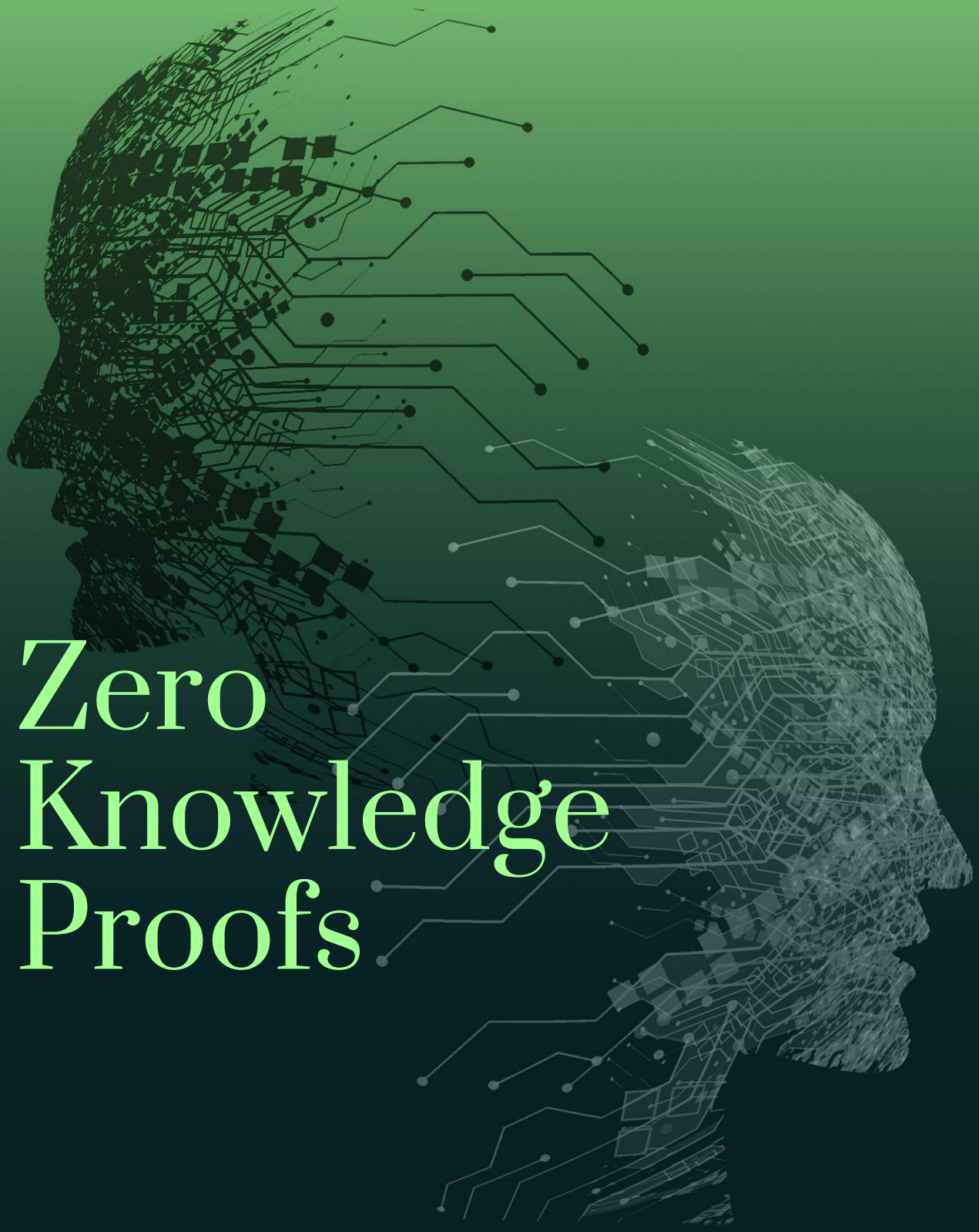
Greengage



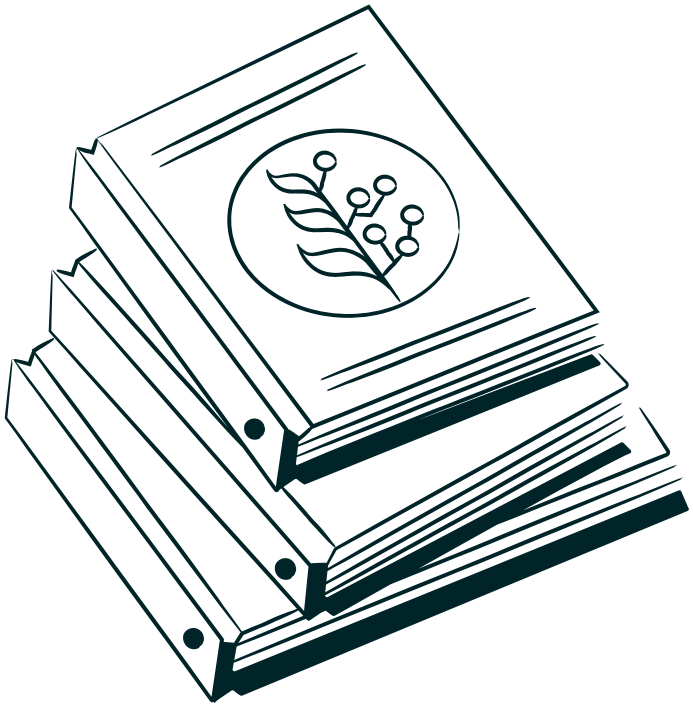
Zero Knowledge Proofs

WHITE PAPER

Contents

Introduction

This paper aims to educate readers on the uses and importance of zero knowledge proofs (ZKPs) in today's growing digital landscape. Starting with the basics, we go on to show where ZKPs are most needed, drawing from real-world examples and research to support. Beyond our organisational aspirations, we hope that this paper highlights the importance of ZKPs to inspire wider adoption of the application throughout industries and sectors where data is at risk and fraud is rife. We strongly believe that this technology has transformative potential that can be of tremendous benefit to society and industry. Let us tell you how.



The story so far

What are Zero Knowledge Proofs?

Zero Knowledge Proofs (ZKPs) are a type of cryptographic protocol based on complex algorithms that allow one party (the prover) to prove to another party (the verifier) a statement is true without revealing any additional information. In simple terms, ZKPs are a precision tool for verifying information by only revealing if a statement is true or false. In the real-world, hospitals could verify patient's records without knowing confidential medical information, banks could confirm sensitive data without being exposed to it and governments could verify citizenship without requiring passport details. A key issue with authenticating sensitive data is that valuable information must be revealed to confirm it is genuine, which exposes it to cyber criminals. If only data could be verified without revealing its source or content, therefore enter ZKPs, a powerful tool for protecting data and preventing fraud.

Where did ZKPs originate?

ZKPs first appeared in a 1985 MIT research paper 'The Knowledge complexity of interactive proof systems'[1] which largely dictates how we define ZKPs today. Since their inception, ZKPs have evolved rapidly, enabling wider access and application in real-world contexts. Notable improvements since the original inception have led to less complexity, greater commercial viability and efficiency gains.

