DELPHI DIGITAL

Zero-Knowledge Proofs: Privacy & Scaling

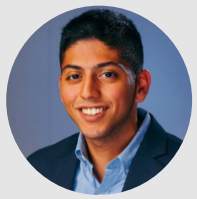
Thematic Insights

April 2019
85 Broad Street
New York, NY, 10004
www.delphidigital.io

Table of Contents

Analysts

Medio Demarco
medio@delphidigital.io



Anil Lulla
anil@delphidigital.io

Executive Summary

A **zero-knowledge proof ("ZKP")** is a cryptographic method that lets one person prove to another person that they know certain information, without having to reveal that information to them. Are you confused yet? If you are don't worry.

The purpose of this Thematic Insights piece is to make a complex topic as simple to understand as possible. We'll provide a high-level overview of the different types of ZKPs, their unique trade-offs and which projects are implementing them. Our goal with this report is to prove (pun intended) how important this technology is, and showcase **the benefits it can offer in terms of privacy and scaling**. Below, we'll provide a few examples to help the concept sink in and a technical definition before moving on to the fun parts.

Examples:

- Transacting in complete privacy but still being able to prove to a regulator you didn't break the law, without having to show them the transactions.
- Proving that you're old enough to buy something (e.g. alcohol), without having to reveal your age.

ZKP Criteria:

1. *Completeness*: if the statement is true, an honest verifier will be convinced by an honest prover.
2. *Soundness*: If the statement is false, a cheating prover can't convince an honest verifier it is true.
3. *Zero-Knowledgeness*: If the statement is true, the verifier doesn't learn anything other than the fact it is true.

zk-SNARKs, Recursive SNARKs, & SONICs:

Zcash | Coda | Matter Labs

zk-STARKs:

StarkWare | Ethereum | 0x

Bulletproofs & MimbleWimble:

Monero | Grin | Beam | Bitcoin

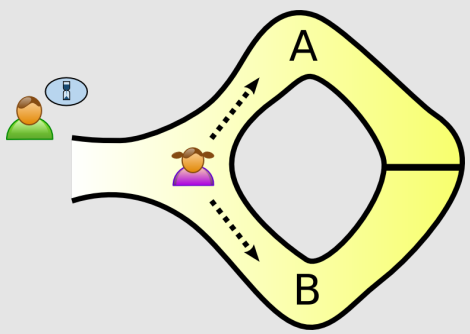
AZTEC Protocol:

AZTEC | Quorum | Ren | CreditMint

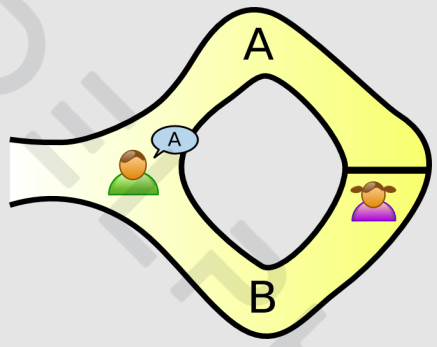
Quick Explainer on ZKPs

The "Ali Baba Cave" was first published back in 1998, and helps explain the fundamental ideas behind zero-knowledge proofs. It is common practice to label the two parties in the example as Peggy (the **prover** of the statement) and Victor (the **verifier** of the statement).

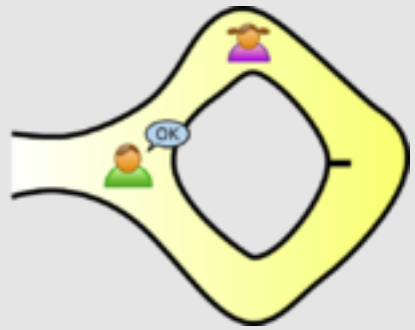
The Ali Baba Cave contains two paths with a magic door in the middle that requires a secret password to open it. Peggy wants to prove to Victor that she knows the secret password, without revealing the password to him.



