White Paper

A Novel DeFi 2.0 Composition Protocol for Derivatives - Aquo

Trevor Lee Oakley

13 August 2023

1.0 Abstract

DeFi composition today is most limited to DEXs and PLFs. We propose a novel DeFi compositional protocol called Aquo aimed at derivatives.

2.0 Introduction

We propose a new novel DeFi compositional protocol which we think will meet investor demand. This protocol is aimed at derivatives. Derivatives depend on an underlying asset and therefore we also consider tokenization and real-world assets (RWAs).

Tokenization solutions are well-known in blockchains and smart contract composition has been used for many years, but DeFi composition is emerging and has not been widely used.

One of the motivations is the TradFi market is driven by derivatives and combining products with CDOs, CMOs, CDSs, SPVs and numerous more structures or products. This has driven the enormous growth into a market of hundreds of trillions of dollars. We hope to mirror this in DeFi.

We introduce some of the risk factors, how Aquo - a novel DeFi composition protocol - can be implemented. We consider this implementation to be part of DeFi 2.0 which is the next version of DeFi extending core DeFi concepts.

3.0 Challenges in Current DeFi Ecosystem

DeFi has a lot of challenges and Carapella et al. confirmed there could be a DeFi financial crisis [20].

3.1 Scope

Lending constitutes most of the DeFi ecosystem[7], 76% in 2020. Kitzler et al. that for DeFi compositions most of the transactions were DEX or PLF based [5]. The scope of DeFi is limited mainly to DEX and PLFs with few Dapps offering derivatives.

In TradFi, the derivatives market is very large, and hence this absence in DeFi is a deficiency in the DeFi market.

3.2 Triangle Problem

The triangle problem is a challenge in DeFi [19, 20] (also called Trilemma). This is when DeFi cannot achieve all of the following: decentralization, scalability, and security. One of the key losses has been in scalability for blockchain networks.

3.2 Liquidity

DeFi uses liquidity providers and investors act with caution only investing in a few LPs [18] and Heimbach et al. only considered DEXs. For derivatives, there is very limited liquidity in DeFi and derivatives as a sector is hardly developed in DeFi. Liquidity could decrease for some Dapps if new innovation emerges which liquidity away from them [20].

3.2 Interoperability

Interoperability does exist in DeFi but mainly limited to DEXs and PLFs [5]. Carapella et al. considered that interoperability would be a key factor in making DeFi challenge CeFi [20].

3.3 Security

Security problems are well known in DeFi. Gudgeon et al. confirmed DeFi lending protocols are liable to a variety of attack vectors [7].

Li et al. [19] published a long survey of DeFi security challenges which identified a number of vulnerabilities as follows:

- Oracles (price feeds)
- Wallets
- Front Running Attack
- Sandwich attack
- Pool Hopping Attack
- Eclipse Attack
- Sybil Attacks
- Smart Contract Vulnerabilities
- Reentry Attack
- External calls unchecked
- Flash Loans
- Pump and Dump Attacks

DeFi protocols have suffered from billions of dollars in losses via theft [22], with the key exploited being composability. Hence this risk of poor composability with complexity provides a significant

security risk to DeFi protocols. Babel et al. also found formal verification methods failed to detect economic security vulnerabilities.

3.4 Innovation

DeFi has largely followed TradFi financial models, but just using a new technology. This has failed to make any serious dent in TradFi markets. The scope of blockchains in tailoring contracts, low cost customization, widespread financial inclusion has hardly been realized. Financial markets are hundreds of trillions of dollars, and DeFi is not even close to trading these figures.

Carapella et al. also confirmed that newer innovations would be a key factor for DeFi to compete with TradFi [20].

3.5 Usability

DeFi is often complex and unfriendly to use. Wallets can be hard to understand, to install, and configure. The concepts can be difficult. There is no customer service, no one to walk through a user what to do, and much of the sector is just driven by coin prices going up and not real financial instruments.

4.0 Understanding DeFi Compositions

DeFi compositions could solve many of the key challenges we identified.

4.1 Compositions

Smart contracts compositions have been researched for a number of years [22, 17]. We are focused on DeFi compositions. DeFi compositions are mainly in DEXs and PLFs, and derivative solutions exist [5]. Kitzler et al. considered a new derivatives protocol using compositions could be needed, especially using sidechains.

DeFi implementations considered a Money Lego [4, 6, 7, 10] or a building blocks approach. With this approach a building block is a DeFi protocol and these are integrated into an execution tree with an execution path.

Aside from the research by Chainspace and the analysis by Kitzler et al, Jensen et al. considered a seamless integration on the same blockchain for composed transactions [8].

Existing smart contract compositions have experienced significant vulnerabilities, involving billions of dollars [22]. Hence a key consideration in Aquo is to provide secure solutions. This is called composable security.

