MEMORANDUM

To: Crypto Task Force Meeting Log
From: Crypto Task Force Staff
Re: Meeting with Representatives of Permuto Capital LLC and Skadden, Arps, Slate, Meagher & Flom LLP

On May 27, 2025, Crypto Task Force Staff met with representatives from Permuto Capital LLC and Skadden, Arps, Slate, Meagher & Flom LLP.

The topic discussed was approaches to addressing issues related to regulation of crypto assets. Permuto Capital LLC and Skadden, Arps, Slate, Meagher & Flom LLP representatives provided the attached document, which was discussed during the meeting.

Proposed Agenda with Permuto Capital

1. Tokenization of Trust Units (Asset Certificates and Dividend Certificates)
2. Unified Markets and Trading
3. Problems with Trading Securities on Most Blockchains
    a. MEV
    b. Centralized Smart Contract Intermediaries
    c. L2 Scaling Solutions
4. Q&A and follow-up

Attendees

1. Gene Hoffman, Co-CEO, Permuto Capital LLC
   https://www.linkedin.com/in/gehoffman/
   hoffmang@permuto.capital

2. Trent Martensen, Co-CEO, Permuto Capital LLC
   https://www.linkedin.com/in/trentmartensen/
   trent@permuto.capital

3. Thomas Chow, Chief Legal Officer, Permuto Capital LLC
   https://www.linkedin.com/in/thomaschow/
   thomas@permuto.capital

4. P. Michelle Gasaway, Partner, Capital Markets, Skadden, Arps, Slate, Meagher & Flom LLP
   https://www.linkedin.com/in/michellegasaway/
   michelle.gasaway@skadden.com

Problems with trading securities on most blockchains

MEV

Many blockchains with poor designs face issues with MEV - Maximal Extractable Value (formerly Miner Extractable Value.) Due to requiring the ordering of transactions in a block a miner/farmer/validator can choose to order transactions in a way optimal for them and not for investors. A prime example of this problem is a Sandwich attack. Sandwich attacks occur when a user's transaction gets trapped, or "sandwiched," between two hostile transactions - one before and one after. As a result, the original transaction executes at a much higher price than necessary, leading to an inflated price for the original trader and an illicit profit for the malicious trader placing the two extra trades. Despite many industry participants handwringing and claiming MEV “enables liquidity”, doing this to a known securities transaction is clearly market manipulation under Section 9(a)(2) of the 1934 Act. Some other blockchains enable another source of MEV to occur by enabling third parties to bid for the right to sequence a block, a feature known as MEV-boost, which leads to further perverse incentives and manipulation for illicit gain when done in the context of a known securities transaction. Some industry participants are trying to redefine MEV as “Efficient Optimization Flows” or “EOF” to avoid the association with market manipulation and other activities that can be used to generate illicit profits.

The design decision on the Chia blockchain was to have all transactions go through in parallel in each block and allow transactions to set rules about how they can be spent. The order of transactions in a settling block on the Chia blockchain does not affect the price of any transaction in that block. Offer files set programmatically enforced rules that only allow them to be settled per the terms of the Offer file itself. Today that means that when a seller offers to sell 1 MSFT DC for $50.00 worth of USDC, the only price that the trade can enter a block and settle is $50. In the future, this can and will be extended to explicitly designate one or a trusted group of price oracles and assert that the offeror will take anything plus or minus the mean of the oracles. Each oracle can only announce one price per block and the announcement or ordering of other oracles has no effect on any other oracle or trade that doesn’t specifically reference it.

The only practical MEV that exists on the Chia blockchain is that a farmer, who also tracked the original Offer file, can step into the shoes of the taker at the same terms and take a good deal for themselves. However, unlike other blockchains, farmers - even in pools - sign their own blocks and due to both the highest node count of any smart contract blockchain and one of the highest Nakamoto Coefficients, it's unlikely for farmers to have many opportunities for such

trades. It also paradoxically increases the total liquidity to the decentralized market on the Chia blockchain as the offeror still receives the price they intended in the funds they specified.

