Concerto
A decentralized crypto-asset investment fund

Elder K[a], Dr. Moo[b], L.ER[c] and Neil Sanchez[d]

[a]Bitcoin Addr: bc1qp6ex9u00d0g0nezvwkx78t943qsgd9uvy9xjgc
[b]Bitcoin Addr: 3GyNheZhqBaZvv93MGwz9ncnYbNPMCEdCi
[c]Bitcoin Addr: 1HSuoW2xVnLZ64tKUFjUcPUU1uoQxYTvyZ
[d]Bitcoin Addr: bc1qe5p0xqzggjrd2j7x45x4jpqw379ylwp3v76m8g

July 15, 2020

Abstract

Concerto, a Decentralized Autonomous Organization (DAO), works on top of Poladot [1], Bulletproof [2], and Game Theory. It is not only a trendy technology of Utopia but is also tailored for the real world. Furthermore, a series of problems related to profitability, decentralization and secrecy that lead to the failure of other DAOs can be solved here. Based on three core principles: profit first, decentralization, and secrecy, Concerto can successfully strip information asymmetry off individual investment behaviour with the help of game theory and zero-knowledge technology. Owing to the secret and verifiable information on Concerto, investors might gain profit easier than in other classic DAOs with traditional methods.

1 Introduction

After Ethereum [3], known as the first blockchain that supports smart contracts, was launched in 2015, people realized that there is an alternative approach to capital management and investment decision. Such motivation has led to the establishment of The DAO (Decentralized Autonomous Organization) [4] the concept of which was first proposed by Daniel Larimer in 2013 [5]. From then on, an increasing number of DAOs were found, including for instance Aragon[5], but unfortunately most of them had failed.

There are two core paradoxes in DAOs. One is between profit and secrecy, while the other is between decentralization and the Tyranny of the Majority (TOM). TOM has been solved by The DAO [4] using its retreat logic, and this solution will be inherited by Concerto. Nevertheless, transparency, the nature of blockchains, which was utilized by most DAOs to solve information asymmetry problems, may put participants in a dilemma.

In game theory [6], games will become complete and perfect information games if people trade without secrecy. Each participant can observe the bid-ask prices of other participants', and the payoff functions of players are commonly known. According to the non-arbitrage pricing principle, such rational payoff price will always point to the Nash equilibrium, where profit will no longer be available.

1.1 Principle

To solve these issues, Concerto will introduce three core principles:

- **Profits first** All activities should be based on positive profit probability. The mission of Concerto is to obtain economic returns for participating members through investment activities, maintaining and safeguarding the interests of all investors.
- **Decentralization** To preclude single points of failure or possible disasters caused by excessively centralized authority, all members govern operations and make group decisions jointly through distributed collaborative governance with no central node or authority.

  Concerto also supports both delegation and opt-out policy to refrain from TOM.
- **Secrecy:** To avoid issues of perfect information game, any economic behaviour must be based on secrecy.

With the three core principles above as Concerto's initial norm, a series of related operating mechanisms and governance rules can be derived. This whitepaper will describe these mechanisms and rules in detail according to this structure. If you do not feel that your values resonate with our core principles, or if you disagree with those principles, we suggest it would be a waste of your time to continue reading.

2 Methodology

Concerto DAO will run on Polkadot. The reason for this choice is to widen the range within which the investment can be targeted. Thanks to cross-chain technology, Concerto can theoretically touch any crypto assets in the blockchain world, and makes it possible to directly perform on-chain asset management.

2.1 Fund establishment

The capital pool jointly managed by Concerto DAO members uses Polkadot's native token DOT as a store of value which is also the form of assets raised at the initial stage of fund establishment. Anyone who is able to send DOTs to the pool will obtain the corresponding proportions of two types of native tokens in Concerto, namely WOOD and NOTE. When the amount of DOTs in the pool reaches the cap stipulated in advance, the fund will be established.

The WOOD token serves as a proof that the member has corresponding assets in the capital pool and also as votes for future investment decisions and other affairs; the NOTE token corresponds to a small portion of the capital raised at the initial stage and will be used for the operation of Concerto DAO and the development and maintenance of necessary online facilities such as smart contracts and user interfaces.

NOTE token holders permanently enjoy future dividends of the entire system, as well as the staking rewards of DOTs from the Polkadot network.

2.2 Investment proposal and voting

After the fund is established, any person or group (hereinafter collectively referred to as "sponsors") can initiate an investment proposal. The contributions of sponsors mainly include identifying high-quality projects as possible investment targets for the fund and coordinating the entire investment process to facilitate the deal. The sponsor may be an investor who expects to profit from a high-quality project, the representative of a startup team who is looking for investors, or a person who wishes to facilitate investment deals through their own labor to earn commissions.

A successful proposal needs to go through three stages before final execution (see Appendix C.3 for details), namely the planning stage, the voting stage, and the announcement stage. The sponsor generates a smart contract on the Polkadot network that conforms to the established proposal format and presents it to the Concerto community members, at which point the proposal is deemed in effect and enters the planning stage. The main purpose of this stage is to spur community members to discuss the proposal and express their interests and intentions.

The sponsor can voluntarily add a guarantee to the smart contract; the sponsor stakes a certain amount of WOOD tokens as collateral in advance. When a proposal has entered the announcement stage but the transaction cannot be successfully executed due to errors by the sponsor, the collateral will be slashed to compensate the investors. The aim of this mechanism is to boost investors' confidence and help the sponsor to obtain more votes from the community.

