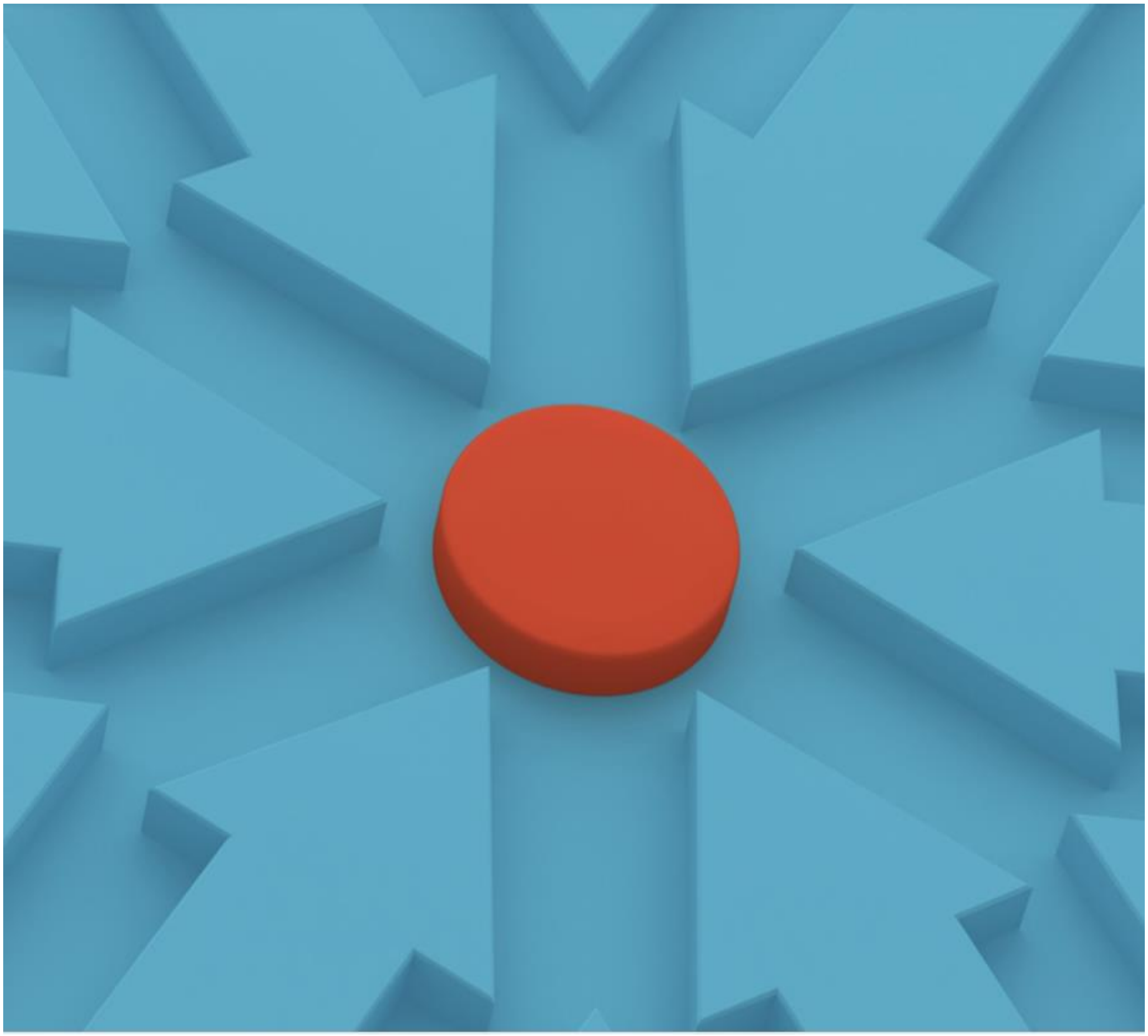


# DECENTRALIZED IDENTITY

## IDENTITY FOR A NEW DIGITAL AGE

GORDON WELLS

# TABLE OF CONTENTS

Summary ..... 3

Issues with Current System ..... 3

- Fraud and Identity Theft ..... 4
- Renewal ..... 5
- Accessibility and Control ..... 5
- Security Breaches ..... 6

Decentralized Identity – Its benefits ..... 7

- Organizations ..... 7
- Individuals ..... 8

Decentralized Identity - Features ..... 9

- Blockchain ..... 9
- Decentralized Identity Wallet ..... 11
- Decentralized Identifier ..... 12
- Verifiable Credential ..... 12