4.2 Compositions & Security

Tolmach et al. provides analysis on a number of security vulnerabilities when using DeFi compositions [23]. For example, an attacker gained 24 million dollars after manipulating the price in Harvest which fed into Curve. There are many more attacks described. They tested with a process-algebraic modeling language which was able to verify the correctness of DeFi composition protocols and could be combined with compositional security.

4.3 DeFi 2.0

There is no clear definition for DeFi 2.0 which as a term is evolving [2].

Binance Academy defines this in terms of solving DeFi problems, e.g. related to liquidity, Thunder Core defines this as bringing complex financial instruments interacting with smart contracts, with a focus on DAOs and a new financial system [3].

There is little academic literature or research papers confirming a definition of DeFi 2.0 but the term DeFi: Finance 2.0 did appear in Werner at al.'s SoK [4] with a discussion considering key elements of DeFi to be non-custodial, permissionless, auditable and composable.

We consider the proposals under Aquo to be DeFi 2.0. We propose an architecture which fundamentally is:

- Interoperable across DeFi Protocols
- Permissionless
- Auditable
- Composable
- Based on DAOs
- Building complex or novel financial products thereby creating a new financial system

4.2 How compositions differ from traditional DeFi approaches

Compositions are about integrating DeFi protocols whereas a traditional DeFi approach is primarily about non-custodial financial products. Auer et al. defines DeFi as:

Decentralized Finance (DeFi) is a competitive, contestable, composable and non-custodial financial ecosystem built on technology that does not require a central organization to operate and that has no safety net.

They define DeFi composition as:

Financial service providers can combine the financial functions of several DeFi protocols to offer novel, complex, and deeply nested financial products without being dependent on any single intermediary.

The key difference is therefore creating nesting and dependence. We are focused in DeFi compositions in linking a series of DeFi protocols to provide one solution whereas non-composed DeFi protocols have no nesting of DeFi protocols.

4.3 Benefits of composability for the DeFi ecosystem

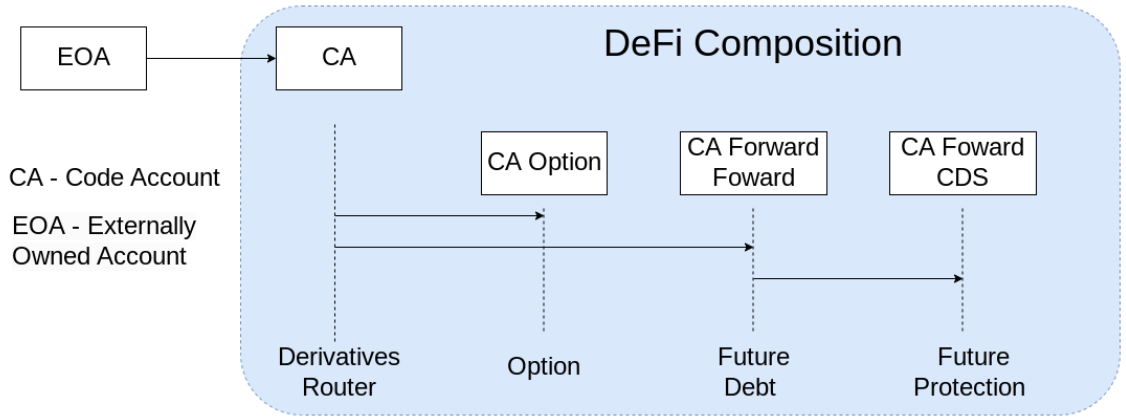
Werner et al. considered that DeFi in its ideal form had composability. The main benefit of DeFi composition is about integrating financial products which is what happens today in TradFi but it is not called composition. In TradFi products are structured so that if there is a mortgage then it can be subject to more debt via various solutions (e.g. a SPV is created and the SPV pays the lender and then mortgage repayments are passed through to the SPV). Also a CDS can be used for protection.
This combination of products in TradFi is what DeFi composition aims to achieve but by a different route. Hence the benefits are:

- Liquidity increased
- More diverse products
- Risk lowered in terms of financial risk itself (assuming there are no technical vulnerabilities)
- Growth improved
- Innovation is possible to create tailored products to meet investor demand

5.0 Building Blocks of Compossibility

5.1 Building Blocks

We use the building blocks concepts derived from the Lego interpretation previously discussed. A building block is a DeFi protocol being invoked. An example is below:



In this example, the original CA integrates into other DeFi protocols, so that an EOA can buy an Option using a future debt with protection. The CAs are all on the same blockchain and hence this is a seamless integration.