All participants can track the progress of the voting from this stage on but can only view the range of votes rather than the exact number. We believe that any kind of financial activity must be accompanied by information barriers, or it will soon become unprofitable even when it is performed on a blockchain. One of Concerto's unique features is that it introduces zero-knowledge proof into the voting system: no one can view the specific number of votes in the current voting process, not even the sponsor, by means of which, individuals or groups outside of DAO are unable to take advantage of the voting information.

2.3 Proposal execution and asset allocation

The passing of a proposal does not mean that only members who voted will participate in the investment; rather, the entire DAO has, by voting, made the investment decision on the project described in the proposal. When executing a proposal, Concerto uses DOT tokens in the fund pool to purchase tokens of the target project. However, even if a proposal is passed, there will inevitably be disagreement among DAO members because it is nearly impossible to obtain 100% of the votes. In reality, a so-called tyranny of the majority can easily occur, harming the interests of the minority. This is also the reason for an additional announcement stage to come into place after the voting stage.

In the announcement stage, any member can initiate a special transaction to the proposal contract, indicating that they are unwilling to participate in the investment proposal that has already been approved by the votes, so that the corresponding funds in the fund pool will not be included in the final execution. When the announcement is concluded and the contract is automatically executed, only the part corresponding to default participating members in the fund pool (that is, those who did not indicate non-participation) is used to invest. In this case, the system carries out an appropriate redistribution of the target assets.

After the tokens from the investee are released, a small portion of the tokens are sent to the sponsor as a reward for their work, and another small portion are placed in a special auction market. Anyone can take part in the auction to purchase these tokens using their NOTE token. These NOTE tokens collected in the auction are then burned, which ensures the system bonus is allocated to all the NOTE token holders. Finally, the majority of the target tokens are distributed among participating members according to the proportion of WOOD tokens held.

2.4 Risks and liquidation

Any member can initiate a special proposal to liquidate Concerto DAO, and if the votes on this proposal exceed 51%, the automatic liquidation process is triggered according to the smart contract, all DOTs in the fund pool being refunded to the corresponding addresses according to the proportion of WOOD tokens. Of course, in general, the easiest way for individuals to opt-out is to sell their WOOD tokens to other individuals or in secondary markets.

Under such a mechanism, there is a potential risk of a person or an organization collecting 51% of the total WOOD tokens to dissolve the DAO through a malicious vote. However, at the same time, this also constitutes a possible arbitrage opportunity: if the cost of collecting sufficient votes is less than the total value of the capital pool, it is profitable to manipulate the vote to dissolve the DAO in order to empty the pool. Since this is an open opportunity for everyone, the design will instead drive the market to always spontaneously push the price of WOOD token above the safety threshold.

3 Fund Establishment and Value Discovery

Most activities in Concerto DAO are based on Polkadot [7]'s decentralized network, so we choose DOT tokens as the base currency for capital injection and fund operations. We believe that DOT as well as Polkadot has a relatively stable valuation and an active developer community, so using DOT will bring us closer to a community ecosystem. The innate cross-chain feature of Polkadot also makes it possible for the interaction of various assets on different blockchains, which adds more possibilities and convenience to the operation of Concerto.

3.1 Fundraising principles

To better make profits for its members, Concerto will start with a fundraising process based on DOT tokens and complete value discovery during the process. We believe that the value of a decentralized DAO is composed of its community value and its capital value in the market. We will abide by the following principles in the fundraising process:

- **Upholding benefits of early participants:** Since early participants will encounter greater decision-making risks, they should be given more benefits.
- **Fairer holding costs:** We hope that costs for the majority of token holders will converge, that is, the mode of holding costs should be equal to the average.
- **Preventing fund expansion:** We want to prevent the excessive expansion of the total amount of DOT tokens in the pool, which often means lower capital utilization and greater challenge in management and higher decision-making risks. Therefore, we will use a steeper exchange curve to suppress the total amount of funds after the scale has met expectations.

3.2 Fundraising process and expectations

Concerto is a decentralized autonomous fund that runs with multiple smart contracts and zero-knowledge proof related technologies. Therefore, we need to extract a portion of the total capital injected as costs for the development of the fund and operation of its community; if the portion cannot cover Concerto's development and operation costs, it means that the fundraising failed and we will return all the DOTs that have already been injected. Since Concerto will only be able to have one effective investment project in each cycle, we need to avoid managing excessively large funds which have lower operating efficiency and higher management risk.

Concerto will run in a fully decentralized way. In the fundraising process, the capital injection and value discovery are completed by a BootVault contract that is deployed in advance. It contains the following logic:

- Receive participants' DOT tokens and transfer them to a Vault secured by a contract.
- Distribute Concerto's WOOD tokens to users according to the token price curve described by Concerto Bar of BootVault.
- If the capital injection fails, return all DOT tokens to WOOD token holders in proportion.

3.3 Concerto Bar

The most important part of BootValue is Concerto Bar (denoted as $\bar{c}$).

We introduce Concerto Bar as a fairer token distribution protocol, which is non-measurable and contains a set of Tokens. The generation of Concerto Bar is like a gashapon game. When a participant injects DOTs into the BootVault, it returns a Concerto Bar which may contain several WOOD and NOTE tokens.

The exact time of Concerto Bar generation cannot be inferred, and later, maybe after a few blocks, it will reveal the results and distribute Tokens it contained to the participants. The number of tokens a Concerto Bar contains is determined by its builtin seed which obey Poisson Distribution.

