

Enabling privacy & trust in DeFi

Litepaper

Version 1.0 | May 2022

Contents

The Pro	blem With Layer-1 Blockchains and Private Finance	3
Our Sol	ution: Panther Protocol	4
Panther'	anther's Privacy Enhancement Stack	
	The importance of zero-knowledge proofs (ZKPs)	6
	zk-SNARKs	6
	Putting Privacy Enhancing Technologies First	7
Panther	's Unique Solutions: A DeFi Privacy Service	8
	zAssets	9
	Panther Pools (Multi-Asset Shielded Pools)	11
	zk and non-zk Reveals	3
	Panther's Private Interchain Bridge	4
	Panther Wallet	5
Realized	d Vision and Use Cases	6
Roadma	p	17
	anther's Native Token	
	A Game Theoretical Pricing Mechanism for Privacy	8
	Tokenomics of \$ZKP	
	Governance and Path to Decentralization	21
	\$ZKP's Value Accrual Mechanisms	
Concen	tualized By	23

The Problem With Layer 1 Blockchains & Private Finance

In a rush to build the future of finance, we have neglected to preserve a core piece of the human experience: *Privacy.* ¹

While decentralized networks seem to be humanity's best bet to create markets and societies that are freer, fairer, and more accessible, most of them contain a critical flaw: the data within them is public by default. This means that all transactions that take place on these protocols are visible to everyone, forever, leaving users exposed in significant ways. In public ledgers, such as Bitcoin or Ethereum, users' movements can be tracked, their decisions undermined, and individual freedoms steadily eroded.

In DeFi, we see how this visibility leads to a major loss of alpha for traders and capital firms. On Ethereum, for example, a third party can observe, track, link, and follow the movements of money from one account to another. As a result, participants have their investment strategies copied, attacked, front-run, and arbitraged. Not only does this limit the prospects of the industry, but it can run afoul of exchange laws in many jurisdictions.

The first wave of players in the blockchain privacy space created coins running in private ledgers, such as Monero and Zcash, with the aim to provide users with absolute secrecy to transact. While the technological accomplishments of these blockchain pioneers were impressive for their time, these coins never reached the level of adoption they intended. Instead, they attracted the ire of regulators and continue to be subject to niche use cases as volatile "store of value" instruments.

The crypto market has, so far, failed to produce affordable and viable means to allow users to control their data. It has also failed to create a DeFi (decentralized finance) ecosystem that is private by default but in which users (whether proactively or upon request) can share their transaction histories. Without all these critical components, any system will fail to gain mass adoption, and fall into the same niche use cases as its predecessors.

¹ Shai Mohan and Anish Mohammed. The New Secret. *Economic and Political Weekly*, 46(13):13–15, 2011.



Our Solution: Panther Protocol

The latest advances in Privacy Enhancing Technologies (PETs) offer the opportunity to evolve the way we share data, with new methodologies that are trustworthy, safe, and acceptable to all parties. Harnessing these developments, Panther has built a generalizable, cross-chain protocol that enables a "privacy toggle" for managing digital asset transactions and on-chain data.

Panther allows any market actor, from institutions to retail users, to *protect their financial movements* from the intrinsic faults of transparent ledgers by leveraging zeroknowledge proofs to rewrite the rules of DeFi.

Our Solution: The Panther Protocol

Panther works by using zero-knowledge proofs, namely zkSNARKS, in a multi-chain environment, to create fully collateralized, privacy-enhancing versions of ordinary digital assets. For a deeper dive into what zero-knowledge proofs are, please see "Privacy Enhancement Stack" below.

Unlike typical tokens, Panther's shielded assets (zAssets) cannot be traced, can be used across different blockchains and distributed applications, and have data trails that can be selectively revealed by their users. Panther, in this way, lets *users decide* who gets to look at their transaction history.

Panther also offers a solution to what is arguably *the biggest challenge facing DeFi*: onboarding institutions, legacy players, and FinTech companies into the new financial paradigm so that the industry can grow by several orders of magnitude.

Currently, DeFi offers an inhospitable environment to these market makers for the reasons mentioned above. Not only does the transparency of ledgers create an unfriendly environment for capital institutions and professional traders (whose reputation rests on their ability to outperform the market), it actively creates downsides for them if they choose to use these solutions.

