Zero knowledge proofs:
Why we need better technical standards

Colin Monroe

Abstract

Zero knowledge proofs are cryptographic proofs which have the ability to prove a piece of information without revealing anything about it. This will be instrumental in creating privacy preserving systems in the future. Currently the most well known use of zero knowledge proofs are zk-SNARKs.They are utilized by the Z-CASH blockchain to provide anonymity to transactions. However, like with any complicated technology computational succinctness is fragile. This means that without the proper oversight by an independent government organisation these proofs may be misused or incorrectly used causing a breach in privacy.

Keywords: Zero Knowledge Proofs, zk-SNARK, computational succinctness, government standards

Introduction

Zero knowledge proofs will be essential in helping to create privacy preserving systems in the future. A zero knowledge proof has the ability to prove a piece of information is valid without revealing anything about it (Uriel Feige, Amos Fiat, Adi Shamir, 1988). While this may sound a bit like magic it is possible through the use of some advanced mathematics. One of the difficulties with zero knowledge proofs is showing succinctness of the computational process (Vitalik Buterin, 2017). This is due to the fragility of computation as any tiny changes can produce a different result (Vitalik Buterin, 2017). So unless you are an expert, it is hard to know if the proof is working as promised. Implementation of new complicated technologies into general society is only as safe as the users intentions. This is why we must consider having companies comply with technological standards which protect the public. Otherwise it could lead to widespread misuse by malicious actors or incorrect setups, leading to breaches in data privacy. Currently there are no regulations or laws in place which dictate the security standards in which software applications are created. Which is why for society to gain the benefits and maintain trust in this technology we need an Food and Drug Administration (FDA) like organisation for oversight of technology. This paper will explore and explain what zero knowledge proofs are. It will also show how valuable they can be to preserving data privacy in an information driven world.

Literature Review

Zero knowledge proofs

Zero knowledge proofs were first mentioned by Shafi Goldwasser, Silvio Micali, and Charles Rackoff in “The Knowledge Complexity of Interactive Proof-Systems” published in 1985. A Zero knowledge proof is when you can prove to another entity that a piece of information is true without revealing anything about that information (Uriel Feige, Amos Fiat, Adi Shamir, 1988). This example of mini-sudoku will demonstrate how the Prover can show that there is a solution for this puzzle to the Verifier without revealing the solution. So to solve this we will need to fill in each row, column, and sub-square with the numbers 1, 2, 3, 4. So that each row and column only have one of each number. All sudoku puzzles have an initial set of numbers given as seen in figure 1 (Christian Reitwiessner, 2017). This process can be used to prove a solution no matter how big the sudoku board.

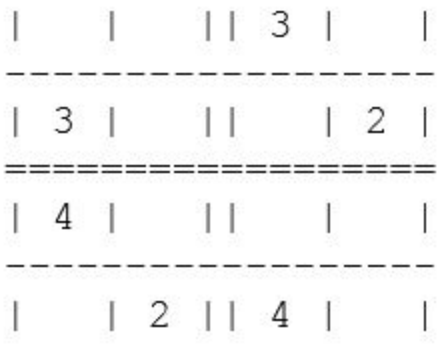


Figure 1. (Christian Reitwiessner, 2017)

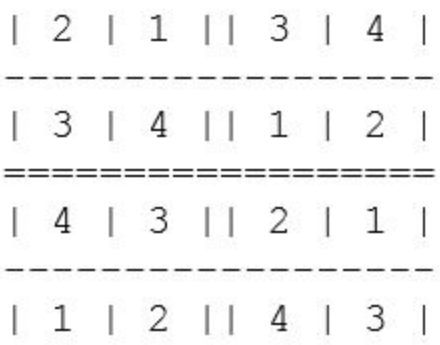


Figure 2. (Christian Reitwiessner, 2017)

So you can see in figure 2 that the Prover has a solution for this particular sudoku puzzle (Christian Reitwiessner, 2017). Now the Prover will mix all of the numbers so now 1 = 3, 2=4. 3=2, 4=1. This results in a shuffled version which is still a solution, as shown in figure 3.