The Concerto Bar protocol is to achieve the goals that:

1. All distributed participants get a closer token amount, i.e., the mode, the median and the mean of the distribution are equal.

2. Fair market price discovery is easier.

3.3.1 Nutlet of $\bar{C}$

Concerto $\bar{c}$ is implementated with Schnoor Protocol [8], which allows us to set up and verify a secret value in a smart contract. The nutlet of $\bar{c}$ is witness w, which is pre-generated and proved via **Schnoor Protocol**. And around it, the nutshell algorithm $[x \leftarrow Poisson(w); w \leftarrow \lambda;]$ will transform w to a point of poisson distribution for measurement.

An algorithm $Poisson$ will transform witness w to a vector of poisson that points to $\bar{c}$. Which obey the poisson distribution:

$$P(k) = \frac{\lambda^k e^{-\lambda}}{k!}$$

Σ protocol of Schnoor(NIZK)

Prover		**Verifier**
$private : sk = a$		$public : PK$
$public : PK = aG$		
$random : r$		
$R = rG$		
$C = Hash(PK, R)$		
$z = r + c \cdot sk$	$\xrightarrow{(R,z)}$	
		$verify :$
		$c = Hash(PK, R)$
		$zG? = R + cPK$

3.4 Token value

Looking back at the token issuance cases for many projects in the past, we easily see that the usual approach is to collect ETH and issue tokens whose value only depends on expectations. These expectations are often difficult to achieve and accompanied by the risk of token price dropping to nothing. WOOD tokens are quite different from the usual cases. The issuance of WOOD is based on DOTs collected in the capital pool so its value can be tightly anchored to the value of DOT assets in the pool.

Based on this design, the DOT assets are locked in the smart contract and cannot be withdrawn instantly. The funds can only be used for investment which should be initiated by proposals and approved by voting. The purpose of this design is to solve the problems of over-centralization in traditional funds. However, people may question why WOOD tokens can always anchor their corresponding DOT value when the funds in the pool cannot be freely and instantly withdrawn and exchanged.

In fact, WOOD is a kind of proof of ownership corresponding to the DOT assets in the capital pool collectively held by the members of Concerto DAO, allowing free circulation in the secondary market. Its value is composed of the corresponding asset value in the pool and the premium on scarce investment opportunities. When the total market capitalization of WOOD is less than the total value of all assets in the capital pool, arbitrage speculators will buy a large amount of WOODs from the market in an attempt to redeem all funds in the pool by dominating voting rights. Therefore, it is the last strong line of defense for the value of WOOD. At the same time, the liquidity of the tokens is also one of our main concerns. Due to the arbitrage opportunities intentionally exposed in the design, whenever the price of DOT changes, the price of WOOD also changes because they are highly correlated. Therefore, we are able to create liquidity for WOOD tokens without market making.

3.4.1 Risk of holding tokens

Since the distribution of tokens will conform to the Poisson distribution, the mode of the token value obtained by the participants will be equal to the average, and 95% of the participants' cost (as well as income) scatter within two Sigmas. If Concerto's capital injection process fails, we will return the amount raised in proportion to the number of WOOD tokens held by the users.

The expectation of comprehensive investment loss for participants will, therefore, approach zero or equal their interest risk over time. Considering the community value of Concerto DAO, their expectation of comprehensive investment return will be greater than the value of DOTs they invested.

3.4.2 Secondary market exchange

Since there is no guarantee that WOOD tokens can be listed on a centralized exchange, the liquidity premium can be positive or negative, so it is possible that the price of WOOD may be higher or lower than fair market price.

3.5 Token Distribution

3.5.1 Airdrop

The conception of Concerto largely draws experience from the great ideas and practice of those who came before us. Therefore, 1% of the total number of WOOD tokens will be airdropped to developers who contributed to decentralized projects. In addition, airdropping is also a common marketing activity in the crypto world, and we firmly believe that good projects will be adopted first by enlightened early adopters and will then be promoted and gradually developed for wider use.

The DAO project was the first case of groundbreaking significance in the practice of decentralized autonomous organizations; both its developers and early participants had extraordinary vision, so they are the first groups to be considered for airdrops. We also hope that Concerto's future success will rebuild confidence in the vision of a decentralized world for the former participants of The DAO. In addition, equally important developer communities such as the Bitcoin Core team, the Parity team, MimbleWimble (Grin), ChainLink, Ethereum, and ZCash developers will also be targets of airdrops.

3.5.2 Total and distribution

WOOD and NOTE tokens represent different Concerto rights and interests. 85% of the total number of WOODs will be distributed during the fund-raising process while the other 15% will be reserved for project development. The total number of NOTEs will be equal to 15% of the total number of WOODs; NOTEs are distributed to investors in a 17:3 proportion to WOODs. 3% of all the tokens of the investment target will be injected into an auction pool and can only be purchased using NOTE, which means only NOTE token holders can participate in the auction. NOTE holders also enjoy the benefits of staking income of DOTs in the fund pool.

3.6 Liquidation mechanism

Concerto's funds are held in the smart contract and cannot be moved by anyone. WOOD holders are not allowed to withdraw the corresponding assets from the pool directly. As a result, the value of WOOD tends to deviate from the corresponding asset price. In response,

we have designed a liquidation mechanism. This mechanism is triggered by a special liquidation proposal; anyone can initiate such a proposal to liquidate Concerto DAO. If the vote exceeds 51%, Concerto DAO will be automatically liquidated according to the existing liquidation contract, and the funds in the pool will be distributed to the corresponding addresses in proportion to the WOOD tokens held.