Global Opportunities ..... 14

Hurdles ..... 14

In Summation ..... 15

References ..... 16

## SUMMARY

Decentralized Identity offers a new approach to how we deal with personal identification and itself brings a host of benefits for both individuals and governments. The current system of personal identification globally both for personal identification in country and for cross-border travel has lagged significantly worldwide regarding advancements in digital identification technology. While digital identification technology has been adopted in limited capacities globally the recent advances in Web 3.0 decentralized technology offers a host of new ways to structure our indentation system and how we conduct security. Current means of the operation and control of identification is still overwhelming administered as physical copies of ID (passport, Drivers License, etc.) with limited options for non-physical identifications. While options for digital versions of ID are being developed and tried, the technology revolving around Blockchain technology can offer a wealth of benefits if applied correctly on a global scale. A decentralized Identity system that leverages the benefits of web 3.0 can provide a breath of advantages. Namely if an adequate infrastructure is designed at both a state and worldwide level a decentralized Identity system can revolutionize identity management for citizens. Allowing far more efficient disbursement of identity and renewal. In addition, the advanced security features of the blockchain system would greatly reduce identity theft and fraud in the future. This system if properly coordinated worldwide can also have a great effect in creating a more effective international travel and cost-effectiveness. These ideals however will need to be tempered with current modern hurdles such as legal and technological hurdles that would require a large level of international cooperation. In addition, many current projects are being researched into how such a system will be implemented, with it currently unknown which project will ultimately be correct path forward. However, if this can be achieved it would lead to a far more secure and effective system for potential billions worldwide.

## ISSUES WITH CURRENT SYSTEM

For generations the main system for personal identification revolved around the creation and disbursement of various physical identification. These ranged in the form of Birth Certificates, Passports, Drivers Licenses, etc. These various pieces of identification operate by compiling vast quantities of personal information of various citizens in centralized databases and information storage departments from which physical identification and various certificates are created for disbursement. How they are dispersed depends on what purpose the identification is meant to serve and what organization is issuing and verifying the personal identity credentials. Organizations such as universities disperse identification such as student cards and certificates, these allows users to have access to campus facilities and have access to private accounts controlled by their respective schools. Libraries in a similar fashion take user information and create library cards that are unique to each user of their respective libraries. Governments are probably the most thought of entities when one imagines identification credentials. Almost everyone in the country currently has or has access to personal identification in the form of Passports or Drivers licenses. How this function is we provide personal information to the governing body, and we receive unique identification documents that is for our eyes only and sent to us as physical copies. Renewing or replacing these identifications must be made through government offices and can be a lengthy and extensive process. While for the most part this system has served society adequately for most of the modern era, there is no doubting that there are significant flaws in the system that haven't been addressed with the current system.

## Fraud and Identity Theft

Fraud is a particularly damaging occurrence that is becoming more and more common in the modern age as thieves and hackers are becoming more efficient in stealing out user information. These occurrences can happen in many different forms with the current identification systems that are currently in place in Canada and beyond. In practical terms having most of our personal identification as physical objects means that they must be kept safe and hidden at all times and this can lead to problems with security. These items can become lost or stolen if an individual is not careful and a knowledgeable criminal can do a significant amount of damage to an individual if this is not dealt with quickly. Adversely this creates issues for individuals as managing many different types of physical identification can become an increasingly frustrating chore as different ID for government and organizations must be considered.

Identity theft is also a significant issue online as well. Phishing scams, hacking and fraudulent personal information requests can lead individuals to have their online personal ID accounts and information stolen. This theft can be particularly serious as individuals may not be made immediately aware of the theft. In addition, depending on what was hacked a significant more amount of data may have been stolen at once. Since the Covid-19 pandemic digital identity theft has risen as much as 218% in theft attempts. In the Americas it was estimated that $56 billion in financial damage was caused by identity theft in 2020 alone. While in Canada it was estimated that identify theft rates had increased by a factor of 6 in the last decade. Some of the most vulnerable information was regarding health and financial information, which was further exasperated by the covid-19 pandemic. In addition, as mentioned most of these cases was from digital identity theft that ranged from brute-force hacking to more simple attempts have managing to steal user passwords and usernames.