Victor waits outside as Peggy goes into the cave. Peggy takes either Path A or Path B. Victor is not allowed to see which path she takes.



Then, Victor enters the cave and shouts the name of the path he wants her to use to return, either A or B, chosen at random.



Once Peggy returns from the path Victor shouted out, it is clear that she either knows the secret password or was lucky enough to have chosen the correct path. This means there is still a 50% chance that Peggy lied about knowing the secret password.

50% is not good enough, so Peggy and Victor repeat this exercise. With each successful iteration, the chances that Peggy lied about knowing the secret password decrease. After 20 iterations they become very low (one in a million). At this point, Peggy (the **prover**) has successfully proved to Victor (the **verifier**) that she really does know the secret password.

Sources: Jean-Jacques Quisquatar, Hackernoon

ZKP Overview & History

DELPHI DIGITAL

Non-interactive ZKPs, which these are, were first created in 1988 and have seen progressive developments since. Below, we have highlighted when each of the following iterations were first developed and a brief summary.

	zk-SNARK	zk-STARK	Bulletproofs	AZTEC Protocol
When and who?	• First published by Eli Ben-Sasson, Alessandro Chiesa, Daniel Genkin, Eran Tromer, and Madars Virza in **December 2013**.	• First published by Eli Ben-Sasson, Iddo Bentov, Yinon Horesh, and Michael Riabzev in **March 2018**.	• First published by Benedikt Bunz, Jonathan Bootle, Dan Boneh, Andrew Poelstra, Pieter Wuille, and Greg Maxwell in **November 2017**.	• First published by Dr. Zachary Williamson in **December 2018**.
What is it?	• **zk-SNARK** stands for **Z**ero-**K**nowledge **S**uccinct **N**on-Interactive **AR**gument of **K**nowledge	• **zk-STARK** stands for **Z**ero-**K**nowledge **S**calable **T**ransparent **AR**gument of **K**nowledge	• Named by Shashank Agrawal and means "**short like a bullet with bulletproof security assumptions**".	• **AZTEC** stands for **A**nonymous **Z**ero-Knowledge **T**ransactions with **E**fficient **C**ommunication
Key Takeaways	• **Smallest proof size** • **Fastest verification time** • 2nd fastest prover time	• **No trusted set-up** • **Fastest prover time** • **Quantum resistant** • 2nd fastest verification time	• **No trusted set-up** • 2nd smallest proof size	• It **enables confidential transactions and assets on Ethereum**
Notable Projects	• Zcash • Coda • Matter Labs	• StarkDEX (StarkWare) • StarkPay (StarkWare) • Ethereum*	• Monero • Grin • Beam • Bitcoin*	• AZTEC Protocol • CreditMint • Quorum • Ren • Carbon

Sources: AZTEC Protocol, Stanford University, Tari Labs, Blockstream, Zooko Wilcox

**Ethereum and Bitcoin haven't implemented these yet but could in the future*

ZKP Features & Trade-Offs

DELPHI DIGITAL

Trusted Set-up

- If required, secret system parameters, or "keys", are generated by a third-party during the initial set-up phase.
- These keys are sometimes referred to as "toxic waste". If an entity were to use them they could prove false facts, and create new coins out of thin air.
- The risk of this can be mitigated by using multi-party computation that destroys the keys after.

Speed (Verifier + Prover)

- The combined time it takes for a Prover to generate a proof, and for a Verifier to verify it.
- While we do not show a scale for speed, Bulletproofs are significantly slower than the rest due to their verification time.

Proof Size

- The size of the generated zero knowledge proof.
- As expected, the smaller the better.
- While we do not show a scale for size, zk-STARKs are significantly larger than the rest.

Quantum Resistant

- In the future, quantum computers could pose a risk to the cryptography that secures existing blockchains.
- zk-STARKs are theoretically secure in a post-quantum world.

