Ethria

Towards global, transparent, inclusive action on Climate

|  |  |  |
| --- | --- | --- |
| **Version** | **Comments** | **Date** |
| 1.0 | Launch version |  |
| 0.1 | Pre-Launch version |  |

|  |  |  |
| --- | --- | --- |
| author | **Karen Scarbrough**  Senior Associate, Digital Science & Engineering | 28/1/2022 |
| AUTHOR | **Yannis Perrakis**  Principal, Digital Science & Engineering |  |
| AUTHOR | **Miranda Wood**  Blockchain Research & Cryptographer, EY |  |
| REVIEWER | **Julian Gray**  VP, Digital Science & Engineering |  |
| REVIEWER | **Tony Fargher**  Head of Transaction Banking, Treasury |  |
| REVIEWER | **Benjamin Fite**  Counsel – Digital & Privacy, Legal |  |
| REVIEWER | **Andy Smith**  Principal Security Architect, Digital Security |  |

bp would like to also recognize the Ernst & Young blockchain team for their work on this project including John Frechette, Andrew Forman, Sooraj Janardanan, Mohammed Shameem, Miranda Wood, and Hariprasath V.

bp would like to also commend and recognize the work from the Digital Science team at bp for their contributions, including Adrian Delgado, Jason Grant, Anthony Saba, Clena Marie Abuan, Richard Debney, and Claudia Perry.

# Abstract

The concept for Ethria was to be an open-source, not-for-profit application for funding research projects with the potential to accelerate the world’s transition to Net Zero carbon emissions. Participation in Ethria would have come from bp and individual donors, and all funding would have taken the form of donations. A transaction relayer would act as a forwarder of donations (transactions) to the blockchain on behalf of other users. There was no expectation of profit or other financial benefit, to bp or to any other contributor from their donations to Ethria. The guiding principles of Ethria’s application design are purposeful innovation, transparency, and inclusion. The Ethria application would allocate these donations through a pseudo-anonymized, semi-private quadratic fund matching method implemented through a zero-knowledge proof design, in a decentralized network (the public Ethereum blockchain). The initial proof of concept will mimic a quadratic funding round and was intended overtime to evolve towards a sustainable decentralized autonomous organization (DAO) for functionality beyond funding. Ethria would explore public blockchain and privacy-enhancing technologies, with the intent to establish and demonstrate how public companies can positively engage with open-source technologies from an innovation, legal, financial, tax and security perspective. Our definition of success is that broader communities improve upon Ethria’s design, towards a sustainable mechanism to further the world’s Net Zero ambitions while upholding the highest standards of governance, transparency and inclusion afforded by technology.

Table of Contents

[Abstract 3](#_Toc133930938)

[1. Introduction to bp 5](#_Toc133930939)

[2. Guiding Principles 6](#_Toc133930940)

[3. Vision and Roadmap for Ethria 7](#_Toc133930941)

[4. Project Selection and Criteria 8](#_Toc133930942)

[5. Ethria Participation 10](#_Toc133930943)

[6. Ethria Design 11](#_Toc133930944)

[Public Blockchain Evaluation 11](#_Toc133930945)

[Ethria User Flow 12](#_Toc133930946)

[Ethria Donation Transaction Design 14](#_Toc133930947)

[Ethria Fund Matching Methodology 18](#_Toc133930948)

[Ethria Zero Knowledge Proof Design 21](#_Toc133930949)

[7. Security and Risk 22](#_Toc133930950)

[Appendix 24](#_Toc133930951)

[A. The Evolution of Blockchain at bp 24](#_Toc133930952)

[B. Trends and Assumptions in Public Blockchains 25](#_Toc133930953)

[C. A Decentralized, Low Trust Design 28](#_Toc133930954)

[D. An Overview of Zero Knowledge Proofs 36](#_Toc133930955)

[E. The Ethria Zero Knowledge Proof 38](#_Toc133930956)

# Introduction to bp

At bp, our purpose is reimagining energy for people and our planet. After more than a century defined by two core commodities - oil and gas – we are pivoting from an international oil company (IOC) producing resources, to an integrated energy company (IEC) delivering solutions for customers. Our ambition is to be a Net Zero company by 2050, or sooner, and to help the world get to Net Zero. This ambition means reshaping our business as we decarbonize and diversify into different forms of energy, such as renewables, biofuels and hydrogen. With more than 100 years of experience in the world of energy, we want to move fast, and to do so with discipline and care.

bp’s new sustainability frame, which underpins our broader Net Zero ambition, includes 20 specific aims[[1]](#footnote-2) across: getting bp itself to Net Zero, helping the world get to Net Zero, improving people’s lives and caring for our planet. We believe technology has a key role to play in enabling those aims, and we believe technological innovation is a tool towards purpose. Since 2017 bp has been exploring blockchain and privacy-enhancing technologies (see Appendix A). To date, solutions have been developed primarily on permissioned blockchains while exploring the achievements in public blockchains. As the public blockchain ecosystem, privacy-enhancing technologies and Web 3.0 applications are increasingly maturing, we believe now is also the right time for bp to more deeply explore and to openly share lessons about how the world’s energy transition can benefit from these technologies. In the future these technologies can enable better governance mechanisms, transparency over decisions, and inclusive, organized dialogues across all stakeholders in the world’s energy transition.

# Guiding Principles

There are three principles that guided the design of Ethria application: innovation with purpose, transparency, and inclusion.

By “**innovation with purpose**”, we mean using technology in new and novel ways to address acute challenges in accelerating the world’s energy transition to Net Zero before 2050. This type of innovation is adaptive and iterative. While building applications and features in small steps, these projects are intended to move fast, to yield practical and shareable insights, and to form a pathway towards a broad global, impact.

By “**transparency**”, we mean making transpicuous in word and in code any decisions or trade-offs for end users. Communicate the alternative design and technology choices that are available, and the rationale of decisions and design choices made. Whether in organizational or technological domains, while we do not assume to have all the “right” answers, we did aspire to make our hypotheses readily accessible for feedback and collaboration. Public blockchain applications we intended to build are examples to promote this open approach to innovation in the energy industry.