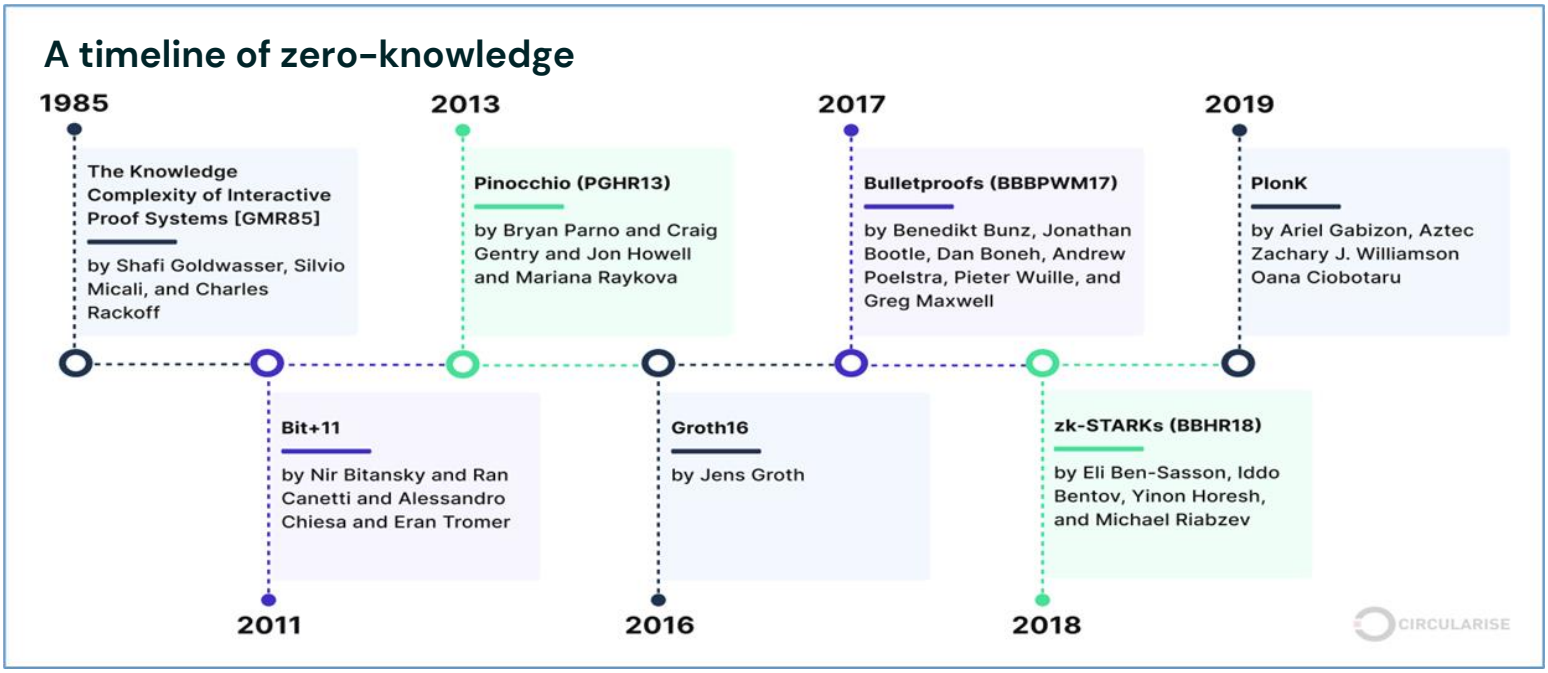


Figure 1: Source Circularise.com 'A timeline of the development of zero-knowledge proofs'[2]

1. The Knowledge complexity of interactive proof systems
2. Zero-knowledge proofs explained in 3 examples (circularise.com)

How do ZKPs work?

The Ethereum organisation states that a ZKP allows you to prove the truth of a statement without revealing the statement's contents or how the truth was found. This occurs when the algorithms that make up a ZKP's DNA take elements of the data and present it as true or false output allowing confirmation or rejection of a statement. A ZKP has the following criteria: [3]

Completeness - if the input is valid, a ZKP protocol will always return true and the proof can be accepted; **Soundness -** If the inputs are invalid, it is impossible for the protocol to return true, thus dishonest provers cannot trick the system; and **Zero Knowledge -** Beyond true or false the verifier knows nothing more about the statement.

What types of ZKPs exist?

Interactive zero knowledge proofs follow the basic principles of ZKPs but both users have to be active and interact repeatedly making independent verification impossible, which make the original concept of ZKPs unviable. It was not until 1988 when the creation of non-interactive zero-knowledge proofs solved this problem. Independent verification via a single round of communication marked a revolution of ZKP technology which are now the main types of ZKP used today. Continual development of the technology and algorithm have led to two main types being predominantly used:

- **zk-SNARKs -** Zero Knowledge Scalable Non-Interactive Argument of Knowledge. zk-SNARKs can: validate information without knowing anything else about the statement; are verified quickly; require one interaction; are extremely difficult to cheat; and cannot be created without access to the secret information.

- **zk-STARKs -** Zero Knowledge Succinct Transparent Argument of Knowledge. zk-STARKS operate in a similar fashion but are scalable, making them faster at generating and verifying information. Additionally, they are transparent by relying on publicly verifiable randomness to generate parameters for verification. As a result, they are more cost-effective than zk-SNARKS.

3. A ZKP has the following criteria

The case for zero knowledge

Why do we need ZKPs?

One answer is fraud. When personally identifiable information is shared with third parties, it is stored in central databases which are vulnerable to hacks. Confidential data is leaked, exposing users to identity theft and other types of fraud. Identify theft is a growing problem and ZKPs offer a pragmatic solution.

