
## BLOCKCHAIN TECHNOLOGY & SYSTEMS

# Privacy protection in Blockchain

WORK INTEGRATED LEARNING PROGRAMMES

This is a controlled document. Unauthorized access, copying and replication are prohibited. This document must not be copied in whole or part by any means, without the written authorization of project members.

# Team

| Printed Name | BITS Roll No |
|---|---|
| ATIN SINGLA | 2021MT12048 |
| M. VENKATA PRADYUMNA KUMAR | 2021MT13115 |
| PRIYANKA MAHAJAN | 2021MT12006 |
| SUBASH CHANDRAN T | 2021MT12330 |

# Revision History

| Date | Description | Author | Comments |
|---|---|---|---|
| 02/11/2022 | v1.0 | Pradyumna M | First draft |
| 07/11/2022 | v1.1 | Priyanka | Monero documentation |
| 11/11/2022 | v1.2 | Subash | Tokenomics, Future roadmap |
| 12/11/2022 | v1.3 | Atin S, Pradyumna M | Added design and research documentation |

# Document Approval

The following Software Requirements Specification has been accepted and approved by the following:

| Printed Name | BITS Roll No | Date |
|---|---|---|
| ATIN SINGLA | 2021MT12048 | 13-Nov-2022 |
| M. V PRADYUMNA KUMAR | 2021MT13115 | 13-Nov-2022 |
| PRIYANKA MAHAJAN | 2021MT12006 | 13-Nov-2022 |
| SUBASH CHANDRAN T | 2021MT12330 | 13-Nov-2022 |

# Contents

# Team Details

| Name | Responsibilities |
|---|---|
| ATIN SINGLA | Detailed Technical Design, Issues & Challenges |
| M. VENKATA PRADYUMNA KUMAR | Introduction, Research & Comparison of privacy focused blockchain technologies, Future research areas |
| PRIYANKA MAHAJAN | Monero - A real world implementation, Federal policies, regulations, Economic, social implications |
| SUBASH CHANDRAN T | Tokenomics, Future Road map , Conclusion |

# Problem Statement

In this assignment, you are expected to perform an in-depth study and write a comprehensive report on the given topic related to the blockchain. P**lease note that marks will be deducted depending on the level of plagiarism present in the report.** So, while you are free to do your research from various sources like research papers, technical blogs, etc., the final writing and thoughts in the submission should be yours. A rough outline of the report is given below. Some of the points may not be relevant to the topic assigned to you and also you may need to include a few other points.

1. Introduction
2. Applications and Stakeholders
3. Detailed technical description (make use of diagrams to explain the technology behind the topic).
4. Issues and challenges (technical and non-technical).
5. Research and Technological gaps between state of the art and market readiness
6. State of the art (gather from research papers, industry or gov projects, - Blogs/machine articles). Identify the key attributes to compare the existing works and make a table to compare them based on the identified attribute/characteristics.
7. Real world project deployments by government and industries - Monero
8. Federal policies and regulations (technical, financial and ethical etc.) - Monero
9. Environmental, Social, Business implications - Monero
10. A detailed discussion on the economic/tokonomics aspects
11. Future prospects
12. Conclusion

*Privacy isn't about hiding something. It's about being able to control how we present ourselves to the world. It's about maintaining a public face while at the same time being permitted to private thoughts and actions. It's about personal dignity.*
*- Bruce Schneier*

## Introduction

In Blockchain technology implementations, there are two types of data privacy scenarios. The first scenario is data privacy. In Public block chains like Bitcoin or Ethereum, there is no transaction data privacy. Because Transparency is the principle by which trustless public blockchains operate. So transaction data has to be not only public, but also has to be replicated into multiple full-nodes. That means if Alice performs a transaction on Bitcoin, that transaction is replicated onto more than 10000 reachable full nodes. All the miners will be able to see the transaction data. There is zero data privacy for transactions. Alice is not able to control how she presents her transaction history to the world. That is decided by Blockchain technology implementation.

The second scenario is that end user identity is not visible because of pseudonymization of identity on blockchain. Though Alice's original identity will not be directly available on the blockchain, her public key can be retrieved. With analytics and profiling, it is easy to map Alice's public key to her real identity. So Alice cannot maintain her public face (due to profiling). This is a serious privacy risk for even her identity (in other words Personally Identifiable Information (PII)). If someone can figure out a way to profile a blockchain user , the pseudonymized identity (i.e. the user public key) is no longer helpful in protecting the privacy of that blockchain user. Pseudonymization of real identity is not enough data privacy. Transactional Data can always carry certain attributes, which can be correlated to derive real identity. In essence, all the data including Person Identity can be made public with advancement of technology automation and a little effort.

The next challenge is that Blockchains are not under any specific jurisdiction of a particular country. But the blockchain operations will have to be regulated by local laws of the land in the interest of stability of life of individuals / society / state / nation. For example, the personally identifiable data has to be protected as per GDPR regulations in the EU region. Similarly multiple countries have privacy laws ( data privacy laws around the world). These nations/states expect the compliance of all enterprises to comply with their laws. Blockchain industry is yet to align well to such privacy standards / expectations. There is an inherent tension between the privacy laws and the fundamental design principles of block chain like "Transparency".

There are different interpretations of anonymity, pseudonymity and privacy law applicability for blockchain implementations.The risks / concerns on privacy law applicability are : 1) Re-identification risk based on various attributes stored in publicly visible transactions is present. 2) On blockchain , how one can identify a data processor or data controller (in controlled fashion) is a challenge as the identity is pseudonymised since there are no central operators in public blockchain. 3) Territorial countrols of nations can create hindrances in blockchain operations for privacy reasons. 4) Cross-border privacy data transfers can not be easily regulated on blockchains as per legal / regulatory requirements. There is no one accountable entity in blockchain operations. The blockchain operators spread across the world living in multiple countries. 5) Legitimate use cases for privacy data processing on blockchain cannot be distinguished from illegitimate usage. All data is visible on a public chain with no central control. 6) Data preservation forever on immutable distributed ledger blocks the individual rights to be forgotten, as blockchain does not permit the permanent deletion of the data.

The above stated challenges require quite a number of technical , algorithmic solutions. Not all problems stated above can be solved purely by algorithms because there is a need for nations/states to come together and agree on basic privacy fundamentals, legal ramifications of the privacy compromises etc.

Many business enterprises look at Blockchain as promising Web 3.0 technology and could unlock new opportunities, at the same time worried about compliance to local laws / regulations of the land. Outside the technology scope, Enterprises will have to find solutions to legal challenges that might arise while implementing blockchain technology based solutions based on the specific interpretations of local privacy laws.

Enterprises may choose a set of tactics to minimize the legal risk. Here are a few tactics to consider. Enterprises may choose to 1) operate on permissioned blockchain technology 2) Use on-chain and off-chain data storage strategies to avoid or minimize privacy data on blockchain 3) Deploy privacy centric technologies like zk-SNARKS 4) Implement additional transformation in hashing and access control. There is no silver bullet to solve this challenge. Rather a methodical solution development and implementation is necessary for compliance. On the contrary, public blockchains may choose to adopt similar strategies except operating a permissioned blockchain and access control, to offer privacy features to a lesser degree. This paper does not attempt to solve all challenges mentioned above. Rather this paper focuses only on the technology solutions available, their current state and how these technology solutions like zkSNARKS, Ring CT, BulletProof privacy solutions can be blended to develop an integrated solution to address some of the privacy related challenges in blockchain implementations.

## Applications and Stakeholders

### Stakeholders

Primary stakeholders for privacy solutions are blockchain end users. Every user has the right for privacy. All blockchain technology providers and enterprises, which use these blockchain technology solutions, are obligated to offer the necessary privacy of data, irrespective of the nature of the blockchain (public or private, permissioned or permissionless).

Enterprise as technology users of blockchain have a responsibility to comply with legal restrictions while reaping business benefits of blockchains. Enterprises (as data custodians) are expected to perform data risk assessments from end users' perspective and classify the data that is being stored on blockchain, choosing a blend of public and private blockchain technology solutions, after risk assessments.

On the other hand, Blockchain technology providers who maintain and update technology stack behind blockchains like Bitcoin and Ethereum also have to consider enhanced technology layers to offer in-built privacy controls (possible in Opt-in mode) that can be exercised by all users of blockchain. The fundamental premise of blockchain is to move the control of transactions back into the hands of decentralized communities and people. Same premise can be applied in implementing privacy focused technical solutions within core technology stacks of these public and private blockchains.

### Applications

The first application of blockchain is on Cryptocurrencies. Cryptocurrencies are treated as safe-assets to hedge against the risks of local/regional/national level financial market risks. Since the assets like Bitcoin are on public ledgers, these assets are visible publicly and attract the attention of hackers. To protect against financial frauds on blockchain, Bitcoin and Ethereum have strong integrity control mechanisms. But these are insufficient to protect the blockchain users (i.e. asset owners). The privacy of the blockchain users identity data is of paramount importance because hackers may indirectly attack blockchain based assets through social engineering , phishing and spear-phishing attacks on the respective asset owners, if the privacy of their asset owners data is compromised.

The first set of decentralized finance (DeFi) applications are already operational and widely popular. The DeFi applications will cover banking, finance, investment banking and insurance. All these businesses have a core operational practice around ledger management. Blockchain with its distributed ledger

management technology is a perfect match for the decentralized applications (DApps) in the above mentioned domains. But the same risks are applicable to the assets in DeFi apps.

Digital rights management is another important application domain. The decentralized pseudonymized identities on blockchain works against tracking the rights ownership of digital assets by specific blockchain users. Even though it is possible to keep track of the integrity of rights in use / distribution, it is hard to identify the exact individual who owns the asset due to pseudonymization. So even if illegal ownership transfers of digital rights happen, the tracking of such events becomes tough.

Many governments can implement citizen welfare services on blockchain. But public blockchain infrastructure with pseudonymized decentralized identities pose the challenge for governments to assess if the rightful owners received the benefits / services or not.

Healthcare applications are very good use cases for blockchain. But privacy laws of healthcare data are very stringent. So adoption of blockchain in healthcare is slow due to privacy / compliance concerns discussed in the "Introduction" section above. Other business domains like supply chain, registry management and legal , benefit a lot with strong integrity of blockchain technology, but will have similar privacy related use cases to be addressed.

The following sections cover high level technology solutions for the privacy requirements in blockchains.

## Detailed technical description

Primary goals of this privacy-centric solution approach are listed below. The solution being discussed in this document is built around the concepts of Blockchain Federated Identity, zk-SNARKs and access control through tokenization.

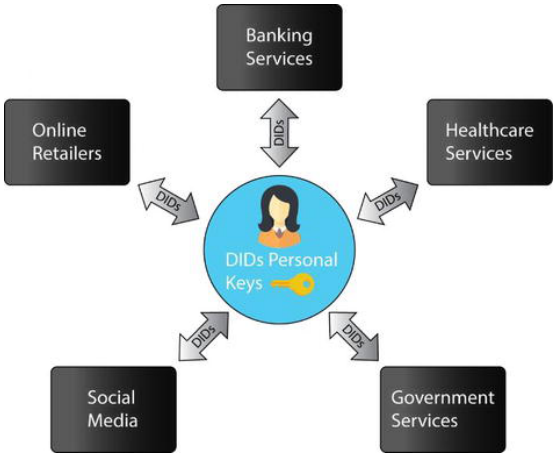
- To Prove to verifier that privacy data is accurate without revealing privacy data for legitimate purposes
- To Protect privacy data from unauthorized access
- To access their personal data (Private data)
- To know what personal / private data is being collected / being sold or disclosed and to whom and to refuse the sale of their personal data
- To request that a business delete any personal data
- Not to be discriminated against for exercising their privacy rights

**Solution Approach (at high level) :**
The integrated solution would comprise the following components in its architecture.

- Support of Decentralized Identity
- Implementation of Blockchain enabled Federated identity (BeFi) Authentication
- Deployment of privacy centric technologies like zk-SNARKS, RingSignature with Stealth address, which enable Zero Knowledge Proofs
- Tokenization for Private Data Validation without storing the original privacy / Private data.

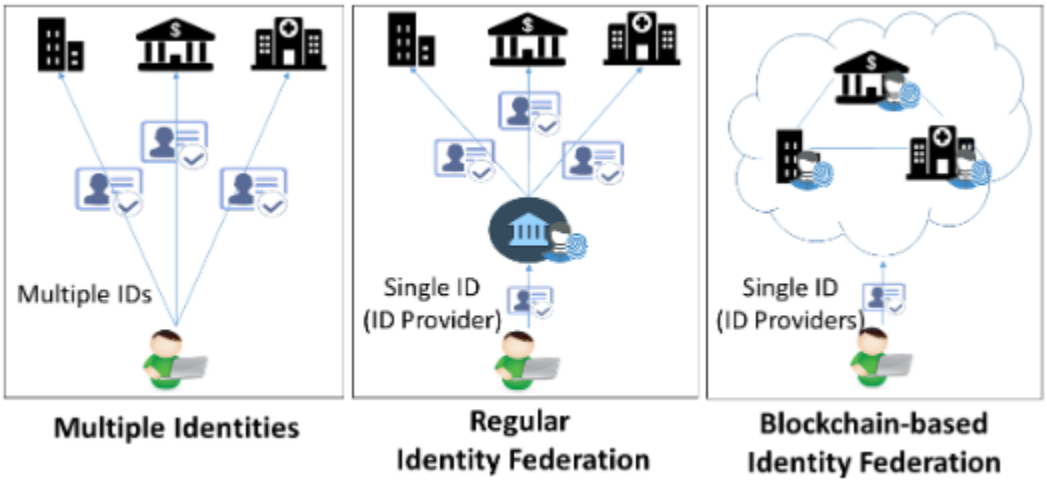
Decentralized pseudonymized identities (DID) of the blockchain users is the foundation for privacy. This DID is necessary , but not sufficient for meeting all privacy requirements. DIDs enable a new use case of "Blockchain-enabled federated identity". The identity of the user is in control of the end user, instead of being the centralized controllers like Google or Facebook. We can start with the way a decentralized and controlled identity system could work for the users to provide a place for the identity storage and management in tokenized form. This will also ensure only selective and required private information will be shared to the requesting applications.

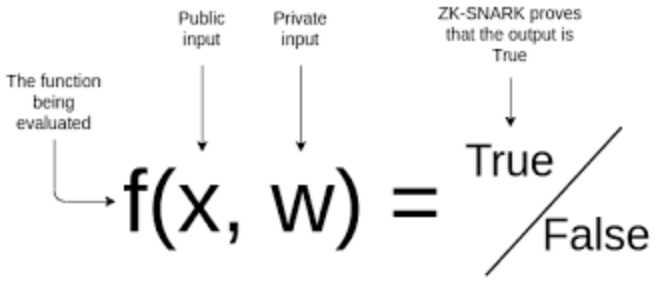
A Decentralized Identity would be a system that holds individuals' identities and also provides the said individual full control over their identity. Such a system could be based on the blockchain open and distributed ledger system and just allow a user to share full or partial information to the requesting systems. Distributed Identity (DI) system would provide a system to store identity information outside the applications in a single system (i.e. blockchain) and provide mechanism for having Identity validation done via token or metadata of the identity provided during the registration process for the user. This would ensure the external systems never have the actual identity of the user, only a token or metadata to the identity validation mechanism. This would also ensure all systems are always having the latest and updated information regarding the user information. Identity information is never out of the owner's control in this model.




In such systems, the DI would be owned and stored by a person rather than by a system provider. The person would have full access to the public and private keys. An encrypted version of the data on the blockchain would only be accessible via the user keys. Hence permitting full control over the information flow control. This eliminates the possibility of correlation across many systems and ensures a single point of reference.

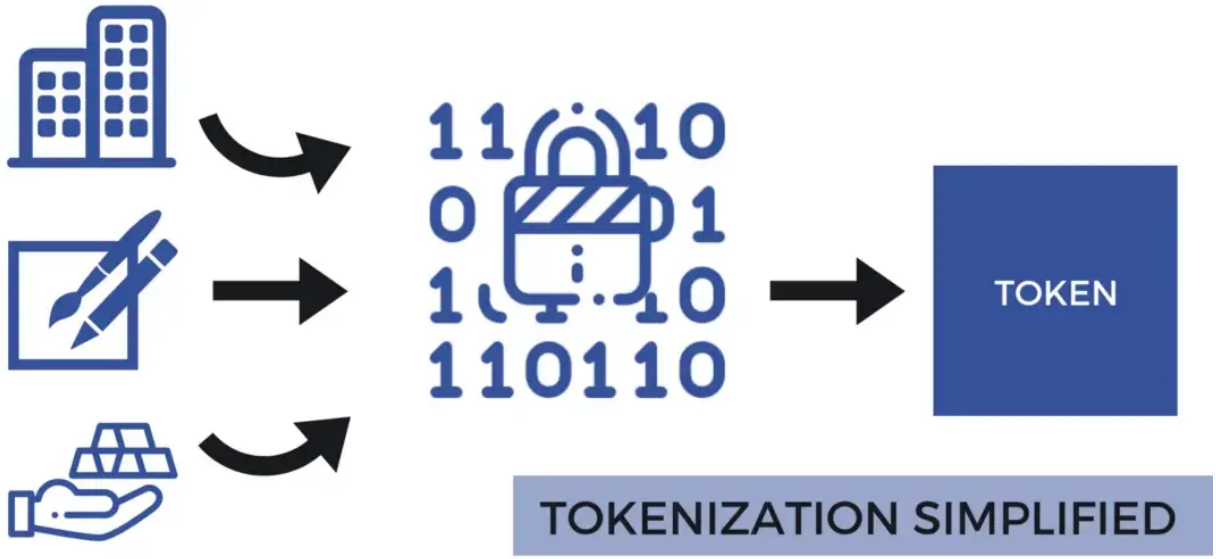
Another component for identity management could be Blockchain enabled Federated identity (BeFi). This would allow the multiple systems to use a single sign-on credential or digital federated identity to access all the services post identity validation. This type of identity, which is typically stored and managed in a central location by a service provider (For example, Google / Facebook), is prone to security vulnerabilities. BeFi removes the roles of such third parties and thus reduces the unwanted external exposure of credentials / identity, because BeFi is based on blockchain technology. The blockchain enables networks to use single sign-on effectively and securely. Users with Federated identity can navigate various systems and networks using a single sign-on system and have full access control via this type of authentication/ authorization system. The various systems can be scattered or connected to each over a common network or across different networks. Auditing facilities on blockchain provide an irrefutable chain of evidence, via the blockchain ledger, ensuring traceability and accountability of each party's action, thereby improving the security of the businesses operating and ensuring private data of end users is well protected.



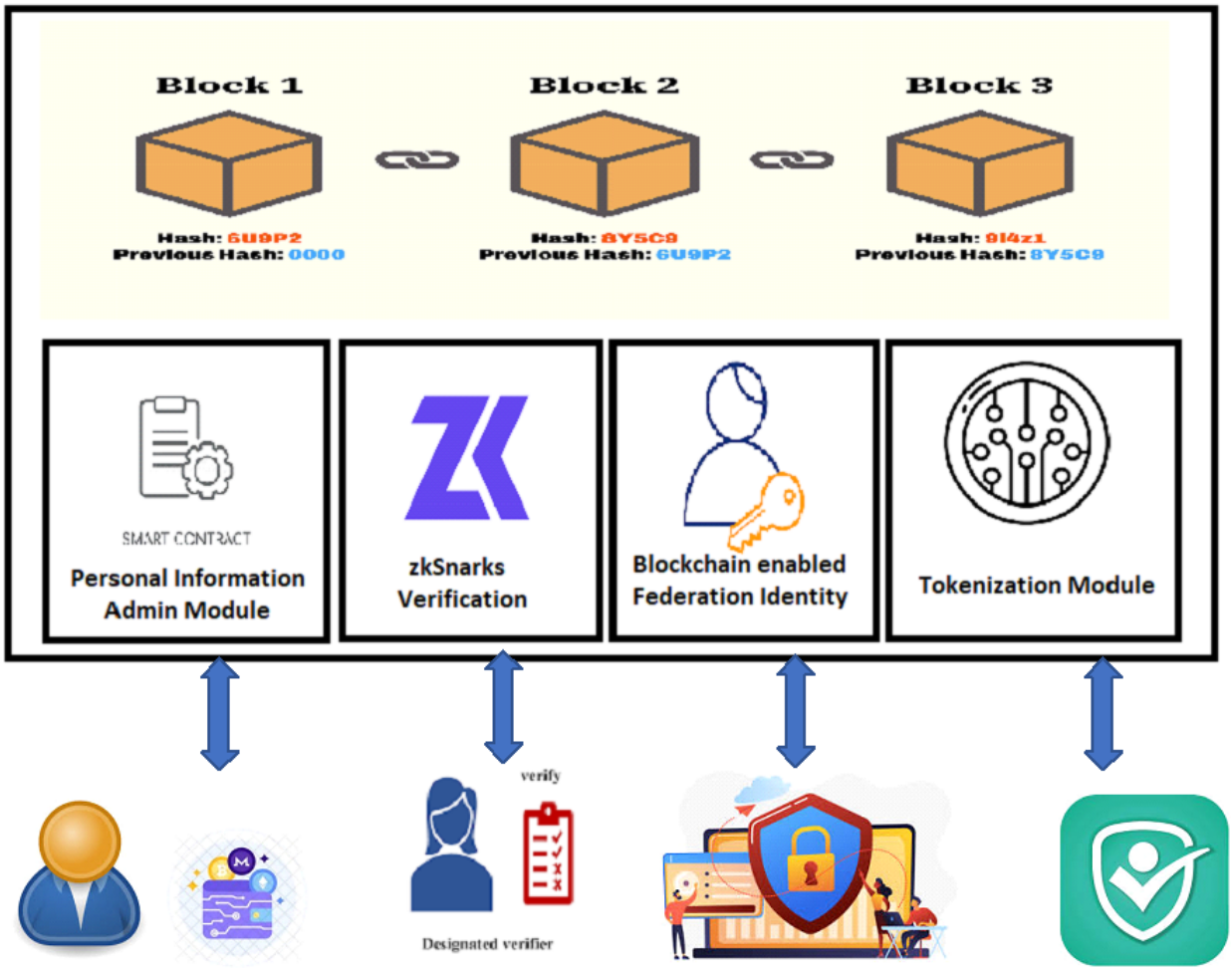



Another component would be to use Zero Knowledge proofs. It uses cryptographic algorithms to mathematically demonstrate to a verifier that a metadata / private data is correct or not. It enables ease of access to identity and other important data while maintaining privacy and control for individuals. Zero knowledge proof (ZKP) works by generating hashes with information and then re-generating the hash at the verifier end, and matching these to validate that the information is correct or not by actually not seeing the information. Only the hashes are visible at the verifier's end. This way private data can be maintained and verified on blockchain without exposing the original data to even verifiers. These zero knowledge tools are powerful tools for maintaining privacy and property control. zkSNARKS will be the backbone for Blockchain enabled Federated identity (BeFi) and Tokenization services.

There may be a need to share a part of privacy data but no more than absolutely necessary in some use cases. Tokenization can help in protecting the control of the owner over his/her own private data, while addressing such business use cases. Private data is an asset. Assets can be protected from unnecessary exposure through tokenization.




Our aim would be to utilize and develop a solution blending these discussed components for best privacy control and user data control mechanisms. We currently have blockchain systems which implement one of these components ,but not all in a single system. We have systems like zCash on zero-knowledge protocol and OASIS for data control by deletion. Our solution would be a combination of these protocols / components for providing maximum privacy options and giving users full control over their private and shared data access control.




- The User would have full control over the Create, Update, Retrieve, Delete (CURD) operations of the personal information being presented to the blockchain. Users will also enable / disable access to private data for all other stakeholders like verifiers, identity authenticating systems and private information validators like banks, financial institutions etc. This Personal Information Admin module will build capabilities, analogous to SPML, XACML and OAuth infrastructure through smart contracts.
- zkSNARKS allow the verification of the personal information without the actual exposing the underlying information to the actual verifier entity. This will be the backbone for BeFi and Tokenization.
- Blockchain enabled Federated identity (BeFi) provided the eternal systems Identity Authentication and Authorisation mechanism without sharing any personal information externally. This can be integrated with SSO with SAML infrastructure for smooth experience for blockchain end users on other web services. Blockchain acts like an idProvider in this type of SSO / SAML infrastructure.
- Tokenization system ensures the privacy data shared is always masked/tokenized and available only to the intended business entity and not exposed to unauthorized systems. Even business entities will not see original private data.

An integrated solution on top of Blockchain technology like zCash would help enforce privacy controls and earn trust of end users as well as comply with privacy regulations like GDPR and CCPA.

## Issues and challenges

Federated identities in centralized systems like Google/Facebook are subject to various threats and attacks and many challenges including identity leaks, centralized management, auditing limitations and long breach investigation processes. Systems are unable to track all outgoing transactions and/or check the data being transferred. The above proposed solution does not expose Personal / privacy information to any external parties. The information is always under the control of the owner of the private information. So this risk does not occur, unless the owner himself is targeted through Social engineering or Phishing.

This era of big data is undermining the user's privacy at a massive level. Very large third-parties benefit from the management of their users' data, by collecting, analyzing, correlating and controlling massive amounts of personal data. These organizations, and their services, are subject to security breaches and user data misuse, which might compromise users' privacy, even without user-awareness. Transactions in the blockchain are not immune to these privacy issues. Besides, individuals are given few options currently to control their personal data and their privacy during their online transactions, encompassing how, when, where, by whom, and which particular personal information is disclosed in each particular transaction. This problem is intensified in blockchain, as the private data included in the ledger is immutable and the user's rights to control and rectify personal information decrease. This situation is aggravated with the coming of IoT scenarios where billions of constrained smart objects, with scarce capabilities to enforce proper security mechanisms, strive to deal with cyber-attacks that might leak their handled data, and ultimately, sensitive and private information of their owners/users. Besides, in IoT, user privacy controls are difficult to apply, as these smart IOT devices/objects usually act on behalf of the user without user control and consent, undermining the adoption of the minimal personal disclosure principle.

On one hand, when it comes to Confidentiality, privacy is seen as the protection of personal data against unauthorized accesses, keeping personal data protected, anonymized and therefore private with regard to the general public. In this sense, many different mechanisms can be employed to anonymize the collected information, secure protected information, encrypt data, protect connectivity channels, etc., thereby ensuring integrity, anonymity, unlinkability, communication protection, undetectability and unobservability. On the other hand, privacy refers also to the right given to citizens to Control and manage their personal data at any time, ensuring user self-determination, as defined in the European GDPR. Privacy as Control can be implemented through Privacy Enhancing Technologies (PET), ensuring selective and minimal disclosure of credentials and personal attributes using, for instance, Anonymous Credential Systems like Idemix, which employs ZKPs to reveal the minimal amount of information to the verifier (usually a service provider), even without disclosing the attribute value itself.

The current challenge is there is no end-to-end solution available based on Blockchain technology to support all requirements of privacy data handling, while unblocking the business use cases with zero Privacy Data Access (zPDA). This zPDA will remain as a research area in the decades to come. Next section dives deep into the details of open research areas.

## Research and Technological gaps between state of the art and market readiness

Current Research related to privacy controls on blockchain platforms is more focused towards specific problems and not approaching privacy as a holistic concept. For example zkSNARKS focuses only on the prover-verifier problem. zkSNARKS tries to eliminate the risk of giving control of privacy of data to any external party, by completely shielding it. But there are use cases where Private data has to be shared. Private data sharing is mainly done for verification , record keeping and (re)validation of Private data.

As blockchains are globally accessible, there are risks of fake Private data being created and published too. So the Private data creation process needs to be so hard that fake data creation is discouraged. This could be supported by enabling Proof-Of-Work consensus or similar mechanism to discourage the practices of fake Private data storage on blockchains. To protect against fake private data being stored on blockchain, The first option to verify the deployed private data is that Identity providers can use zkSNARKS for verification of Private data. The second option is Oracle integrations to various Identity providers can be deployed to the top of the blockchain. These Identity providers can help with certifying the authenticity of Identity data (through zkSNARKS / Oracle integrations), published by end users on blockchain. For example, blockchain may not know if a given Social Security Number is authentic or fake, unless it is certified by the SSN Identity providing authority. These external identities will continue to co-exist with self-sovereign identities, created by individuals. No individual can simply avail services / benefits from the community without these external identities, issued by external Identity providing authorities. This is a research area on how to make self-sovereign identities on blockchain can co-exist with external identities (i.e. private / personal data).

"Private data on blockchain" problem statement brings multiple factors into consideration. 1) A particular transaction can be verified by a verifier without reviewing the original data. A prover can create fictitious data on blockchain and tries to participate in zkSNARKS verification without submitting original data. This is mitigated by the mathematical model of polynomials 2) Private data is not like transactional data (for example, currency transferred in $s) for performing other types of validations like reconciliation of numbers. If person A submits fictitious Private data for person B as part of transaction on blockchain and verifier is able to verify that the transaction is valid, then the removal of fictitious data from blockchain becomes a challenging aspect. Rectification of error would be difficult too due to the nature of immutability. 3) Same case with data erasure or support for "Right to be forgotten", which are fundamental privacy rights as per privacy laws around the world. 4) