Zoracles:

Confidential Data to Smart Contracts

leonard@zoracles.com

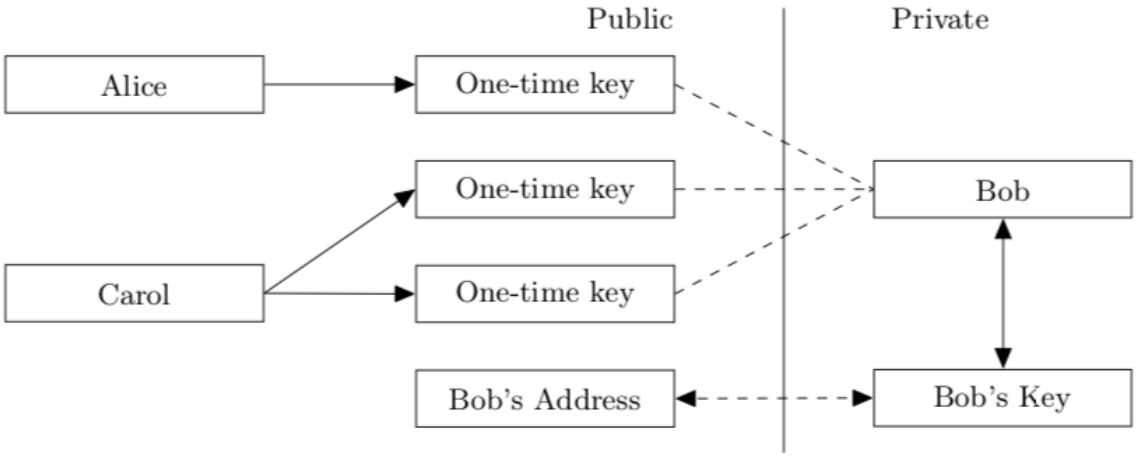
Introduction: Cryptocurrencies and blockchain technology have evolved in such a way that will change every aspect of modern society. Current socioeconomic structures and relationships will transform to impact our world in ways we currently can't imagine today. While this rapidly evolving industry has the potential to shift paradigms, without strong privacy guarantees, it will be impossible to truly realize its full potential for individuals or enterprises.

1. Background

Bitcoin was launched over a decade ago and gave rise to early cryptocurrencies including Litecoin, Namecoin & Peercoin. Each of these projects was similar to Bitcoin in functionality but lacked privacy.

It was widely believed in Bitcoin's early existence that the payment system was pseudonymous. Once exchange data was collected, it became a lot easier to link Bitcoin addresses to individuals. Privacy on Bitcoin had been compromised and real solutions to include anonymity into Bitcoin Core have not been implemented.

Since its launch in 2014, Monero's implementation of Cryptonote has been the most widely adopted privacy project. RingCT technology [1] was leveraged to provide users with plausible deniability.



The foundation of RingCT technology relies on obfuscation [1]. As seen above, participants' keys are involved in a mixing process that originally was believed to break transaction linkability and eliminate a transaction graph.

Fundamentally, Monero's technology has its limitations because mixins [1] were code-harded into the Cryptonote Protocol and an adversary could simply observe the network, run analysis and make reasonable assumptions of where most of the transactions originated. Other currencies that used RingCT attempted to increase privacy by allowing users to determine the size of mixins.