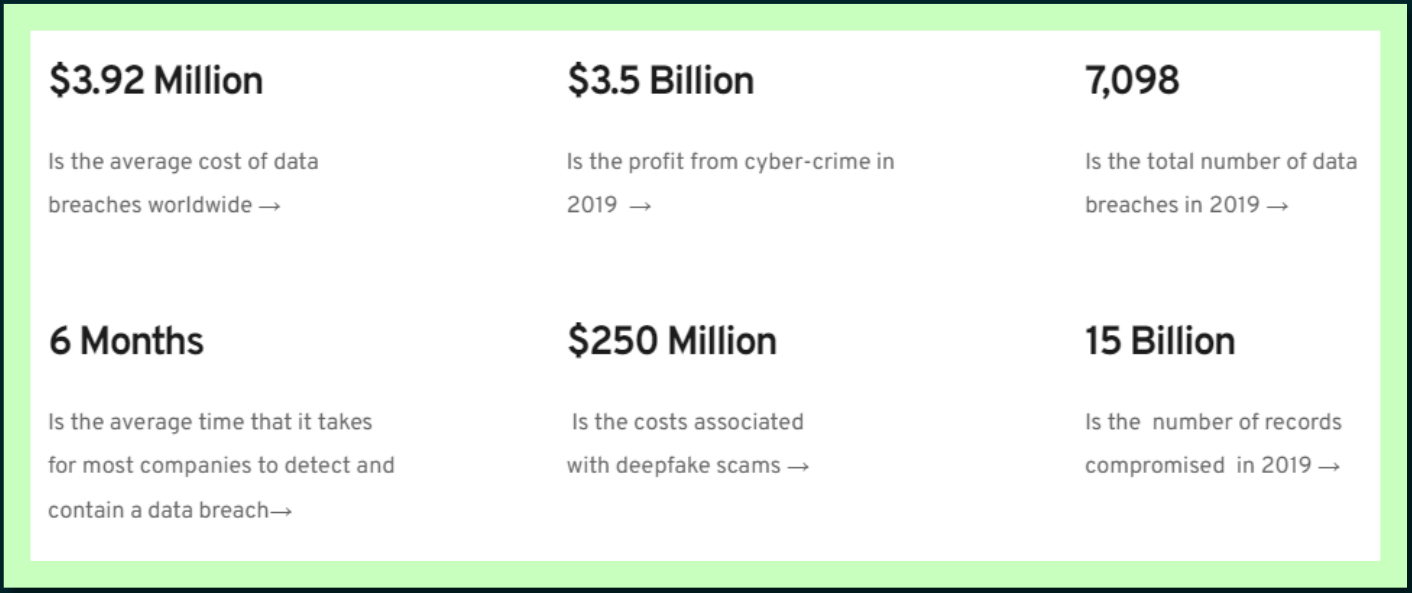


Figure 2 : Source Zeroknowledge.com [4]

British consumers and businesses lose £4 billion annually to fraudsters[5] which is enough to pay the heating bills for 1.8 million British homes [6] for an entire year. In the US where the issue is worse, identity thieves stole $52 billion from 42 million Americans[7] in 2022. A Price Waterhouse Coopers[8] (PWC) global fraud survey found that over half of organisations encountered platform fraud resulting in financial loss, with over a quarter losing $1 million and financial services being the worst affected sector. On top of financial loss, businesses face reputational risk, business disruption, lower productivity, higher costs and loss of new business opportunities. These alarming statistics highlight a need for a revolution in data protection.

Figure 4 shows the financial services sector is the biggest victim of fraudulent activities. Logically, financial services is likely to be the first sector that sees the widespread application of ZKPs due to the frequency that confidential information is shared and subsequently stolen. We are already seeing ZKPs being deployed by companies like ING, Aztec, Mina and Nuggets to protect sensitive data, but these companies are the exception. So, with all this data at risk how are ZKPs being used and who is using them?

4. Source Zeroknowledge.com
5. £4 billion annually to fraudsters
6. 1.8 million British homes
7. $52 billion from 42 million Americans
8. PriceWaterhouseCoopers

