sedicii

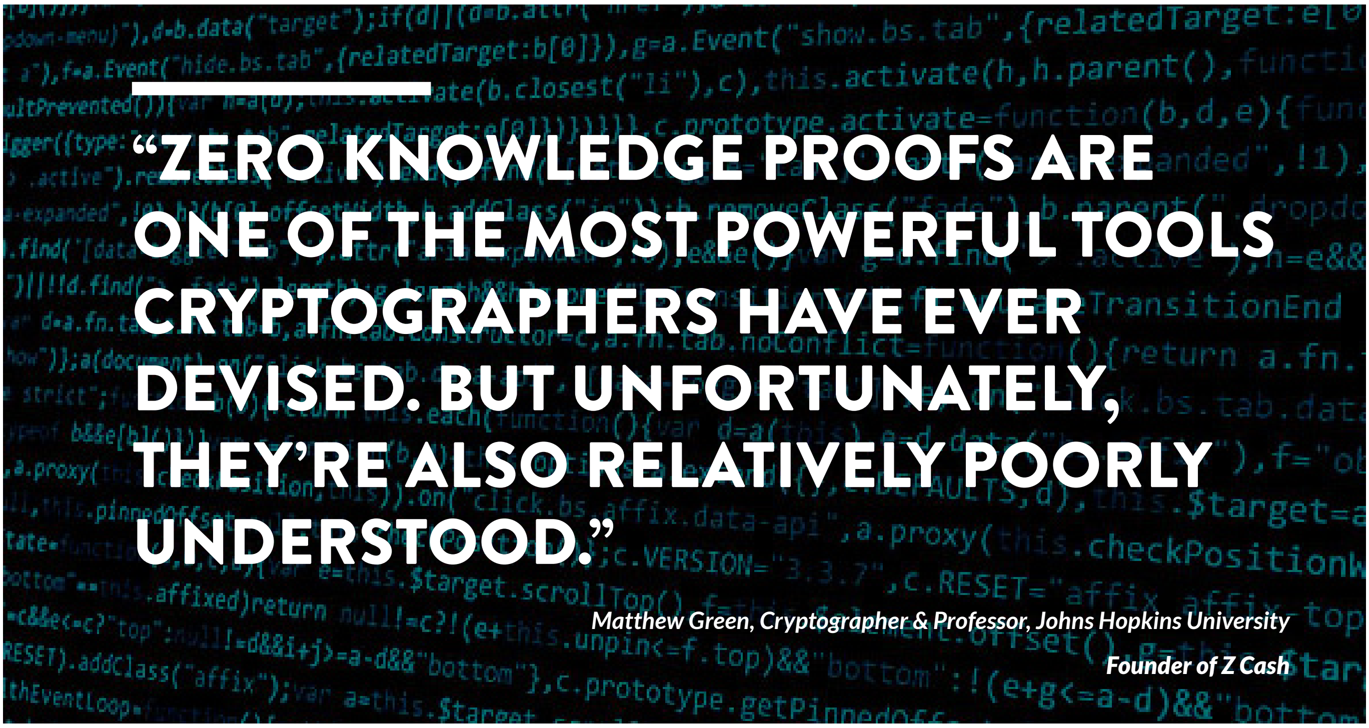
Securing Identities

ZERO KNOWLEDGE PROOF IN BLOCKCHAINS

Whitepaper

Confidentiality Statement

This document contains Sedicii confidential information. This document (including any part thereof) is not to be disclosed or transferred outside your organisation without prior written consent from a duly authorised Sedicii representative.



> “ZERO KNOWLEDGE PROOFS ARE ONE OF THE MOST POWERFUL TOOLS CRYPTOGRAPHERS HAVE EVER DEVISED. BUT UNFORTUNATELY, THEY’RE ALSO RELATIVELY POORLY UNDERSTOOD.”
>
> *Matthew Green, Cryptographer & Professor, Johns Hopkins University*
> *Founder of Z Cash*

INTRODUCTION

There are two significant challenges concerning the use of personal data in or with blockchains, which Sedicii’s ZKP (Zero Knowledge Proof) technology can address.