3.7 WOOD's value anchoring

3.7.1 Value

The value of WOOD tokens comes mainly from two aspects: the corresponding assets value in the capital pool and the premium generated by its own community and ecosystem.

WOOD tokens correspond to DOT assets in the pool, so they have an inherent value anchor. Under the liquidation mechanism detailed above, there is an arbitrage opportunity where a person or an organization can try to collect 51% of the total number of WOODs and then initiate a liquidation proposal and manipulate the results. If the cost of collecting enough votes is less than the total value of the capital pool, the operation is profitable. However, because WOOD tokens are freely tradable in the secondary market, and this is an open arbitrage opportunity, this mechanism will instead cause the market to spontaneously push the price of WOOD tokens above the safety threshold, thereby realizing the anchoring of WOODs' value to DOT assets.

In addition, Concerto DAO utilizes collective wisdom through a rational system to direct investment decision-making towards a better path. This will bring investment income, and when the community is strong enough it will also generate sufficient voice and bargaining power in the industry. These things will bring an additional premium to WOOD tokens.

3.7.2 Long-term expected value

For a fair market price for Concerto WOOD tokens, we give the following definition:

$$WOOD_{price} = \frac{DOT_{price} + V(c)}{S}(1 + DV \cdot E(I))$$

With denotes:

$V(c)$: Valuation of community and ecosystem

$S : TotalSupply$

$DV.E(I)$: Discounted value of expected income

3.7.3 Interchangeability

Under the default settings and in most scenarios, user accounts are in normal mode. WOOD tokens are interchangeable in this mode, and any transfers as well as secondary market or OTC transactions are permitted. However, during each voting and execution cycle for investment proposals, there are two special modes: security lock mode and voting lock mode.

Security lock mode: When an investment proposal is approved in a vote but not all members are willing to participate in the corresponding investment activity, this may lead to the problem of tyranny of the majority. To solve this problem, Concerto has designed a security lock mechanism. When a user transfers WOOD to their security mode account, the user will not participate in the voting by default and will cancel all existing proxy relationships. To ensure the rights and interests of users, such users will not be able to obtain revenue from the voting process and funds may not be transferred until the settlement of the investment project is completed and WOODs exit the security lock mode.

Voting lock mode: Tokens used for voting are in voting lock mode. They are not interchangeable.

4 Voting and Governance

Concerto DAO does not investigate any background information regarding the sponsor and does not require the sponsor to provide any proof of qualifications or ability. After the fund is established, any sponsors can initiate an investment proposal.

4.1 Proposal content

The content of the proposal should fully disclose information regarding the investee and the sponsor at the request of Concerto members. The information involved includes but is not limited to information pertaining to the sponsor, project, and related risks. We will build a smart contract for the disclosure of general information.

A sponsor should obey the following principles:

1. Proposal information should be as complete, accurate, and valid as possible.

2. Sponsors should minimize the risk of participation for joint decision-makers.

3. Sponsors must be responsible for the common interests of joint decision-makers

4.1.1 Information contained in the proposal

Following the basic principles for making proposals, we require that the sponsor provides credible and verifiable information based on their community relations, including:

- **Identity of the sponsor:** The sponsor can be an individual or group using their real name or remaining anonymous. However, the completeness of the information provided will to a large extent determine its credibility within the community. We provide the option of staking collateral for proposals to help anonymous sponsors or groups with less credibility to demonstrate the validity of the proposal information in order to prove their commitment and increase the credibility of the proposal. At the same time, we hope full discussions between sponsors and voters during the off-chain stage can lead to a consensus among them.
- **Information about the target project:** The sponsor should fully ensure the validity and authenticity of information regarding the target project. Any deception will be condemned by the community. To minimize the risk for the community, we will display project information in

the form of an on-chain smart contract announcement. We will require different levels of completeness and accuracy of the information at different proposal stages, taking into account the project schedule.

4.2 Off-chain preparation

Strictly speaking, off-chain work is not a fixed stage in the voting process. Participants will complete many related off-chain activities throughout the whole voting process. For example, before the proposal is announced, the sponsor may already have conducted preliminary negotiations with the investee, or conducted full discussion and information exchange with the community online, including through forums and group chats. During the period from the start of voting to the final execution of the proposal, the sponsor must also go back and forth between the investee and the community to carry out negotiation and other necessary work.

4.3 Proposal Stages

On-chain voting is divided into three stages: the planning stage, the voting stage, and the announcement stage. The threshold for each stage is a ratio of the number of votes obtained to the total number of possible votes. The exact value of this ratio is not disclosed throughout the voting process. However, the zero-knowledge proof ensures its authenticity; the system will provide proof when the value crosses the threshold of each stage, announcing detailed data after the voting process ends.