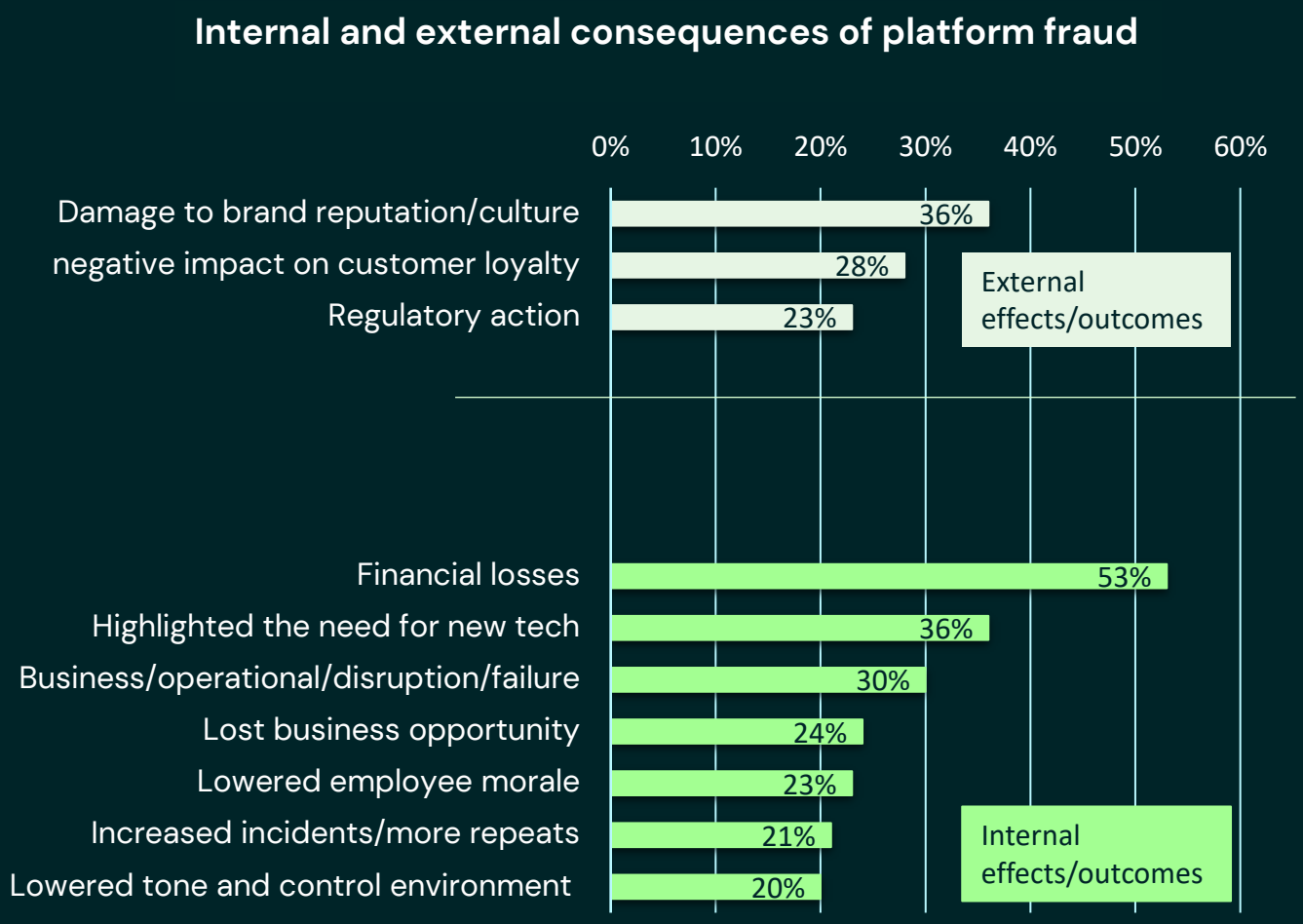


Figure 3 : Data from PWC's Global Economic crime and Fraud Survey 2022

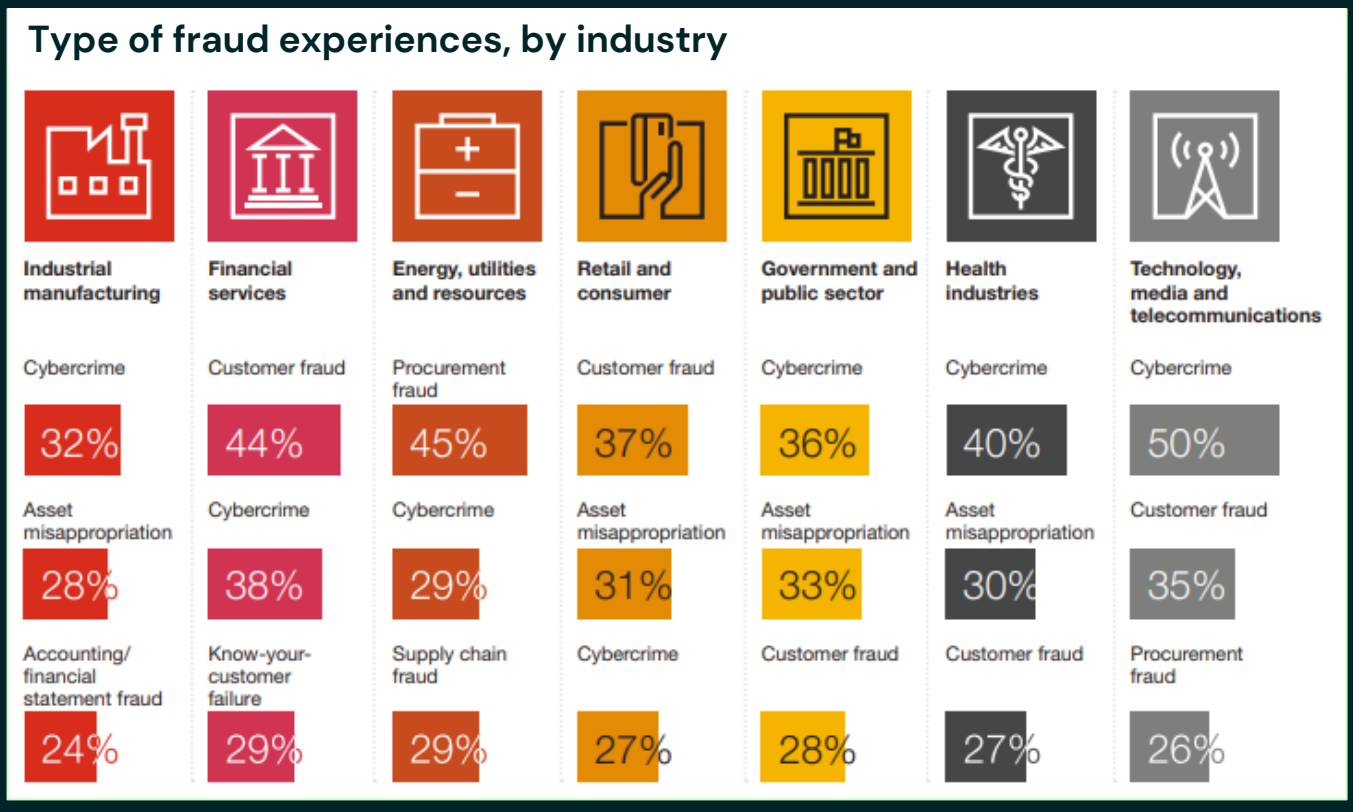


Figure 4: PwC's Global Economic & Crime Survey

The proofs in the pudding

How are ZKPs being used so far?

Bitcoin uses a 'proof of work' consensus algorithm which requires significant computational capacity. When a new participant joins the network, they need to check all the transactions right back to the first block to ensure correctness, which means checking 100's of gigabytes of data, and not everyone has access to this level of computational capacity, or at the very least this is time consuming and expensive. Increasingly, people then begin to trust intermediaries who claim to know the correct state of the blockchain, meaning that the process become less decentralised (a positive inherent feature of crypto in that it connects peer to peer).

Mina[9], the world's lightest blockchain, captures a snapshot of the blockchain using zk-SNARKS instead of the entire chain. The snapshot verifies the entire blockchain, increasing efficiency and scalability. Impressively, an infinite increase in the size of the information does not affect the size of the snapshot.

Wallet provider Nuggets[10] has vastly reduced fraud and made data safe using ZKPs. Users benefit from reusable decentralized identity and fast approvals all whilst retaining control over their own data. Zero trust is required on anything, anywhere, on any network. Banking giant ING has incorporated ZKPs allowing customers to prove their secret banking numbers, the amount in their bank accounts and their EU status all without revealing the details. Consequently, ING operates more efficiently and customers are safer.

What else could ZKPs have to offer?