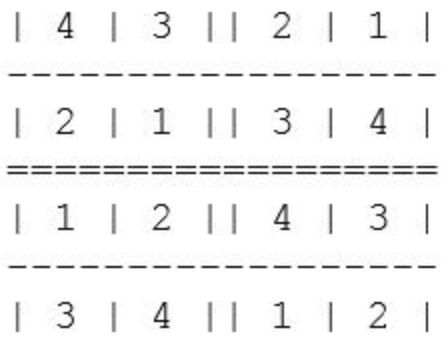


Figure 3. (Christian Reitwiessner, 2017)

Now the Prover covers all of the squares of the sudoku puzzle and presents it to the Verifier:

Figure 4. (Christian Reitwiessner, 2017)

The Prover then gives the verifier the ability to choose only one of the following options:

1) Reveal a certain row
2) Reveal a certain column
3) Reveal a certain subsquare
4) Reveal the initially filled squares and the shuffling

Once the Verifier chooses a step and sees the result then a new round begins where the:

1) Prover shuffles the numbers
2) Prover covers all squares

3) Verifier chooses an option once again
4) Prover reveals
5) Verifier checks

Each time the Verifier checks an option they are able to see that it is a valid answer. Since the Prover keeps re-shuffling the numbers, it does not allow the Verifier to gain the actual solution. If the Prover is trying to cheat, the likelihood that they are discovered increases with each round. This means that the process must be done many times as the more times it is done, the more certain the Verifier is that the solution is valid (Christian Reitwiessner, 2017).

While this example shows the zero knowledge process, it cannot be used for practical purposes (Christian Reitwiessner, 2017). This is due to the fact it cannot be used for general computations (Christian Reitwiessner, 2017). More importantly though, it takes too many rounds of interactions due to there being a possible “error” in any single cell (Christian Reitwiessner, 2017). This is why Zero Knowledge Proof applications are now using low degree polynomials. The theorem of polynomials that says: Two different polynomials of degree up to n can coincide in at most n points (Vitalik Buterin, 2017). This means that anyone who tries to cheat will be easily spotted since the polynomial generated will only intersect at n points. As seen in figure 5 the only difference in the polynomials is $2x^4$ vs. $1x^4$ and they are almost completely different.

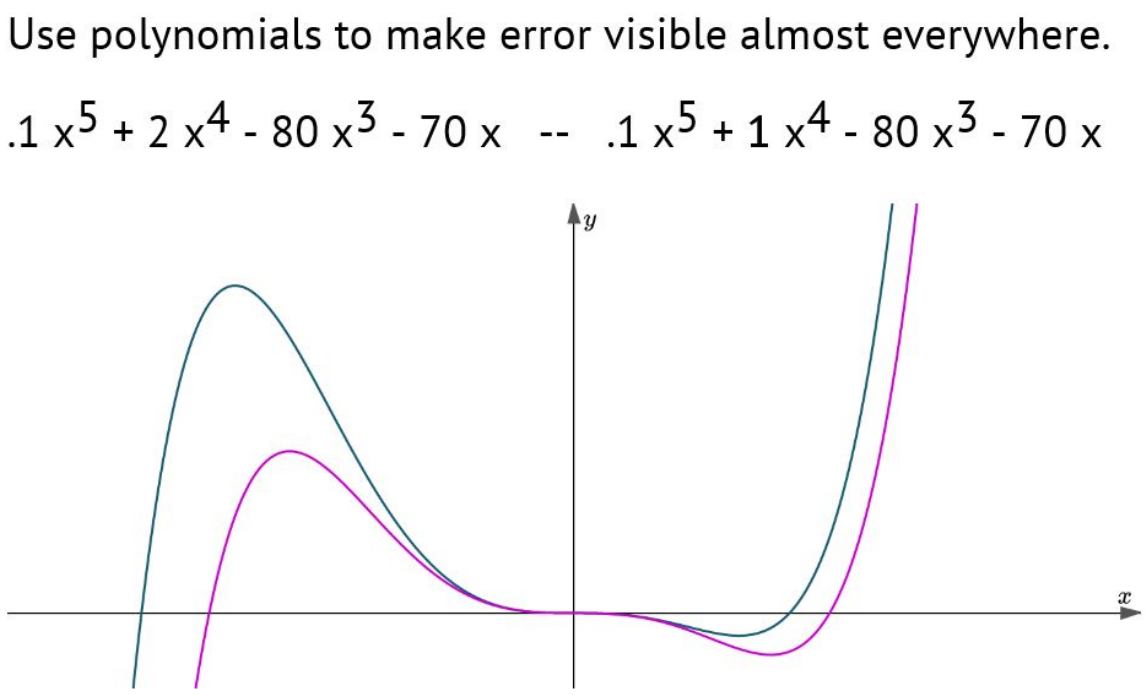


Figure 5. (Christian Reitwiessner, 2017)

Succinctness is probably one of the hardest things to show in computation due to its fragility (Vitalik Buterin, 2017). In very long and complex computations any tiny change like a 1 to a 0 could lead to a different result (Vitalik Buterin, 2017). This can be accomplished by using some advanced math using polynomials to compare millions of points against each other.