Finally, we recognize in the context of the world’s energy transition that governments, institutions, companies, and every private individual in the world is a stakeholder. By “**inclusion**”, we mean that these diverse stakeholders should be represented in technological innovation that we develop and should benefit from its outcomes. Furthermore, participation should be equitable to align community interest best with funding resources.

# Vision and Roadmap for Ethria

Our vision for the Ethria application was to connect those working on some of the hardest problems of Climate Change with the resources of companies, institutions, and individuals. We aimed to explore the scale at which public blockchain and privacy-enhancing technologies can organize such connections in a way that is global, transparent, and beneficial for all parties.

We recognize that achieving this vision will be a multi-disciplinary effort. For everyone from public companies to private individuals to participate in Ethria, we will have to innovate not just on technology but also across the associated legal, financial, tax, security, and regulatory compliance domains. As such, launching the initial iteration of Ethria would be an incredibly important first step in a multi-year roadmap.

We expected Ethria to move through several iterations to optimize towards improved user experience, trustlessness, privacy, scalability, and sustainability. Timelines should be adjusted based on lessons learned, how technologies evolve, and how regulations may change.

Initial goals of Ethria are listed below. USDC amounts are represented as variable letters for demonstration purposes.

1. bp will explore the potential of decentralized applications built on the public Ethereum network combined with quadratic fund matching for the allocation of resources to open-source projects that address climate action.
2. bp will ensure Know Your Customer (KYC) requirements are implemented for donors to Ethria in a manner that optimizes user experience and transaction cost, while allowing bp to reach an adequate decentralized user base and ensuring compliance.
3. The matching pool from bp to be used in the quadratic funding mechanism will be “X” USDC in total. Since this is a new funding mechanism for bp and the university projects alike, each of the five participating projects will be allocated “Y” USDC to ensure projects can produce minimum deliverables. This leaves “Z” USDC for the quadratic funding allocation (5\*Y+Z=X). Funding is exclusively towards non-commercial, open-source climate projects at this stage. Ethria is not operated for profit, and all donations to bp’s Ethria are donations toward open-source work for public goods, with no expectation of profit, or other financial benefit, for any of the participants or bp.
4. The initial Ethria quadratic funding round will be capped at “A” USDC, which includes the “B” USDC from bp. This means donors may give up to “C” USDC in total (B+C=A). There is a limit of “A/100” USDC donation per individual.
5. Projects eligible for funding from Ethria are pre-selected by bp. bp has chosen this method for compliance and speed of execution to complete the initial quadratic funding proof of concept.
6. The matching pool distribution will be calculated off-chain. Proof of the correct decryption of tally will be verified on chain through a zero-knowledge proof system, and the on-chain funding allocation will be shown to align with those results. For the purposes of the initial proof of concept, bp details the trust assumptions and tradeoffs required from the user in subsequent sections of this paper.
7. bp will demonstrate how public companies can begin interacting with public blockchains by using solutions for enterprise-level custody, security, and legal compliance.

# Project Selection and Criteria

For the Proof of Concept, bp wanted to select five projects that are eligible to receive funding as research initiatives from a respected institute. Funding would have been in the form of grants, not investments. There is no direct financial return to bp or donors. Additionally, bp will not receive any rights to intellectual property from these projects.

In selecting eligible projects, bp applied the following criteria:

* The project output (e.g., research or code) must be publicly available and freely accessible. In addition, the resulting work should not be proprietary or patented.
* Project outputs must contribute to achieving global Net Zero carbon emissions.
* Projects must be involved in one or more of the following categories: social impact/engagement related to Climate Action, carbon emission reduction, carbon removal, renewable energy, electric vehicles, battery storage, energy efficiency, green hydrogen.
* Projects must be able to receive payment on the Ethereum blockchain in United States Dollar Coin (USDC) for purposes of transparency.

# Ethria Participation

Participation in Ethria is open to any individual that successfully passes a KYC (know-your-customer)/AML (anti money laundering) process. Participation will be available on a first-come, first-served basis and is subject to reaching the monetary cap of the initial fundraising round. The initial fundraising round will be capped at a total of “X” million USDC. “Y” USDC will come from bp, leaving a cap of “C” USDC from potential donors.

For the initial stage of Ethria, we would expect that participants have existing familiarity with public Ethereum, digital wallets and decentralized applications. Decentralized application users are those that interact directly with decentralized applications on public blockchains using self-custodial wallets. Hence, individuals that own or trade cryptocurrency solely through custodial exchange accounts do not meet the criteria to be classified as decentralized application users. bp would not facilitate the purchase of Ether or United States Dollar Coin (USDC) on behalf of users. Introducing new users to self-custodial Ethereum wallets is not a key objective for this initial version.

In future iterations, we aspired for participation from an increasingly broader audience as a key objective.

# Ethria Design

In the proof-of-concept, bp will use a smart contract system on the public Ethereum blockchain to collect and allocate donations among the five selected Climate research projects. This smart contract system will mimic a quadratic funding round. Future iterations are intended to become a long term sustainable decentralized autonomous organization (DAO).

## Public Blockchain Evaluation

We considered public blockchain technologies with the most active users and aimed to position Ethria for collaboration in the future; thus, we sought a public blockchain platform with significant developer activity. In addition, sufficient stable coin liquidity was a design requirement. The USDC stable coin was chosen as the funding token to decrease the risk of cryptocurrency price volatility to Ethria projects. bp is cognizant that the use of a stable coin does not eliminate the risk of cryptocurrency price volatility.

An important factor was the ability of a public blockchain to iterate and improve over time. These iterations and improvements may come from the core developer team of the blockchain or other teams building decentralized applications on top of the protocol. A core premise of innovation in public blockchains is decentralized and open participation in both consensus as well as activity, such as transactions or developer access. While the speed of transactions is important, speed can be achieved through tradeoffs that lessen decentralization of consensus or participation. In our view, should a public blockchain not achieve decentralization in either form, consensus or participation, the case for its use becomes much weaker versus existing mainstream technologies that can be more easily implemented.