So far we have seen anonymous authentication, fully decentralized transactions and scalable efficient technology. But what else could ZKPs have to offer? Anonymous verifiable online voting could be made possible through ZKPs. Governments and the public would be able to see that everyone had voted without seeing their names, sex and address, thus increasing security at elections- an issue of growing importance in recent years.

Perhaps the greatest prize of all is that zero knowledge proofs complement the concept of financial passports. A financial passport is essentially a digital identity uniquely linked to a legal person – that enables said person to port information and value between platforms and service providers. Financial intermediaries and the entity would have instant access to an open architecture suite of financial products and services, providing the ability to instantly onboard clients. Financial services providers could see the costs associated with KYC/AML compliance diminish as passports grant instant authentication. The concept is a decentralised progression of what we are currently seeing with open banking and as implementation scales up and regulation is developed we are likely to see financial passports help bridge the gap between TradFi and DeFi; merging the ecosystems into an open architecture.

9. Mina
10. Nuggets

Challenges ahead

Too good to be true?

ZKPs are not proofs in a sense because there is an extremely small possibility they can be cheated. However, the mathematical probability of this is so minuscule it is unlikely to be of genuine concern to users. Another threat to ZKPs is the development of quantum computing which may be able to break the algorithm of zk-SNARKS, though zk-STARKS will be immune due to collision-resistant hashes for encryption.