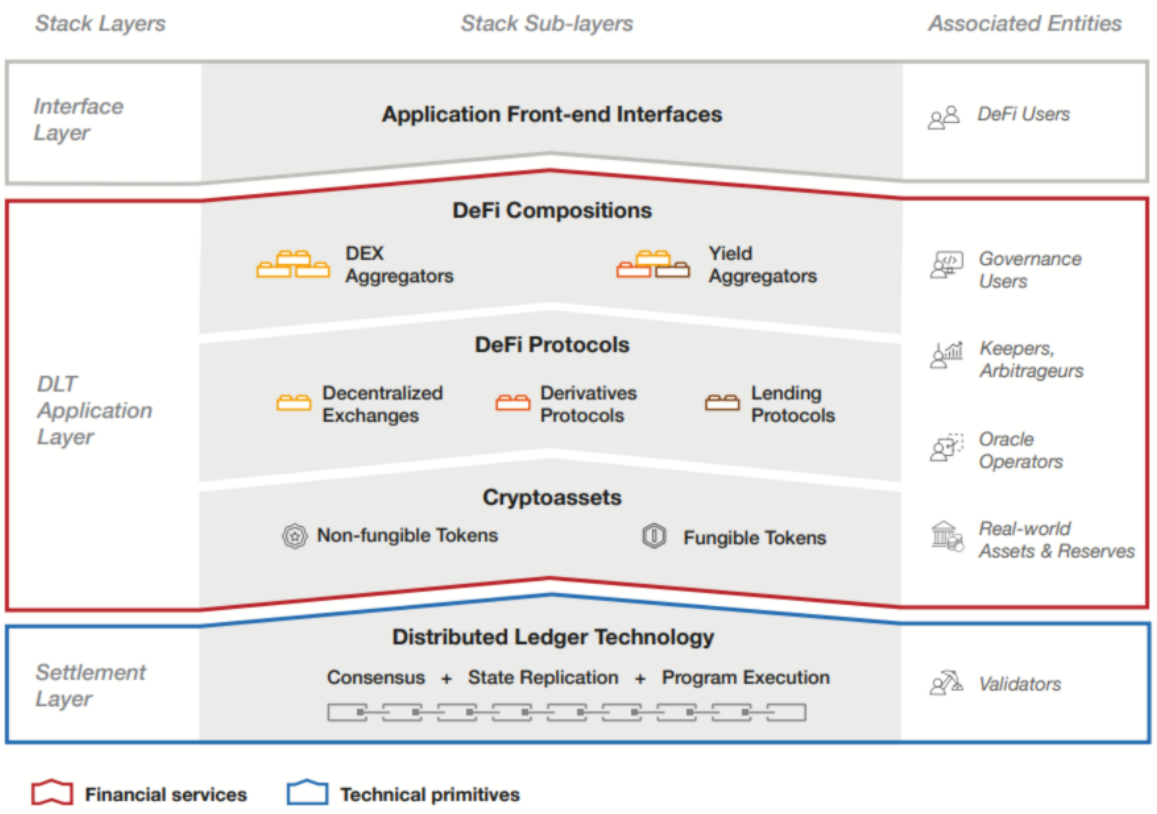
Hence, we could consider a tenant who lives in a house and agrees to rent the house with an option to buy it. This option takes into account market moves. The house is now valued at 400K USD and if the price moved to 500K then the tenant could buy it at 450K on an option. But he might not have the 450K and hence wants a future loan promise at the time of buying the option (forward forward) and then also wants to arrange loan protection should there be a default (variation on a CDS).

This can be completed via DeFi composed transaction in which the option is purchased, the loan promised, and protection given. This is also innovative finance and we are not taking standard finance contracts, but tailoring contracts and creating new markets. Providing we have liquidity and can safeguard against counterparty defaults (via collateralization) then these new markets can develop.