Based on these considerations, we chose the public Ethereum blockchain as the underlying protocol for Ethria. This is a fast-moving space, so as technologies evolve in 2023+ this choice will be continuously re-evaluated.

## Ethria User Flow

Prior to an in-depth discussion on the technical aspects of the application, a high-level user journey explanation will give more context on the design choices we made. First, we wanted to ensure the user, or donor, was only required to submit one Ethereum transaction to contribute to Ethria to minimize gas fees. We wanted to avoid the scenario in which donations to multiple projects required more than one Ethereum transaction.

The first Ethria funding round in its first year of deployment allows users to browse all projects. As the user identifies a project that they would like to support, they will enter how much they would like to contribute to that project in the form on the website and will click to add the project to a checkout basket. Users will be able to add multiple projects to their basket at different contribution levels. This process is akin to browsing the products of an ecommerce platform and adding them to a checkout basket. For example, a user could add Project A for 100 USDC and Project B for 200 USDC. The maximum amount a single user may contribute to Ethria in total is 9,999 USDC. When the user has finished selecting projects to fund, they will ‘check out’. During the browsing process, users are not required to be signed into their Ethereum wallet.

At any point in this process, required before moving forward with KYC, the user will log into their respective Ethereum wallet and sign a message with their private key to prove their ownership of the wallet. Users will then step through a KYC/AML process to ensure that bp is compliant with all regulations required to host Ethria. KYC services will be provided through Acuant[[2]](#footnote-3). When KYC/AML is completed successfully, users will be ready to complete their contribution to the Ethria.

Users will then select how they would like to pay for their transaction fees. bp will pay for Ethereum transaction fees on a first come, first serve basis through a transaction relayer. bp’s transaction relayer will be limited to the equivalent of $10,000 in Ether to fund transactions. A user must contribute 100 USDC in total to qualify for using the relayer funds.

We anticipate the transaction relayer fund to be depleted. Hence, alternatively, if the Ethria funding period is still open and the Ethria cap of “X” USDC has not been reached, the user may pay for transaction fees themselves. If a user elects to pay their own gas fees, they may contribute any amount they like up to 9,999 USDC. The transaction design is further detailed in the next section.

Regardless of whether bp is paying for transactions fees or not, when the user submits the contribution, the total amount of funds will be sent to Ethria in one transaction. For example, if a user plans to contribute to Project A for 100 USDC and Project B for 200 USDC, 300 USDC would be sent from the user to Ethria in one transaction. On the backend, the 100 USDC for Project A and the 200 USDC for Project B will be recorded as encrypted ‘votes’ off chain towards the respective projects to be used in the quadratic funding allocation at the end of the Ethria fund raising round. At the end of the fundraising round, the outcome of these votes will be posted on chain as part of the zero-knowledge proof system, detailed later in this paper.

After the Ethria funding round has concluded donors, or observers, who have provided their email address specifically for correspondence will receive updates from bp as the funded projects move through the deliverables that they committed to in their proposals. These deliverables are provided in the project information pages on the Ethria website. These updates will also be shared on the Ethria website for anyone to view.

## Ethria Donation Transaction Design

The cost of transactions on the public Ethereum main network has fluctuated drastically over the past year and notably increased. Those unfamiliar with public blockchain may not be aware that the transaction fees on Ethereum rise and fall based on the level of network activity. Users determine the fee which they are willing to pay for a transaction to be mined. For example, if network activity is very high, users may start to pay higher fees to have their transactions processed more quickly. However, if network activity is low, users will seek to pay lower fees as they are competing with less activity to have their transactions processed.

This fee market is essential in incentivizing miners and validators to participate in the consensus of the network and ensuring developers consistently look for ways to optimize transaction fees to accommodate for growth in the network, thus avoiding spam transactions. Consequently, high transaction fees are not necessarily a signal of failure for public blockchain but rather a signal that users are using the network and that miners or validators have an incentive to secure it. Rather, consistently prohibitive high transaction fees for users on a decentralized application would be a detriment as it would lessen user adoption, which is why it is imperative for bp to stay attune to systems that optimize transaction fees, maintain decentralized security, ensure system liveness, attract developers, and see user adoption.

In addition to absolving users of the transaction cost, a transaction relayer will also allow for bp to manage the KYC/AML process with slightly less complexity. A transaction relayer allows a specific Ethereum account to act as a “forwarder” of transactions to the blockchain on behalf of other users. This design allows the relayer to pay transaction fees on behalf of the original transaction signer. In this respect, users will have to trust that the bp relayer does not censor any transactions by not sending them to the blockchain. However, users can be assured with this method that transactions cannot be falsified on their behalf.

In the case that bp pays transaction fees on behalf of a user, after completing KYC, the user will need to sign a message authorizing this transaction. *Signing a message* is a different method than *sending a transaction*. In signing a message, a user will use their corresponding public key and private key to digitally “sign” their agreement to a message or code. Signing a message is akin to the digital version of signing a physical contract with a personal signature.

In contrast to sending a transaction, signing a message is not something that is broadcast to the blockchain itself as it does not involve any changes of blockchain state. In other words, signing messages cannot be used to complete activities such as sending a token. Signing a message does not require any transaction fees in Ethereum.

For Ethria, for bp to pay for transaction fees on behalf of the user, the user will need to sign a message authorizing bp to send their respective USDC to the Ethria smart contract system. The message will be prompted and signed through the user’s respective Ethereum wallet. After the user signs the message, the user will need to click to confirm their contribution, and bp will relay the transaction to the main Ethereum network. In relaying the transaction, bp will not have access to user funds at any point. The relaying account acts as a forwarding address and will only broadcast the original transaction sent to Ethria to the Ethereum network, paying user fees on their behalf.

Diagram

Description automatically generated

Figure 1 Ethria User Flow #1 - bp paying transaction fees on the behalf of users

Should a user elect to have bp pay for transaction fees, he or she should be aware that they will not have control of the timing of their transaction processing, which may take several minutes based on network activity and transaction fees at the time. bp will seek to optimize transaction fees from relayed transactions to allow for the greatest number of users to benefit. To optimize transaction costs and handling, bp will be using Infura Transactions (ITX).

