participants create a block isn't based on their ability to solve hash challenges as it is with Proof of Work. Instead, it's determined by how many staking coins they are holding.

Some might argue that the production of blocks through staking enables a higher degree of scalability for blockchains. This is one of the reasons the Ethereum network is planned to migrate from PoW to PoS in a set of technical upgrades collectively referred to as ETH 2.0.

What is Delegated Proof of Stake (DPoS)?

An alternative version of this mechanism was developed in 2014 by Daniel Larimer called Delegated Proof of Stake (DPoS). It was first used as a part of the BitShares blockchain, but soon after, other networks adopted the model. These include Steem and EOS, which were also created by Larimer.

DPoS allows users to commit their coin balances as votes, where voting power is proportional to the number of coins held. These votes are then used to elect a number of delegates who manage the blockchain on behalf of their voters, ensuring security and consensus. Typically, the staking rewards are distributed to these elected delegates, who then distribute part of the rewards to their electors proportionally to their individual contributions.

The DPoS model allows for consensus to be achieved with a lower number of validating nodes. As such, it tends to enhance network performance. On the other hand, it may also result in a lower degree of decentralization as the network relies on a small, select group of validating nodes. These validating nodes handle the operations and overall governance of the blockchain. They participate in the processes of reaching consensus and defining key governance parameters.

Simply put, DPoS allows users to signal their influence through other participants of the network.

How does staking work?

As we've discussed before, Proof of Work blockchains rely on mining to add new blocks to the blockchain. In contrast, Proof of Stake chains produce and validate new blocks through the process of staking. Staking involves validators who lock up their coins so they can be randomly selected by the protocol at specific intervals to create a block. Usually, participants that stake larger amounts have a higher chance of being chosen as the next block validator.

This allows for blocks to be produced without relying on specialized mining hardware, such as ASICs. While ASIC mining requires a significant investment in hardware, staking requires a direct investment in the cryptocurrency itself. So, instead of competing for the next block with computational work, PoS validators are selected based on the number of coins they are staking.

The “stake” (the coin holding) is what incentivizes validators to maintain network security. If they fail to do that, their entire stake might be at risk

While each Proof of Stake blockchain has its particular staking currency, some networks adopt a two-token system where the rewards are paid in a second token.

On a very practical level, staking just means keeping funds in a suitable wallet. This enables essentially anyone to perform various network functions in return for staking rewards. It may also include adding funds to a staking pool, which we’ll cover shortly.

Liquid Proof-of-Stake (LPoS)

In LPoS, delegation is optional. Token holders can delegate validation rights to other token holders without custody, meaning that the tokens remain in the delegators’ wallet. Additionally, only the validator is penalized in case of security fault (e.g. double-endorsing or double-baking). LPoS also offer voting rights, except that as a token holder you get to vote directly in the protocol amendments, and not only in who secures the network like in DPoS.

LPoS was first introduced by Tezos, an on-chain governance protocol, created by Kathleen and Arthur Breitman, which has been running smoothly in mainnet since September 2018. LPoS in Tezos has proven to be very successful, with a current stake rate of approximately 80% spread across 450 validators and 13,000 delegators. The number of delegators is technically limited by the bond size minimum requirement, and with current parameters could go up to around 70,000—Great decentralization □.

Bonded Proof-of-Stake (BPoS)

BPoS is very similar to LPoS: delegation is optional, non-custodial, and token holders benefit from voting rights in protocol amendments. Although, there is a reason why it is called BPoS: in case of safety or liveness fault, a portion of the validators and delegators’ stake will be slashed. In LPoS, only the validator is at risk of slashing, while the delegator’s only risk is to miss on some rewards/interests in case its validator is dishonest or not efficient.

This BPoS mechanism has the advantage of providing a clear solution to the issue of staking ratios (similar to capital requirements) that some validators on LPoS protocols have to maintain if they do not want to become over-delegated and disappoint some of their delegators. While it solves this issue, it also means that delegators need to conduct extra due diligence before delegating, and remain active in verifying the performance of their validator.