## Renewal

The renewal of expired, missing or damaged identification is an affair likely many of us are forced to deal with. Due to the need of identification existing in a physical state this has led to issues regarding getting new ones. Namely in order to verify one's identity in order to get new or updated identity items we often must bring other forms of ID as verification. Which can be a cumbersome requirement for renewal or replacement. As for example these items can also be lost or damaged, especially in the case with rarely used pieces of identification, such as birth certificates. These items can be stored away for years at a time and can feasibly be misplaced during this time. Subsequently than efforts would have to be made to replace these now non-available pieces of ID, which even in a developed first-world country such as Canada can be difficult. With the process often being very lengthy and time-consuming for the recipients often involving bringing on individuals close to the holder to act as verifiers of identity along with struggling to uncover any ID samples they can give to bring to government departments. Even after all this is done the process by which their information is tested is lengthy and often frustrating. With sometimes weeks or even months going by as an individual's personal information and forms are having to be sent to have them reviewed and approved. With any errors resulting with the process starting from scratch all over again. Even if the process is a success new physical copies of ID will still need to be created and sent to the recipient which again can take time. While ways to expediate the process exist, the costs involved are not always an option for some individuals and a back-up system can still result in delays. For example, during the final days of the lifting of lock-down restrictions during Canada's Covid-19 restrictions led to a rush of individuals looking to renew expired licenses all at once. Near unprecedented line-ups and backlogs occurred as people literally waited in line for hours to even days than had to suffer through an extremely congested system. Again, showing the inefficiencies of a system that requires multiple institutions working seamlessly to expediated physical identification copies.

## Accessibility and Control

Personal identification as we have now can best be described as highly Federated and Centralized. We deal with vast amounts of identity identifiers in all different forms throughout our lives. Indeed, some may say we are starting to reach a limit on what is manageable. For example, ID and identifiers can take the form of anything that pertains to a unique individual and is used for the purposes of accessing privileges or information. For example, your email, password and recovery systems are all personal identifiers and are unique to you as a person and backed up by an existing third party. Such as your email and password privileges whenever you enter a personal Google account. Or your personal drivers license that is distributed for your use to validate your competency to drive in your personal Canadian Province.

What is lacking from all this is proper control of personal information with the users. When applying your information to apply for identification you often must release a significant amount of personal information in order to verify your own personal identity while often dealing with several different groups of verifiers. These entities often share significant amount of a user's information within each other without any real consent from the owners. Now obviously certain practicalities with this method must be observed. As of course with sheer millions of people being processed, efficiency and expediency requires that organizations not take much input from users. However, the fact that individuals have little to no say or knowledge of who has access to their personal information or where it is stored or used at most times means that simple trust in the institutions that we choose to handle our information is often our sole pillar-of-support in these endeavors.

In addition, if we wanted to take a more global view of the problem it is reported that more than a billion worldwide lack proper proof of identification. These can range from a number of factors however it is most apparent from the poorest regions of the world. With roughly half of those deprived of proper identification coming from 20% of the poorest regions. Reasons range from cumbersome and underfunded identification paperwork processes, expense, lack of access and the simple lack of knowledge and education regarding personal identity all contribute to a staggering number of individuals worldwide who may lack proper identification on any global census or government. This is very severe for many people as proper identification is essential for many aspects of modern life that we take for granted, such as applying for many jobs, banking or accessing government services.

## Security Breaches

With the rise in the digitalization of information more information exists in digital format than ever in past decades. Consequently, that has meant attempts to steal this data has risen significantly as well. Every year of the past decade more and more data breaches have occurred resulting in billions of files being stolen or potentially compromised. The nature of these can vary from simple usernames or passwords to full on important personal identification such as SIN numbers and health information. This is a constant threat for many identification systems as with centralized databases governments and organizations in Canada must be on constant alert for hackers or viruses that may attempt to steal user information. This is not to say that centralized data repositories are not useful and have their advantages. But having so much critical user data in singular locations is still leaving them vulnerable.

# DECENTRALIZED IDENTITY – ITS BENEFITS

With the various issues currently facing the world regarding personal identity management from a lack of control over your personal information, to inefficiencies with distribution and creation of physical identification. While many alternative approaches have been proposed the recent advances in Web 3.0 and blockchain have opened new avenues that simply did not exist in previous years. Decentralized Identification (often used interchangeably with the term Self-Sovereign-Identity). Has been proposed as a more effective and modern method for dealing with the shortcomings of user identity and security.

Decentralized identity is a relatively new type of identity management system that would allow individuals to control their own digital identities without having to rely or depend on outside service providers to the same degree as with centralized and federated systems. Instead of relying on many and often cumbersome physically pieces of identity or have to remember endless passwords or verifiers individuals would have their identification fully digitalized and secured with their personal phones. Their identification stored in a digital wallet. This system would greatly improve the efficiently and safety of both personal data and verifiable proof of existence. Namely it can provide a berth of benefits not just to individuals but also to organizations and even developers.