A key feature of a blockchain is decentralisation. This means that no central administrator or application logic is required in order to run it. Instead, the whole blockchain acts as a consensus mechanism to ensure all nodes stay in sync, enabling each one of them, independently, to verify every single transaction.

Decentralisation is important since it guarantees there is no single point of failure. That is, the blockchain is not affected in the event that an attacker corrupts the data in a few chain nodes. Moreover, in order for an attacker to control the blockchain, he would need to hack more than half of its nodes, which in most blockchains requires computational resources beyond the reach of any person or organization on the planet.

However, decentralisation comes at the cost of privacy. Every node on the chain must verify every transaction independently, and this in turn means that it sees what everyone else is doing.

Secondly, privacy legislation, particularly the EU General Data Protection Regulation (GDPR), requires the “right to be forgotten”, whereby personal data has to be deleted and purged in a system. If this right were applied to a blockchain containing personal data, the deletion of any data in the blockchain would break the chain, causing a ‘hard fork ’ or worse, to destroy the chain altogether. Hence, there is a need to have the means to use blockchains to manage personal data, without having personal data on the blockchain itself.

ZKP is one of the most important breakthroughs in cryptography in the last few decades, with extensive applications in the domain of digital identity protection. Most notably, ZKP solves these two privacy problems in blockchains.

BLOCKCHAIN 101

Blockchains can be permissionless or permissioned. Only a permissioned blockchain contains data attributes to support accountability.

The governance for permissionless blockchains is distributed and unaccountable by design, which makes it unsuitable for government and regulatory compliant industry purposes. Bitcoin is probably the largest permissionless cryptocurrency blockchain, specifically designed to be completely decentralised and anonymous, and to avoid centralised governance and banking rules. As legitimate cryptocurrency customers move away from anonymous, permissionless blockchains to regulated permissioned blockchains, so Bitcoin is increasingly becoming used for speculation and criminal activities. Despite being anonymous, such permissionless blockchains, including Bitcoin, are vulnerable to transaction association – the ability to link transactions associated with an anonymous person to a point where it may be possible to identify the person.

A hard fork makes previous or subsequent blocks/transactions invalid.

:(
Your computer ran into a problem and needs to restart.
It's collecting error info and will restart in: 0 seconds

To follow governance norms and regulatory compliance requires permissioned blockchains, where activities are accountable and controlled, and risks can be managed. This is essential for both legally-compliant cryptocurrencies and for DLTs used for payment and non-payment purposes.

Distributed Ledger Technologies (DLTs) are enabled by blockchains. A block is just a set of data records, as in a database or spreadsheet, which is cryptographically sealed and linked to the previous block. The sequence of linked blocks form a chain that cannot be altered without breaking the chain: the records are immutable.

The simpler the data record, the faster and cheaper the blockchain can potentially be to operate. Hence, a blockchain is good for managing unique identifiers that have to be used consistently across multiple systems to ensure data integrity and avoid data fragmentation that leads to fragmented processes and reduced organisational effectiveness.

DLT is a game changer because it provides new levels of:

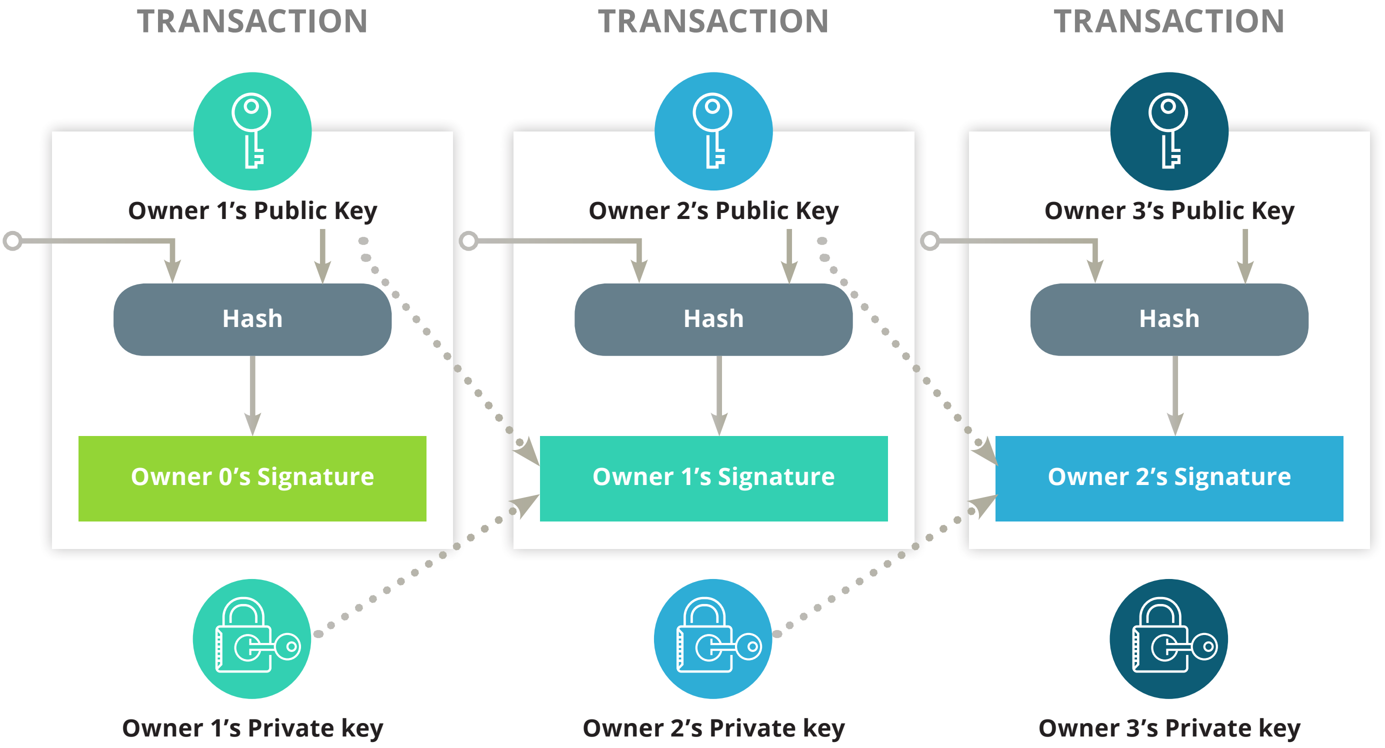
- Immutability. Data cannot be altered by anyone on the chain;
- massively distributed information and no intermediation/confusion;
- speed;
- support for authoritative, legally admissible data;
- management of data identifiers, enabling more systems to interoperate;
- cross-organisational harmonisation, data re-use and significant efficiencies, cutting out redundant and outdated manual processes. In some situations, DLT could cut out 99% of interactions.

The majority of business use cases for permissioned blockchains involve requirements for traceability and accountability across a community of organisations, providing exactly the same visibility of transactions at the same time, but with privacy preserved.

THE PRIVACY PROBLEM – PERMISSIONLESS BLOCKCHAIN

Alice and Bob are not directly identified by name on a chain. Instead, each transacts under one or more addresses. Addresses are long alphanumeric strings that bear no relation to their real-world identities. However, there are several ways in which the connection between users' identities and their addresses can be inferred (transaction association):

1. First, in order for Alice to transact with Bob on a blockchain, she needs to know at least one of Bob's addresses. So, if Alice sends Bob some money, she can see where that money goes next, and if she's receiving the money, she can see where it came from.
2. Second, once Alice knows one of Bob's addresses, she can often work out which other addresses Bob owns and uses, by monitoring the full flow of funds on the chain. In fact, there are companies such as Chainalysis and Skry who do this as a service for Bitcoin.
3. Third, if Alice happens to know something about Bob from the real world (e.g. at which time of the day he trades and what types of assets), she can search the chain's activity for corresponding patterns, and then infer Bob's address with a high level of confidence.



THE PRIVACY PROBLEM – PERMISSIONED BLOCKCHAIN

An organisation has two challenges

- To use personal data, such as customer data, as part of their business transactions on a blockchain that is seen by multiple organisations using a DLT, but to do so in a way that does not put the blockchain at risk to "right to be forgotten" or to the possibility of leaking customer's personal data. These are the most common concerns amongst Sedicii's customers today.
- To protect the privacy of users who access data on the blockchain, yet still remain accountable.