6.0 Architecture of DeFi Compositions

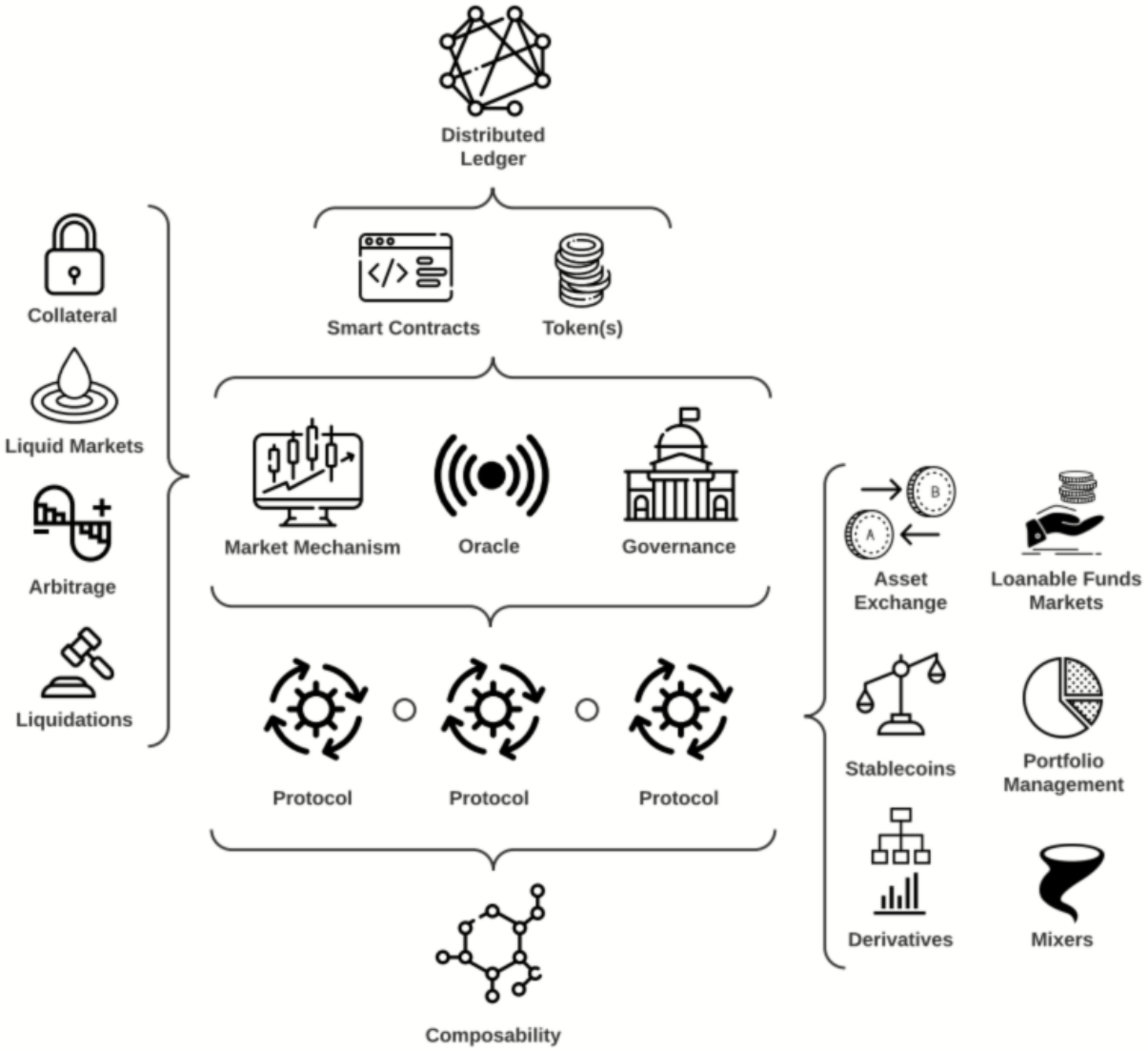
6.1 Existing Architectural Designs

Auer et al. [9] considered composability (shown below):



This layer structure is commonly seen in the literature. It shows how DeFi compositions access multiple DeFi protocols.

Werner et al. considered compositions as follows:



This shows a far wider meaning in accessing oracles, liquid markets, stablecoins, portfolio management, and derivatives.

7.0 Aquo Architecture

We consider the critical part of composition to be derivatives. No financial market can operate effectively without liquidity and we also consider liquidity pools to be critical to Aquo's architecture.

7.1 RWAs

Derivatives themselves are reliant on underlying assets, these are real-world assets (RWAs) or real-assets in financial terms. Due to the nature or RWAs decentralized oracles are needed to provide their prices which should be used in trading. If this were not done, the the token market cap could differ to the actual RWA value which could lead to asset stripping (sale of assets to make a profit as

the value is less than the token market cap), or investor loss who bought tokens are a price higher than the actual RWA value.

Therefore, RWA tokens themselves (traded as synthetic assets) would only be traded at the oracle price. This is a stablecoin concept with the price pegged to the actual asset value.

7.2 Currency Forward Contracts and the USD

RWAs will have real value in local currencies (usually), there are exceptions e.g. oil. DeFi is a long way from stablecoins in the numerous currencies globally and even some major stablecoins have been unstable.

Hence we propose that RWAs are priced in USD regardless of their jurisdiction. The actual real asset would of course trade in the real economy and then a **currency forward contract** is needed to maintain the price, this is another derivative.

This example will explain how this works. A house is valued at 400K GBP and tokenized. Whatever agreements are reached by the contracting parties, they want to settle finally in GBP. But Aquo works via USD.

Therefore a currency exchange rate is agreed at the current one when the house is tokenized and then this same rate is guaranteed via a forward derivative. Therefore if the Forex market moved from 1.2 USD for 1 GBP to 1.3 USD for 1 GBP, the RWA investor has no loss.

The new derivative is simply fashioned from the normal derivatives markets with Bid/Asks and in this case different traders will hedge and speculate on currency which will then give rise to the RWA price protection.

7.3 Synthetic Assets

The use of synthetic assets is well established in DeFi [10]. In the context of derivatives and RWAs, the most essential use case is for synthetic assets to track the RWA price. Hence we have a tradable token based on the RWA. A synthetic asset is another derivative. It is a contract based on an underlying asset (the RWA).