	Trusted Set-Up	Speed (Verifier + Prover)	Proof Size	Quantum Resistant
zk-SNARK	**Yes**	**Middle**	**Smallest**	**No**
zk-STARK	**No**	**Fastest**	**Biggest**	**Yes**
Bulletproofs	**No**	**Slowest**	**Middle**	**No**

Sources: StarkWare's State of the STARK, D

zk-SNARK Implementations

Project	*Description*
Zcash	• **Zcash**, a privacy focused cryptocurrency, is a fork of Bitcoin that **launched in October 2016**. **ZEC** is it's token. • It was the **first widespread application of SNARKs**. Zcash integrated the Zerocash privacy protocol, first published in May 2014, with Bitcoin's code to create a new cryptocurrency that allowed **users to choose between transparent and private (shielded) addresses**. • The development team behind Zcash has continued its research into SNARKs, which it has used to enhance the network. This can be seen in the improvements from the recent 'Sapling' upgrade.
Coda	• **Coda** is a new blockchain under development from **0(1) Labs**. It **published its whitepaper in May 2018**. • It's attempting to create **a constant-sized blockchain compressed into 1 kilobyte using Recursive SNARKs**. If successful, this would be a significant advancement for scaling blockchains. • Coda uses **a single SNARK proof to represent the entire history of blockchain data**. Rather than having a user check the entire blockchain, they only need to check the SNARK proof to know it is correct. Validators produce these SNARKs to prove they are updating the blockchain correctly. • It **will have a token**, which will be necessary for it's Proof-of-Stake consensus mechanism (using Ouroboros). • Coda's **testnet is currently live**.
Matter Labs	• **Matter Labs** is building the **Franklin Network**, a **layer 2 scaling solution implementing Plasma and SNARKs**. • It's token will be the **FNT**, which will be necessary for the Delegated Proof-of-Stake consensus mechanism. • In **February 2019, the Ethereum Foundation provided Matter Labs with a grant** to further layer 2 scaling efforts. • In **January 2019**, a paper was published for **a new type of SNARK called a 'Sonic',** which could minimize the risk involved with trusted set-ups. As a result, Matter Labs is working to deliver a practical implementation of Sonics.

Sources: Zerocash Paper, Zcash, Ethereum Foundation, Sonic Paper, Coda Paper, Alex Gluchowski (Founder of Matter Labs)

StarkWare

DELPHI DIGITAL

Starkware, a startup based in Israel, is aiming to improve scalability and privacy in blockchains using STARK technology, providing cryptographic proofs that are zero-knowledge, succinct, transparent (no need for a trusted set up), and post-quantum secure.

Key Personnel

Eli Ben Sasson
Co-Founder
Chief Scientist in the East

Alessandro Chiesa
Co-Founder
Chief Scientist in the West

Michael Riabzev
Co-Founder
Chief Architect

Dr. Eli Ben Sasson was a former founding scientist at Zcash and co-authored the whitepapers for zk-SNARKs and zk-STARKs. He is also a Professor of Computer Science at Technion the Israel Institute of Technology.

Dr. Alessandro Chiesa was a former founding scientist for Zcash and co-authored the whitepaper for zk-SNARKs. He is also an Assistant Professor for Electrical Engineering & Computer Science at UC Berkeley. He has a PHD in Computer Science from MIT.

Michael Riabzev is a PHD student at Israel Institute of Tech.