Without a serious upgrade, this remains unlikely to change any time soon, while threats and instability can be too dangerous to meet the requirements of fiduciary responsibility.

Panther offers a breakthrough for all market actors by using PETs to dramatically reduce these risks. Strategies can be both protected from observers while also selectively disclosed. Panther uses privacy to give users a granular level of control and an unparalleled sense of protection. The protocol invites financial professionals to return to the true promise of DeFi by saving time, removing intermediaries, and unlocking new, composable possibilities.

Panther's Privacy Enhancement Stack

The importance of zero-knowledge proofs (ZKPs)

A zero-knowledge proof is a protocol that allows one party (the prover) to convince another party (the verifier) that they possess a piece of private information without having to actually reveal it. Sometimes referred to as *moon math* due to their sheer complexity and potential, zero-knowledge proofs have only recently become practical for real-world use in finance, despite being decades old. The implications of the technology are enormous: *ZKPs are able to maintain blockchains' accuracy and make scalability possible with ease and precision.* Their users can also know with complete clarity how their data is being used, only needing to share what's absolutely necessary for a given transaction. With ZKPs, users also no longer need to re-execute every transaction in a ledger, as they can instead check a succinct proof.

zk-SNARKs

Panther also utilizes zk-SNARKs², which stands for "Zero-Knowledge Succinct Non-Interactive Arguments of Knowledge". Thanks to zk-SNARKs, and just like with ZKPs, a prover can prove their possession of information without revealing it. However, the added benefit of zk-SNARKs is that they also allow for this to happen without both parties interacting. This helps further users' privacy.

zkSNARKs are:

Succinct

The size of the proof is small compared to the size of the statement being proved.

Non-interactive

zk-SNARKs do not require rounds of interaction between the prover and verifier except for a negligibly small probability.

Argument

A weaker notion of a mathematical proof where we assume the prover has bounded computational resources.

Knowledge

The prover cannot construct a proof without knowing a particular witness for the statement. This would be the equivalent of knowing "what to look for", or "what to decode".

² A. Nitulescu. zk-snarks: A gentle introduction, 2020.

Panther's Privacy Enhancement Stack

In addition to zk-SNARKs, Panther will explore integrating zk-STARKs, (Zero-Knowledge Scalable Transparent ARguments of Knowledge), which in addition to most of SNARKs' functions are quantum resistant.

Putting Privacy Enhancing Technologies first

In addition to zero-knowledge proofs, Panther uses differential privacy³, homomorphic encryption⁴, Secure Multi-Party Computation⁵, and selective disclosure schemes⁶. Each of these mathematical and technical building blocks plays different roles in supporting the enablement of privacy and scalability. By drawing upon these technologies, *Panther facilitates a shift in trust from regulatory frameworks and organizational practices to trustless mathematical proofs and their interpretation.*

Furthermore, Panther's core technical foundations are:

Panther's design choice to put PETs first constitutes a milestone for the DeFi space,

Multi-Asset Shielded Pools to protect our users' privacy. Strong APIs to connect to the whole crypto industry. Complete SDKs to allow anyone to build on top of Panther. A robust system of bridges to interconnect multiple protocols through private interchain asset transfers.

mainly as the protocol heavily focuses on data ownership. By setting up a system of PETs that interconnects open-source, public blockchains and adds a privacy layer to them, Panther manages to achieve a rarity in the space: to provide privacy in a clear, transparent way, without jeopardizing users' data by doing so.

³ Cynthia Dwork. Differential privacy: A survey of results. In Manindra Agrawal, Dingzhu Du, Zhenhua Duan, and Angsheng Li, editors, Theory and Applications of Models of Computation, pages 1–19, Berlin, Heidelberg, 2008. Springer Berlin Heidelberg.

⁴ Alexander Viand, Patrick Jattke, and Anwar Hithnawi. SoK: Fully Homomorphic Encryption Compilers, 2021.

⁵ David Evans, Vladimir Kolesnikov, and Mike Rosulek. A Pragmatic Introduction to Secure Multi-Party Computation. Foundations and Trends® in Privacy and Security, 2(2-3):70–246, 2018.