4.3.1 Planning stage

When the sponsor publishes the proposal on the chain in a format specified by the smart contract, the proposal enters the planning stage. At this time, members can use WOOD to vote on the proposal; when the number of votes reaches 1% of the total supply of WOOD, Zero Knowledge Range Proof (ZKRP) will give a proof. This gives the sponsor a clear signal from the members of Concerto DAO that there is considerable interest in the investment plan, so it is necessary to conduct further negotiations with the investee based on this proof. After the planning stage is completed, the system asks the sponsor to submit more detailed information about the project which includes:

- **Background information**
  - Sponsor identity or group members
  - Name of investment project
  - Project introduction
  - Project members
  - Project contact
  - Sponsor's credit evaluation of the project
  - Declaration of interest between sponsor and project
  - Signatures of sponsor and contact
  - Sponsor collateral (optional)
- **Information regarding the investment**
  - The name of the target token
  - Token contract address
  - Token unit price
  - Total investment
  - Investment logic
  - Expected return
- **Information regarding implementation**
  - Contract address
  - Sponsor collateral (if applicable)

Sponsors should disclose the above information as much as possible when initiating the proposal. After entering the planning stage, members of the Concerto DAO can begin voting on the proposal using their WOODs to express their willingness to invest.

4.3.2 Voting stage

The votes for a proposal during the voting stage and the planning stage are continuous. When a proposal enters the voting stage, the sponsor must communicate closely with both the investee and community members, and provide as soon as possible the proposal information that could not be determined at the planning stage. We hope that the project information at the voting stage is sufficiently complete and accurate, because once the votes obtained by the proposal exceed the voting stage threshold, it will automatically enter the next stage and changes to the proposal information will be prohibited.

A proposal only needs to obtain a small number of votes to cross the first threshold so as to enter the voting stage. This indicates that there is interest in the proposal within the community, so the sponsor may start preparations to connect with the investee. In fact, there is no absolute boundary between the planning stage and the voting stage, and the significance of crossing such a low threshold is to convey a clear signal from community members to the sponsor: we are interested (and serious)! The sponsor should complete the previously missing items in the proposal as soon as possible during the voting stage.

- **Information regarding the investment**
  - The name of the target token
  - Token contract address
  - Token unit price
  - Total investment
- **Information regarding implementation**
  - Contract address
  - Sponsor collateral (if applicable)

4.3.3 Announcement stage

When a proposal is passed, the entire DAO should by default invest in the project described in the proposal, i.e., use DOT tokens in the fund pool to purchase tokens of the target project. However, even if a proposal has been taken into effect, there will inevitably be disagreement among DAO members because it is nearly impossible to obtain 100% of the votes. In reality, a so-called tyranny of the majority can easily occur, harming the interests of the minority. This is also the reason for an additional announcement stage to come into place after the voting stage.

When the proposal exceeds a voting threshold of 51%, it is officially passed. Proposal information cannot be changed at this time, and the project enters the announcement stage that lasts for 24 hours. During this stage, detailed information such as voters and voting ratio will be announced for verification and reference by the community. No new votes or changes are accepted during this period, so the result of the proposal will not be affected. However, it does leave time for members who are not willing to participate in this investment to freely opt-out.

In the announcement stage, any member can initiate a special transaction to the proposal contract, indicating that they are unwilling to participate in the investment proposal that has already been approved by the votes, so that the corresponding funds in the fund pool will not be included in the final execution.

4.4 Details of proposal execution

4.4.1 Conditions for execution

After the proposal has gone through the 24-hour announcement stage, it will be automatically executed according to the relevant proposal information in the smart contract. Since the proposal cannot be changed during the announcement stage, if the sponsor fails to complete the information in the voting stage and the proposal cannot be executed successfully by the contract, the proposal will automatically be invalidated. If the sponsor voluntarily chose to provide assets as collateral in the proposal, the provided assets will be forfeited.

4.4.2 Preventing tyranny

From the first time when DAO was defined, Jentzsch raised the problem of the "majority robbing the minority" [Citation]. The Concerto DAO also faces a similar unavoidable problem, which we call the "problem of tyranny." When an investment proposal is voted through, the vote actually obtained may represent the opinion of the majority, or it may only represent the intention of a small number of people because the vote threshold for the proposal to take effect is not very high. In some cases, the main advantage allowing the proposal to win may be nothing more than being ahead of other proposals in the same period. Because of this, we do not distinguish between the majority or the minority, but regard it as a challenge that we call the "problem of tyranny."

When the proposal is finally announced and is about to be executed, some members will be dissatisfied with it. If the proposal is executed, it will cause damage to their rights and interests, but forking is not the optimal solution here because it runs counter to the initial motivation behind the organization's formation. Concerto's solution is to allow anyone to choose to exempt some of their assets in the pool before each proposal is executed; that is, they can choose to retain some of their funds and not participate in the investment activity. If no signal of refusal is received during the announcement stage, the default behavior of the smart contract is to include the corresponding funds in the execution of the proposal. 3% of the investment target tokens will be deducted by the system. This portion of the investment target will be auctioned later, and anyone can use NOTE to participate in the auction to buy the target tokens. NOTEs obtained by the system will subsequently be burnt.

5 Proposal execution

When the announcement stage ends, the contract automatically exchanges tokens on the chain according to the exchange rate stated in the proposal. The investment target tokens automatically enter the Concerto fund pool, and the corresponding WOOD tokens enter the address given by the investee in advance. If the information given in the proposal is invalid or the sponsor fails to provide valid information before the announcement, contract execution will fail and the proposal will become invalid.

5.1 Asset allocation

During proposal execution, the DOTs involved in the investment are transferred to the investee and the corresponding investment target tokens are collected. Of these target tokens, 2% are rewarded to the sponsor and investors who participated in the voting and 3% are injected into a special auction pool. The remainder is allocated according to the proportion of WOODs invested by the community members and transferred to their personal addresses.