If a user is paying transaction fees on their own behalf, he or she will be able to more closely control the time required for transaction processing. For example, the user can elect to pay a higher gas fee to have their transaction processed faster on the Ethereum network. bp will not provide transaction fee suggestions to users as these can be obtained through other community websites and tools that have more experience monitoring fluctuating Ethereum transaction fees. Users that pay for transaction fees on their own behalf will be required to provide a digital signature authorizing the USDC transaction and allowing bp to provide a digital signature to KYC the respective Ethereum address for an on-chain transaction. Subsequently, users that pay for their own transaction fees will need to submit their contribution transaction on the main Ethereum network for processing, setting their desired transaction fees.

Diagram

Description automatically generated

Figure 2 Ethria User Flow #2 - user paying transaction fees on their own behalf

bp recognizes that a transaction relayer that pays for users’ transaction fees is not a sustainable solution for Ethria. However, by allowing for a portion of users to participate in the initial proof of concept on the public Ethereum mainnet without concern for transaction fees, bp has opened Ethria to a larger amount of decentralized application users and has decreased some barriers to entry by providing this service. In the future, bp would look to other methods of managing transaction costs through Layer 2 scalability designs or other public blockchains. bp does not expect to continue to pay transaction fees on behalf of users.

## Ethria Fund Matching Methodology

To move towards greater inclusion, we considered several fundraising methodologies. For the initial version of Ethria that was going to be deployed, bp was to allocate “X” USDC between five distinct projects. We considered these projects as “public goods” in that these projects will be delivering results for the community that contribute to non-rivalrous and non-excludable resources, e.g., clean air, in an open-source manner. The Ethria team was keen to investigate new methods for addressing challenges that are typically encountered in distributing resources for public goods.

In funding public goods, if decision making is determined wholly by those with the largest financial resources, then the preferences of individuals with lesser financial resources are underrepresented. A common alternative to this approach is the allocation of one vote per person to determine funding allocation; however, this methodology provides for only for a singular level of interest. Consider an example of voting on fund allocation for open-source software grants. Developers and programmers will have greater interest in this category and may be content to pay a higher price to have more voting power to determine where funds are allocated.

bp looked to successful fundraising designs employed by communities in the public Ethereum ecosystem that encourage participation across all levels of financial donations. Notably, Gitcoin, an organization that promotes the sustainability of open-source software and other public goods has raised over $51.6M in funds since its inception in 2018[[3]](#footnote-4). A particularly successful fundraising design used by Gitcoin has been around a methodology termed *quadratic funding.*

Quadratic funding uses a novel method of fund matching to reflect the preferences of donations in alignment to group preferences over individuals’ preferences, thus achieving a more democratic methodology of funding. This is accomplished by aligning fund matching according to the preferences of the largest *number of individual donations* over the largest *donations.* Quadratic funding does this by matching funds based on square of the sum of the square root of each contribution. In this way, funds are matched with a more democratic method across a group.

Multiple individual donations can make a more significant impact over a single large contribution when directing the allocation of the fund matching pool. Hence, quadratic funding addresses, in part, the challenge of getting people to think in terms of a community rather than individually because even small actions matter. When using a limited matching pool, as in bp’s case with Ethria, the funding matching allocation mirrors the allocation of an unlimited pool yet restricted to the capped amount.

Imagine a charity organization is fundraising for Project A, Project B, and Project C. This charity organization has a generous philanthropist who is committed to matching all funds donated across all projects. In this fundraising, two large donors contribute $5000 each to Project A, 50 donors contribute $100 each to Project B, and 100 donors contribute $50 each to Project C. In a conventional fund matching scheme, where contributions were matched on a one-to-one basis, Project A would receive an additional $10,000 in matching at the preference of two large donors. Project B would receive $5,000 in matching, and Project C would receive $5,000 as well, although Project C had *double* the number of donors than that of Project B and *50x* more donors than that of Project A.

In contrast, quadratic funding allocation aligns fund matching to the largest number of individual donors over the donation amount. This method accounts for the preferences of the total contributor group over the preferences of the largest donors.

As aforementioned, quadratic funding accomplishes this by matching funds based on square of the sum of the square root of each individual contribution. In unlimited matching, Project A would be match by or roughly $20,000. Project B would be matched by or $250,000. Project C would be matched by or $500,000! Through this mechanism, one can see how matching is weighted towards the number of donors over the amount contributed. In quadratic fund matching, donors can be confident in that even with small contributions, with multiple donors, their funding will be even further amplified.

For the initial year of deployment, Ethria would have used a quadratic fund matching approach so that bp matching funds can be allocated based on the preferences of individual donors over large donors. The matching pool in Ethria will be limited and hence will be allocated in alignment with quadratic funding distributions. For example, continuing in the above example, Project A receives $20,000 from an unlimited matching pool but would receive ~2.6% of the total matching pool in a limited scenario. (In the example, a total of $20,000 would be donated to Project A, $250,000 to Project B, and $500,000 to Project C for a total of $770,000. $20,000 is about 2.6% of the matching pool.)

A challenge of note in quadratic fund matching is that systems may be vulnerable to collusion in which a group of individuals may be bribed to contribute to a project to amplify the matching pool contribution. KYC (Know Your Customer) requirements can help to thwart such activity as the barriers to entry in contributing to the projects are heightened.

Another project running on the Gnosis Chain network, clr.fund[[4]](#footnote-5), has also used this fundraising allocation methodology. In addition, the Ethria team looked to clr.fund’s use of the MACI (Minimum Anti-Collusion Infrastructure)[[5]](#footnote-6) zero-knowledge proof design for inspiration in Ethria’s zero knowledge design. The MACI zero knowledge proof design does provide for a measure of collusion resistance in voting systems; however, the bp zero knowledge proof design cannot make as heightened of guarantees in this category.

In the future, we propose that other large corporations contribute only to the matching pool, which does not provide for any voting or decision making as to where the funds are allocated. This is an area of active research, and we expect this design to evolve for 2023+ versions (if Ethria were deployed), as we introduce external ESG (environmental, sustainability and governance) oracles and move towards an increasingly more dynamic determination in other decisions of Ethria activity, such as project selection. For example, participants with externally attested higher ESG ratings might receive more voting credits.