Funding

Raised

$40M

Equity + EF Grant

Investors

PANTERA

MULTICOIN CAPITAL

METASTABLE BITMAIN

SEQUOIA

ConsenSys Ventures

POLYCHAIN CAPITAL

Notable Tweet

Kyle Samani
@KyleSamani

Wow

Shit is getting real in ZKP land

> **StarkWare** @StarkWareLtd · Mar 22
> This just in from our presentation at the ZK-Summit in Berlin #ZK0x03:
> 1/ StarkDEX, our settlement engine for non-custodial exchanges (DEXes) is now able to settle over 500 trades/second, costing less than 1,000 gas per trade.
> Show this thread

R&D

15 engineers

Strong scientific consultants

Currently being tested

Github
View here

Key Takeaway

Significant scaling benefits

Sources: Circle Research, Multicoin, Starkware

zk-STARK Implementations

Project	*Description*
 **Ethereum**	• Integrating STARKs into Ethereum is **currently on the roadmap for "Ethereum 3.0"**, however, there is little information available at this point. • In **July 2018**, **StarkWare received a grant from the Ethereum Foundation worth $4m and 6k ETH performance-based bounties**. Excluding the bounties, this is the second biggest grant the EF has given out behind Parity Technologies. • The purpose of the grant is for **StarkWare to explore STARK-friendly hash functions, develop its technology, and to offer open source code to the ecosystem.**
 **StarkDEX**	• In December 2018, StarkWare **announced** that the first application of STARK technology would be **a settlement engine for DEXs** called **StarkDEX**. • On **March 22, 2019** at the ZK-Summit in Berlin, StarkWare **unveiled test results** for their StarkDEX. It was able to **settle over 500 trades/second, fit 8,000 trades/block, and with each trade costing less than 1000 GAS**. This represents a **200x scaling increase relative to Ethereum**. • StarkDEX allows trades to be processed off-chain by a third-party ("Prover"), who then generates a proof which can be quickly verified on-chain. • StarkWare announced they're **working with 0x Protocol to launch a StarkDEX testnet in mid April**.
 **StarkPay**	• On **March 4, 2019**, StarkWare **announced a scalability solution for payments** called **StarkPay**, and compared it to Bitcoin's Lightning Network. Like StarkDEX, transactions are processed off-chain, and confirmed on chain with a proof. • According to StarkWare, **StarkPay will be able to support over 10,000 payments in a single block**, per Ethereum's current GAS constraints. The amount of on-chain computational resources consumed by StarkPay grows logarithmically with the size of off-chain computation. For example, **if StarkPay grew 10x, the on-chain resources consumed would grow by less than 50%.** • Other benefits include capital-efficiency (no extra funds need to be locked up beyond what each payer wishes to pay), liveness-free (updating a balance doesn't require a payee to be online), and it is non-custodial. • Notable disadvantages include data availability, initial centralization (run by StarkWare), latency, and the fact that Bitcoin in its current form cannot support it.

Sources: State of STARK (October 2018), Github, Ethereum Foundation, StarkWare Medium, StarkWare Twitter, Circle Research

Bulletproof Implementations

Cryptocurrency	*Description*
Monero	• **Monero**, a privacy focused cryptocurrency, implemented Bulletproofs for their Confidential Transactions in **October 2018**. **XMR** is it's token. • As a result, the **average data size on the blockchain per payment was reduced by ~73%**, and the **average $ based fees were reduced by ~95%**.
Grin **Beam**	• **Grin & Beam**, are privacy focused cryptocurrencies, launched in January 2019 that run the MimbleWimble protocol. **GRIN** and **BEAM** are their respective tokens. • **MimbleWimble** ("MW") was first published in July 2016 by "Tom Elvis Jedusor". Fun fact, both the name and author are Harry Potter references. • MW offered an improvement over existing Confidential Transactions techniques and, when coupled with Bulletproofs, can produce a **private and highly compressed blockchain**. • While Grin is it's own blockchain, some consider it a MimbleWimble **"testnet" to assess it's viability for a potential implementation on Bitcoin** in the future.
Bitcoin	• **Bitcoin** has not implemented Bulletproofs yet, however, it could in the future to improve privacy and scalability. • Prominent Bitcoin developers Andrew Poelstra, Pieter Wuille, and Greg Maxwell helped co-author the Bulletproof paper. Afterwards in 2017, Pieter Wuille stated that Bulletproofs were "far too premature to propose for inclusion into Bitcoin." • According to Stanford University, "If all Bitcoin transactions were confidential and used Bulletproofs, then the total size of the UTXO set would be only 17 GB, compared to 160 GB with the currently used proofs." This is equates to a **reduction in blockchain size by a factor of 10**. • zk-STARKs have also recently been mentioned for Bitcoin sidechains.