## Organizations

The advantages Decentralized Identity can have with organizations are enough to warrant coverage. One of the advantages of DI (Decentralized Identity) is that individuals can instantly verify their identity or credentials themselves without having to rely on outside third party to both verify and deliver judgement on a person’s identity or status. Using DI’s credential verification systems an identity or credential could be ascertained in quick time, rather than having to rely on foreign organizations and systems in order to accomplish this. At its worst these processes can take days or weeks as credentials would have to be sent out to governmental or organizational verifiers in addition to likely heavy paperwork and have them verified and sent back. A highly inefficient process when applied against every individual in the organization.

Cyber attack deterrents can also be a strong benefit to organizations or even foreign government offices. As DI utilizes a decentralized system it provides an added layer of security regarding data and data security. As centralized systems (while again they will always have their uses) will always serve as a central point of failure for any one system. With singular repositories serving as storage for thousands if not millions or billions of files it will always be a point of attack and failure for any given system. In addition to this it can take a long time to ascertain when systems have been compromised (as much as 200 or more days to identify if a system is breached depending on the system) and even more time to restructure the system to prevent further ones. Thusly it is imperative to cut down on them as much as possible in the first place. In this regard the decentralized nature of the DI's system means no single point of breach will endanger thousands of other ID holders, while also providing less opportunities for attacks on the system.

In this regard as well DI's public-key cryptography system for data integrity is also a big bonus for data safety. Each holder of a DID credential has their data protected by advanced cryptographic systems that utilize both a public and private key to decrypt individual data. With these protections individual data is very heavily secured that further makes data breaches highly unlikely.

In addition, much like its value to individuals DI's use of blockchain technology and Cryptology provides a substantial protection from attempts to create identity fraud. As since files and information on the blockchain networks are unalterable, fake IDs would not be capable of being created without the system rejecting it. In addition, without access to an individuals personal Digital Identifier any attempt to create a fake id would immediately be flagged as false and rejected from the network.

## Individuals

Decentralized Identity offers many different benefits to individuals as well, one of the bigger ones being a greater control of their data. Through Decentralized Identity individuals could have more control with how they share and use their data, as with DI when needing to submit identification or authorization they would not be needed to submit their entire identification information as they are now. Instead of needing a drivers license for example, they can use their personal phone to submit verifiable credentials that prove that they have a valid license and that it belongs to them. All this could be carried out with their personal phone and with perhaps the need of a scanner. Governments and businesses could verify this information without needing full info, creating a much faster and more private exchange. This also would prevent the uncontrolled spreading of their private information between businesses and Governments as what we have with the current systems.

In addition, one potential benefit of this is that depending on the make of the Decentralized Identity system once the identities are stored on an individual's phone they cannot be taken as it is now stored exclusively with the individual (on their personal wallet for example). This can be of great use for individuals especially worldwide where unstable political situations are a possibility being able to have greater control of your personal information can be of great importance to individuals.

Above all this process would be far more efficient process than with physical identification or centralized digital id. All that is required is Digital Identifiers for specific individuals and needs and thanks to the nature of Blockchain they can be verified and approved with cutting out of the often-unnecessary red tape attached.

## DECENTRALIZED IDENTITY - FEATURES

After so much talk on Decentralized Identification you may be curious on how exactly it works and how it would function. Currently there are many organizations, think-tanks and individuals working on this very concept. In fact, in can be said there is no one way to build or design a Decentralized Identity System, as the architecture and structure can take on many different formats and innovations. However, there are some essential features that would likely be included in a system.

### Blockchain

A blockchain is in basic terms a decentralized database or ledger that is shared among multiple computers that make up the blockchain network. What makes blockchain so appealing to many is how it records and inputs data into the decentralized ledger. In essence all transactions that take place over a blockchain are included in a block that after being verified by the network are posted to the blockchain. Each block contains a timestamp of when it is added, a cryptographic hash that links to the previous block, and the transaction data recorded. Any attempt to change any of the blocks already posted would cause a change to the hash value which would immediately trigger a response from all other nodes on the network. Figure 1 below gives a simplified view of the network. In essence it means any posting to the chain cannot be changed or altered after they have been created. In addition, the ledger is copied and shared among all nodes in the network meaning there is no one point of attack as one compromised machine would not affect the overfall network. Thus, this eliminates one of the biggest threats to centralized repositories, namely a significant data breach effecting the entire repository.