For the Ethria funding round, after one month of open donations, the funding allocations would be tallied and verified on-chain through a zero-knowledge proof. Ethria is intended to reflect the desired allocation across all projects by participants. Funding allocation will be executed programmatically; therefore, we expect that funding allocation could beweighted towards one project or another.

bp will execute a function to send the funds from the Ethria smart contract to the respective projects’ Ethereum accounts. The research institute with the climate projects would use their own discretion to continue to operate in USDC or convert their funding to fiat currencies.

## Ethria Zero Knowledge Proof Design

As participants donate to Ethria, their contributions will be recorded as votes that will be used to determine where the bp matching fund is allocated. An on-chain voting methodology was avoided so as not to incur additional transaction fees. Also, storing full voting information on the Ethereum main network is not a practical long-term solution for extensive data storage in voting systems.

# Security and Risk

To take a structured approach to security and risk, we adopt the evolving World Economic Forum framework for classifying risks for Decentralized Finance (DeFi) applications[[6]](#footnote-7). As the 2022 version of the Ethria application is not a financial investment, many of the risks listed in the WEF framework will not be applicable, but we believe this approach is prudent because: a) it allows us to systematically capture and assess risk from the beginning, and b) it allows us to scale into managing more complex, and more material risks, as Ethria scales towards a more general purpose vehicle, which could eventually include financial use cases, if aligned to its overall principles.

In addition, all versions of Ethria smart contracts will at a minimum undergo an independent security audit. The 2022 launch has been audited by Least Authority, a leading smart contract security firm. We have chosen to publish the results of the security audit at Least Authority’s Reports site[[7]](#footnote-8), available for public viewing.

Graphical user interface, application

Description automatically generated

Figure 3: World Economic Forum DeFi Risks

# Appendix

# The Evolution of Blockchain at bp

Since 2016 bp has explored private and consortium-based blockchains, in fields such as supply chain, energy trading and energy management. We continue to explore private blockchain use cases with relevant partners, especially where they can serve the purpose of testing new business application designs in a high velocity, low risk manner.

Longer-term, we see the largest promise and expect the largest value from blockchain technologies to come from public networks. We see public blockchain as a novel way to construct general purpose, decentralized applications, and we currently focus our research and development efforts in this area. While public blockchain as emerging, rather than mainstream, use cases like decentralized finance and identity in public blockchain have made significant progress towards maturity in the past five years. Further, we recognize that for public companies such as bp, building public blockchains applications is only partly about technology innovation. It also requires innovation in law, finance, tax and security practices – these are key areas of research for us, and areas on which we’d welcome collaboration.

Finally, as public blockchain technologies continue to evolve, we don’t believe bp needs to take a “settled” position on what will be the “winning technolog(y)ies” of the future. We believe that will be eventually determined by the confluence of end users and developers around specific design choices, some of which are emerging now and others that have yet to appear. bp’s choice of public blockchain for a particular application is likely to remain “tactical” for the near future, which is to say determined on a case-by-case basis. We do expect that, in the spirit of contributing to innovation in the broader public blockchain ecosystem, bp will continue to openly share its design choices, the trade-offs we experience, and any lessons learned.

# Trends and Assumptions in Public Blockchains

We consider the following six trends and assumptions as important, in guiding the trajectory of public blockchains.

First, public blockchain has the potential to develop as a significant settlement layer for value. Of note in January 2021, the US Office of the Comptroller of Currency released a statement in which federally chartered banks may use stable coins on public blockchain networks as a means for payment activities[[8]](#footnote-9). More recently the Ethereum network settled 6 trillion dollars’ worth of transactions since the October 2020[[9]](#footnote-10). Of significant note, sixty percent of these transactions occurred with stable tokens involved.

Second, there has been a rise in users participating in direct to customer non-custodial financial services through the advent of decentralized finance applications. Users of decentralized financial protocols use accounts, or wallets, with direct access to public blockchain networks that can operate independently of central exchanges as users are in control of their respective private key which allows for transactions to be sent directly from such an account. In January 2020, less than 100,000 accounts existed that used decentralized finance applications. To date, this has grown to over 4.3 million[[10]](#footnote-11). Although challenges continue to exist for self-custodial accounts in the realm of user experience and account recovery, the growth in usership is a notable trend.

The third trend that bp notes in public blockchain development is the growth of tokenized value representing assets, bonds, and securities in public blockchain networks. For example, earlier this year the European Investment Bank issued its first digital bond on a public blockchain[[11]](#footnote-12). Also, Switzerland’s tokenized securities law also took effect to allow for security issuance on public blockchains[[12]](#footnote-13).

The fourth trend that bp has identified is the growth in the tokenization of national currencies in the form of stable coins or tokens. Most recently, as of the end of May 2021, public stable coins have exceeded $132 billion in value[[13]](#footnote-14). United States Dollar Coin (USDC) has grown from a market cap of $3.5 billion at the beginning of 2021 to exceeding $33 billion at the time of writing. With over 200 stable token projects in existence, stable tokens exist on a spectrum of decentralization, transparency, and methods from 1 to 1 collateralization with fiat currencies to algorithmic methods with may or may not be collateralized by other cryptocurrencies.

Stable tokens are not without fault or risk. In attempting to maintain a peg to fiat currencies, stable tokens do experience fluctuation; however, the degree to which some stable tokens have been able to maintain a consistent peg is of note and enables users to transact with a higher degree of confidence in a stable value transfer. Outside the development of public stable tokens, 80% of central banks are exploring use cases with digital currencies, and 40% of those central banks are already testing proof-of-concepts[[14]](#footnote-15).

The fifth trend identified is a move to community owned or managed organizations using decentralized autonomous organizations (DAOs) in public blockchains. The ethos of decentralization reverberates in the governance of public decentralized applications through DAOs. A decentralized autonomous organization (DAO) is an organization whose decisions, finances, and funding are not controlled by a single entity or decision maker. Actions are determined based on the predefined consensus of the participants and executed through code. Participation may be open or require qualifications for participation. In 2021, the impact of DAOs has grown tremendously as they now manage over $1 billion in funds[[15]](#footnote-16). Among the most well-funded DAOs, approximately 70% of them were only just launched in 2020 and later[[16]](#footnote-17).