BPoS was first introduced by projects such as Cosmos and IRISnet (which build on the Cosmos SDK / Tendermint). Both are very interesting inter-chain protocols to have a look at □. We've written a short introduction to IRISnet if you are curious. In BPoS protocols such as Cosmos and IRISnet, there will be a limited number of validators, starting at 100, with selection based on the size of their total stake (own stake + delegations).

Entrothy

We believe this approach can lower costs and enable new functionality while giving maximum flexibility and control to the Darkpool network for how the Darkpool payment system is used in their countries. The creation of DOLLAR has needs to be defined by active circulations from the Darkpool network and the DOLLAR must be minted by a fixed calculation and it is defined as entropy. The active serving amount for staking validator with DAP can be burned for the amount of DOLLAR to be entropied. This consensus mechanism allows the external liquidation providers to swap DOLLAR with USDT. As the result, the increase of price in DAP makes entropy of DOLLAR which is backed by ERC20 USDT with 1:1 peg to USDT playing role of a hedge against a bear market or a true mean of exchange without explicit volatility. It allows decentralized stablecoin to take part in broader financial applications like decentralized exchanges and financial marketplaces, creating a wide space for DeFi development.

De-centralized governance and ownership

The most exciting part is that everyone can participate in the project's evolution and own a share of the network. All participants who stake native token DAP will be rewarded for effective governance depending on transaction fees, total supply emission and repaid loan fees. Darkpool ecosystem is designed with existing assets like BTC or XRP in mind. If we assume that just 1% of BTC will take part in DeFi it will result in more than 1,5 billion USD value injection also adding to a scarcity of BTC positively influencing the cryptocurrency market in general.

Circulations

Initially, the Association expects to offer a small number of single-currency stablecoins based on the presence of highly liquid and safe government securities markets in the relevant currencies. We hope to work with regulators, central banks, and financial institutions around the world to expand the number of single-currency stablecoins available on the Darkpool network over time and to explore the technical, operational, and legal requirements to access direct custody with them. In particular, if adoption in a region without a single-currency stablecoin on the network generates concerns about currency substitution, then the Association could work with the

relevant central bank and regulators to make a stablecoin available on the Darkpool network. The Association welcomes feedback on how it can help support local monetary and macroprudential policies.

Transfer

For countries that do not have a single-currency stablecoin on the Darkpool network, we believe DOLLAR is a neutral and low-volatility alternative that could ensure users in such regions can benefit from accessing the network and increased financial inclusion. In this context, DOLLAR could operate as a settlement coin in cross-border transactions, and people and businesses could convert the DOLLAR they receive into local currency to spend on goods and services through third-party financial service providers. For example, consider a Darkpool user in the US wanting to send money to their family in another country. The sender in the US would likely use DOLLAR as their default Darkpool stable coin to make the transfer. If the receiver lives in a region with a different single-currency stablecoin on the Darkpool network, the sender could transfer that single-currency stablecoin or the receiver could convert USDT to that single-currency stablecoin or local currency through a third-party financial service provider, providing a convenient and simple option for the receiver to access and use the funds. If a single-currency stablecoin is not available, the transfer could be made in DOLLAR. The receiver could convert DOLLAR into their local currency through a third-party financial service provider to buy goods and services in that currency. The Darkpool network would not itself provide for, record, or settle conversions between Darkpool Coins and fiat currency or other digital assets; instead, as noted, any such exchange functionality would be conducted by third-party financial service providers. Regardless of the region, we expect to require all Virtual Asset Service Providers (VASPs), such as currency exchanges that have addresses on the Darkpool Blockchain to hold and transfer Darkpool Coins, to fully comply with all applicable foreign exchange limitations and capital controls in order to mitigate currency substitution risk.