Sources: Bulletproofs Whitepaper, Stanford University, Andreas Antonopoulos, Pieter Wuille, Blockstream, Tari Labs, Forbes

AZTEC Protocol

DELPHI DIGITAL

AZTEC Protocol (based in London) is a new type of zero-knowledge proof that enables private transactions on Turing-complete blockchains, such as Ethereum. It also enables the creation of encrypted, private assets on Ethereum. They are building a suite of tools to facilitate private transactions and interoperability between dApps building on Ethereum.

Key Personnel

Tom Pocock
CEO

Dr Zac Williamson
CTO

Tom Pocock has a BA & Masters in Mathematics from Cambridge, Graduate Diploma in Law from City Law School, and is a CFA Charterholder.

Dr. Zac Williamson has Doctorate in Particle Physics from Oxford and was a former physicist at CERN at T2K Japan. He created AZTEC Protocol.

Funding

Raised

$2.1M

Seed

Investors

CONSENSYS

SAMOS INVESTMENTS

R&D

5 engineers

Live on Ethereum

Currently being tested

Github
View here

Notable Tweet

Maker
@MakerDAO

Whoa. 👀

alex van de sande @avsa · Nov 30, 2018
A zero knowledge DAI implementation working live on the main chain: github.com/AztecProtocol/...
Programmable, private, stable. We're slowing approaching the holy grail of currencies.

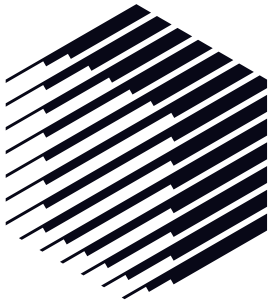
11:15 AM · Nov 30, 2018 · Twitter Web Client

Key Takeaway

Selective privacy on Ethereum

Sources: AZTEC Protocol, ConsenSys, Crunchbase

AZTEC Implementations

Project	*Description*
J.P.Morgan  **Quorum**	• In **February 2019**, it was announced that **JPMorgan is testing AZTEC on Quorum**, their private version of Ethereum's blockchain. • While JPMorgan's focus has been on private blockchains so far, the AZTEC testing is **important because it would allow them to maintain their privacy on a public blockchain**. • An insider at JPMorgan confirmed they are "looking to industrialize zero-knowledge proofs for Quorum".
 **Ren**	• **Ren** is a protocol that enables the creation of private, decentralized financial applications, such as dark pool DEXs. REN is it's token. • On **March 5, 2019**, **Ren announced that they would be implementing AZTEC**. • Utilizing AZTEC, **RenEx will be the first decentralized exchange to offer complete privacy** without revealing trades or their value. • AZTEC will also underpin Ren's zero-knowledge transaction layer. By default, **this will allow any application built using Ren to have private transactions on Ethereum**.
 **CreditMint**	• **CreditMint** was **started in March 2018 by the founders of AZTEC** as a platform for originating, trading, and settling debt on Ethereum. • They soon realized that they wanted privacy and the benefits of a public blockchain. This led Dr. Zac Williamson to create AZTEC and later implement it on CreditMint. • CreditMint later received backing by prominent investors (e.g. ConsenSys) and is now **focused on building tools that will allow traditional assets, such as loans and bonds, to be issued on Ethereum**.

Sources: Aztec Protocol, Ren, Coindesk

Leader Commentary

To get some further insight, we reached out to people within the community.

Kyle Samani
CoFounder of Multicoin

What application of ZKPs are you most excited about?