ENCRYPTION IS NOT THE SOLUTION

In a permissionless situation, encryption of this nature cannot be used. If Alice and Bob were to encrypt their transaction, then the other nodes in the chain would not be able to verify it. They would lose track of where these assets actually are.

There are two possibilities in this scenario that are both unsatisfactory:

- Tokens are visible, which can be a problem in scenarios where blockchain participants are in competition or where regulation forbids it.
- Tokens are encrypted, which means the settlement remains external to the chain since nodes are not able to verify transactions.

In the permissioned situation, encryption cannot be used because it is not legally sufficient to satisfy regulatory requirements under GDPR, it hampers the ability of organisations to prevent data leakage and it raises significant practical challenges, such as the distributed management of the cryptographic keys.

ZERO KNOWLEDGE PROOF

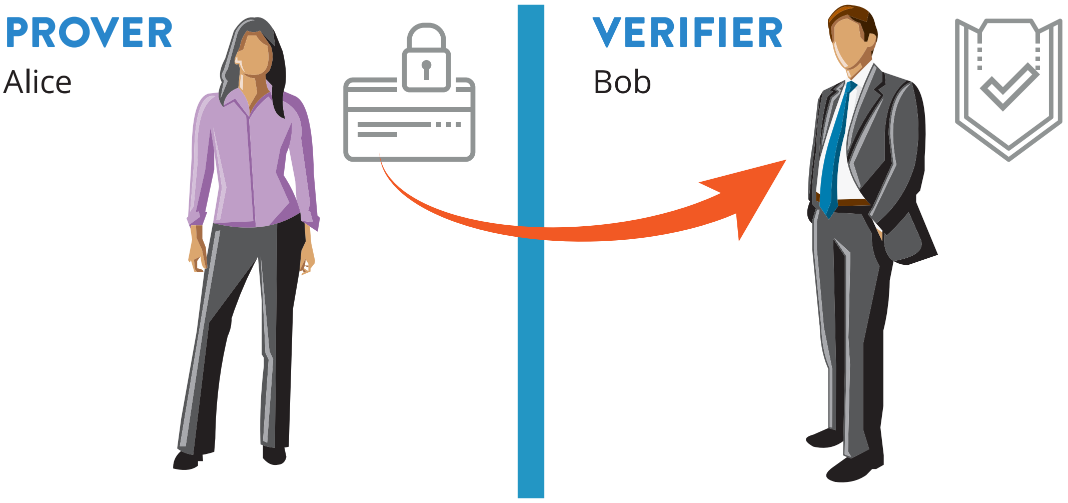
The Zero Knowledge Proof (ZKP) authentication protocol is used in cryptography systems to allow a party to prove that he/she knows something, for example a credential, without having to transmit this credential. There are two parties involved in ZKP; the prover Alice and the verifier Bob. ZKP allows a prover Alice to show that she has the credential (for example, a credit card number or a password), without having to give Bob the exact details of the credential. With Zero Knowledge Proof there is no transmission or storage of password / credential hashes on the authentication server and the fundamental benefits of ZKP in the authentication process are as follows:-

- **Zero-knowledge:** if the statement is true, the verifier will not know anything other than that the statement is true. Information about the details of the statement will not be revealed.
- **Completeness**: if the statement is true, the honest verifier (that is, one following the protocol properly) will be able to prove that the statement is true every time.
- **Soundness**: if the statement is false, it is almost impossible, to an astronomically small chance, that someone could fake the result to the verifier that the statement is true.

Zero Knowledge Proof (ZKP) allows Alice prove to Bob that she knows or controls a piece of information without revealing it to Bob.

For example, let's say Alice wants to prove to Bob that she knows the passcode associated with an automated teller machine (ATM) card. Therefore, she withdraws some cash from the ATM without divulging the passcode entered. Alice has performed a zero knowledge proof since the passcode was never revealed to Bob because she can prove it to him by demonstrating possession of the cash.