The RWA is just tokenized via an SPV with NFTs [11]. These models with SPVs which are bankruptcy-remote and NFTs which are claims on shares in an SPV are well known. The regulatory certainty comes from the share itself being transferred to the NFT holder in the simplest model.

Synthetic assets extend the model so that synthetic assets are tradable and this creates liquidity without having to trade the actual NFTs. This is equivalent to how securities are settled without having the actual certificates but based on a digital transaction. There is a contractual claim by the synthetic asset to the underlying NFT which allows the NFT asset to be claimed by the synthetic asset holder.

Tokenizing a RWA will not create liquidity unless the synthetic assets have a large market. That cannot happen unless the values are large. To avoid the problem of only tokenizing large assets, the actual synthetic assets would be the basis of liquidity pools (LPs) which would be aggregated as

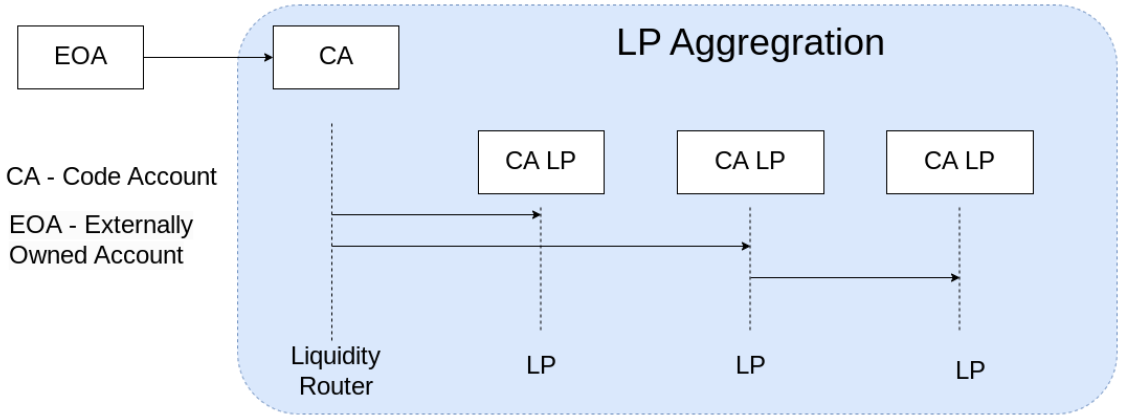
explained later. This then solves the liquidity problems. Also for this to work synthetic assets would be rated in a fashion akin to securities ratings today [12].

7.4 Oracles

Oracles are well established in DeFi and oracles would be used to feed prices.

7.4 Liquidity

Without liquidity the market will fail. One key aspect of Aquo is to allow liquidity to be aggregated via DAOs. One design is shown below:

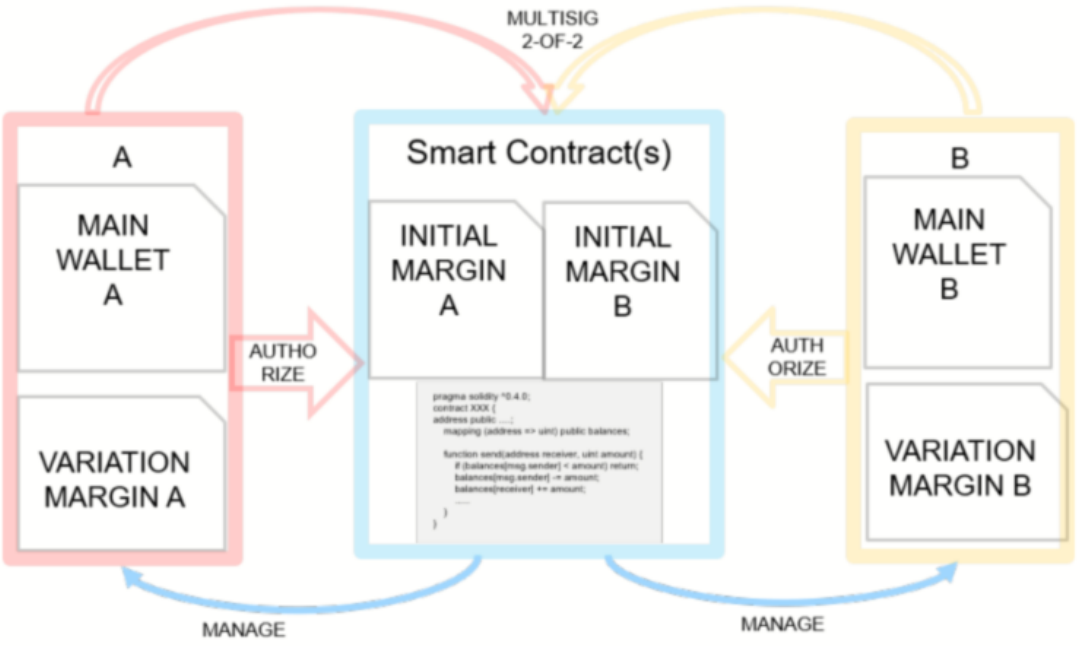


A variation on this design is to merge LPs into a large L based on DAOs.