This issue is technology neutral as blockchains could upgrade and re-architect to enable parallel transaction processing instead of sequencing. That would enable most or all of the most toxic forms of MEV to be eliminated, such as sandwich attacks and payment for order flow.

Centralized smart contracts versus Coins

For Ethereum Virtual Machine (“EVM”) and EVM-like chains such as Ethereum and Solana, for developer convenience, assets are not actually nor directly issued to individual wallets. Instead, they are issued within a centralized smart contract under control of the securities issuer (or others, see discussion below). This is effectively a single ledger of which public key pair owns how much of a given asset. This creates added risk versus other designs as it leaves a single point of failure where, if for example a nation state is able to find a backdoor or a weakness, itcan drain the entire contents of the issuance from that contract into their control.

The Chia blockchain actually places each issued asset (a Coin) in a wallet or vault controlled by the investor. To compromise every coin, barring some fundamental flaw in the Chia Asset Token standard (which has been audited two times with one severe issue identified and fixed), an attacker must compromise each investor's individual holdings across all investors - to reach the same attack success.

Smart contracts on the Chia blockchain are more aptly described as smart Coins because each Coin contains a puzzle that enables composability and programmability, but with a narrower attack surface.

Who has control of other smart contracts?

Though it is feasible for developers to actually cede control of an Ethereum smart contract (for example as Tornado Cash has done), most developers and project teams keep the ability to upgrade the smart contract with a set of required multi signature keys (for example as many versions of Uniswap have done). The power to upgrade is the power to do anything with the then state of the contract. To the extent that a security is being traded or pledged in such a centralized or controlled smart contract, the developers would almost certainly need licensure as one or more of a broker-dealer, exchange, or ATS. This is because they actually have full and final custody of any assets under the control of any smart contract that possesses securities on behalf of investors. While such developers have labeled autonomous transactions using smart contracts as “Peer to Peer” or even “decentralized finance”, these are misnomers at best and deliberately misleading at worst. Most transactions are Peer to (Controlled and/or Centralized) smart contract (which serves as an intermediary) to Peer.

Peer to Peer trading with Offers on the Chia blockchain does not have a third party involved. Assets remain in the custody of the maker and the taker until a valid settlement is reached on

the Chia blockchain when those assets are atomically swapped into the other's self custody possession. At no point does anyone have the ability to redirect those assets to anyone other than the maker and taker. The only two exceptions are that, as above, a farmer could attempt to step into the role of one side or could decide not to include a transaction in the block they are making. One side of the trade will get exactly what they want and the other will lose nothing but the opportunity cost. Again, the decentralized nature of farmers on the Chia blockchain also make it quite difficult to predict when a farmer will make the next block and severely limit the likelihood that any censored transaction will not be able to easily get into the next transaction block - which is also a major disincentive to a farmer not including the transaction for the transaction fees in the first place.

L2 Scaling Solutions

Unlike Bitcoin, Ethereum has coalesced on centralized optimistic rollup scaling solutions. Neither, for example, Base nor Polygon are currently decentralized in any meaningful definition of the term. Ethereum has opted to track stages of decentralization and at the time of writing, none of the 20 largest rollups are more than Stage 1 where Stage 2 is mostly decentralized. As such, any security that is bridged to Base or Polygon would require the runner of the sequencer of those L2s to have one of a broker-dealer, ATS, or exchange license as they have full control over any asset held on that L2. Though it may be technically possible for these rollup scaling solutions to become decentralized enough that no investor runs the risk of the operator misappropriating their funds, in practice these solutions have not gotten there.

L2s on Chia will be state channels which is the generic term for things like Lightning Payment Channels. These scaling solutions rely only upon the underlying blockchain for settlement and anti-cheating enforcement. They are voluntarily opened or joined by investors or payors and allow an investor to leave and settle back to the chain in ways that can not be stopped by any other party (though enforcement of anti-cheating rules may subject them to short delays.) As such, there is no human to trust and the rules of the state channel enforce proper behaviour on all parties utilizing that state channel.