Moreover, our hope is that as central banks develop central bank digital currencies (CBDCs), these CBDCs could be directly integrated with the Darkpool network, removing the need for Darkpool Networks to manage the associated Reserves, thus reducing credit and custody risk. As an example, if a central bank develops a digital representation of the US dollar, euro, or British pound, Hong Kong dollar the Association could replace the applicable single-currency stablecoin with the CBDC.

Single-currency stablecoins simplify the design of DOLLAR. DOLLAR can be implemented as a smart contract that aggregates single-currency stablecoins using fixed nominal weights (e.g., DOLLAR 0.50, EUR 0.18, GBP 0.11, etc.). This approach to the DOLLAR design is similar to what is used by the International Monetary Fund (IMF) in the Special Drawing Rights (SDR). Because DOLLAR is composed of fixed amounts of single-currency stablecoins that are supported by the network, DOLLAR is fully backed by the Reserve assets backing each single-currency stablecoin.

The Darkpool network is intended to support global, cross-border exchanges by extending the functionality of fiat currencies, which are appropriately under the governance and control of the consensus BPOS. Under this new approach, we seek to reduce concerns around monetary sovereignty and help usher in more accessible payments and financial products for people and businesses around the world.

The Darkpool Reserve and protections

A key objective of the Darkpool network's economic design is building trust in an efficient payment method. Each stablecoin on the Darkpool network will be fully backed by a Reserve of high-quality liquid assets and supported by a competitive network of resellers and exchanges buying and selling each coin. That means that Darkpool Coin holders should have a high degree of assurance they can convert their Darkpool Coins into local currency.

Custody and Designated Dealers

The assets comprising the Reserve will be held by a geographically distributed network of well-capitalized custodian banks to provide both security and decentralization of the assets. We expect that these institutions will already have a number of risk mitigation practices in place. The Association proposes to put additional measures in place with these custodians that are designed to ensure that Reserve assets cannot be used for lending, pledging or repledging, or otherwise be removed, even temporarily, from the Reserve's account or encumbered to secure an obligation of a custodian unrelated to the custody services provided to Darkpool Networks.

Darkpool Networks will not directly interface with consumers, but will instead partner with a select number of Designated Dealers to extend liquidity to consumer-facing products, such as wallets and exchanges. These Designated Dealers will commit to making markets within tight spreads and will be able to accommodate high volumes of trading. If extreme circumstances occur and Designated Dealers no longer make markets in Darkpool Coins, Darkpool Networks will call on a pre-existing arrangement with a third-party administrator or dealer to assist, in an administrative capacity, in burning Darkpool Coins for end users and liquidating assets comprising the Reserve to make payment as appropriate. These emergency operations will always be implemented under the guidance of the consensus government.

Inter-blockchain Communication Protocol (IBC) is a reliable and secure method for any DP-SDK based blockchain to communicate. At a fundamental level, the IBC is responsible for relaying 'packets' from one blockchain to another while abstracting away from the complexity of maintaining the connection, data integrity and real-time communication from the application developer. Recently, Cosmos has released the IBC spec, a relayer implementation and

example code for building cross-chain applications. While the IBC spec is full of technical concepts and jargon, you do not need to understand how the IBC is implemented on the protocol level — the DP IBC implementation already abstracts away most of the complexity. In fact, application developers only need to understand two key components to work with IBC:

1. Packets

A particular data structure with sequence-related metadata (defined by the IBC specification) and an opaque value field referred to as the packet data (with semantics defined by the application layer, e.g. token amount and denomination)

2. Relayer Process

A relayer process is an off-chain process responsible for relaying IBC packet data & metadata between two or more machines by scanning their states & submitting transactions.

Band Protocol is a cross-chain data oracle platform built on the DP-SDK that aggregates and connects real-world data and APIs to smart contracts. Blockchain smart contract is great for immutable storage and deterministic, verifiable computations — however, they still cannot access data and APIs available outside the blockchain networks. Band Protocol enables smart contract applications to be built on-chain with full flexibility for developers to specify their data type, data sources, and aggregation method without relying on the single point of failure or a centralized oracle.