The final outcome is an aggregated liquidity pool is created.

7.5 Collateralization

Collateralization models in DeFi and more generally in TradFi are well known [13]. For derivatives trade the risks involved are mitigated by requiring collateralized payments as the prices move. Below shows a diagram from Morini:



This can be shown by a simple example. Someone has an option to sell oil at 100 dollars (put option), and the market price was 100 dollars when the option was created but then fell to 80 dollars. The option writer would be facing a loss of 20%. That is a high loss, hence the option writer would be forced to make collateralization payments as the price fell, otherwise the option would default before the 80 dollar price was reached. The option writer could be required to pay collateral into the contract before the price fell and the option holder would have no loss except the premium (cost of the option).

7.6 Clearing and Settlements

Clearing Houses are well known in TradFi to reduce counterparty risk by maintaining account systems. They work on collateralized models.

Decentralized clearing networks work on similar principles to TradFi clearing houses, except the risk is maintained via DAOs [15]. This implementation would bolster use cases involving collateralized contracts.

7.0 Composability Use Cases

We focus on derivatives.

7.1 Liquidity Aggregation

This was partly explained before about how LPs can be merged or aggregated during a contract execution for a financial instrument.

This is one of the most important use cases.

7.2 Complex Products

Examples were given of linking up products (e.g. options and debt) and complex products are about nesting derivatives and making financial instruments include a lot of products.

7.3 Tokenization and Synthetic Assets

Tokenization models are well established in DeFi [21], Kölbel et al. researched tokenization considering its potential and conducting almost anything can be tokenized.

Composability opens the possibility for novel tokenization models. It is likely the standard SPV-NFT model will usually be used, but synthetic assets themselves are derivatives. This derivative could also be subject to composition. For example, a synthetic asset could be priced based on the values of different NFTs. This could introduce concepts similar to common stock and preferred stock and different voting rights. These again are all contractual conditions so the actual final asset could be adjusted accordingly.

7.4 Collateralization

As with other models, composability gives a lot of possibilities about collateralization. Collateralization itself is designed to lower risk but risk can also be tied and also passed to third parties via standard models such as CDOs and CMOs in TradFi.

In DeFi 2.0, we could for example link a collateralization requirement to a risk level and if the price moved too much, the contract could require a debt obligation to reduce risk (i.e. the lender takes risk of a default).

7.5 Innovative Products

Compatibility allows innovation at the EOA and CA level. These are not necessarily complex products but just innovative. A tenant for example could buy a future to buy his tenanted house which also required the landlord to clean the windows every week. If the landlord failed, then the contract would be voided and the obligation would not apply.

7.6 Decentralized Derivative Insurance

Compositions can facilitate the creation of decentralized insurance products that cover risks associated with derivative positions. By combining different protocols, users can secure protection against derivative-related vulnerabilities.

8.0 Technical Implementation

8.1 Smart Contract Infrastructure

8.1.1 Overview

It is a standard feature of solidity that one contract can execute another [16]. This contract execution path is the basis of the DeFi composition execution tree.

As smart contracts are created, they need to be registered into a **smart contract registry** maintained via Aquo. This provides a list of building blocks. For example, if there is a contract to create an option, that is an options contract.

```
// SPDX-License-Identifier: MIT
pragma solidity ^0.8.0;

interface ISyntheticAsset {
    function transferFrom(address sender, address recipient, uint256 amount) external returns (bool);
    // Add other functions related to the synthetic asset contract
}

contract OptionContract {
    address public writer;
    address public holder;
    uint256 public strikePrice;
    uint256 public expiration;
    uint256 public premium;
    bool public exercised;
    bool public expired;
    ISyntheticAsset public syntheticAsset;

    constructor(
        address _holder,
        uint256 _strikePrice,
        uint256 _expiration,
        uint256 _premium,
        address _syntheticAssetAddress
    ) {
        writer = msg.sender;
        holder = _holder;
        strikePrice = _strikePrice;
        expiration = block.timestamp + _expiration;
        premium = _premium;
        exercised = false;
        expired = false;
        syntheticAsset = ISyntheticAsset(_syntheticAssetAddress);
    }

    modifier onlyHolder() {
        require(msg.sender == holder, "Only the holder can call this");
```

```
        _;
    }

    modifier onlyWriter() {
        require(msg.sender == writer, "Only the writer can call this");
        _;
    }

    modifier notExpired() {
        require(!expired, "Option has expired");
        _;
    }

    function exercise() external onlyHolder notExpired {
        require(block.timestamp <= expiration, "Option has expired");
        require(!exercised, "Option has already been exercised");

        exercised = true;

        // Perform synthetic asset transfer or settlement logic here
        syntheticAsset.transferFrom(writer, holder, strikePrice);

        // Emit an event to log the exercise
        emit OptionExercised(holder, strikePrice);
    }

    function expire() external onlyWriter {
        require(block.timestamp >= expiration, "Option has not expired yet");
        expired = true;

        // Emit an event to log the expiration
        emit OptionExpired(holder, strikePrice);
    }

    event OptionExercised(address holder, uint256 strikePrice);
    event OptionExpired(address holder, uint256 strikePrice);
}
```

This contract would be deployed onto the blockchain and then the address be stored in the smart contract registry.