Lastly, the sixth trend identified is the increasing reliance on cryptographic proofs to enable scaling of transaction throughput while maintaining decentralization. To date, blockchains have relied on miners and nodes to replay transactions in order to validate their occurrence. This method restricts a blockchain system to only scaling linearly as more transactions and more complex transactions coincide with equally increased replay time required, which does not take into account the security requirements around sync time for validators.

In the Ethereum ecosystem, two scaling techniques have arisen to contend with this challenge. Optimistic rollups rely on a system of fraud proofs to prove a series of transactions that occur off the main network chain and that can be validated on chain to establish legitimacy and challenged, if needed to reconcile. Zero knowledge rolls rely on a system of validity proofs to prove a series of off-chain transactions as well. Both methodologies enable a batch of off-chain transactions to be validated within a single on-chain transaction, thereby, increasing transaction throughput through the use of proofs, not transaction replay or centralized off-chain systems.

# A Decentralized, Low Trust Design

The current iteration of Ethria is adapted from a near trustless, decentralized design.

The trusted setup for the initial Ethria design will be performed by bp. Users will need to trust that this setup has been completed with integrity such that bp cannot use the toxic waste to generate malicious proofs. In the future, bp will look to explore the facilitation of trusted setup ceremonies with public participation or the use of zero knowledge proofs which do not require trusted set ups.

In a future zero knowledge proof design for Ethria, increased decentralization and trustlessness would come from tallying user-submitted votes on-chain autonomously. Using homomorphic encryption, the tally would update continually without interaction from the coordinator *and* without revealing votes.

Diagram

Description automatically generated

Figure 4 The potential future Ethria Design

This high-level diagram gives a rough overview of the contribution stage of a future decentralized Ethria. Here, for simplicity, the encrypted votes are referred to as (V) rather than E([Vi]) as above.

A user wishing to vote without interacting with the coordinator will:

* Encrypt their contribution and vote split with the encryption public key, hosted in the contract.
* Create a zero-knowledge proof attesting to:
  + The validity of the vote
  + The validity of the contribution split and sum
  + Correctness of encryption using the public key, Y
* Create a signature allowing the Ethria contract to withdraw USDC equal to the total contribution sum.
* Submit the proof, USDC signature, encrypted vote split, encrypted contribution split, and total contribution to the contract.

If the signature resolves and the verification passes (assuming the user has also passed the KYC checks), the encrypted vote and contribution are ‘added’ to a running pair of tallies; total contribution, (F), and votes, (T). Recall that these values are elliptic curve points, added using the group operation of the elliptic curve, which is performed autonomously on-chain. The coordinator gets no say in when or how the votes are tallied this way.

For the initial version of Ethria, bp will using a third party, Acuant, to provide KYC services. For the future purposes of extending decentralization, we anticipate that an external decentralized KYC provider will eventually be able to confirm a user’s eligibility on-chain (e.g. adding their address to a contract mapping). This KYC provider would be need to be able to ensure and prove that KYC met all compliance and regulatory standards.

Currently designed for mainnet, the initial implementation includes an option for the user to forgo gas fees and relay their transaction through bp. Essentially, the user trades gas cost for a higher trust in the coordinator. Given the expense of verifying a GM17 proof on-chain, this relayer option intends to increase participation in Ethria. No proof is required in this method since the checks which occur in the circuit are instead completed off-chain by the application, and the transaction only relayed if those checks pass. This ensures that the pool funding relayed transactions does not diminish too quickly, though it does mean that even users voting themselves will have to trust that bp is not censoring valid relayed votes and not adding invalid votes of their own through the relayer.

For a near trustless solution, this relaying option would either also contain an on-chain proof verification or not exist. If a future iteration utilized a Layer 2 solution with precompiles suitable for GM17 verification, it’s likely that the costs would be low enough to eliminate the need for a relayer.

A user wishing to have their contribution relayed by bp takes the same steps as the direct method, but instead of generating a proof they sign a message containing the public information: the USDC signature, encrypted vote split, encrypted contribution split, and total contribution. This signature is checked on-chain to be valid and from the address the relayer claims is contributing (i.e. the signed message has the same author as that of the USDC authorization signature), ensuring that the coordinator cannot mutate votes.

Diagram

Description automatically generated

Figure 5 The current design of Ethria

In the future design, once the voting round is complete, we have some publicly known variables in the Ethria contract, namely:

* The final encrypted tally, (T), split by project
* The final total for contributions, (F), split by project
* The matching pool, M, equal to the sum of USDC contributed by bp
* The funding pool, P, equal to the sum of USDC contributed by users
* The encryption public key, Y

To initiate distribution, the coordinator provides a proof as described at the end of the ZKP section attesting to their knowledge of the decrypted tallies, T and F. The contract verifies this proof against the public variables Y, (T), and (F), and computes a check that the sum of contributions found in decryption (recall that the user funding F is split per project) is equal to the funding pool P.

With all the information required for quadratic funding available in the contract, the funds are distributed according to the previously described formula. Since the source of this information is either autonomously calculated on-chain or proven to be correct, users do not have to trust the coordinator to trust the result. Alternatively, in the current version, the presence of the relayer does mean that the coordinator can censor and provide invalid votes. We intended for future iterations to allow for lower gas usage and hence no need for the relayer to lessen the cost burden on users.

Diagram

Description automatically generated

Figure 6 The future proving stage design of Ethria

While this design still relies on a coordinator to initiate voting and distribution, we are not aware of a quadratic voting system which does not (MACI, for instance, also requires a coordinator). It protects against the coordinator:

* Censoring direct, valid on-chain votes
* Mutating relayed votes before being added on-chain
* Removing or mutating on-chain votes
* Providing an incorrect tally (or any value related to distribution)

Without the relayer, the coordinator is also prevented from censoring any vote and providing ‘votes’ of their own without a proof of validity. They may, however, choose to never initiate distribution, effectively locking user funds in the contract. Adding a distribution timer which counts down to some predetermined limit and refunds users at its end would mitigate this risk.