In the auction, anyone can use NOTE to make purchases from the pool. The starting price is 50% of the price in the investment proposal. The auction conversion mechanism uses the Bancor model with a purely linear CW = 2 price change curve. Under this distribution plan, the value of NOTE can be regarded as the income that represents future sustainable management revenue of the Concerto DAO under discounted cash flow model.

5.1.1 Zero-knowledge

We believe that security is the foundation of any economic activity, so all voting processes are protected by RangeProof zero-knowledge proof technology to maintain their anonymity. BulletProof is a non-interactive RangeProof method. For an anonymous voting process, we will prove to the parties concerned that their votes are in the [0, a] interval, [a, b] interval, or [b, +] interval according to the three stages of voting. RangeProof is the key to anonymous voting. We keep the identities and number of votes of all voting users strictly confidential until voting enters the announcement stage.

6 Liquidation

Since Concerto uses non-rigid payment contracts, providing a reasonable liquidation channel is the best way to ensure value and protect the interests of community members. This will directly affect the expected value in the secondary market and maintain the price stability of WOOD.

Concerto is a community experiment based on privacy and decentralized governance, so rational liqui-

dation rules are also conducive to stopping investment losses if the experiment fails.

6.1 Liquidation voting

To avoid the tyranny of the minority or majority, we will not allow proxy voting on liquidation proposals. All liquidation votes should be transparent, so that participants are clear about who participated in the vote. This will be detrimental to their trustworthiness in the community of those who vote for liquidation.

The voting period for liquidation is 1000 blocks' time. During this period, voting is irreversible, irrevocable, and there are no dissenting votes; once the liquidation threshold is reached, the liquidation process will be triggered automatically.

6.2 Liquidation process

The liquidation contract will be triggered automatically when the vote reaches 51%. All DOTs in the capital pull will be immediately transferred to WOOD holders according to the proportion of tokens held.

6.3 Contract burn

After the completion of asset liquidation and their return to the owners, contracts will automatically be burned and after this point no operations can be performed any more.

6.4 Capital exhaustion

When Concerto DAO's fund is insufficient for further operation (for example prone to manipulation, etc.) and/or when the ROI is satisfactory, a second round of fundraising will be opened to supplement the fund pool. At the same time, a reasonable proportion of WOOD may be issued as compensation for previous community members. The specific details will be based on the consensus reached by voting from community members.

7 Summary

People's investment decisions are often affected greatly by one-sided propaganda from investees, and it is difficult to access a competitive information market. This is also an important factor of failures for many crypto investors in the past. Concerto has established a competitive information market to provide investors with relatively complete investment-related information and a rational mechanism for decision-making by voting. It aims to provide all participants with a better rate of return than previous investment activities while also offering the possibility of an alternative method for fund management.

References

[1] Parity. Polkadot is a sharded protocol that enables blockchain networks to operate together seamlessly.

[2] Benedikt Bünz, Jonathan Bootle, Dan Boneh, Andrew Poelstra, Pieter Wuille, and Greg Maxwell. Bulletproofs: Short proofs for confidential transactions and more. Cryptology ePrint Archive, Report 2017/1066, 2017. `https://eprint.iacr.org/2017/1066`.

[3] Vitalik Buterin. Ethereum whitepaper, 2013.

[4] The DAO. The dao whitepaper, 2013.

[5] Daniel Larimer. The hidden costs of bitcoin.

[6] Drew Fudenberg and Jean Tirole. Game theory. 1991. Translated into Chinesse by Renin University Press, Bejing: China.

[7] DR. GAVIN WOOD. Polkadot: Vision for a heterogeneous multi-chain frameworkdraft, 2013.

[8] Ronald Cramer, Ivan Damgård, and Berry Schoenmakers. Proofs of partial knowledge and simplified design of witness hiding protocols. In Yvo G. Desmedt, editor, *Advances in Cryptology — CRYPTO '94*, pages 174–187, Berlin, Heidelberg, 1994. Springer Berlin Heidelberg.

[9] Jan Camenisch and Markus Stadler. Efficient group signature schemes for large groups (extended abstract). 1997.

[10] G. E. P. Box and Mervin E. Muller. A note on the generation of random normal deviates. *Ann. Math. Statist.*, 29(2):610–611, 06 1958.

Appendix A Range Proof

With Camnisch and Stadler notation [9], we describe a ZKRP as:

$$PK\{(\delta,\gamma) : y = g^{\delta}h^{\gamma}; (\upsilon \leq \delta \leq \nu)\}$$

Most of ZKRP implementations depend upon a trust setup, except Bullet Proof [2]. The idea of bulletproof is based on inner product. We denote an inner product as:

$$\langle \mathbf{l}(\mathbf{X}), \mathbf{r}(\mathbf{X}) \rangle = \sum_{i=0}^{d} \sum_{j=0}^{i} \langle \mathbf{l}_i, \mathbf{r}_j \rangle \, \mathbf{X}^{i+j} \in \mathbb{Z}_p[\mathbf{X}]$$

We can prove a sercert $v \in [0, 2^n]$ by doing:
1. Prove that $\mathbf{a}_L \in 0, 1^n$ is the bit-decompositing of v:

$$\langle \mathbf{a}_L, \mathbf{2}^n \rangle = v$$

2. Define $\mathbf{a}_R$ as the component-wise complement of $\mathbf{a}_L$, thus for every $i \in [0, n]$, if the i-th bit of $\mathbf{a}_L$ is 0, then the i-bit of $\mathbf{a}_R$ is equal to 1. Conversely, if it's 1, then the i-th bit of $\mathbf{a}_R$ is equal to 0. This condition can be shortly described by Equations:

$$\mathbf{a}_L \circ \mathbf{a}_R = \mathbf{0}^n$$
$$\mathbf{a}_R = \mathbf{a}_L - 1^n (\mod 2)$$