⁶ Hao Lei and Dengguo Feng. Selective Disclosure on Encrypted Documents. In Data and Applications Security and Privacy XXV, DBSec 2011, page 255–262, Richmond, VA, USA, 2011. International Federation for Information Processing.

Panther's Unique Solutions: Fully Disclosable PriFi

Moving transactions onto Layer-2 protocols stands as one of the most promising ways to increase the throughput of today's most-used blockchains. By taking hundreds of transactions and bundling them together into a single transaction, Layer-2s increase speed, reduce cost, and decrease network congestion.

One approach to this method, known as zk-Rollups, uses zero-knowledge proofs to verify the validity of information, thereby reducing the amount of data held in a transaction. This requires far fewer computing resources. Transactions on L-2s are periodically synchronized onto the main blockchain in a highly compressed form.

Panther's core DeFi Privacy Service works very differently than traditional privacy services. Panther consists of a series of Multi-Asset Shielded Pools (see below), interconnected to multiple blockchains "peerchains" by relayer nodes.

Panther Pools provide access to compliant DeFi privacy through shielding and selective disclosures.

Any user can request deposits into, transfers within, and withdrawals from these pools, which are then submitted to relayers and processed in a privacy-preserving way on the user's behalf and forwarded to the relevant peerchain.

Let us take a look at some of the core components of the Panther Protocol:

Panther's Unique Solutions

zAssets

In DeFi, we've become accustomed to the idea of "wrapping" a token - taking a digital asset, locking it into a smart contract, and then issuing a new asset with additional functionalities to use in its place. Wrapped tokens in Panther are near-perfect, 1-to-1 representations of the original asset.

For example, one wBTC token on the Ethereum blockchain is equal in value to one BTC on the Bitcoin blockchain even though the two operate on different protocols. Panther builds upon this idea to enable the creation of shielded digital assets or tokens that are infused with privacy, called *zAssets*.

These are 1-to-1 collateralized, untraceable digital tokens that harness the power of zero-knowledge proofs to give the user full control over what information is disclosed about their transaction history.

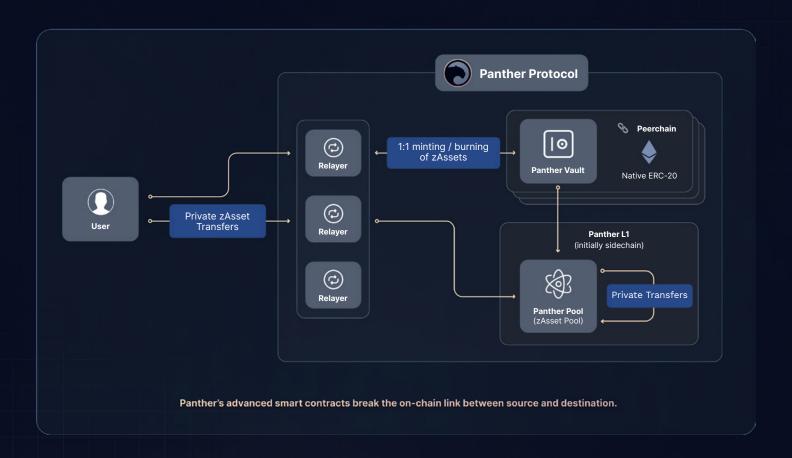


Panther's Unique Solutions

Right now, if a user wants to send a large amount of USDC from their wallet to a DeFi protocol, they run the risk of being attacked or front-run in transit. Using Panther, the process is far safer and more discreet.

First, the user deposits USDC into a *Panther Vault* smart contract, which mints the corresponding amount of zUSDC from within a *Panther Pool* smart contract. The user can then transact with zUSDC in any way they may want to, with the full benefits of enhanced privacy.

When a user's transactions are complete and they want to redeem zUSDC for the original underlying currency, their collateralized USDC is sent to a new stealth address and the corresponding zUSDC is burned and removed from circulation.



Panther Pools (Multi-Asset Shielded Pools)

Many of the existing Layer-1 blockchain networks do not have privacy capabilities, nor do they allow their users to wrap tokens. And, even if they do, it's just plain impractical for the user to be constantly wrapping and unwrapping assets across multiple networks to meet all of their different limitations. Therefore, it is very useful to create wrapping points that also provide privacy to the collateralized principal assets.

