Abstract

Panther is an interoperable, decentralised custodian and smart contract platform that enables privacy of digital assets on peer blockchains (“peerchains”). At the core of Panther’s design are Panther Pools, on-demand dark pools for Decentralized Finance (DeFi) which enable institutional and retail Users to securely store, obfuscate and transact compliantly on peerchains using Panther Assets (“zAssets"). zAssets are created by issuing 1:1 collateralized, zero knowledge digital tokens on peerchains.

As Panther is built and the ecosystem scales, it is likely we will see zAssets proliferate across peerchains with trading pairs for zAssets of most types. The added value that this obfuscation brings to investors and Users will carry a premium. Panther’s design objective is to create a liquid decentralized marketplace for privacy as a common good to enable onchain transactional anonymity in a regulatory compliant fashion.

The Problem

Every transaction tells a story, whether we like it or not. That’s the problem institutional investors are having with Decentralized Finance (DeFi), a movement that leverages decentralized networks to transform old financial products into trustless and transparent protocols that run without intermediaries (Ong). Despite their growing interest in participating, the ecosystem’s lack of core privacy functions makes it difficult to conduct large trades effectively and confidentially.

Today, DeFi applications are predominantly built on the Ethereum (Buterin) protocol (with a market cap of over $200B USD as of February 2021) (Concourse Open Community). Ethereum transaction history and balances are public by default. This poses a series of challenges for money managing professionals and individuals alike who both value financial privacy. Even though transactions conducted between parties are pseudonymous, the protocol does not offer strong privacy guarantees due to the public decentralized nature of the ledger.

Current trading environments are risky, and the existing solutions for privacy (Béres et al.) are inadequate given the rapid growth of public, permissionless DeFi applications. There is the concern of being front run (Guo et al.) when executing trades and transactions, whereby systematic traders track what is about to happen on the Ethereum blockchain and use that advance information to profit (Daian et al.). Even more damaging for the fungibility of stablecoins (Moin et al.) and utility tokens acting as monetary instruments are the common practices of onchain transaction graph analysis; this renders some tokens tainted and impairs their fungibility and properties as sound money. At the same time, existing privacy-preserving currencies are price volatile, which makes them unsuitable for commerce. This lack of transactional obfuscation puts a limit on the sophistication of trades and transactions that are practical to carry out on Ethereum and poses major trade-offs for all institutions wishing to carry on financial services onchain.

info@pantherprotocol.io

While Bitcoin and Ethereum are popular as stores of value, neither offer privacy or price stability. Zcash offers privacy but is not compatible with DeFi. Stablecoins and other assets may offer price stability, but they also lack privacy and other key features.

Meanwhile, current Ethereum mixers, services that allow individuals to preserve their privacy by mixing their coins with others (Piotrowska et al.), only allow the User to act in a constrained manner. Because denominations are in fixed amounts transactions are cumbersome and do not allow payments of any size. These services are also difficult to operate, easy to make privacy-destroying mistakes with, and have challenging User interfaces.

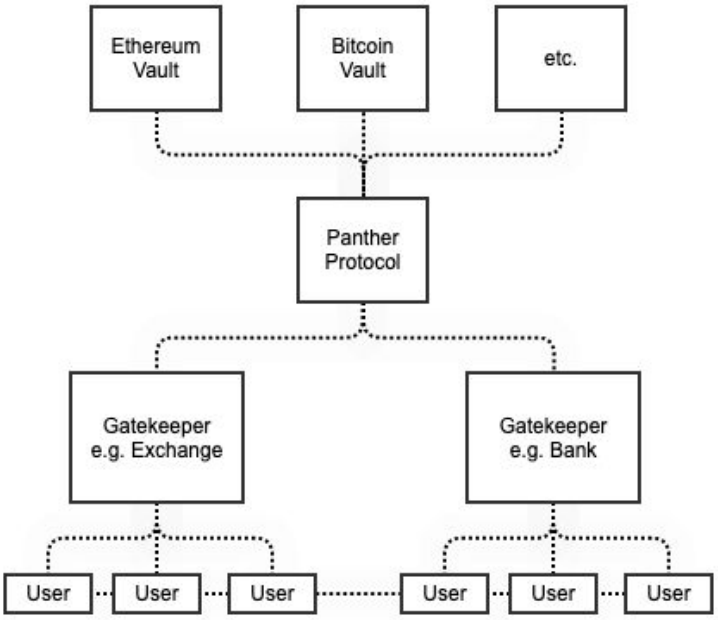
The Solution

Out of this problem space Panther emerges as a privacy-preserving, 1:1 tokenization layer for Ethereum-based assets, as well as those on other peerchains. Panther tackles a number of privacy issues by anonymizing transactions from the payment's sender and homogeneously standardizing the construction of payments and interactions within DeFi ecosystems. It focuses on five key areas: privacy network effects, increased transaction speeds, correct User behavior, usability, and interoperability:

- Privacy Network Effects - Tokenizing underlying collateral and transacting with zAssets drives powerful liquidity network effects. To reinforce these, Panther promotes minting and discourages burning using fee incentives, e.g. 0.25% mint and 0.1% burn fees, paid in the native Panther Token. This leads to a growing pool of zAssets. As the number of zAssets locked and transacted increases, the ability to anonymize transactions grows stronger and the protocol becomes more efficient encouraging widespread adoption.
- Increased Transaction Speeds - As different peerchains compete for transaction speed superiority, zAsset Users can move assets from one protocol to another to meet their needs for transaction finality and speeds.
- Correct User Behavior - Utilizing native assets on public peerchains exposes Users to a number of deanonymizing threats, such as address reuse, conspicuous transaction fee amounts and human errors. zAssets enforce correct behavior to maximise privacy at a protocol level bringing simple User experience along with high levels of privacy. This in turn encourages transaction volume and enhances privacy network effects.
- Usability - Minting zAssets on peerchains with well adopted standards, such as Ethereum's ERC20 standard, allows Users to interact with the growing DeFi ecosystem and network of accepting exchanges, stores and financial institutions using these standards.
- Interoperability - By issuing the native assets of one peerchain on another as zAssets Users are able to benefit from the unique advantages of different protocols. Examples of the types of optimizations brought by different protocols are transactions per second, affordability, decentralization, and composability.

	Ethereum	Zcash	Panther	Bitcoin	Cash
Energy Efficient	YES	NO	YES	NO	NO
Censorship Resistant	YES	YES	YES	YES	NO
Private	NO	YES	YES	NO	YES
DeFi Composable	YES	NO	YES	NO	NO
Interoperable	NO	NO	YES	NO	NO

How It Works



The different stakeholders involved in the Panther ecosystem include:

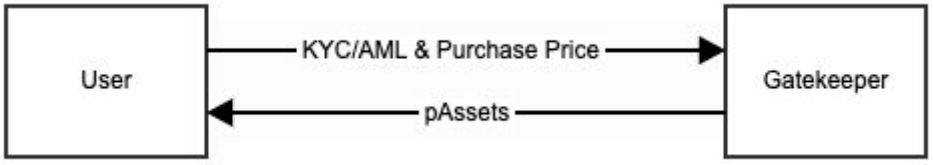
- Gatekeepers responsible for verifying Users and custodying collateral in Panther Vaults. Gatekeepers are the exclusive minters and burners of zAssets and play a key role in the distribution of zAssets;
- Privacy Miners who stake zAssets to provide liquidity to the Panther Pools, and pay relayer node fees;
- Users that hold zAssets and carry out transactions on any peerchain with a Panther Pool and Vault;
- The Panther Foundation responsible for steering Panther to full decentralization and encouraging community growth;
- Panther Tokenholders who vote on governance decisions and fund proposals through the Panther DAO; and
- Community members who make proposals to improve the Panther ecosystem and are involved in many ways but are not specifically invested in any single function of Panther.

Minting and Burning

Minting (creating) and burning (destroying) zAssets is a process handled by peerchain self-custodial smart contracts, known as a Panther Vault. The process of doing this however, is initiated by Gatekeepers responsible for providing collateral to Panther Vaults, and who act as the elected custodians. zAssets are minted and burned at a 1:1 ratio to ensure assets are always backed by the same amount of collateral. e.g 1USDT = 1zUSDT.

Verification

Users and enterprises wishing to buy newly minted zAssets, or redeem zAssets bought on secondary markets for the underlying collateral, are required to complete KYC/KYB (Know Your Customer/Business) verification through a Gatekeeper.



Transacting with zAssets

zAssets minted on a peerchain inherit all of the core properties of that peerchain's native assets and can interact with DeFi ecosystems with the added benefit of onchain privacy.

Phases of Development

When initially launching permissionless protocols, developers should seek to gradually remove themselves as intermediaries. This permits fixing bugs quickly in a production environment. This also facilitates rapid product iteration and evolution. Panther will be launched in incremental stages with increasing functionality being added over time towards full decentralization.

Phase 1 - Ethereum Panther

In the first phase of development, zAssets are minted and burned by Panther Users through an Ethereum based Panther Vault which forms part of Ethereum Panther. Ethereum has been chosen for the first deployment as it is a highly composable and liquid DeFi protocol and is the ideal mechanism for proving protocol robustness, adoption and effectiveness of Panther Pools. Initially, the Panther treasury will be managed by the Panther Foundation, however, Phase 1 will see the migration of these funds over to the control of the community governed Panther DAO (Decentralized Autonomous Organization) (Buterin), which will also be deployed on Ethereum. The Panther DAO will be responsible for setting privacy miner rewards, mint and burn fees, bug bounties, education and software development grants.

Phase 2 - Panther Protocol

In the second phase of development, the Panther Protocol will be built and launched following a public sale of Panther tokens. Envisioned as a decentralized custodian enabling the minting and burning of zAssets across any peerchain, Panther protocol will extend the utility of Panther to multiple blockchains and brings with it a number of advantages:

1. End to end private smart contract execution;
2. Aligned governance incentives from Panther Token holders to the Panther Protocol vs. any one Panther peerchain deployments;
3. Solving scaling problems that come with peerchain-to-peerchain direct bridges, enabling seamless, interoperability between peerchains;
4. Optimized blockchain designed for censorship resistance decentralized custody using 51% censorship resistant Ouroboros consensus.

Phase 3 - Panther on Multiple Peerchains

In the third phase of development Panther's decentralized community of developers will be focused on interoperability between chains and the building out of a private DeFi ecosystem, all of which will be governed by Panther Token holders and funded through the Panther DAO. With the core Panther Protocol responsible for managing one of the private keys for Panther Vaults on each peerchain, and supporting turing complete, private smart contracts, there will be an emergence of new Panther deployments on other peerchains to enable privacy on and between these growing ecosystems.

Panther Technology

There are seven technology components which make it possible for Panther deployments to provide obfuscation of transactions in peerchain DeFi ecosystems:

1. Panther Pools
2. Gatekeepers
3. Vaults
4. Wallets
5. Privacy Miners
6. Panther Token
7. Panther DAO

1. Panther Pools

Panther Pools allows Users to privately transact on any peerchain through the use of zAssets issued on that peerchain. This is achieved by randomly shuffling zAssets of the sender, other Users and Privacy Miners, to send an equivalent amount to the receiver anonymously. Meanwhile, the underlying 1:1 collateral assets are custodied in Panther Vaults that form part of the peerchain Panther deployment and can be redeemed at any time through Gatekeepers. In order to provide a practical, scalable, and trustless cryptographic proving system, HALO Zero Trust Step (Bowe et al.) for recursive proofs is used to eliminate reliance on a trusted third party setup.

2. Gatekeepers

Gatekeepers are a federation of globally distributed and independent financial institutions and enterprises responsible for minting and burning zAssets. Additionally, Gatekeepers play the important role verifying and maintaining regulatory compliance for Users wishing to buy or sell zAssets. Panther will launch with a minimum of 3 Gatekeepers at launch.

Due to their capabilities, privacy-preserving blockchain-based projects can find themselves facing scrutiny. It is anticipated that questions regarding the regulatory intricacies of Panther's privacy protocol might arise and are worth addressing at the outset. Panther does not keep lists, maps, registers or documents on Panther Users, is unable to ascertain the parties to a transaction, does not impose restriction on Users transacting with zAssets, and does not take responsibility for the adherence of Gatekeepers to their local regulations and licensing requirements. The protocol does, however, enable onchain publishing of zero knowledge proofs to IPFS (Benet) that associate a given wallet address with a verified User. That proof directs the querying party to the Gatekeeper responsible for processing the Panther User at the time they bought newly minted zAssets or sold existing zAssets to redeem the underlying collateral.

There will be transparency between Gatekeepers and aggregated statistics provided on the network in a dashboard, these include:

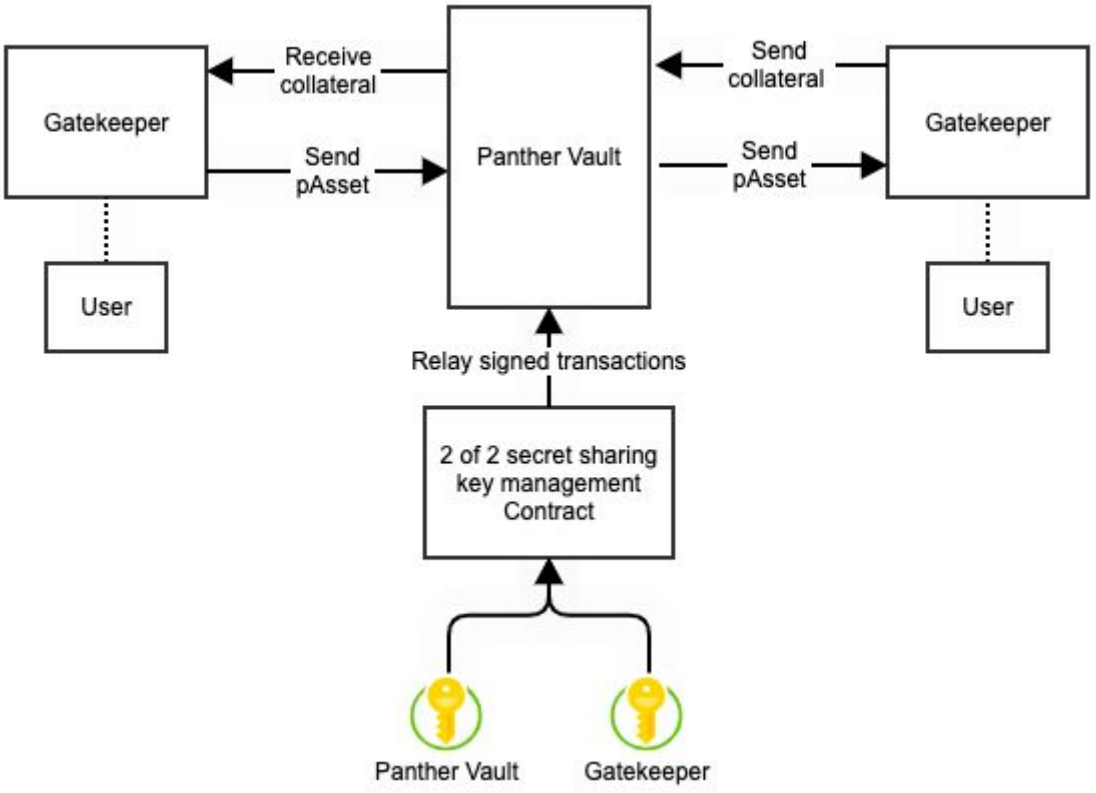
- Names and corporate details of the current Gatekeepers;
- Mint and burn statistics;
- Panther Vault balances; and
- Number of verified Users per Gatekeeper.

Given the outsized value that transactional privacy provides to society, we believe that Panther Protocol's approach is both forward-thinking in its approach to regulatory compliance and also in line with the industry's best practices.

3. Panther Vaults

Panther Vault are autonomous, zero knowledge (Goldwasser et al.) self-custodial smart contracts that allow Gatekeepers to act as decentralized custodians for collateral assets created on any single peerchain. As long as a Gatekeeper has membership to the federation they can freely mint and burn zAssets of any type.

Signing of mint and burn transactions are managed by Panther Vaults in a 2-of-2 multisignature scheme consisting of the:
1) Gatekeeper; and
2) Panther Vault.



By default, Gatekeepers sign burn/redeem requests with the protocol which will auto-sign provided the Gatekeepers federation membership is valid and they are burning zAssets at a 1:1 ratio for the collateral. In the event a Gatekeeper behaves maliciously and refuses to release collateral assets, Panther Token token holders can vote to revoke the Gatekeepers membership. At the same time, zAsset holders can burn their assets through another Gatekeeper to access the collateral. In this way, control of onchain collateral always remains with Panther token holders.

4. Panther Wallet

The Panther Wallet is a browser-based self-custodial wallet. Panther Wallets fill a number of key roles within Panther in addition to the traditional role of blockchain based wallets (send, request, store and transaction history):

- Address reuse prevention;
- Private connections to Ethereum DeFi protocols using proxy addresses;
- Voting on governance proposals.

5. Privacy Miners

Privacy Miners are nodes running on Panther peerchains which provide zAsset liquidity to Panther Pools in exchange for Panther Token paid in transaction fees and through rewards granted by the Panther DAO. The privacy that Panther brings to each peerchain's DeFi

ecosystem is directly proportional with the volume flowing through Panther Pools; in other words, the greater the transaction volume from unique addresses, the larger the anonymity set. As the early network is launched, the role of Privacy Miners will be critical to bootstrap liquidity in Panther Pools. As the protocol scales organic transaction volume, it is expected that privacy mining rewards will diminish naturally. At the same time, as volume increases the cost of privacy decreases, creating a virtuous cycle.

In Panther there is a lower bound privacy threshold below which transactions will not be sent on the network as they are not sufficiently obfuscated. In order to ensure minimum privacy thresholds are met, transaction fees adjust dynamically. When there is not enough pool liquidity, the transaction fees increase to encourage more deposits. The opposite happens when there is excess liquidity in the pool.

In addition to the function of providing liquidity to Panther Pools, Privacy Piners also provide relayer services. Relayer nodes services involve providing the native gas token, such as ETH on the Ethereum peerchain, to newly created proxy addresses to pay for the transaction fees connected with sending zAssets on that chain. This service protects the sender from deanonymization. Privacy Miners are chosen by Verifiable Random Function (VRF) (Dodis and Yampolskiy) from all available miners on that peerchain and rewards are paid proportionally to the zAssets locked for mining across the peerchain.

6. Panther Token:

The Panther Token is a finite supply, privacy-preserving gas token used to pay for fees within the Panther ecosystem that also represents a right to vote on governance issues. It is used in several instances to support the function of the protocol and provide incentives for its growth and maintenance. zAssets are designed to improve usability and privacy through enforcement of correct User behavior at the protocol level. The token has the following functions:

Phase 1 Utility
In the first phase, the Panther Token will work in the following ways:

- the Panther Token is used to pay for mint and burn fees associated with zAssets managed by Panther Vaults;
- the Panther Token is used to pay transaction fees for sending zAssets;
- the Panther Token is used to pay incentive fees to Privacy Miners;
- the Panther Token is used to pay privacy miner’s relayer service fees;
- the Panther Token is used to provide rewards to anyone staking zAssets in Panther Pools, from a dedicated token allocation in the Panther DAO; and
- the Panther Token is staked and used to vote on governance matters, such as Panther Improvement Proposals (PIPs), Gatekeeper federation membership and requirements, privacy thresholds, community and education grants, and privacy miner rewards.

Phase 2 Utility

When the Panther Protocol is developed, the Panther Token will work in the following additional ways:

- the Panther Token is delegated to or staked directly by validators responsible for securing the Panther Protocol and processing transactions on the native chain;
- the Panther Token is used to provide rewards to Privacy Miners from the Panther DAO;
- the Panther Token is bonded by Privacy Miners proportionally to the value locked in Panther Vaults; and
- Vault Maintenance fees are paid by zAsset holders to incentivize honest network behavior.

Governance and the Panther DAO

Governance, being central to the success of the Panther ecosystem, will be initially managed by the independently run Panther Foundation which will be responsible for treasury management. Once the Panther DAO is launched, all the Panther Tokens held by Panther Foundation will be transferred and Panther Token holders will take over treasury management, token economics and funding PIPs by way of a quadratic voting system (Buterin) based on the Panther Token holder balances. Voting will be done in a completely transparent way through a public portal.

Panther Token holders can vote on specific budgets and projects to be funded, such as new peerchain Panther deployments, and play a critical role in the direction the protocol is going. Functioning like a decentralized crowdfunding platform, the budget can be used for anything that creates value within the ecosystem.

Timeline:

The fundraising and development schedule for Panther will be as follows:

1. In Q1 2021, Panther will begin with a pre-seed raise for the development of the Ethereum based Panther Wallet, Panther Pool and Panther DAO.
2. In Q2 2021, Panther testnets on Ethereum will be released for private and then public feedback.
3. In Q3 2021, the Ethereum Panther ecosystem will be released and a public sale will be conducted for the Panther Protocol.
4. In Q4 2021, research and development for Panther Protocol will begin.

Definitions:

- Panther Token - a finite supply, privacy-preserving gas token used to pay for fees within the Panther ecosystem and represents a right to vote on PIPs.

- PIPs - Panther Improvement Proposals are proposals for modifications to governance, economics, or technology voted on by Panther Token holders.
- Peerchains - third party layer 1 blockchains which run Panther Vaults.
- zAssets - 1:1 collateralized, zero knowledge digital tokens that institutional and retail Users employ to securely store, obfuscate and transact compliantly.
- DAO - an entity that lives on the internet and exists autonomously, but also heavily relies on hiring individuals to perform certain tasks that the automaton itself cannot do (Buterin), such as Panther DAO.
- Gatekeepers - institutions responsible for verifying Users and are the exclusive minters and burners of zAssets.
- Vaults - peerchain self-custodial smart contracts which handle minting (creating) and burning (destroying) zAssets.
- Privacy Miners - nodes in the Panther ecosystem which provide zAsset liquidity to Panther Pools in exchange for Panther Token paid in transaction fees and through rewards granted by the Panther DAO
- Wallets - a browser-based extension self-custodial wallet.

About Us:

Panther Ventures Limited is a Gibraltar-based distributed ledger technology company committed to using peer-to-peer innovations to solve major problems of providing unencumbered access to financial services to the unbanked and underbanked.

References:

Benet, Juan. “IPFS - Content Addressed, Versioned, P2P File System.” *arxiv*, 14 July 2014, https://arxiv.org/abs/1407.3561. Accessed 5 January 2021.

Béres, Ferenc, et al. “Blockchain is Watching You: Profiling and Deanonymizing Ethereum Users.” *arxiv*, 14 October 2020, https://arxiv.org/pdf/2005.14051.pdf. Accessed 5 January 2021.

Bowe, Sean, et al. “Recursive Proof Composition without a Trusted Setup.” *International Association for Cryptologic Research*, 10 09 2019, https://eprint.iacr.org/2019/1021.pdf. Accessed 5 January 2021.

Buterin, Vitalik. “DAOs, DACs, DAs and More: An Incomplete Terminology Guide.” *Ethereum*, 6 May 2014,

https://blog.ethereum.org/2014/05/06/daos-dacs-das-and-more-an-incomplete-terminology-guide/. Accessed 5 January 2021.

Buterin, Vitalik. “Ethereum Whitepaper.” *Ethereum*, 2013, https://ethereum.org/en/whitepaper/. Accessed 5 January 2021.

Buterin, Vitalik. “Quadratic Payments: A Primer.” *Vitalik Buterin*, 7 December 2019, https://vitalik.ca/general/2019/12/07/quadratic.html. Accessed 5 January 2021.

Concourse Open Community. “DeFi Pulse.” *DeFi Pulse*, 2020, https://defipulse.com/. Accessed 5 January 2021.

Daian, Philip, et al. “Flash Boys 2.0: Frontrunning, Transaction Reordering, and Consensus Instability in Decentralized Exchanges.” *arxiv*, April 2019, https://arxiv.org/pdf/1904.05234.pdf. Accessed 5 January 2021.

Dodis, Yevgeniy, and Aleksandr Yampolskiy. “A Verifiable Random Function with Short Proofs and Keys.” *International Association for Cryptologic Research*, 2004, https://eprint.iacr.org/2004/310.pdf. Accessed 5 January 2021.

Goldwasser, Shafi, et al. “The Knowledge Complexity of Interactive Proof Systems.” *MIT Computer Science and Artificial Intelligence Laboratory*, February 1989, https://people.csail.mit.edu/silvio/Selected%20Scientific%20Papers/Proof%20Systems/The_Knowledge_Complexity_Of_Interactive_Proof_Systems.pdf. Accessed 5 January 2021.

Guo, Dongchao, et al. “Graph Structure and Statistical Properties of Ethereum Transaction Relationships.” *Researchgate*, April 2019, https://www.researchgate.net/publication/332272335_Graph_Structure_and_Statistical_Properties_of_Ethereum_Transaction_Relationships. Accessed 5 January 2021.

Moin, Amani, et al. “SoK: A Classification Framework for Stablecoin Designs.” *International Financial Cryptography Association*, 18 September 2019, http://fc20.ifca.ai/preproceedings/119.pdf. Accessed 5 January 2021.

Ong, Edwin. “Awesome Decentralized Finance.” *Github*, 23 April 2019, https://github.com/ong/awesome-decentralized-finance. Accessed 5 January 2021.

Piotrowska, Ania M., et al. “The Loopix Anonymity System.” *Usenix*, August 2017, https://www.usenix.org/system/files/conference/usenixsecurity17/sec17-piotrowska.pdf. Accessed 5 January 2021.