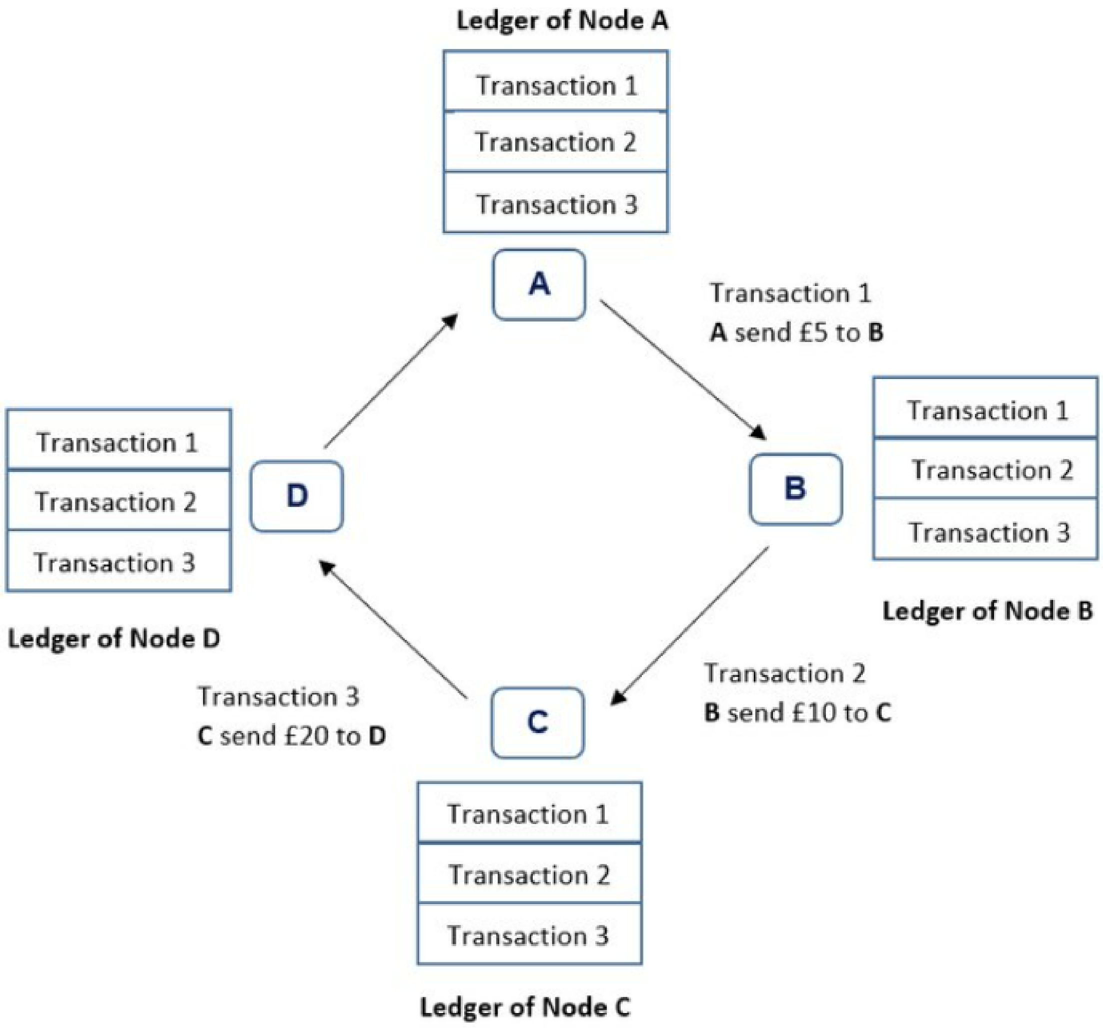
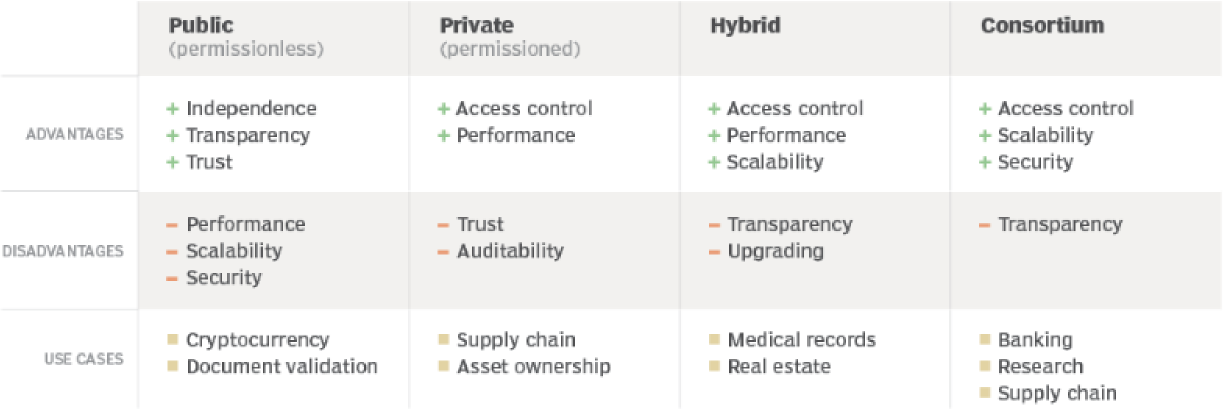