Within a pool, users can deposit their tokens in a way in which they, and only they, know how much they put in, as well as how much they're allowed to withdraw. Users can also transact within the pool to send their tokens both to themselves and to others.

However, not all tokens are created equal, and not all assets are the same. One of the most significant innovations of Multi-Asset Shielded Pools (MASPs) is that they support tokens of many kinds and sources. This boosts user privacy since all sorts of assets, including tokens of different standards can co-exist in the Pool, which is called Diverse Pool Privacy.



Panther's Unique Solutions

The Pool then gets large enough to preserve privacy heterogeneity, i.e. have so many transactions happening within it that *it becomes impossible to track users*.

Panther Pools utilize zk-SNARKs and ZKPs to prevent users from analyzing what's happening within them, having transactions obscured.

Panther Pools utilize zk-SNARKs and ZKPs to prevent users from analyzing what's happening within them, having transactions obscured. By allowing users of multiple kinds of assets to enter the Pool, users of every compatible chain can participate in the same mechanisms for privacy, regardless of their native chain's liquidity and activity.

While a Pool for rarely-used assets would struggle to find much security due to the relatively low volume of transactions, Panther MASPs can quickly build critical speed and provide much-needed privacy to the long tail of digital assets and cryptocurrencies.

Panther Pools also have built-in mechanisms to align the incentives of every user, rewarding those that contribute to shielding by adding tokens to the pool. Pools are fully composable with DeFi, allowing users to deploy tokens to smart contracts seamlessly. MASPs also create a single-stop, private point of connection amongst multiple chains.

Users of Pools can transact within them privately or withdraw their tokens into known or stealth addresses/wallets generated by Panther. **Users have an option to disclose their DeFi history, even retrospectively.**

zk and non-zk Reveals

It's been said that KYC regulations and DeFi are diametrically opposed and cannot co-exist, but this is based on a set of assumptions that Panther renders obsolete.

Panther uses zero-knowledge proofs to flip the issue of trust on its head. Instead of users sharing their personal information with every institution or protocol they interact with, Panther instead allows them to interact only once with only one trusted party (a **Trust Provider**) per use case (e.g. one for proof of address, one for identity, etc.) which can verify their information and issue a signed cryptographic attestation.

Users can then use these attestations to issue an unforgeable mathematical proof, verifiable on- and off-chain, which can be referenced and verified by Service Providers.

This serves as sufficient evidence that the user is in possession of whatever attributes, credentials, or reputation is needed in order to participate in a transaction, with selective sharing of personal data.

The user has an option to make a given Panther Reveal zero-knowledge (carrying no personal data), or non-zk (carrying personal data). Both would be verifiable by anyone if submitted on-chain. Furthermore, zk Reveals are generalizable across other segments such as **private identity, insurance, credit scoring, Web3 authentication and other services.**

Panther lets users reveal as much or as little information as they want to on a caseby-case basis. Panther does not learn anything about any user, and those receiving proofs only learn the disclosed data.

Once a Service Provider (such as a KYC verifier, institutional DeFi solution or Web3 protocol) receives a Panther zk Reveal, they do not get to learn what the underlying information is, only that the proofs are valid and the users' claims are true. Not only that, but the Trust Providers who issued the attestations never learn anything about when or how users use those attestations when interacting with Service Providers.

Panther's Private Interchain Bridge

There are currently billions of dollars of value spread out across a myriad of blockchain protocols, unable to communicate or create synergies with each other. Connecting these chains together is no simple endeavor; each has its own consensus model, operations, and internal constraints.

If a DeFi user wants to privately move tokens from one chain to another without a centralized exchange, the options are limited. And, for institutions, there are no options that guarantee the full privacy and ownership of their data at all. Thorchain facilitates cross-chain swaps, Uniswap facilitates deep pools of liquidity - but neither offers transactional obfuscation or selective disclosure for compliance.

What is needed is a super-highway to interconnect these protocols – a way to allow any market actor to route their assets across bridges to a variety of different peerchains, all while being able to choose what information is shared about their movements.

Panther is paving the road to cross-chain privacy value exchange through the creation of private bridges between chains that maintain security as a priority. Bridges in the blockchain ecosystem are not to be taken lightly, as poor constructions and a lack of adequate security audits can put users at risk and undermine cross-chain integrations as a whole.