In order to prove that $\mathbf{a}_L$ and $\mathbf{a}_R$ satisfy relations, we can verify it by randomly choose $y \leftarrow \mathbb{Z}_p$ and compute:

$$\langle \mathbf{a}_L, \mathbf{a}_R \circ \mathbf{y}_n \rangle = 0$$

$$\langle \mathbf{a}_L - \mathbf{1}^n - \mathbf{a}_R, \mathbf{y}^n \rangle = 0$$

With Fiat-Shamir heuristic, we describe the bulletproof algorithm $Proof_{RP}Verify_{RP}$(based on inner product commitmennt $commit_{IP}$, $proof_{IP}$ and $verify_{IP}$) as:

Algorithm 1 Bulletproof $Proof_{RP}$

Input: $params_{RP}, \nu$
Output: $proof_{RP}$
$V = g^{\nu}h^{\gamma} \in \mathbb{G} \mid \gamma \leftarrow \mathbb{Z}_p$
$\mathbf{a}_L \in 0, 1^n \mid \langle \mathbf{a}_L, \mathbf{2}^n \rangle = \nu$,
$\mathbf{a}_R = \mathbf{a}_L - \mathbf{1}^n \in \mathbb{Z}_p$,
$\mathbf{A} = h^{\alpha}\mathbf{g}^{\mathbf{a}L}\mathbf{h}^{\mathbf{a}R} \in \mathbb{G}$,
$y, z = Hash(A, S), Hash(A, S, y) \in \mathbb{Z}_P$,
$T_1, T_2 = g^{t_1}h^{\tau_1}, g^{t_2}h^{\tau_2} \mid \tau_1, \tau_2 \leftarrow \mathbb{Z}_p; T_1, T_2 \in \mathbb{G}$,
$x = Hash(T_1, T_2) \in \mathbb{Z}_p$,
$\mathbf{l} = l(\mathbf{X}) = \mathbf{a}_L - zl^n + s_L\mathbf{X} \in \mathbf{Z}_p$,
$\mathbf{r} = r(\mathbf{X}) = \mathbf{y}^n \circ (\mathbf{a}_R + zl^n + \mathbf{s}_R\mathbf{X}) + z^2\mathbf{2}n \in \mathbf{Z}_p$,
$\bar{t} = \langle \mathbf{l}, \mathbf{z} \rangle \in \mathbb{Z}_p$
$\tau_x = \tau_2x^2 + \tau_1x + z^2\gamma \in \mathbb{Z}^p$
$\mu = \alpha + \rho x \in]mathbbZ_p$
$commit_{IP} = Commit_{IP}(params_{IP}, \mathbf{l}, \mathbf{r})$
$proof_{IP} = Proof_{IP}(params_{IP}, commit_{IP}, \bar{t}, \mathbf{l}, \mathbf{r})$,
$proof_{RP} = (\tau_x, \mu, \bar{t}, V, A, S, T_1, T_2, commit_{IP}, proof_{IP})$
return $proof_{RP}$

Algorithm 2 Bulletproof $Verify_{RP}$

Input: $params_{RP}, proof_{RP}$
Output: $True \vee False$

$y, z, x = Hash(A, S), Hash(A, S, y), Hash(T_1, T_2)$
$h_i = h_i^{y^{-1+1}} \in \mathbb{G} \mid \forall i \in [1, n]$
$P_l = P \cdot h^{\mu}$
$P_r = A \cdot S.\mathbf{g}^{-z} \cdot (\mathbf{h}')^{z \cdot \mathbf{y}^n + z^2 \cdot \mathbf{2}^n} \in \mathbb{G}$
$output_1 = P_l \stackrel{?}{=} P_r,$
$output_2 = g^{\bar{t}} h^{r_x} \stackrel{?}{=} \mathbf{V}^{z^2} \cdot g^{\delta(y,z)} \cdot T_1^x \cdot T_2^x,$
$output_3 = Verify_{IP}(Proof_{IP})$
return $output_1 \wedge output_2 \wedge output_3$

Appendix B Concerto Bar

Conerto Bar contract contains a series of hidden seed $\left[\mathbf{C} = Proof_{schnoor}(\mathbf{c}) \mid \mathbf{c} \leftarrow N(\mu, \sigma^2)\right]$. They can be verified via $Verify_{Schnoor}$ after c_i is revealed.

Algorithm 3 NIZK Schnnor $Proof_{Schnoor}$

Input: $params_{Schnoor}, \nu$
Output: $proof_{Schnoor}, PK = vG$

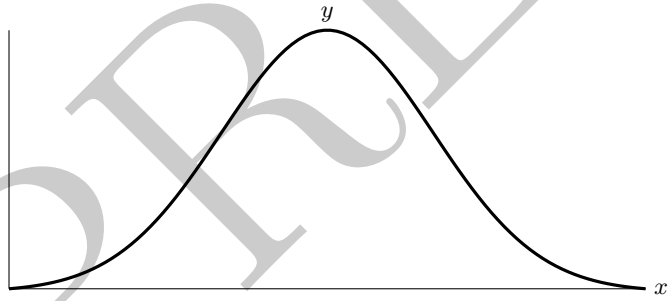
$r \leftarrow \mathbb{F}$
$c = Hash(PK, R)$
$R = rG$
$z = r + c \cdot sk$ $Proof_{schnoor} = R, z$
return $proof_{schnoor}$

Algorithm 4 NIZK Schnnor $Verify_{Schnoor}$

Input: $proof_{Schnoor}, PK = vG$
Output: $True \vee False$

$c = Hash(PK, R)$
RETURN $zG \stackrel{?}{=} R + cPK$

The variable c_i should obey poisson distribution. We denote it as $\mathbf{c} \sim N(\mu, \sigma^2)$, which will be pre-generated by Box-Muller Transform [10] $Transform_{BM}$.