In a real-world ZKP, the ATM is replaced by a set of mathematical challenges that Alice must satisfactorily respond to. If Alice knows the passcode, she will be able to correctly respond to all challenges. If she does not know the passcode, the probability that Alice correctly responds to a challenge by pure chance is 50%, which is very high. However, the probability that Alice correctly responds to all N challenges by mere chance is $1/2^N$, which means that (from Bob's perspective) the probability that she actually knowns the passcode or secret is $1-(1/2^N)$. For a sufficiently large number of challenges Bob can be sure beyond reasonable doubt that Alice knows the passcode, although it was not revealed to him.



ZERO KNOWLEDGE PROOF SOLVES THE BLOCKCHAIN PRIVACY CHALLENGE

Let's revisit the privacy problem in blockchains, now armed with the power of ZKP. We want to operate a blockchain to manage Ownership and Transfer of Assets that protects the identities of Alice and Bob.

ZKP enables Alice prove to the nodes in the chain that she owns any piece of information without revealing it. If we use her identity as that piece of information, **she will be therefore able to prove to the nodes in the chain her identity without revealing it.** The same applies to Bob, and to the amount of assets traded.

Indeed, with ZKP, blockchain nodes can prove the statement "this asset transfer is valid" without knowing anything important or sensitive about the transfer itself. That is, without revealing:

1. the identity of the sender of the assets
2. the identity of the recipient of the assets
3. the traded asset value

With ZKP it's possible to combine public and protected transactions by using protected (i.e., using ZKP) and public (i.e., not using ZKP) addresses. If a transaction is initiated from a protected address to a public address, the received balance is revealed. If a transaction is initiated from a public address to a protected address, the received value is protected.

In a permissioned chain situation, personal data would be held off the chain situation, but linked to an identifier on the chain, which can be managed. The problem comes when the identifier is itself considered to be personal data. Sedicii's ZKP allows the personal data in systems off the chain to be linked to identifiers on the chain without any linking of the data itself. So there is no personal data on the chain at all. This meets the requirements of governments, such as Japan and Germany, which have specified that a cryptographic hash of personal data is still personal data, so a hash cannot be used to link a blockchain to personal data off the chain. Sedicii is planning a demonstrator to meet this very significant requirement.

SEDICII'S ZKP

There are many different mathematical approaches to ZKP. Zk-SNARK is a famous ZKP approach that is used in Zcash and Haws, arguably two of the most important ZKP blockchains.

The main challenge preventing ZKP blockchains from reaching mass adoption is performance. Even though it is relatively quick to verify an anonymous transaction using zk-SNARK, creating each of these transactions carries a serious computational burden. According to the Zcash Speed Center (**https://speed.z.cash)**, it currently takes 48 seconds on a high-end server, and over 3 GB of memory. This makes it impractical to transact anonymously from mobile devices and older desktops and laptops.

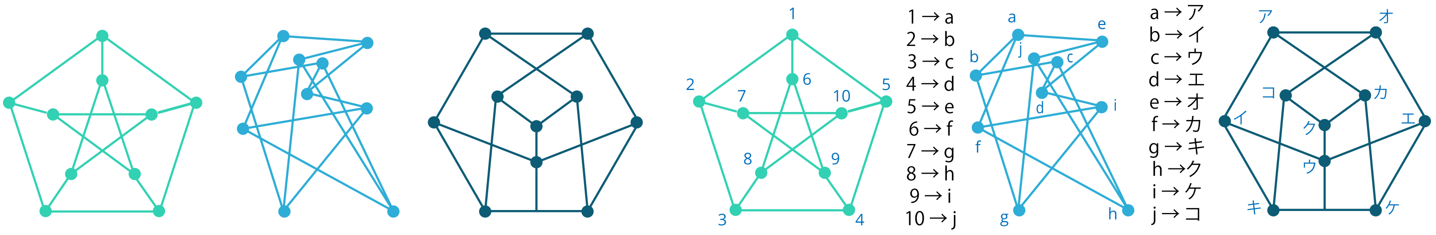
Sedicii's unique approach to ZKP using isomorphic graphs has proven to exhibit millisecond performance, even when running on mobile or Javascript-powered web applications.