This solution will be powered by Panther's core technologies and integrated with existing protocols and dApps (such as DEXs). This will allow Panther to offer state-of-the-art, private, institution-friendly cross-chain swaps with minimal risk, as well as groundbreaking financial products such as permissioned pools (subnets).

Within these pools, creators are able to set special rules for membership, such as geographical location, business relationship, or compliance status, all verified through zero-knowledge proofs, allowing for a wide variety of arbitrage opportunities.

Panther Wallet

Panther's Unique Solutions

Every digital wallet is created to encourage a specific set of behaviors. With Panther Wallet (the protocol's native wallet), the focus is on helping users preserve and maintain the confidentiality of their personal information and transaction history while freely interacting with their digital assets across all of DeFi.

Upon launch, Panther Wallet will be a private web dApp that allows users to:

- Connect to Panther and access services provided by Panther.
- Transfer assets into Panther Vaults.
- Send digital assets to other users, preventing anyone from tracking the chain of senders and recipients without worrying about zAssets' minting process.

Initially, the wallet will be used primarily for private transactions. It will later gain greater functionality. Panther Wallet will support multiple tokens and assets, further integrating additional blockchains and supporting interchain transfers.



Realized Vision and Use Cases

Panther's decentralized, disruptive approach to privacy and data ownership offers a major leap forward for several different industries: While Panther primarily deals with financial transactions right now, the core underlying components of the system offer the ability to extend into many other fields where privacy, auditability, and tracking are the key to providing business value. Many use cases which would once require a private blockchain or were not feasible due to data exposure can now be executed efficiently through Panther's smart contracts.

Some of the key use cases for Panther include:

- DeFi and a fully private crypto economy.
- **Digital Identity:** The ability to prove a series of characteristics about a user without having to share any underlying documents, names, or unnecessary personal information.
- **Tax Disclosure:** The ability to proactively share a series of transactions with authorities and government officials for the purpose of determining or declaring taxable funds.

Other functionalities that could be developed by third parties taking advantage of Panther's primitives are:

- **Insurance Claims:** The ability to share with a third-party the occurrence of an event or transaction without dispute.
- **Credit Scoring:** The ability to establish a reputation or a series of behaviors by selectively disclosing a series of payments or transactions in a given time.
- **Supply Chain Management:** The ability to restrict outside parties from examining the movements of goods, services, and the interaction of connected devices on a network.
- **Private Voting:** Panther launched as a fully decentralized protocol thanks to private voting. Thanks to Panther's efforts, any project in the crypto sphere can conduct private voting rounds and even launch in a decentralized manner.

Roadmap

Panther is currently developing the launch of its v1 on Polygon. It is also in the design phase of its APIs, SDKs, and developing strategic partnerships for research and integration with Layer-1s that are EVM-compatible. Panther is also exploring DEXs, wallets, and liquidity providers that would like to integrate a privacy toggle or are interested in adding privacy-enhancing features to their applications.

Panther aims to become a fully decentralized protocol by 2023. For a fully updated roadmap, please visit https://pantherprotocol.io/roadmap

Q4 2021 **Q1** 2022 **Q2** 2022

Core Protocol Phase 1 Development

- Development of Multi Asset Shielded Pool
- Panther Relayers
- ZKP circuits & trusted setup
- Panther Phase 1 Audit
- ✓ Panther dApp development

Staking Rewards Development

- \$ZKP Staking
- ✓ Panther Initial Rewards (PRPs)
- Wallet prototype

Trust and Data Ownership Phase 1

 Build Selective Disclosure of Transactions

Decentralization Phase 1

- Private Launch DAO
- ✓ Initial DAO Setup with Off-Chain Voting

\$ZKP Token Launch and Listing

- Token vesting and distribution
- Trading begins on Huobi, Bittrex, other exchanges

\$ZKP Staking Launch

- ✓ Classic Staking Mainnet
- Advanced Private Staking
- ✓ Classic Staking Polygon

Core Protocol - Polygon Development

- Incentivized Testnet
- Multi-Asset Shielded Pool
- Bridge to Polygon

Decentralization Phase 2

• DAO with On-Chain Voting

Third Party Wallet Integration - R&D

Prototype with one third-party Wallet

Private Interchain Transfers Phase 1 - R&D

- Interchain private transfers research
- Privacy price discovery

Defi Integration

- Integration with one DeFi protocol
- Wallet Integration Prototype
- Further DeFi integrations
- Wallet Integrations