The most well known zero knowledge proof application is called a zk-SNARK used by the Z-Cash blockchain to protect their transactions (ZCASH, 2017). Their potential successor is called a zk-STARK which eliminates the need for a trusted setup and elliptical curve cryptography (Eli-Ben Sasson, 2017).

In this case, with the example of zk-SNARKs you can see that there are many more components required. By using polynomials to create zero knowledge proofs you need to utilize other techniques to help preserve privacy. First a trusted setup must be conducted to create the

parameters for the zero knowledge proof. By knowing what you are proving, in this case validity of transactions, this trusted setup can create a reusable point (x) to verify polynomials (ZCASH, 2017). This not only dramatically speeds up the proof verification time but allows the proof to be non-interactive. In the sudoku example the process was done with an interactive verifier, but most of the time this is not practical. Next the Prover has their information transformed into a polynomial. This is accomplished by first flattening the information into the smallest logical steps possible creating an arithmetic circuit (ZCASH, 2017). A Rank one constraint system is used to check the travel path of all values (ZCASH, 2017).. Now the Prover has a secret polynomial and the Verifier has a secret point. Neither can give these secrets to the other as they could just then cheat and construct a polynomial or pick a point that would prove validity. This is why in zk-SNARKs, Homomorphic encryption pairings are used which gives the ability to perform calculations on encrypted data (ZCASH, 2017). In this way the point can be calculated on the polynomial without either side knowing the exact properties. The pairing is created using elliptical curve cryptography (ZCASH, 2017). In this process, currently, the trusted setup is the biggest concern with zk-SNARKs, as if there is collusion between the parties they may create forged proofs compromising the entire system.

Findings

Why use zero knowledge proofs?

In an age where everyone from malicious actors to organisations, are trying to collect personal information, data privacy is hard to come by. The application of zero knowledge proofs to current and future systems will be incredibly important for creating actual data privacy. The ability to prove a piece of information without revealing it means that no other party can obtain that information. This is in contrast to current systems where even if you are using

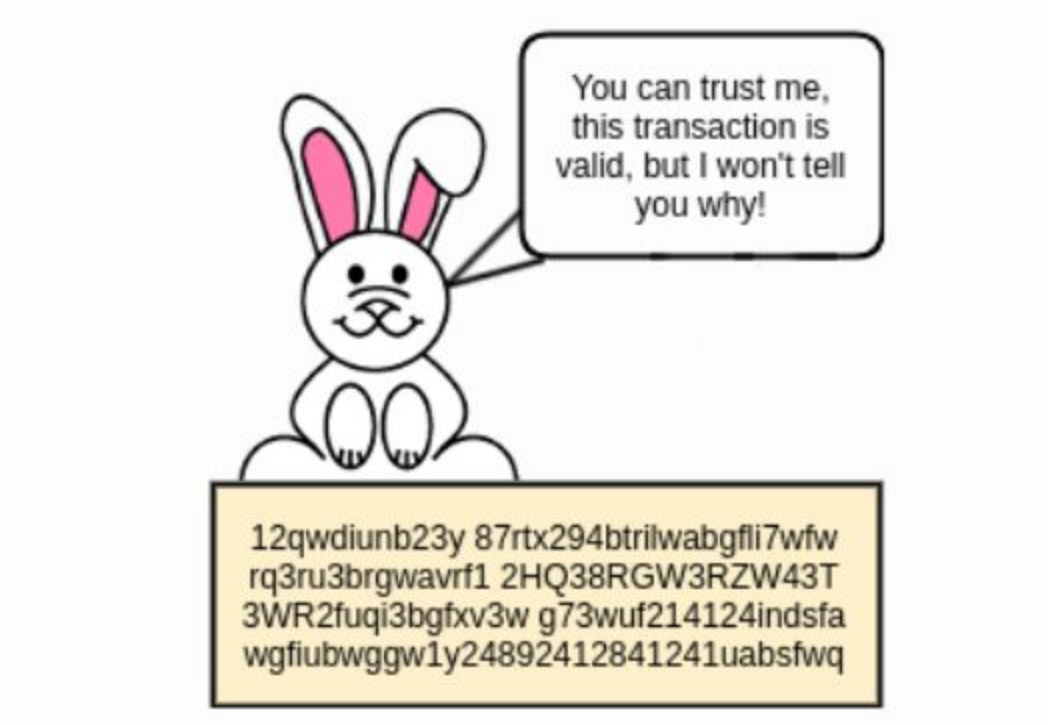
cryptography the information can be intercepted and decoded. It is also always vulnerable at the endpoints once decryption occurs. Many systems also base their privacy on pseudonyms which have been proven to be not effective in maintaining privacy (Vitalik Buterin, 2017). This has been shown with the users of Bitcoin, which uses pseudonyms for identification, who have been tracked by law enforcement through their transactions and other metadata (Anton Zuenko, 2017).

Zero knowledge proof applications will be an integral tool to preserve data privacy in decentralized systems. Since almost all decentralized systems will have their information completely public it is important to shield a user's actions. Even if these systems use pseudonyms a user can still be identified through tracking and metadata (Vitalik Buterin, 2017). As an example, if you were bidding on a house against several other parties you would want to make sure that they are not able to see your bid. Using zero knowledge proof applications you would be able to mask the transaction or smart contract you were using (Anton Zuenko, 2017). Also, you would need to prove to the bank that you have enough money to loan or buy the property. Usually you would have to produce certified documents proving that your account has X amount of money in it, which satisfies the requirements. With a zero knowledge proof you could prove that you have the minimum required money without revealing your exact bank balance (Anton Zuenko, 2017). This preserves privacy by not having to give out information that is not essential to the transaction.

Are there risks to society in using Zero knowledge proofs?

Zero knowledge proof applications can be used to provide privacy for many different systems. However, the fact remains that they incorporate many techniques that can be

easily manipulated allowing a change in their results. As shown the computational succinctness of zero knowledge proofs are very fragile. If proper standards are not laid out people's perception of zero knowledge proofs could end up like this:



Since most people do not trust in something that they cannot fully understand. Until it has proven itself, they will trust in the organisation using it and not in the technology itself. As an example, most people do not know how the facial ID for Apple works but they still use it because they trust Apple. This means that if an organisation misuses it in an incorrect or malicious fashion it will damage the reputation of the technology itself. At worst, the technology could be shunned aside by the public and not allowed to fulfill its potential. At the very least, it could be used in a fashion which unknowingly to the public could compromise their privacy. One scenario could be if a trusted financial institution announced that they were going to use their own zero knowledge application. While they guarantee that it will provide anonymity to their customers transactions they do not publish the proof for this application due to it being

proprietary. A year later people find out that the zero knowledge proof had a backdoor in it allowing the institution to monitor all transactions. They took this data and used it for themselves and sold some to data brokers. While this should just make people wary of the institution not the technology. However, since people do not fully understand the technology they will become wary of other institutions making similar claims. This could lead to institutions moving away from using them as from a business PR point of view it would be easier.

Technical Standards

How should a consumer know what to trust if there is no way for them to independently verify a piece of technology? This is the same question that people ask when they go to buy pharmaceutical products. You do not have the knowledge that is necessary to know if the chemical compounds that make up product X is safe or not. You do not know if product X will be able to do what it claims. You rely on the FDA to screen these using set standards to protect your safety. This is why to protect the consumer and the technology there needs to be an organisation that reviews and verifies which applications are safe.

Why an independent government organisation?

An independent government organisation should be used instead of a private one simply because it can provide an incentive for organisations to comply. Whether it is done through liabilities or regulations, financial incentive can be created to maintain honesty. To make sure that growth is not stunted in the production and research, the organisation should only assess zero knowledge proofs that have been called into question. If organisations wish to submit their proofs for review and upon review they are considered valid, they should be put up as recommended applications. This way a consumer could go onto their website and be able to

quickly see what proofs have been approved. While they may choose to go with a company that does not use one of the approved ones they are now at least educated about which proofs are guaranteed to be safe.

Recommendations/Improvements

An independent government organisation, equivalent of the FDA, should be created to maintain oversight of new technologies like zero knowledge proofs. This organisation should be created in the same fashion as the National Institute of technology NIST. Where new technologies are verified and validated through research and competitions like the AES algorithm (NIST, 2001).

In its formation there should be creation of strict set of standards that must be followed by developers and organisations. If they are found to have not complied with these standards they should be found liable and have to compensate all damaged parties. For zero knowledge proofs some of the standards could possibly be:

1) All elliptical curve cryptography must use curves which are proven through research to be sound.

2) Zero knowledge proofs will provide complete anonymity for the users from all other parties.

3) If using a trusted setup the company must prove through a public demonstration that the verifier key is completely erased.

A Challenge system should be developed for the general public and academic community. If they find that an implementation of a zero knowledge proof does not meet the

required standards they can submit it for review. To prevent rival companies from constantly challenging each other the rules for posting a challenge could be: If X amount of private citizens sign a petition or if Y amount of independent academic experts sign a petition then a challenge is successful. Then a company would need to hand over their zero knowledge proof even if they are claiming it is proprietary knowledge. The results of a challenge would in ,zero knowledge fashion, only reveal if the proof is valid.

Future Work

For zero knowledge proofs to be fully trustworthy the elimination of the trusted setup and elliptical curve cryptography is needed (Eli-Ben Sasson, 2017).

There needs to be a better way with possibly a game or video that explains how the computational succentiness of this technology works to the general public.

The creation of better standards with properly defined definitions and with their corresponding technical standards is needed.

Conclusion

Data privacy is a right and should be available to everyone. Current data privacy techniques while effective do not provide complete anonymity. Zero knowledge proofs provide the tools to create complete anonymity for the user. This is why it is a vitally important piece of technology for society. Like other complicated technologies it is not verifiable unless you are an expert in the field. To prevent incorrect and misuse of this technology which could potentially make it obsolete oversight must be established. A government organisation should be formed that can provide the consumers with guidance and the organisations with financial incentive to remain honest.

Bibliography

Buterin, V. (Nov. 9, 2017). STARKs, Part I: Proofs with Polynomials. Retrieved on 11/14/17 from http://vitalik.ca/general/2017/11/09/starks_part_1.html

Buterin, V. (Nov. 9, 2017). STARKs, Part II: Thank Goodness It's FRI-day. Retrieved on 11/14/17 from http://vitalik.ca/general/2017/11/09/starks_part_1.html

Buterin, V. (Feb. 3, 2017). Quadratic Arithmetic Programs: from zero to hero. Retrieved on 11/14/17 from https://medium.com/@VitalikButerin/quadratic-arithmetic-programs-from-zero-to-hero-f6d558cea649

Buterin, V. (Jan. 15, 2017). Exploring Elliptic Curve Pairings. Retrieved on 11/14/17 from https://medium.com/@VitalikButerin/exploring-elliptic-curve-pairings-c73c1864e627

Feige, U, Fiat, A, Shamir, A. (1988) Zero Knowledge Proofs of Identity. Retrieved on 11/14/17 from http://www.fi.muni.cz/~xslaby/jirislaby/jiri_slaby/kr/9/p210-fiege.pdf

Goldwasser, S. Micali, S. Rackoff, C. (1985) The Knowledge Complexity of Interactive Proof-Systems. Retrieved on 11/10/17 from http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.419.8132&rep=rep1&type=pdf

NIST, (November 26, 2001) FIPS 197, Advanced Encryption Standard (AES). Retrieved on 12/01/17 from http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.197.pdf

Reitwiessner, C. (November, 2017) Introduction to zk-SNARKs. Retrieved on 12/02/17 from https://chriseth.github.io/notes/talks/intro_to_zksnarks/#/22

Sasson, E. (November 16, 2017) Introduction zk SNARKs STARKs Eli Ben Sasson Technion Cyber and Computer Security Summer School. Retrieved on 11/17/17 from https://www.youtube.com/watch?v=VUN35BC11Qw

Sasson, E. (November 16, 2017) STARKs II - Low Degree Testing Eli Ben Sasson Technion Cyber and Computer Security Summer School. Retrieved on 11/17/17 from https://www.youtube.com/watch?v=L7tZeO8ihcQ

ZCASH. (2017) How zk-SNARKs work in Zcash. Retrieved on 11/14/17 from https://z.cash/technology/zksnarks.html

Zuenko, A. (May 15, 2017) Zero-Knowledge Explained -- Part 1: Use Cases. Retrieved on 12/03/17 from http://blog.stratumn.com/zero-knowledge-explained-part-1-use-cases/