This positions Sedicii's ZKP as a very compelling approach to large ZKP blockchain implementations.

Sedicii is a ZKP framework which allows companies to implement a proven cryptographic protocol to allow for secure identity verification without the need for transmitting the attribute or hash over the network. ZKP eliminates the need to store credential or attribute hashes in a database, thus, if a hacker is able to obtain access to the database, he/she will still not be able to crack the credential or attribute. The process is based on the graph isomorphism problem which is a problem that requires exponential time to solve (nth power) in the case of n inputs being provided. An example of graph isomorphism is shown below. Each of the three graphs is isomorphic to the others beside it but all appear to be different.

Utilizing a NP(Non-deterministic Polynomial time) Problem, Graph Isomorphism Problem

NP Problem: a problem which requires exponential (n-th power) time to solve in the case that n-inputs are given



In Sedicii's case the graph is 4,096 bits long (64x64 matrix). A permutation between graphs is used as the key for authentication or identity verification.

Sedicii's ZKP can be used in blockchain transactions to decouple the transaction from the identity of the parties involved in the transaction. As we can see in the diagram on the next page, rather than using the private key to directly sign the transaction, an abstraction derived from the private key is used to sign it. The abstraction must be capable of proving that the signer, and only the signer, has control of the private key that was used to initiate the transaction. In this way the parties to the transaction are completely anonymised.

SEDICII'S ZKP CTD...