Here are some examples of DeFi applications that you can build using IBC & Band Protocol:
1. Stablecoins
2. Lending platforms
3. Derivative tokens (mirror price of other assets)
4. Margin trading
5. Decentralized Exchanges
6. Prediction markets

Application Architecture
The ecosystem of DAP Chain comprises of 4 different components:
1. DAP Chain — a DP SDK based blockchain we are building.
2. Darkpool Hub — a blockchain hosting DAP token. It provides underlying value for the DOLLAR tokens being minted on Darkpool Chain.
3. BandChain — a blockchain for decentralized data oracle. It enables DAP Chain to consume traditional exchange trading symbol (traded symbol for gold) and DAP price feed from external sources.
4. Relayers — third-party software that relay packets between multiple blockchains. They allow multiple blockchains to interoperate in a secure and trustless manner.

ETH Bridge Zone

Unidirectional Peggy is the starting point for cross chain value transfers from the Ethereum blockchain to DP-SDK based blockchains as part of the Ethereum DP Bridge project. The system accepts incoming transfers of Ethereum tokens on an Ethereum smart contract, locking them while the transaction is validated and equitable funds issued to the intended recipient on the Cosmos bridge chain.

Unidirectional Peggy focuses on core features for unidirectional transfers. This prototype includes functionality to safely lock and unlock Ethereum, and mint corresponding representative tokens on the Cosmos chain.

The architecture consists of 4 parts. Each part, and the logical flow of operations is described below.

1. The smart contracts
2. The Relayer
3. The EthBridge Module
4. The Oracle Module

The smart contracts

First, the smart contract is deployed to an Ethereum network. A user can then send Ethereum to that smart contract to lock up their Ethereum and trigger the transfer flow.

In this prototype, the system is managed by the contract's deployer, designated internally as the relayer, a trusted third-party which can unlock funds and return them their original sender. If the contract’s balances under threat, the relayer can pause the system, temporarily preventing users from depositing additional funds.

The Relayer

The Relayer is a service which interfaces with both blockchains, allowing validators to attest on the Cosmos blockchain that specific events on the Ethereum blockchain have occurred. Through the Relayer service, validators witness the events and submit proof in the form of signed hashes to the Cosmos based modules, which are responsible for aggregating and tallying the Validators’ signatures and their respective signing power.

The Relayer process is as follows:

continually listen for a LogLock event
when an event is seen, parse information associated with the Ethereum transaction
uses this information to build an unsigned DP transaction
signs and send this transaction to Tendermint.

The EthBridge Module

The EthBridge module is a DP-SDK module that is responsible for receiving and decoding transactions involving Ethereum Bridge claims and for processing the result of a successful claim.

The process is as follows:

A transaction with a message for the EthBridge module is received
The message is decoded and transformed into a generic, non-Ethereum specific Oracle claim
The oracle claim is given a unique ID based on the nonce from the ethereum transaction
The generic claim is forwarded to the Oracle module.
The EthBridge module will resume later if the claim succeeds.

The Oracle Module

The Oracle module is intended to be a more generic oracle module that can take arbitrary claims from different validators, hold onto them and perform consensus on those claims once a certain threshold is reached. In this project it is used to find consensus on claims about activity on an Ethereum chain, but it is designed and intended to be able to be used for any other kinds of oracle-like functionality in future (eg: claims about the weather).