Core Protocol - Polygon

Mainnet Launch

Support More Layer 1s

- Flare/Songbird
- Aurora

Private Interchain Transfer Phase 2 - Dev

 Interchain Consensus mechanism with EVM chains

Trust and Data Ownership Phase 2

- Trust provider technology
- Voluntary disclosure of statements
- Zero-knowledge proofs
- Service provider technology

Private Interchain Transfers - MVP

- MVP in Testnet
- Bridges
- Interchain consensus mechanism with non-EVM chains

Rollups and Scaling - R&D

Support More Layer 1's

Trust and Data Ownership Phase 3

- First service providers
- First trust providers
- KYC with one Vendor

Private Interchain Transfers - Mainnet

Deployment with few integrated chains

Rollups and Scaling MVP

DeFi Integration on Different L1's

\$ZKP: Panther's Native Token

A Game-Theoretical Pricing Mechanism for Privacy

As Panther scales, so does the quality of privacy provided by its liquidity pools – by design. The more transactions that take place on Panther, the cheaper it is to use, and the greater strength of its privacy protection for everyone involved. This acts as a feedback loop continually sustaining Panther's operations while improving and expanding its entire ecosystem.

Keeping the network functioning as intended requires incentivizing the right behaviors. This means aligning the interests and behaviors of all network participants while minimizing destabilizing behaviors to the greatest extent possible. Game theory offers a way to model these intentions and understand how they work within the system and different sets of parameters. These, in turn, create optimal cost structures for using and contributing to Panther Shielded Pools, as well as helping inform governance decisions.



Some of the utilities of \$ZKP and the behaviors it incentivizes are:

- Privately staking \$ZKP and other tokens in MASPs to earn rewards for increasing the privacy set. This decreases the availability of \$ZKP and drives its value up.
- Relayers paying fees privately on behalf of users, furthering privacy, to earn \$ZKP.
- Staking \$ZKP to secure the interchain bridges in an AMM model.
- Governance-focused staking to encourage long-term governance participation.
- Paying for protocol-delivered services at a discounted rate, such as:
 - (i) mint and burn fees associated with zAssets;
 - (ii) transaction fees for sending zAssets;
 - (iii) Panther Reveal fees; and
 - (iv) DEX trades.
- \$ZKP is used by the DAO to pay for services provided to the protocol such as:
 - (i) incentive fees to privacy stakers and transactors;
 - (ii) relayer service fees;
 - (iii) DEX stakers securing vaults;
 - (iv) DEX liquidity providers (LPs); and
 - (v) voting stakers.

Tokenomics of \$ZKP

Some key metrics, such as the total supply of \$ZKP and its initial allocation can be found in the diagram below:

Key Metrics

\$ZKP

Token Symbol

ERC 20 (ETH)

Token Type

1 Billion

ZKP Total Supply

110M ZKP

Initial Circulating Supply

\$49.5M USD

Circulating Marketcap at Launch

50M ZKP (5.0%)

Supply Sold at Token Sale

ZKP Token Allocation



Protocol Rewards

Early Team & Advisors 20%

Foundation

Public Sale

5.0%

Private Rounds

15%

Governance and Path to Decentralization

Panther is, from Day 1, a fully decentralized entity, launched in a private and decentralized manner through its sister protocol, LaunchDAO. All major decisions within the protocol are made by the Panther DAO, a decentralized autonomous organization for protocol governance. This requires a level of technical and organizational maturity that starts with creating the base-layer tools to make private DeFi a reality.

One of the unique features that will be observed in the later stages of the DAO is the eventual inclusion of quadratic voting, a mechanism to infuse systems with fairness by reducing the voting power of whales. A major problem identified throughout the DeFi space is that, when governed by DAOs, voting power tends to get concentrated in the hands of the wealthier users, often founding members and major investors. Quadratic voting and mathematical proofs should help the Panther DAO fairly distribute voting power amongst its token holders.