Appendix C Smart Contract

Concerto has three major contracts: Concerto Bar Contract $\bar{C}$, Fund Vault Contract V, and Governance Voting Contract G.

C.1 Concerto Bar $\bar{C}$

Algorithm 5 ConcertoBar::Exchange $\bar{C}_{Exchange}$

Input: $\bar{\mathbf{C}}, DOTs, EX_{Rate}$
Output: $[\bar{C}_i]$
  $ret = []$
  while $len(DOTs) - EX_{Rate}$ **do**
    $append(ret, car(\bar{\mathbf{C}}))$
  end while
  $\bar{C}_{TransTo}(FundVault)$
  RETURN ret

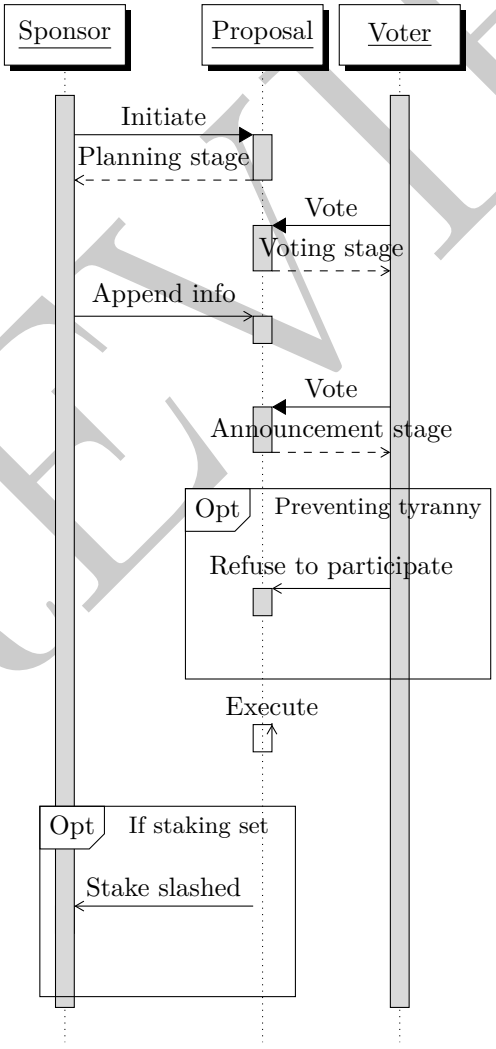
C.2 Fund Vault Contract V

Abbreviated.

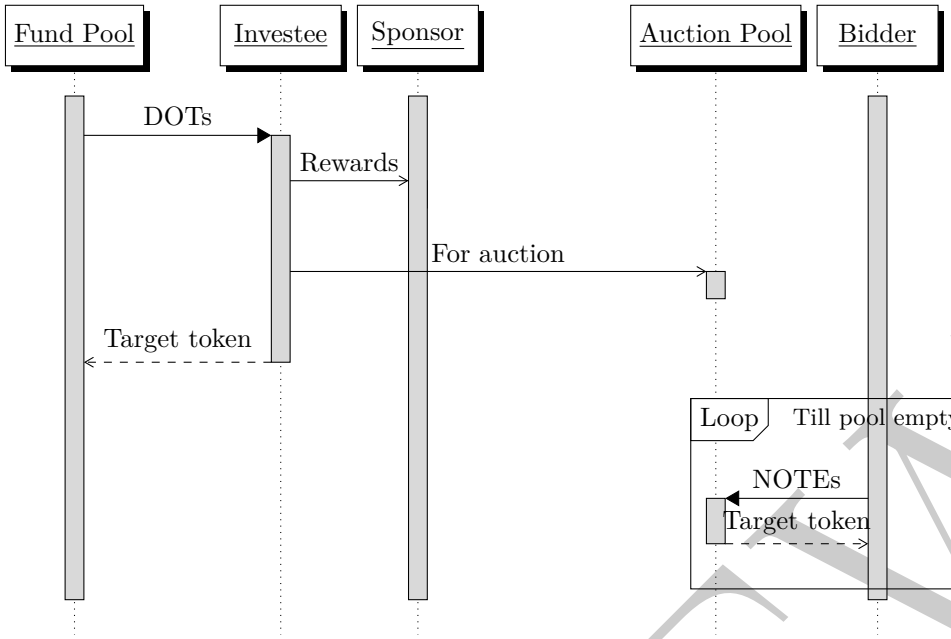
C.3 Governance Voting G

The governance voting contract is used for organizing the whole voting process and the following asset allocation once the investment proposal is passed.

The voting process can be described with the following sequence diagram:



If the proposal is passed, the contract will automatically allocate the assets, the detailed process of which can be described with the diagram below:


Fund Pool
Investee
Sponsor
Auction Pool
Bidder
DOTs
Rewards
For auction
Target token
Loop
Till pool empty
NOTEs
Target token