A composite transaction would specify the addresses in the transaction driven by the EOA initiated transaction. In other words, the Dapp client would determine which compositions would be used and construct the entire execution tree into the EOA transaction.

This would be done by the Dapp client reading the registry and then making a decision about what to use. For example, if the user wants to buy an option and the have a forward forward, the Dapp client would search the registry for a suitable contract for each use case and construct the transaction.

The search itself would use some metadata to determine the functionality, eg interface construction.

8.1.2 Role of Smart Contracts

The smart contracts will execute all the DeFi protocol functions. This includes derivatives, liquidity, DAOs.

The smart contracts are the building blocks and hence we expect some kind of encapsulation so the code can be executed by numerous combinations in the compositions. Also an interface would be used in the smart contract so there would be portability of the code.

8.2 Decentalized Oracles

A standard oracle solution would be implemented, eg using Chainlink [23]. Prices for RWAs will be updated into the oracle via an agreed party when the RWA is created with the SPV (e.g. an accountancy company will set the asset price). Then the oracle will feed that to the smart contract which requests the price. This will determine the selling price of the synthetic asset which tracks the prices.

In a full composed solution, this is not part of the Aquo protocol but these are separate components, but they would be part of the overall infrastructure.

8.3 Layer 2 Solutions

8.3.1 Scaling DeFi Compositions with Layer 2

An improvement to the core design of composition on a blockchain would be to implement a sidechain. This could peg synthetic assets to a sidechain which then allowed derivatives trade.

Al-Bassam considered in Chainspace some aspects of this [17] but for a non-DeFi use case. Their work could be applicable in some areas.

A layer 2 solution is also consistent with what Kitzler et al. determined for a DeFi composed solution.

8.3.2 Improving Transaction Speed and Cost Efficiency

A sidechain solution [25] has the benefits of lowering gas costs in a far smaller blockchain using two-way pegging and interoperability can also be achieved. Additionally in the DeFi many financial matters need to be private due to the constraints in the off-chain financial world. A sidechain also allows the possibility of a private sidechain.

These would be further developments to Aquo and not immediately available.

8.4 Security Measures

8.4.1 Auditing and Code Review for Protocol Safety

The core design is that building blocks are trusted when used extensively and tested. The approaches taken by Tolmach et al. would be implemented to improve security.

8.4.2 Addressing Security Vulnerabilities in Compositions

The guidelines in the security section of this document would be adopted.

8.5 Protocol Governance

8.5.1 Decentralized Governance Mechanisms in Compositions

The project is decentralized as far as possible and hence governance is via existing models on for example Ethereum.

A sidechain implementation would have suitable governance depending on whether private or public.

8.6 Composability Standards

Standards are needed to ensure integrations can be achieved. Just as ERC20 defined a set of tokens for tokens, we propose standards for composed protocols, to define what functionality should be implemented.

We provide an example for an Option.

8.6.1 Options

Below is an example of a standard set of functions for an option.

```
interface IDeFiDerivative {
    // ... Existing functions

    function createOption(
        address _underlyingAsset,
        uint256 _strikePrice,
        uint256 _expirationTimestamp,
        bool _isCallOption
    ) external returns (address optionAddress);

    function tradeOption(
        address _optionAddress,
        address _counterparty,
        uint256 _premium
    ) external returns (bool success);

    function executeOption(address _optionAddress) external returns (bool success);
```

```
}
```

8.6.3 Liquidity Pools

A liquidity pool could have standards as shown below.

```
interface ILiquidityPool {
    // Create a new liquidity pool
    function createPool(
        address[] memory _tokens,
        uint256[] memory _initialBalances,
        uint256 _feePercentage
    ) external returns (address poolAddress);
}
```

8.6.4 Standards

We proposed developing standards so the entire spectrum of derivatives can be included in composition.

9.0 Regulatory Considerations

There is no custody in the Aquo design and this limits regulatory controls. Project registration is done in a suitable jurisdiction, e.g. BVI.

10.0 Economic Models and Incentives

In derivatives potential rewards are high, and Aquo is customizable by design. Hence economic models would be derived from the actual smart contracts themselves and the rewards they bring to users.