**Figure 1**

Blockchains themselves can vary in their structure and governance. For example, some blockchains are completely open and free to use for anyone wishing to utilize or be a part of the system. Bitcoin is probably the most well know of these **Public-Blockchains.** While others can be **Permission-Blockchains,** in that only actors that are permitted by the blockchains verifiers or overseers may have access to the ledger and participate in the chain. Of course, there also exists many different types of chains that exist between these two extremes, all created for different purposes of the groups using them. Figure 2 is an example of this.

In terms of Decentralized Identity Hyperledger Indy is a particularly notable Blockchain as it was developed specifically to handle sponsor it. Unlike some other blockchain platforms, such as Ethereum, Hyperledger Indy does not have a built-in **smart contract** capability. Instead, Hyperledger Indy provides a set of **APIs** and **SDKs** that allow developers to build decentralized identity management applications. These applications can interact with the Hyperledger Indy ledger to create and manage digital identities and associated data. In addition, it is possible to use it in conjunction with other Hyperledger frameworks, such as Hyperledger Fabric, which do support smart contracts to create more full rounded Decentralized Identity applications.



| | Public<br>(permissionless) | Private<br>(permissioned) | Hybrid | Consortium |
|---|---|---|---|---|
| ADVANTAGES | + Independence<br>+ Transparency<br>+ Trust | + Access control<br>+ Performance | + Access control<br>+ Performance<br>+ Scalability | + Access control<br>+ Scalability<br>+ Security |
| DISADVANTAGES | − Performance<br>− Scalability<br>− Security | − Trust<br>− Auditability | − Transparency<br>− Upgrading | − Transparency |
| USE CASES | ■ Cryptocurrency<br>■ Document validation | ■ Supply chain<br>■ Asset ownership | ■ Medical records<br>■ Real estate | ■ Banking<br>■ Research<br>■ Supply chain |

**Figure 2**

## Decentralized Identity Wallet

A decentralized identity wallet (or a self-sovereign identity wallet) is a digital wallet that enables individuals to control their personal identity data and to share it securely with others without the need for intermediaries. Unlike traditional identity systems where personal data is stored on centralized servers controlled by third-party organizations, a decentralized identity wallet allows individuals to store their personal identity data, such as biometric data, government-issued IDs, and other credentials, on a decentralized network such as a blockchain. This gives users greater control over their personal data and reduces the risk of data breaches and identity theft.

Decentralized identity wallets use advanced **cryptographic** techniques such as public key cryptography, digital signatures, and **zero-knowledge proofs** to ensure that personal data remains private and secure while allowing users to authenticate themselves and access services in a decentralized and trust less manner. These wallets are becoming increasingly popular to provide secure and user-controlled digital identity solutions that can be used across various applications and services.

## Decentralized Identifier

A Decentralized Identifier (DID) is a unique identifier that is associated with a specific entity or object on a decentralized network such as a blockchain. Unlike more traditional identifiers such as usernames or email addresses a DID is a self-sovereign identifier that is controlled by the entity or object to which it is associated.

A DID is typically represented as a string of characters and is designed to be interoperable across different networks and applications. It allows individuals and organizations to manage their own digital identity without relying on centralized identity providers or intermediaries.

DIDs are created using a combination of public key cryptography and blockchain technology, and they can be used to verify and authenticate individuals, objects, or devices in a secure and decentralized manner. They can also be used to store and manage personal data, credentials, and other sensitive information, giving users greater control over their personal data and reducing the risk of data breaches and identity theft.

## Verifiable Credential

A Verifiable Credential (VC) is a digital representation of a set of claims that has been issued by a trusted issuer and can be cryptographically verified by a third party to ensure its authenticity and integrity. Essentially it is the digitalized version of identification that replaces physical identification or perhaps certificates. These are generally stored in a user’s private digital wallet. A VC typically consists of a set of data fields, such as a person's name, ID, address, or educational qualifications, that are digitally signed by the issuer using public key cryptography. The VC can then be shared with a third party, such as a private organization or a government agency, who can verify the authenticity of the credential without needing to contact the issuer directly. The VC system is over

Virtually any type of claim can be represented as a VC, from personal identity, educational qualifications, employment history, and more. VCs are designed to be interoperable across different networks and applications, making it easier for individuals and organizations to manage their own digital identity and share their credentials securely and efficiently.