There are several possible user-based attacks on voting systems. Using the proof, we prevent invalid votes (e.g. negative amounts, amounts differing to the USDC donation) and non-decryptable values. Users cannot manipulate the tally since it is only updated when a valid vote is received in the contract.

Sybil attacks, however, are particularly severe since ten votes of $10 are worth more than one vote of $100 in quadratic funding. In this design and the current iteration, we allow one contribution call per user. While it is possible to combine separate donations, it would require removing the user’s ‘old’ contribution and replacing it with a new one equal to the cumulative sum so far. We would need a separate circuit to prove this new donation, and its square root vote, is valid and has the correct sum before subtracting the old vote from the tally.

We also assume that our KYC provider adequately prevents one person voting with multiple addresses, and blocks addresses known to be involved in hacks or suspicious activity. Using a separate provider for voter uniqueness, such as BrightId, may also solve the former.

In order to simplify an initial proof of concept and adapting to current high gas costs, for this initial round we made trade-offs on decentralization and coordinator interaction. In summary, the increasingly decentralized design above comprises of the stages:

* Voting: Encrypted vote and contributions sent on-chain with **proof of correctness**
* Contributing: USDC transfer of total contribution
* Tallying: Tally computed with elliptic curve addition on-chain
* Proving: Coordinator sends proof of decryption of tally on-chain

The first limiting factor in gas cost is the proof of correctness for votes. Even with precompiles, this is a heavy operation for GM17 and G16 proving systems and could easily cost more in gas fees than the user’s donation. We traded this cost for interaction with and trust of the coordinator, replacing the proof with an admin signature. This signature is only provided if the checks present in the circuit pass. However, this increases the requirement for users to trust that the coordinator will not censor votes or allow other invalid votes into the contract.

The next limiting factor is tallying. Not a simple addition, two elliptic curve points per project must be combined with another pair on-chain. At the time of writing, it would cost around $55 in gas fees to perform ten (=5 projects \* 2 points) elliptic curve additions and update the storage variables. This is still less than the cost of providing a proof that the vote is valid and a new tally has been calculated correctly, but not low enough for typical users.

Therefore, the next stage of gas saving compromises reaches:

* Voting: Encrypted vote and contributions sent on-chain with **coordinator signature**
* Contributing: USDC transfer of total contribution
* Tallying: Tally computed with elliptic curve addition on-**chain or new tally sent with each vote, confirmed by coordinator signature**
* Proving: Coordinator sends proof of decryption of tally on-chain

Considering that a mainnet USDC transfer costs around $20 in fees alone, the combined cost of storing votes on-chain was still considered too high for adequate participation. For this round, we took votes off-chain to provide the initial design:

* Voting: Encrypted vote and contributions **sent off-chain**
* Contributing: USDC transfer of total contribution **with coordinator signature**
* Tallying: Tally **computed off-chain**
* Proving: Coordinator sends proof of decryption of tally on-chain

bp is keen to leverage the scalability afforded by Layer 2 technologies to further decentralize the zero knowledge proof design in future revisions of Ethria.

# An Overview of Zero Knowledge Proofs

In exploring public blockchain use cases, bp is conscious of future privacy requirements for retail consumers, industry peers, and other business partners. Of equal importance is the ability to scale public blockchain systems. bp recognizes that zero knowledge proofs can provide potential solutions in both categories.

Zero knowledge proofs are a class of cryptographic protocols in which one can prove honest computation without revealing the inputs to that computation. A simple high-level example of a zero-knowledge proof is the ability to prove you are of legal voting age without revealing your respective age. In a zero-knowledge proof system, there are two participants: a prover and a verifier. A prover will present a mathematical proof of computation to a verifier to prove honest computation. The verifier will then confirm whether the prover has performed honest computation based on predefined methods. Zero knowledge proofs are of particular interest to public blockchain activities as the verifier can be codified in smart contracts as opposed to trusted parties or third-party intermediaries.

More subtly than the name implies, zero knowledge proofs offer a compelling manner of scaling public blockchain activities as well. Zero knowledge proofs are composed of a proving system and a privacy layer. In solely using the proof system, although privacy is negated, scaling can be achieved.

In traditional blockchain consensus mechanisms, validators or miners must completely replay a transaction to verify the transaction happened correctly. For example, if Bob sends Alice 3 Ether, a miner or verifier must completely replay that code to check for transaction integrity (e.g., Did Bob sign the transaction with the correct private key? Did Bob have enough Ether in his account to send 3 Ether to Alice?) In proving systems, instead of replaying fully transactions to verify integrity, the transaction integrity is checked through a condensed mathematical proof.

A mathematical proof is an argument for a mathematical statement that convinces an audience of its truth. For example, if one makes the assertion that , (.9 infinitely repeating) is equal to 1 in mathematics, how can this be verified? One may attempt to show that as is elaborated to and so on so that the value will eventually approach 1 even closer. This approach would certainly be very time consuming and burdensome. However, one may also consider how is equal to , and + is equal to 1, implying that or must also be equal to 1.

In the same way in which the logic for the above example was compressed and expedited through a mathematic proof so are other mathematical methods that can be verified by code. Blockchain lends itself to this design pattern as every transaction is based on its mathematical viability. For example, when a user signs a transaction with his or her private key, the key’s integrity is checked through math, not a database housing records of public keys and their respective private key correlation.

Verification of transactions through mathematical proofs provides a faster way in which to validate transactions rather than replaying transactions, and the design of blockchain itself lends itself to the use of zero knowledge proofs. Notably, not all zero knowledge proof systems that are designed for scalability include privacy; however, bp expects this conflation of objectives to increase with more research in the future.

# The Ethria Zero Knowledge Proof

If Ethria were deployed, bp would employ a zero-knowledge proof to provide a proof of tally of the votes. The current zero-knowledge proof design is not completely trustless. We will explicitly call out the trust assumptions required from users in the first Ethria proof of concept, and we will identify how Ethria may lessen the trust assumptions required from the users in the future.