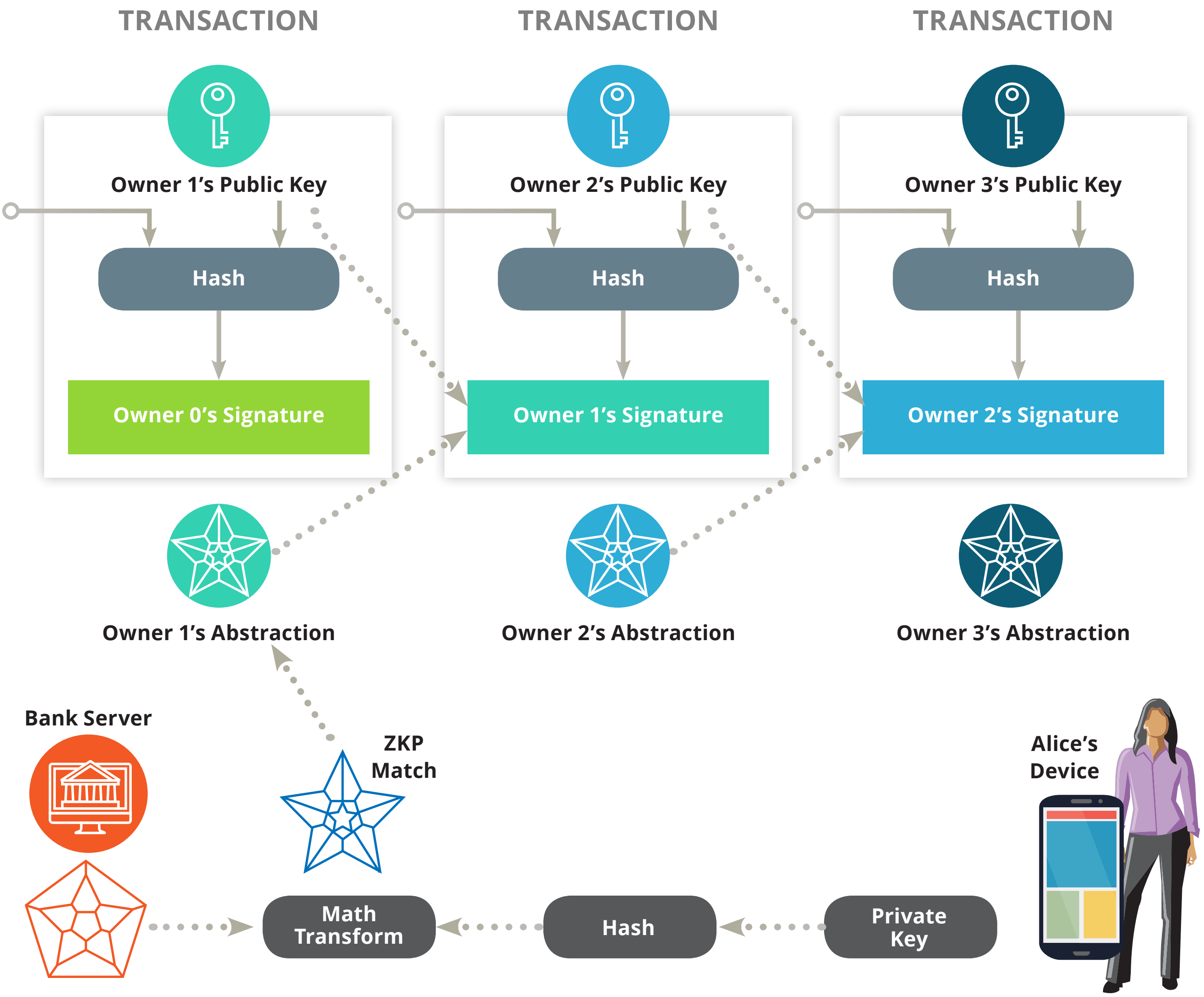


Fig. 2 Anonymised Blockchain using ZKP to prove the signing key can be recreated

In this example, Alice is the only person who knows her Private Key because it is never shared with anyone or exposed outside her device. Equally, the information stored by the bank is stored under a different identifier than that which is recorded in the blockchain with Alice being the only person capable of recreating the link back to it

CONFIDENCE BUILDING

There are a few questions that arise concerning ZKP.

First, and most importantly, is Sedicii's ZKP computationally sound and robust? Demonstrations of Sedicii have impressed experts and governments. Consequently, Sedicii is expected to complete the UK Government's CTAS – Tailored Assurance Scheme, operated by the UK National Cyber Security Centre – in February 2018, which would allow its use in very high assurance situations, exceeding almost all requirements for non-military uses.

Isn't ZKP new? No, it isn't. ZKP has been around for twenty years or more, but technological advances have enabled major improvements. The draft International Standard ISO 27551 – Unlinkable Authentication, mentions four models for ZKP of which Sedicii's is the only one that covers all the major ZKP functional characteristics. Sedicii's ZKP is state of the art.

Why don't more people, particularly CEOs, know about it? There is a general lack of awareness about many important digital technologies at board level across industries and governments. As a WEF Technology Pioneer and winner of many awards, as a participant in the development of international standards for ZKP and blockchains, and through speaking at many international events, Sedicii is doing as much as it can to raise its profile and the general level of awareness around ZKP, blockchains and the digital society. Sedicii is also working on new proof of concepts and pilots, backed by tailored business case documentation, to help companies and governments develop their awareness and understanding, and to plan pilots to learn more and to de-risk plans for operational use.

WAY AHEAD

Because Sedicii's ZKP technology is so fundamentally different in the way that it does attribute matching without sharing any data, it is able to support technological and business functions that no other solution can today. Harnessing ZKP with blockchains has highlighted a number of areas where Sedicii's ZKP can be used to meet different requirements.

Sedicii is developing its operational platform now, for an initial operational capability (IOC) in January 2018 and for UK government CTAS certification in February 2018, followed by quarterly phased releases of major improvements through 2018 in response to requirements.

Managing competing requirements is becoming a challenge. Sedicii has over 25 customer dialogues at present, and has grouped common requirements into customer clusters, where to satisfy one customer would be to satisfy them all. All of these clusters have requirements for Sedicii to support privacy-friendly customer facing interactions, but they also have other internal and cross-organisational traceability and accountability requirements that may require the use of blockchains, where Sedicii would work to address these requirements too. As more customers and more clusters emerge, so Sedicii's landscape of opportunity will expand. Once IOC becomes live, indications are that there will be a step increase in international demand.

The stretch potential of Sedicii is still being explored because it is so flexible. The Sedicii team will provide an update to this initial document in January 2018, complete with more supporting information.