Practical flaws include hardware and initial verification costs, as the computing power needed requires expensive specialized machinery. However, the costs involved are no different to any other business model requiring initial investment to reap later returns. Whilst individuals and service providers using the service will bear these costs, the total is likely less than current transaction costs but with greater speed and security. It is true ZKPs are still in early development, but the rapid rate at which technology is developing means it is entirely possible that we could see ZKPs being widely used over the next decade. Since there is money to be saved and efficiency to be gained, we expect too see companies flock to this technology.

Like the internet, ZKPs require a network effect to unlock full potential requiring mass adoption which ultimately relies on participation from large institutions and government. We are unlikely to get there one start up at a time. However, we may be closer than we think. On the 9th February 2023, the industry, Research and Energy Committee included the standard of ZKPs in its amendments to the European digital identity framework (eID)[11]. If further proceedings are successful, we could see ZKPs as part of EU legislation in the roll out of digital IDs. Once in legislation, we would quickly see an emergence of new business models and digital solutions embedded in ZKP protocols.

What does this mean for Greengage?

Greengage spends a great deal of physical and financial resources onboarding clients for our e-money service to meet industry standards for AML/KYC compliance. Progression of digital IDs and financial passports would redefine the cost structure of providing financial services. Greengage and companies alike could shift resources toward growth and service development, which is ultimately what companies need to scale up and capture market share. Additionally, a lesser threat of platform fraud is always welcome which preserves our working capital and reputation. If the UK government is to fulfil his crypto promises, we must start seeing greater discussion and legislation involving the development of crypto based technologies. Without government support, the industry will lag behind competing nations and UK firms will be held back from the technology needed to grow exponentially.

11. European digital identity framework

What does Greengage think?

The team at Greengage is watching the evolution of ZKPs closely and we are keen to be an early adopter of the likes of "financial passports" once these have been tested, potentially even in schemes such as Open Banking. Our view on the future of banking is that the infrastructural "plumbing" around payments and market transactions will undergo considerable transformation in the coming years, and that the real value a company such as Greengage can add throughout these changes is by serving clients with trusted relationships empowered by intelligent data, so that the wider range of products accessible on the likes of DeFi or TradFi rails can be surfaced where appropriate to a client on a consistent basis. We do not think that the current "tied agent" model which most banks deploy – where they essentially provide only their own products and services to their clients, which unfortunately are not always best-in-class – will be sustainable in a Web3 future and so we are keen to build payment solutions which are future-proofed to be resilient and relevant for our clients.

Concluding remarks

Zero knowledge proofs offer a practical solution to a deep societal problem that strangers are mutually distrustful. To gain trust people are expected to hand over personal information and secrets which annually costs £4 billion worth in fraud in the UK. Practical application of ZKPs offer a solution enabling multiple parties who do not trust each other to collaborate without sharing any information beyond what is needed to prove authenticity. ZKPs do not solve the issue of mistrust but go further, circumventing it altogether and allowing cooperation without trust. Complex mathematics and technology bypass the human mechanism and solve one of the most important problems we face in the world today. ZKPs have the potential to revolutionise auditing, international trade, payment systems, healthcare and data security. Though implementation is juvenile, the possibilities to cut costs, improve efficiency, bolster security, and reduce administration are endless. We at Greengage are excited and prepared for what's to come next.

We are an ambitious scale-up of digital natives, aspiring to pioneer a new era in digital finance. Working at the intersection of traditional financial services and new digital innovations, we combine broad expertise to provide a highly client-focused experience for today's ever-changing market.

Combining the high-end care and bespoke personal service found in traditional British financial institutions with leading-edge technology, our evolving platform aims to support entrepreneurs, SMEs, family offices and digital asset firms with a wealth of innovative products and services which facilitate cost-effective transactions within and across traditional currency as well as digital assets. Our purpose is to liberate digital finance in the future.

To find out more about this research please do not hesitate to contact us at info@greengage.co.

Important Research Content Disclosures (1/2)

Greengage
This communication has been prepared by Greengage. "Greengage" refers to any entity within the Greengage Group of companies, where the "Greengage Group" comprises Greengage & Co. Limited and any of its subsidiaries or affiliates.

Conflicts of Interest
Greengage has a published a Conflicts of Interest Policy to which Greengage would refer all recipients of this document. Please contact Greengage directly if you are unable to access this policy;
https://www.greengage.co/conflicts-of interest-policy

Not Research
The information provided does not constitute 'investment research' or a 'research report' and should not be relied on as such. Investments, products or services undertaken by your decisions should not be based upon the information provided.