The process is as follows:

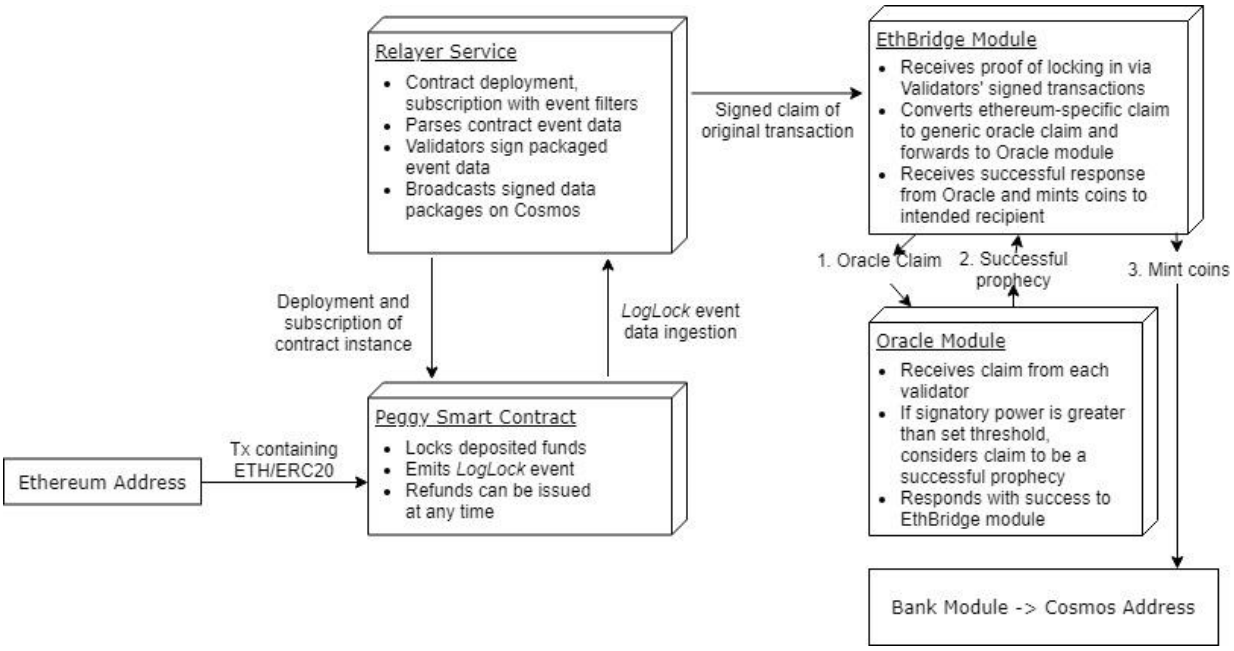
A claim is received from another module (EthBridge in this case)
That claim is checked, along with other past claims from other validators with the same unique ID
Once a threshold of stake of the active Tendermint validator set is claiming the same thing, the claim is updated to be successful
If a threshold of stake of the active Tendermint validator set disagrees, the claim is updated to be a failure
The status of the claim is returned to the module that provided the claim.

The EthBridge module also contains logic for how a result should be processed.

The process is as follows:

Once a claim has been processed by the Oracle, the status is returned
If the claim is successful, new tokens representing Ethereum are minted via the Bank module

Architecture Diagram



How to get involved

The Association envisions a vibrant community of developers building apps and services to spur the global use of the Darkpool network. The Association defines success as enabling any person or business globally to have fair, affordable, and instant access to their money. For example, success means that a person working abroad has a fast and simple way to send money to family back home, and a college student can pay their rent as easily as they can buy a coffee.

Our journey is just beginning, and we are asking the community to help. If you believe in what the Darkpool network could do for billions of people around the world, share your perspective, and join in. Your feedback is needed to make financial inclusion a reality for people everywhere.

If you are a researcher or protocol developer, a preview of the Darkpool testnet is available under the Apache 2.0 Open Source License, with accompanying documentation. The testnet is still a prototype under development, but you can read, build, and provide feedback right away. The Association is committed to building a community-oriented development process and opening the platform to developers. The Association's TSC has appointed a Lead Maintainer and an initial group of Maintainers and has established open and transparent processes for the acceptance of technical proposals for Darkpool Improvement Proposals (DXP). These will be published shortly.

If your organization is interested in applying for social impact grants from the Association, read more here.