VCs are a key component of the emerging decentralized identity ecosystem, which aims to provide individuals with greater control over their personal data and reduce the reliance on centralized identity providers. They are being developed and standardized by organizations such as the World Wide Web Consortium (W3C) to develop and create good practices with its development. In addition, the VC system generally consists of three components further illustrated in Figure 7:

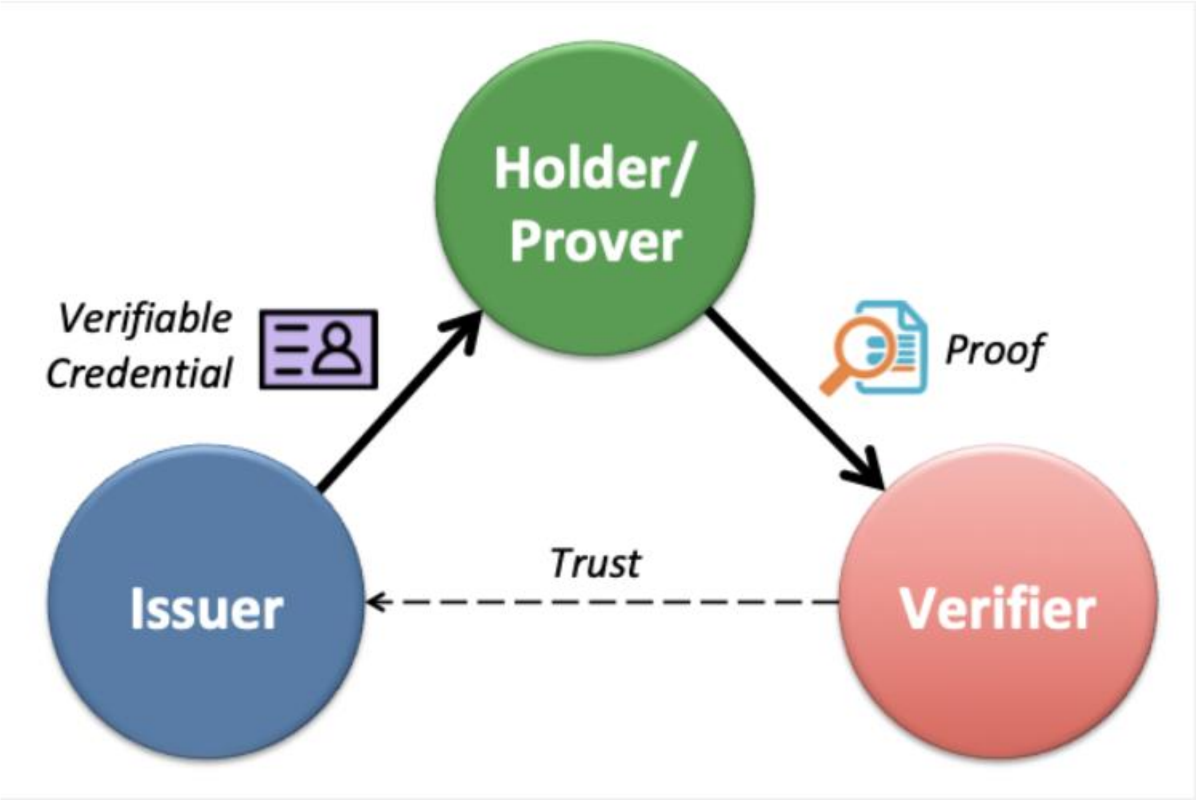


**Figure 3**

**Issuer**: The issuer's public DID and associated public key is on the blockchain. When an issuer, like a licensing organization, provides a credential to a holder like a driver's license, the issuer signs the credential with their private key.

**Holders**: Owner of the Verifiable Credential (e.g. driver's license) has their public DID on the blockchain.

**Verifier**: A verifier like an on-demand driving company can check the blockchain to ensure that the licensing department that they trust did in fact issue the license and who it was issued to.

These three parties act in concert that while all separate entities allow for the verification of information in a seamless and predictable manner that greatly reduces overhead and expenses for the users.