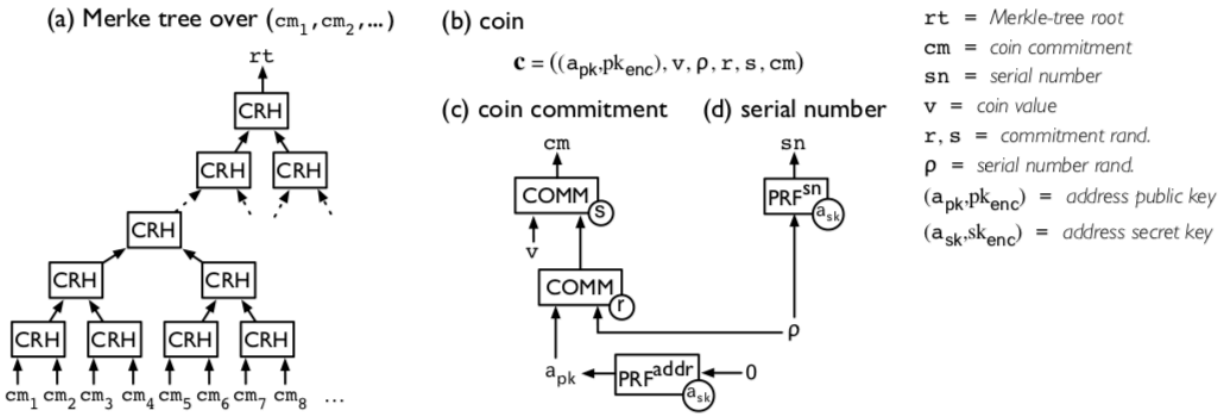
Monero users assumed their transactions were completely anonymous due to original claims of the Monero community. This was later disproven [2].

RingCT failed to prevent linkability and a transaction graph was constructed by researchers [2]. Transactions prior to their research were exposed and Monero developers were forced to increase the size of mixins. Today it is set at 11.

	Before 2-mixin hardfork			After 2-mixin hardfork			After 0.10.1, prior to Apr 15, 2017		
	Total	Deducible	(%)	Total	Deducible	(%)	Total	Deducible	(%)
1 mixins	683458	608087	(88.97)	0	–	–	0	–	–
2 mixins	250520	206276	(82.34)	1882681	1209259	(64.23)	732251	308926	(42.19)
3 mixins	634520	480500	(75.73)	564525	376920	(66.77)	126795	65738	(51.85)
4 mixins	217493	156767	(72.08)	376432	192348	(51.10)	145687	33022	(22.67)
5 mixins	87077	43214	(49.63)	48806	26599	(54.50)	3900	950	(24.36)
6 mixins	115199	65546	(56.90)	224202	119716	(53.40)	24817	7890	(31.79)
7 mixins	3671	1680	(45.76)	4499	1770	(39.34)	1711	235	(13.73)
8 mixins	2216	1067	(48.15)	5048	1968	(38.99)	1458	249	(17.08)
9 mixins	1811	838	(46.27)	3264	1069	(32.75)	264	48	(18.18)
10+ mixins	57363	11997	(20.91)	46791	12970	(27.72)	9145	1682	(18.39)
Total	2053328	1575972	(76.75)	3156248	1942619	(61.55)	1046028	418740	(40.03)
Overall					(62.94)				

An alternative to mixing technology was first proposed by researchers from John Hopkins University. Their paper entitled “Zerocoin” was later updated to a proposal to build a separate blockchain with zero-knowledge proofs. “Zerocash [3]” was exceptionally innovative in its approach to privacy because it solved the linkability issues experienced in mixing coins.

Using advanced mathematics, Zcash [3] has been able to provide near anonymity for transactions. This is important to distinguish from other privacy technologies that are just mixing or obfuscating transactions.



Central to privacy technology is anonymity set. Mixing technologies have low anonymity sets where zero-knowledge systems are very high.

PRIVACY TECHNOLOGY	Zerocoin	CoinJoin variant	Ring signatures	Zerocash
ANONYMITY SET PER TX	Thousands[5]	3 with each mix	4 by default	All mint TX
REQUIRES TRUST OF MIXER	No	Yes	No	No
HIDES TX AMOUNT	No	No	Yes with RingCT	Yes with shielded tx
TX SIZE	~0.3kb for normal tx 25kb per Zerocoin tx	~0.3kb	12-25kb per tx	<200 bytes for normal tx 1+kb for private tx
PRUNABLE BLOCKCHAIN[6]	Yes	Yes w/ core upgrade	No	Yes
COMPUTATION TIME FOR PRIVATE TX	Seconds	<1 second	<1 second	Minutes
INCENTIVIZED NODES	Znodes	Masternodes	No	No
TRUSTED SETUP	Yes[7]	No	No	Yes[8]
AUDITABLE SUPPLY	Yes	Yes	No	No
OPTIONAL PRIVACY	Yes	Yes	No	Yes
DEVELOPMENT FUNDING	10% of total supply	10% of block reward	Pro-bono	10% of total supply

Higher anonymity sets allow stronger privacy guarantees for users.

Individuals may not value their privacy as much as enterprises. It is absolutely necessary for large enterprises to keep confidential data when working with suppliers and business partners. Moving forward, we see the industry adopting stronger privacy technologies to accommodate the needs of larger enterprises.

2. Oracle Problem

When smart contracts were deployed on the Ethereum network, the range of possible dApps were endless. From derivative contracts to stablecoins, these revolutionary digital agreements opened a world of opportunity for decentralized finance.

Although Ethereum enabled turing-complete programs to build new open financial applications, due to the deterministic nature of blockchains, they faced an obstacle interfacing with real-world data. This is known as the oracle problem and has been addressed with a variety of solutions ranging from whitelisted data sources to proof of work mining to submit values on-chain.

Zoracles was developed to solve the oracle problem using zero-knowledge proofs. Our solution provides confidential data to smart contracts. Our mission is to offer the highest level of anonymity for smart contract transactions. This will bring new opportunities for enterprises to build on Ethereum.

3. Open Oracle

There are many oracle designs currently offered to dApp developers. It is our belief that these solutions will become commodities over time as developers simply select the most secure and economical solution.

Since our main expertise and focus will be building zero-knowledge proofs systems to retrieve data for smart contracts, our approach is platform agnostic.

We carefully evaluated several options and selected the Open Oracle developed by Compound [5] as the most realistic long-term alternative to Chainlink. As shown below, this will allow us to securely gather and transmit price data for Bitcoin, Ethereum and many other cryptocurrencies for smart contract execution.


```
  "prices": {
    "BTC": "11877.189999999999",
    "ETH": "416.46000000000004",
    "XTZ": "3.86165",
    "DAI": "1.00409",
    "REP": "21.16",
    "ZRX": "0.6360034999999999",
    "BAT": "0.368587",
    "KNC": "1.6998",
    "LINK": "15.87674",
    "COMP": "182.82999999999998"
  },
  "reporter": "0xfCEAdAFab14d46e20144F48824d0C09B1a03F2BC"
},
"okex": {
  "messages": [
```

4. Zero-Knowledge Proofs

Our core competency is developing zero-knowledge proofs (ZKPs) for oracles. This will allow confidential data to transmit from data providers to smart contracts. At launch, we will have a few trusted exchanges such as Coinbase that will sign and verify the data provided [6].

`0xfCEAdAFab14d46e20144F48824d0C09B1a03F2BC`	`BTC, ETH, DAI, REP, ZRX, BAT, KNC, LINK, COMP`
`0x419c555b739212684432050b7ce459ea8e7b8bda`	`BTC, ETH`

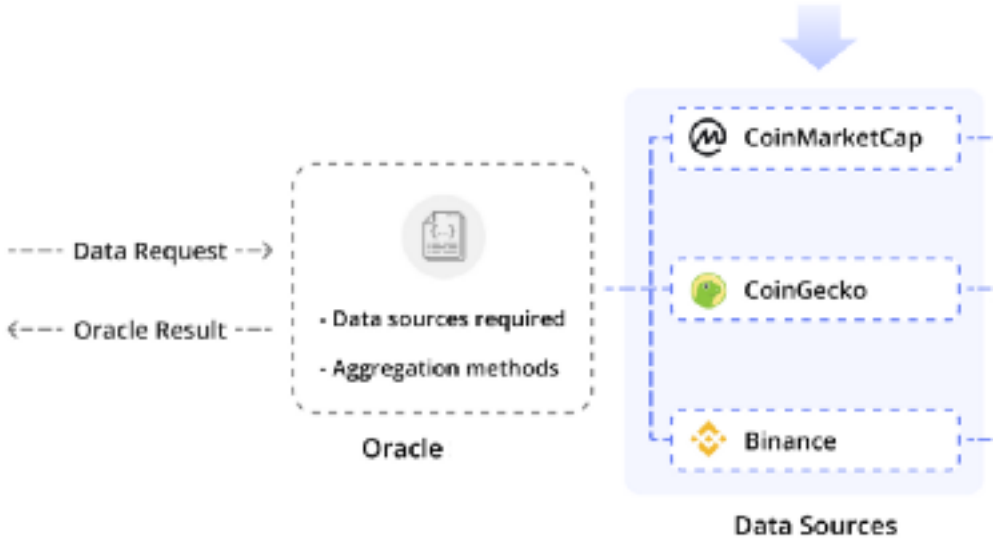
The Zoracles development team comprises of 2 full time developers and a part-time team member. Each is committed to building Zoracles and is very experienced in privacy technology. Collectively, they have built some of the most well-known privacy solutions deployed in crypto. To protect any conflict of interest, they will remain anonymous and just push code.

An active github is critical to the project's success. Also, developing new proving schemes and quick verifications are essential for any zero-knowledge proof system to function efficiently.

Work has already begun building and deploying Ethereum contracts with ZKPs.

5. Data Sources

Open Oracle architecture allows for dApp developers to select trusted data sources to feed information into their applications. Using the features of HTTPS, Zoracles will be able to provide a framework where data sources can eventually sign the data they provide to further ensure high quality information.



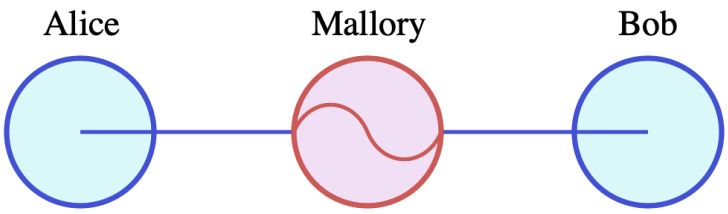
This framework will provide a level of decentralization in acquiring data. Unlike Band/Chainlink, where nodes provide redundant data at a high cost, Zoracles data feeds will be free.

6. Man-in-the-middle attack

Current oracle solutions have not addressed privacy in a meaningful way. There will be a barrier for adoption for enterprises unless strong anonymity is developed.

A well-understood vector for decentralized oracle networks is a man-in-the middle attack. For enterprises or an adversary, they can monitor what data is sent by an oracle network. This is very similar to the early internet where most sites were HTTP. Zoracles expects our ZKP solutions to become the default privacy protocol (HTTPS) that is common for all website data transmission today.

Here is an example of how the man-in-the-middle attack works [7]:



“Suppose Alice wishes to communicate with Bob. Meanwhile, Mallory wishes to intercept the conversation to eavesdrop and optionally to deliver a false message to Bob.

First, Alice asks Bob for his public key. If Bob sends his public key to Alice, but Mallory is able to intercept it, an MITM attack can begin. Mallory sends Alice a forged message that appears to originate from Bob, but instead includes Mallory's public key.

Alice, believing this public key to be Bob's, encrypts her message with Mallory's key and sends the enciphered message back to Bob. Mallory again intercepts, deciphers the message using her private key, possibly alters it if she wants, and re-enciphers it using the public key she intercepted from Bob when he originally tried to send it to Alice. When Bob receives the newly enciphered message, he believes it came from Alice.

1. Alice sends a message to Bob, which is intercepted by Mallory:

   Alice *"Hi Bob, it's Alice. Give me your key."* → Mallory Bob
2. Mallory relays this message to Bob; Bob cannot tell it is not really from Alice:

   Alice Mallory *"Hi Bob, it's Alice. Give me your key."* → Bob
3. Bob responds with his encryption key:

   Alice Mallory ← *[Bob's key]* Bob
4. Mallory replaces Bob's key with her own, and relays this to Alice, claiming that it is Bob's key:

   Alice ← *[Mallory's key]* Mallory Bob
5. Alice encrypts a message with what she believes to be Bob's key, thinking that only Bob can read it:

   Alice *"Meet me at the bus stop!" [encrypted with Mallory's key]* → Mallory Bob
6. However, because it was actually encrypted with Mallory's key, Mallory can decrypt it, read it, modify it (if desired), re-encrypt with Bob's key, and forward it to Bob:

   Alice Mallory *"Meet me at the van down by the river!" [encrypted with Bob's key]* → Bob
7. Bob thinks that this message is a secure communication from Alice.

This example shows the need for Alice and Bob to have some way to ensure that they are truly each using each other's public keys, rather than the public key of an attacker. Otherwise, such attacks are generally possible, in principle, against any message sent using public-key technology. A variety of techniques can help defend against MITM attacks."

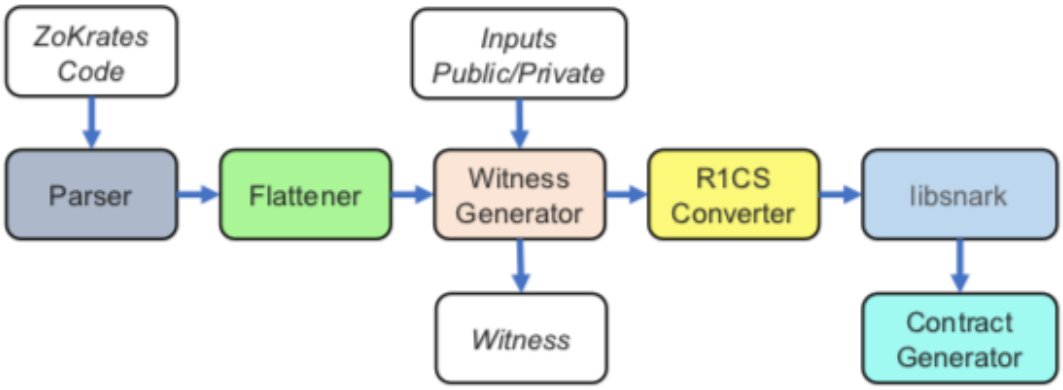
Zoracles solves the man-in-the middle attack with zero-knowledge proofs. DeFi will need this solution to protect billions and eventually trillions of dollars. Financial data is some of the most sensitive data we transmit and protecting this information is our core mission.

A number of mixing option solutions have been proposed by other oracle networks. This will be insufficient to prevent data interception because the data is simply obfuscated instead of never revealed like ZKPs. This is Zoracles' protocol powerful competitive advantage and unique value proposition for dApp developers, enterprises and individuals.

7. Zokrates

To quickly deploy ZKPs into Open Oracle, Zoracles has decided to use Zokrates [8] for creating and compiling Ethereum Solidity Contracts containing proving schemes and quick verifications.

This system allows our developers to greatly accelerate the software development cycle and is a good starting point for building a solution with ZKPs.



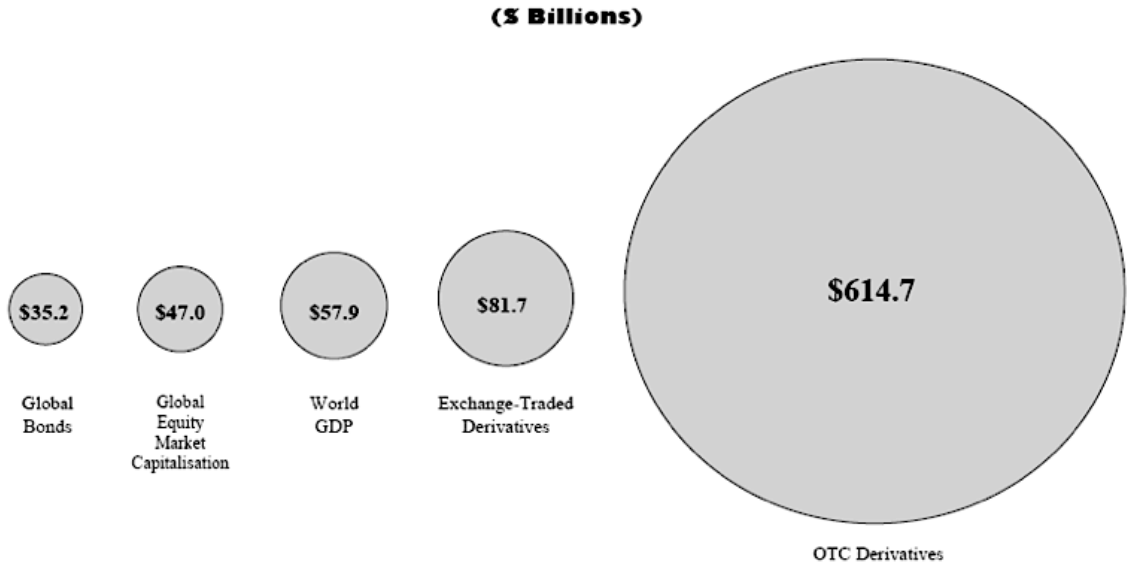
Running complex computations on the Ethereum network results in high gas fees. Building with Zokrates allows us to construct zk-SNARKS that will only need to be verified on-chain.

This is important for the benefits of privacy without additional costs. Zoracles off-chain proving schemes and verifications, allows dApp developers the freedom to focus on building their core products.

8. Adoption

Zoracles is focused on providing the framework for dApp developers to expand their offering with private data. We believe this is a necessary step for enterprise adoption.

The global market for derivatives is quickly approaching a quadrillion dollars [11]. It's financial data is currently being protected by trusted third parties that use the highest level of banking security and encryption to ensure privacy. We anticipate a similar need for DeFi as the industry matures.



As the industry evolves and privacy becomes the default approach, Zoracles should be well-positioned with ZKPs ready for multiple smart contract platforms.

9. Roadmap

The decision to build on top of Open Oracle will allow an easy transition for future projects. We anticipate the industry migrating to this oracle standard and leveraging our ZKPs to ensure privacy of their price feed data.

We believe confidential data delivery is mandatory for enterprises and will pave the way for distributed ledger technology.

We are building ZKP solutions for Ethereum with Solidity Contracts. These will be available for any project to use on a self-serve basis. As ZKPs prove themselves over time, we anticipate larger projects to engage our developers for custom solutions that will have more complex requirements. We will then develop arithmetic circuits similar to those built by Zcash [3].

We have already begun work with libsnark but Zokrates will be initially utilized for our standard implementation. The following are estimates for our software releases:

Q4 2020: ZKPs system deployment

Q1 2021: Partnership Integration w/ZKPs + Open Oracle

Q2 2021: Custom ZKPs arithmetic circuits developed

10. Tokenomics

The proof of work oracle design by Tellor or node operators of Chainlink, in our opinion, is overkill for retrieving price information that can easily be gathered in a Google search.

Google Finance

Region	Exchange Code	Description	Delay (minutes)
Global	CURRENCY	Morningstar	3
	CRYPTOCURRENCY	Coinbase, Inc.	3

The idea that dApps will need to incur tens of thousands of dollars in costs from widely available data is not a sound approach to oracles.

Therefore, we don't believe a utility token is necessary. Most oracle solutions have a native token for node operators to acquire for retrieving data or staking.

This is fundamentally a broken system for open source projects. The real value is consistently providing accurate and reliable data. Zoracles plans to accomplish this with a governance token that steers the project and product.

Here is a breakdown of Zoracles (ZORA) token supply:

- **Early Supporters** comprise 5.00% of the total token supply.
- **Developers** will comprise 35.00% of the total token supply.
- **Strategic Partners** will comprise 25.00% of the total token supply.
- **Board Observers** will comprise 15.00% of the total token supply.
- **Marketing** comprises 10.00% of the total token supply.
- **Advisors** will comprise 7.00% of the total token supply.
- **Community** will comprise 3.00% of the total token supply.

11. Governance

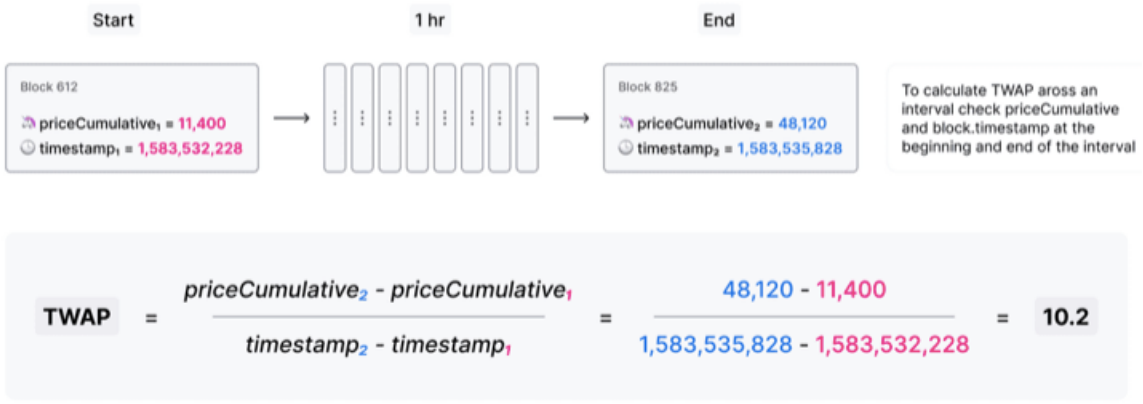
Zoracles governance model is as simple as Bitcoin's "1 cpu = 1 vote [8]." We created a total of 100 Zoracles (ZORA) tokens and each represents a vote on the board that will determine development priorities, strategic partnerships and general administrative decisions.

Each vote is similar to a board seat where projects can acquire influence over Zoracles direction by accumulating votes. For example, if Zoracles plans to develop ZKPs on a new oracle platform, that decision will go to the board and if its gets a majority of the members in favor of developing on a new platform, developers will be assigned to begin work. This process is called "Snarks as a Service."

We anticipate "Snarks as a Service" to expand once our standard implementation is deployed. Governance with majority votes will play a key role in determining priority for projects seeking ZKPs built into any oracle solution.

12. Uniswap V2

Key to delivering accurate and reliable data confidentially to smart contracts is having each Zoracles price signed by a data provider. These prices will be compared to a time weighted average from Uniswap v2 Oracles [10].



An acceptable range is determined and a standard deviation is set to anchor prices retrieved from Zoracles price feed.

This not only prevents a single point of failure with an additional measure to validate prices, but it also protects against sudden spikes or adversarial influence.

13. Conclusion

Zoracles is building ZKPs to add anonymity to oracle data. Our decision to utilize an oracle standard as the base layer is similar to Zcash building on top of Bitcoin Core. We believe this will attract enterprise development of smart contracts as they will require end-to-end privacy.

Our team is committed and dedicated to further expanding the capabilities allowed with ZKPs. Zokrates is a great starting point for building our standard implementation, but custom arithmetic circuits will probably be required for more advanced smart contract development.

We look forward to building more flexible ZKPs as enterprises with more extensive requirements become part of the Ethereum ecosystem.

References

[1] Nicholas van Saberhagen, "CryptoNote v 2.0," https://cryptonote.org/whitepaper.pdf, October 17, 2013

[2] Malte Möser*, Kyle Soska, Ethan Heilman, Kevin Lee, Henry Heffan, Shashvat Srivastava, Kyle Hogan, Jason Hennessey, Andrew Miller, Arvind Narayanan, and Nicolas Christin,"An Empirical Analysis of Traceability in the Monero Blockchain," https://arxiv.org/pdf/1704.04299/, April 23, 2018

[3] Eli Ben- Sasson, Alessandro Chisea, Christina Garman, Matthew Green, Ian Miers, Eran Tromer, Madars Virza, "Decentrazlied Anonymous Payments from Bitcoin," http://zerocash-project.org/media/pdf/zerocash-extended-20140518.pdf May 18, 2014

[4] Zcoinofficial, "An overview of blockchain privacy mechanisms and how Zerocoin in Zcoin $XZC (not Zcash) stack up, 2017

[5] https://prices.compound.finance

[6] https://compound.finance/docs/prices#architecture

[7] Man-in-middle attack https://en.wikipedia.org/wiki/Man-in-the-middle_attack

[8] Jacob Eberhardt, Stefan Tai, "ZoKrates – Scalable Privacy – Perserving Off-Chain Computations, "https://www.ise.tu-berlin.de/fileadmin/fg308/publications/2018/2018_eberhardt_ZoKrates.pdf

[9] Satoshi Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," https://bitcoin.org/bitcoin.pdf, October 31, 2008

[10] https://uniswap.org/docs/v2/core-concepts/oracles/

[11] Soren Financial Management, http://sorensenfinancial.com/the-state-of-todays-market/financial-derivatives-the-next-crash-waiting-to-happen/derivatives-graphic/