Suggested short & medium-term applications

The following are ways in which Panther can capture a TVL that generates sufficient revenue from fees (within Panther, users pay a varying fee to access varying degrees of privacy) to become self-sustainable:

• Putting institutional dark pools on-chain: Institutional dark pools are traditional versions of what Panther aims to create. Within them, capital institutions pool assets to trade with each other privately, preventing their trades from making a public record that drives prices in one direction or the other. According to some experts, dark pools "have grown so much over the years that experts are now worried that the stock market is no longer able to accurately reflect the price of securities." Some estimates say that dark pools are responsible for 18% of U.S. and 9% of European trading volumes, with some extreme calculations pointing to figures closer to 40% worldwide. With an estimate between 18-40% of trading volumes and the advantages outlined above, Panther is well-positioned to port this kind of system into DeFi. Permissioned pools within Panther will be called "subnets".

\$ZKP: Panther's Native Token

- A token-agnostic private digital economy: The blockchain ecosystem needs an equivalent to cash, whose total value (M1 supply) sits around \$20+ trillion. A proxy to this, stablecoins, are among the most critical assets of the crypto economy. Panther does not aim to create decentralized stablecoins, but proposes a solution for existing ones by enabling private, token-agnostic transactions on Multi-Asset Shielded Pools on the Polygon network (eventually integrating other peerchains) with access to cross-chain interactions. As the system remains token agnostic, existing stablecoins, shielded as Panther 1:1 collateralized zAssets, do not threaten the Panther ecosystem. Should any one of them fail to maintain their peg, users will simply move on to use another shielded stable asset. Users wrapping stablecoins in Panther to enable private exchanges will also get rewards for doing so.
- Interconnecting chains privately: The Panther protocol is chain-agnostic and bets on a multi-chain future. With many Layer-1 and 2 blockchains, all proposing different values, ideas, and mechanisms, Panther creates the infrastructure to connect them privately, rather than expecting one of them to take over everything. This makes Panther able to address the whole DeFi market as opposed to just sections of it. Furthermore, Panther's bridges will make it possible to connect multiple blockchains and have the TVL locked in them migrate back and forth (a key concept) among them.
- The need for zk Reveals: While institutional DeFi needs to happen privately due to institutions' unique market needs, this has to happen with full privacy and data ownership, which none of the incumbents accomplishes. zk Reveals (explained above) introduce a such a solution for institutions to participate in DeFi privately without falling prey to the dangers of transparency. This, in turn, opens the gate for more of them to participate in the crypto economy and continue fueling innovation in the space. With zk Reveals, institutions can use Panther to protect themselves on-chain while still disclosing their transaction history at will to whomever they deem necessary.
- **DeFi composability:** Each of the tools mentioned here can be used and leveraged by the entire ecosystem, exposing Panther to serendipity and network effects. Panther is a general-purpose tool and, thanks to the project's open-source nature, the protocol will deploy primitives that will strengthen and empower the entire crypto industry.

Originally conceptualized by:



Oliver GaleCo-founder, CEO

Oliver is a serial entrepreneur, CBDC pioneer, investor, advisor, and global advocate of distributed ledger technology. He currently serves as Founder and CEO of Panther Protocol, an end-to-end privacy protocol for digital assets that can be deployed compliantly on any public blockchain. Oliver also serves as Founder and Chairman of Elemental, a web 3.0 credit lending platform focused on democratizing affordable credit for underserved communities.

Oliver has been a leading global advocate, championing policy making discussions and thought leadership at central banks, government entities, and organizations including the UN, International Telecommunications Union (ITU), Commonwealth Secretariat, Caribbean Development Bank, MIT, Columbia University, and the IMF.



Dr. Anish Mohammed

Co-founder, CTO

Anish is the CTO and co-founder of Panther Protocol and has over 20 years in security and cryptography that includes design or audit of several blockchain protocols. He co-founded the UK Digital Currency Association, was a reviewer of Ethereum's Orange paper, and serves on advisory boards for leading companies including Ripple, Hyperloop, and Adjoint.

Anish is a frequent speaker on Blockchain, cryptocurrency, fintech, cybersecurity, and AI, with lectures at institutions worldwide including MIT (DCI), Carnegie Mellon, UCL, Imperial, and University of Coventry.

Partners





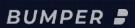


















Investors

























ellipti









AU21 CAPITAL



rarestone