In using the public Ethereum main network, bp is seeking to appeal to the largest pool of decentralized application users. However, bp is cognizant of the transaction fees incurred on the Ethereum main network. In avoidance of higher transaction fees for users, the ‘voting’ for where the allocation of funds go will be stored by bp off chain, rather than posted by users on chain. Thus, users will need to trust that bp does not censor any votes in Ethria, nor include additional votes.

bp considered Layer Two solutions and side chains; however, both the number of users and the readiness of the technology to support the risk incurred from bp as an enterprise company was deemed to be too much of a compromise to support an initial proof of concept in public blockchain. The development work to produce such solutions on alternative networks would have also imputed more complexity on the overall project.

For the initial Ethria funding round, the zero-knowledge proof will work as follows.

Assume a case in which a user wishes to donate a value CA to Project A, CB to Project B, and CC to Project C. The user will contribute Ctotal = CA + CB + CC to Ethria on chain. Off chain, bp will account for CA, CB, and CC as votes towards where the user wanted their funding to go. Recall that quadratic fund matching deals in the square roots of contributions. Many numbers do not have whole number square root values, which presents a problem with the modular arithmetic required by zero knowledge proofs. Thus, we will use a method to convert all contribution votes as whole numbers in the voting system by employing the following methodology for votes VA, VB, and VC:

This vote approximation may leave a 0.5% inaccuracy in the conversion from contribution amounts to voting, depending on the original donation amounts.

From here, the votes and project donors will be encrypted with a public key managed by bp using Elliptic Curve Elgamal encryption:

Text

Description automatically generated

Where capital letters (here, G, R, S, V, and Y) represent elliptic curve points, and operations on those points are performed with point addition and multiplication formulae. The key property of such formulae is that, for large scalar n and elliptic curve point P, calculating nP = Q is easy, but deriving n from Q is so difficult that it’s considered impossible (with current technology). This means that an observer cannot derive our private vote/contribution without knowing the private key x.

Another property of this encryption crucial to this project is its additive homomorphism. Instead of decrypting each vote individually and adding them up to find the final tally, we can instead add the *encrypted* votes using point addition:

Therefore, no decryption of private votes/donors is required until all the votes have been tallied.

To summarize, we encrypt a user’s contribution for each project and its corresponding vote; CA, CB, CC, and VA, VB, VC.

When the user’s USDC transaction is sent to the bp relayer or from the individual themselves, we will check that (1) votes are encrypted using our public key, (2) the contribution data matches the encrypted data, and (3) the user has passed all KYC checks. During the contribution transaction, in lieu of an expensive proof verification, bp provides a signature attesting that these checks have passed, which is confirmed on-chain. Hence, at this point, prior to transactions sent to the Ethereum network, bp will ensure that all votes have been properly included.

When the funding round has completed, bp will generate a proof demonstrating that we can decrypt the cipher texts representing the final tally with our corresponding private key. We prove that:

* Bp owns the private key corresponding to the encryption public key.
* Using this private key, each (encrypted tally for each project i) decrypts to the stated .
* Each (encrypted total contribution for each project i) decrypts to the stated.
* The stated is indeed the hash of all the public inputs to the circuit (all encrypted values, plaintext vote tally, plaintext total donors):

Thereby proving correct decryption of the encrypted tally. For the initial Ethria, the tally of the votes themselves are ultimate trusted; however, in the future, this tally would ideally be public and trustless. See Appendix C for an overview of this initial low trust design.

On successful verification of this proof, Ethria will then distribute the funds according to the below methodology.

Recall that each project will receive a baseline contribution from bp of “X” USDC for their participation. The total donations per project will be sent to their respective Ethereum account from the Ethria smart contract, ensuring that Ethria funding recipients will not have to pay transaction fees to receive their respective funds.

1. For details of bp’s sustainability frame and 20 Aims [see here](https://www.bp.com/en/global/corporate/who-we-are/our-ambition/our-aims.html). [↑](#footnote-ref-2)
2. See <https://www.acuant.com/> [↑](#footnote-ref-3)
3. Gitcoin, <https://gitcoin.co/> [↑](#footnote-ref-4)
4. Clr.Fund, <https://clr.fund/#/> [↑](#footnote-ref-5)
5. MACI, <https://appliedzkp.github.io/maci/> [↑](#footnote-ref-6)
6. For details of the framework, [refer to the WEF here.](https://www.weforum.org/whitepapers/decentralized-finance-defi-policy-maker-toolkit) [↑](#footnote-ref-7)
7. <https://leastauthority.com/security-consulting/published-audits/> [↑](#footnote-ref-8)
8. OCC, <https://www.occ.gov/news-issuances/news-releases/2021/nr-occ-2021-2.html> [↑](#footnote-ref-9)
9. Yahoo News, <https://www.yahoo.com/now/ethereum-settles-over-6-trillion-151045645.html> [↑](#footnote-ref-10)
10. Dune Analytics, <https://dune.xyz/rchen8/defi-users-over-time> [↑](#footnote-ref-11)
11. European Central Bank, <https://www.eib.org/en/press/all/2021-141-european-investment-bank-eib-issues-its-first-ever-digital-bond-on-a-public-blockchain> [↑](#footnote-ref-12)
12. Coindesk, <https://www.coindesk.com/switzerland-tokenized-securities-law-new-chapter-seba-sygnum-six-sdx> [↑](#footnote-ref-13)
13. Cryptoslate, <https://cryptoslate.com/cryptos/stablecoin/> [↑](#footnote-ref-14)
14. Coindesk, <https://www.coindesk.com/about-80-of-central-banks-are-exploring-cbdc-use-cases-bison-trail-report-says> [↑](#footnote-ref-15)
15. Decrypt, [https://decrypt.co/70405/over-1-billion-is-now-managed-by daos?utm\_source=reddit&utm\_medium=social&utm\_campaign=sm](https://decrypt.co/70405/over-1-billion-is-now-managed-by%20daos?utm_source=reddit&utm_medium=social&utm_campaign=sm) [↑](#footnote-ref-16)
16. Openorgs.info, <https://open-orgs.info/> [↑](#footnote-ref-17)