For Information Only
This information has been prepared by Greengage. It is provided for information purposes, is intended for your use only and does not constitute an invitation or offer to subscribe for or purchase any of the products or services that may be mentioned. The information provided is not intended to provide a sufficient basis on which to make an investment decision. Information and opinions presented in this material have been obtained or derived from sources believed by Greengage to be reliable, but Greengage makes no representation as to their accuracy or completeness. Any information, analytic tools, and/or models referenced herein (and any reports or results derived from their use) are intended for informational purposes only. Greengage has no obligation to update this information and may cease provision of this information at any time and without notice.

No Offer
Greengage is not offering to sell or seeking offers to buy any product or service or enter any transaction.

No Liability
Neither Greengage nor any of its directors, officers, employees, or representatives accepts any liability whatsoever for any direct, indirect or consequential losses (in contract, tort or otherwise) arising from the use of this communication or its contents or reliance on the information contained herein, except to the extent this would be prohibited by law or regulation.

No Advice
Greengage is not acting as a fiduciary. Greengage does not provide, and has not provided, any investment advice or personal recommendation to you in relation to any transaction and/or any related investments, products or services described herein and is not responsible for providing or arranging for the provision of any general financial or specialist advice, legal, regulatory, accounting, auditing or taxation advice or services or any other services in relation to the transaction and/or any related investments, products or services described herein. Greengage strongly advises all parties to seek professional advice. Certain high-volatility opportunities can be subject to sudden and significant falls in value that could equal or exceed the amount invested. The value of investments can go down as well as up and the implementation of any approach described does not guarantee positive performance. Any reference to potential asset allocation and potential returns do not represent and should not be interpreted as projection or advice. Value and income from investments, products or services may be adversely affected by exchange rates, interest rates, or other factors. Past performance of a particular product
is not indicative of future results.

Greengage is under no obligation to, and shall not, determine the suitability for you of any investments, products or services described herein.

Important Research Content Disclosures (2/2)

Information Provided May Not Be Accurate or Complete and May Be Sourced from Third Parties
All information is provided "as is" without warranty of any kind. Greengage is not responsible for any errors or omissions in the information contained herein. Greengage is not responsible for information stated to be obtained or derived from third party sources or statistical services. Greengage makes no representation and disclaims all express, implied, and statutory warranties including warranties of accuracy, completeness, reliability, fitness for a particular purpose or merchantability of the information contained herein.

Past & Simulated Past Performance Any past or simulated past performance including back-testing, modelling or scenario analysis contained herein is no indication as to future performance. No representation is made as to the accuracy of the assumptions made within, or completeness of, any modelling, scenario analysis or back testing.

Opinions Subject to Change
All opinions and estimates are given as of the date hereof and are subject to change as a result of market changes. Greengage is not obliged to inform the recipients of this communication of any change to such opinions or estimates.

About Greengage
Greengage is an ambitious scale-up of digital natives, aspiring to pioneer a new era in digital finance. Our evolving platform supports entrepreneurs, SMEs, family offices and digital asset firms with a wealth of innovative products and services, facilitating cost-effective transactions within and across traditional currency and digital assets. We currently offer clients diverse products and services across fiat currencies and digital asset classes.

Greengage & Co. Limited is registered in England No. 11904803.

Further Conflicts of Interest
This article may include forward-looking statements. These forward-looking statements may include comments with respect to objectives and strategies, as well as the of hopes or vision of our business or industry. However, by their nature, these forward-looking statements involve numerous assumptions, uncertainties and opportunities, both general and specific. The risk exists that these statements may not be fulfilled, and they are therefore to be treated as projections or opinions and not a statement of fact. We caution readers of this article not to place undue reliance on these forward-looking statements as several factors could cause future results or expectations to differ materially from these statements. It is Greengage's position that the information contained within this article is both objective and reliable and that it reflects the truly held opinions of individuals that contributed to it. Greengage further confirms that no inducement has been received by it in the form of business or compensation in relation to any recommendations within this article. Notwithstanding the above individuals that contributed to this article may have a financial interest in some of the products noted within this article however these are not deemed to be material, and these have been reviewed and approved by Greengage in accordance with its Conflicts of Interest Policy.

Greengage

For more info:

info@greengage.co

Painters' Hall,
9 Little Trinity Lane,
London EC4V 2AD UK

www.greengage.co