## GLOBAL OPPORTUNITIES

While ultimately the adoption of Decentralized Identity and the embracement of the latest technology of web 3.0 obviously functions as an improvement too society, there are ways to help quantify these developments. For example, from research conducted by the World Bank that lack of proper identification or access to essential services such as banking or health care is resulting in billions in lost potential GDP globally. In fact, they estimate that increased access to these essential services through DI could generate up to $10 trillion in future business value by the end of the decade assuming it was adopted globally. Along with a report by the United Nations that estimates a successful implementation of DI could lead to millions of job growth opportunities in developing nations. Studies made by entities such as McKinsey & Company estimate that literal billions could be saved each year both in north America and globally from the reduction in fraud and streamlining compliance processes. The Decentralized Identity Foundation also estimates has made estimates that the inherent costs of identity verification could be cut by as much as 90% with the adoption of DI. This especially rings true for all aspects of Canadian and global life as identity verification is a function from government to banking and one, we all have to deal with.

## HURDLES

While DI ultimately brings many potential benefits and opportunities for both the country and the world, a full adoption is still held back by certain hurdles.

One large one is standardization, there is currently no true standardization in various decentralized identity systems. This bodes true not only for the country but also globally with many open-source and foundation projects in both America and the European Union working on independent projects on the matter. So, a way to standardize and integrate a global system doesn’t currently exist. In addition, in this regard scalability is a major concern especially regarding a global system as the systems will need to be able to handle large volumes of users and transactions. This also doesn’t even speak the infrastructure requirements regarding areas such as data-storage, network requirements and support for operations. This can be an issue given the current limitations in both blockchain and other distributed ledger technologies. This also doesn’t even consider an inevitable user adoption hurdle will need to be overcome. The system will have to be user-friendly and understandable that it will not be debilitating to use in Canada and beyond.

Beyond technical issues the system would also have to be able to live up to regulatory requirements and legal frameworks in in Canada at both the provincial and federal level. This also doesn't even consider differing legal and regulatory requirements worldwide for this to be implemented on a global scale.

## IN SUMMATION

Decentralized Identity ultimately at the writing of this report more as a theoretical idea rather a framework for implementation. Currently there exists many different potential frameworks a Decentralized Identity system can take. With organizations such as Sovran Foundation and Support offering for example potential frameworks for how a system could be created. While similar they can have major differences in how their systems operate, especially regarding network configuration and how data storage is carried out (such as with on-chain and off-chain storage). At this time, it is still unknown how the technology will develop in the coming years, or in fact how it will evolve as advances in technology and changes in legal frameworks both in Canada and abroad are adjusted to changing societies.

While ultimately any realistic application of this technology on a country-scale implementation, let alone a world implementation, is still many years off. However, think tanks and experts all agree that this technology will likely see major considerations if not actual adoption before the end of the decade at the time of this writing. As ultimately besides any current hurdles, the potential benefits this could bring are too staggering to simply ignore.

## REFERENCES

Blockchain-enabled decentralized identity management: The case of self-sovereign identity in public transportation: https://www.sciencedirect.com/science/article/pii/S2096720921000099#sec2

12 Scary Identity Theft Canada Statistics: https://reviewlution.ca/resources/identity-theft-canada-statistics/

Digital ID in Ontario: https://www.ontario.ca/page/digital-id-ontario

The passport to Web3-DID revolutionizes digital identity: https://medium.com/@OneBlockplus/the-passport-to-web3-did-revolutionizes-digital-identity-4b46d753d325

Decentralized Identity: Passport to Web3: https://medium.com/amber-group/decentralized-identity-passport-to-web3-d3373479268a

U.S. Consumer Data Breach Report: https://www.forgerock.com/resources/view/92170441/industry-brief/us-consumer-data-breach-report.pdf

Blockchain in Digital Identity: https://consensys.net/blockchain-use-cases/digital-identity/

Decentralized Identity: The Ultimate Guide 2023: https://www.dock.io/post/decentralized-identity#how-decentralized-identity-works

Exploring Identity Theft Statistics in the Age of Data Breaches: https://dataprot.net/statistics/identity-theft-statistics/#:~:text=Victims%20spend%20an%20average%20of,to%20%2425.6%20billion%20in%202020.

Cost of a Data Breach Report 2022: https://www.ibm.com/downloads/cas/3R8N1DZJ

Self Sovereign Identity & Decentralized Identity – An Unlimited Guide: https://101blockchains.com/self-sovereign-identity-and-decentralized-identity/

Introduction to Self-Sovereign Identity.: https://walt.id/white-paper/self-sovereign-identity-ssi

Decentralized Identity: The Ultimate Guide 2023: https://www.dock.io/post/decentralized-identity#what-is-a-decentralized-identity

A new approach for identity in a digital world: https://www.accenture.com/_acnmedia/PDF-173/Accenture-Decentralize-Digital-Identity.pdf