11.0 Roadmap and Future Developments

Time	**Description**

0-3 Months	RWA and SPVs implemented
3-6 Months	LPs for on chain (mainnet) implemented with DAOs
6-18 Months	Derivatives implemented with compositions
18+ Months	Setting standards extending ERC standards, add more derivatives, building Layer 2 solutions

12.0 Conclusion

Aquo is a DeFi 2.0 solution using compositions. It is aimed at derivatives. This document describes how the protocol could be implemented.

13.0 References

1. Auer, Raphael, et al. *The Technology of Decentralized Finance (DeFi)*. Bank for International Settlements, Monetary and Economic Department, 2023.
2. https://academy.binance.com/en/articles/what-is-defi-2-0-and-why-does-it-matter
3. https://news.thundercore.com/what-is-defi-2-0/#htoc-the-emergence-of-defi-2-0
4. Werner, Sam, et al. "Sok: Decentralized finance (defi)." *Proceedings of the 4th ACM Conference on Advances in Financial Technologies*. 2022. https://arxiv.org/pdf/2101.08778.pdf
5. Kitzler, Stefan, et al. "Disentangling decentralized finance (DeFi) compositions." *ACM Transactions on the Web* 17.2 (2023): 1-26.
6. Katona, Tamás. "Decentralized finance: The possibilities of a blockchain “money lego” system." *Financial and Economic Review* 20.1 (2021): 74-102.
7. Gudgeon, Lewis, et al. "The decentralized financial crisis." *2020 crypto valley conference on blockchain technology (CVCBT)*. IEEE, 2020.
8. Jensen, Johannes Rude et al. “An Introduction to Decentralized Finance (DeFi).” *Complex Syst. Informatics Model. Q.* 26 (2021): 46-54.
9. Auer, Raphael, et al. *The Technology of Decentralized Finance (DeFi)*. Bank for International Settlements, Monetary and Economic Department, 2023.
10. Popescu, Andrei-Dragos. "Transitions and concepts within decentralized finance (Defi) Space." *Research Terminals in the social sciences* (2020).
11. Odinet, Christopher K., and Andrea Tosato. "The Intersection of NFTs and Structured Finance." *Boston University Law Review, Forthcoming* (2023).
12. Cantor, Richard, and Christopher Mann. "Analyzing the tradeoff between ratings accuracy and stability." *Journal of Fixed Income, September* (2006).
13. Morini, Massimo. "Managing derivatives on a blockchain. A financial market professional implementation." *A Financial Market Professional Implementation (May 5, 2017)* (2017).
14. Csóka, Péter, and P. Jean-Jacques Herings. "Decentralized clearing in financial networks." *Management Science* 64.10 (2018): 4681-4699.

15. Surujnath, Ryan. "Off the chain: A guide to blockchain derivatives markets and the implications on systemic risk." Fordham J. Corp. & Fin. L. 22 (2017): 257.
16. Wohrer, Maximilian, and Uwe Zdun. "Smart contracts: security patterns in the ethereum ecosystem and solidity." 2018 International Workshop on Blockchain Oriented Software Engineering (IWBOSE). IEEE, 2018.
17. Al-Bassam, Mustafa, et al. "Chainspace: A sharded smart contracts platform." *arXiv preprint arXiv:1708.03778* (2017).
18. Heimbach, Lioba, Ye Wang, and Roger Wattenhofer. "Behavior of liquidity providers in decentralized exchanges." *arXiv preprint arXiv:2105.13822* (2021).
19. Li, Wenkai, et al. "A survey of defi security: Challenges and opportunities." *arXiv preprint arXiv:2206.11821* (2022).
20. Carapella, Francesca, and Nathan Swem. "Decentralized Finance (Defi): Transformative Potential &Amp; Associated Risks." (2022).
21. Kölbel, Tobias, et al. "Spotlight on DeFi Centerpieces: Towards an Economic Perspective on Asset Tokenization Services." *Pacific Asia Conference on Information Systems*. 2022.
22. Babel, Kushal, et al. "Clockwork finance: Automated analysis of economic security in smart contracts." *2023 IEEE Symposium on Security and Privacy (SP)*. IEEE, 2023.
23. Tolmach, Palina, et al. "Formal analysis of composable DeFi protocols." *Financial Cryptography and Data Security. FC 2021 International Workshops: CoDecFin, DeFi, VOTING, and WTSC, Virtual Event, March 5, 2021, Revised Selected Papers 25*. Springer Berlin Heidelberg, 2021.
24. Breidenbach, Lorenz, et al. "Chainlink 2.0: Next steps in the evolution of decentralized oracle networks." *Chainlink Labs* 1 (2021): 1-136.
25. Back, Adam, et al. "Enabling blockchain innovations with pegged sidechains." *URL: http://www. opensciencereview. com/papers/123/enablingblockchain-innovations-with-pegged-sidechains* 72 (2014): 201-224.