"There are really only two categories of use cases. Privacy and scaling. I'm more excited about the latter than the former as I think it unlocks far more value."

Alex Gluchowski
Founder of Matter Labs

What challenges do you see for implementing ZKPs?

"The learning curve for ZKP is quite high and the talent pool of people capable to understand them is limited."

Richard Burton
CEO of Balance

What is an important point about ZKPs that most people should know, but don't?

"[The potential for] selective privacy [on Ethereum]."

If you enjoyed the report, please feel free to Tweet about it.

Disclosures

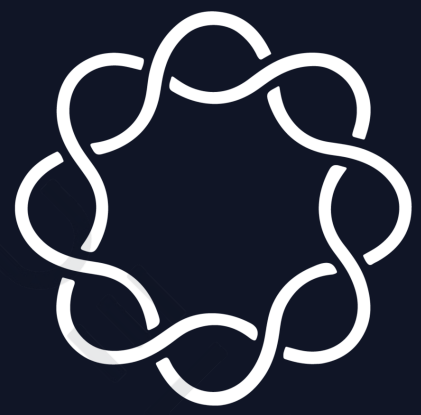
The Research Team may own the tokens represented in this report, and as such this should be seen as a disclosure of any potential conflict of interest. Anyone can contact Delphi Digital for full token disclosures by team member at Team@DelphiDigital.io. This report belongs to Delphi Digital, and represents the opinions of the Research Team.

Delphi Digital is not a FINRA registered broker-dealer or investment adviser and does not provide investment banking services. This report is not investment advice, it is strictly informational. Do not trade or invest in any tokens, companies or entities based solely upon this information. Any investment involves substantial risks, including, but not limited to, pricing volatility, inadequate liquidity, and the potential complete loss of principal. Investors should conduct independent due diligence, with assistance from professional financial, legal and tax experts, on topics discussed in this document and develop a stand-alone judgment of the relevant markets prior to making any investment decision.

Delphi Digital does not receive compensation from the companies, entities, or protocols they write about. The only fees Delphi Digital earns is through paying subscribers. Compensation is not received on any basis contingent upon communicating a positive opinion in this report. The authors were not hired by the covered entity to prepare this report. Delphi Digital did not receive compensation from the entities covered in this report for non-report services, such as presenting at author sponsored investor conferences, distributing press releases or other ancillary services. The entities covered in this report have not previously paid the author in cash or in stock for any research reports or other services. The covered entities in this report are not required to engage with Delphi Digital.

The Research Team has obtained all information herein from sources they believe to be accurate and reliable. However, such information is presented “as is,” without warranty of any kind – whether expressed or implied. All market prices, data and other information are not warranted as to completeness or accuracy, are based upon selected public market data, reflect prevailing conditions, and the Research Team’s views as of this date, all of which are accordingly subject to change without notice. Delphi Digital has no obligation to continue offering reports regarding this topic. Reports are prepared as of the date(s) indicated and may become unreliable because of subsequent market or economic circumstances. The graphs, charts and other visual aids are provided for informational purposes only. None of these graphs, charts or visual aids can and of themselves be used to make investment decisions. No representation is made that these will assist any person in making investment decisions and no graph, chart or other visual aid can capture all factors and variables required in making such decisions.

The information contained in this document may include, or incorporate by reference, forward-looking statements, which would include any statements that are not statements of historical fact. No representations or warranties are made as to the accuracy of such forward-looking statements. Any projections, forecasts and estimates contained in this document are necessarily speculative in nature and are based upon certain assumptions. These forward-looking statements may turn out to be wrong and can be affected by inaccurate assumptions or by known or unknown risks, uncertainties and other factors, most of which are beyond control. It can be expected that some or all of such forward-looking assumptions will not materialize or will vary significantly from actual results.



DELPHI DIGITAL

85 Broad Street
New York, NY, 10004
www.delphidigital.io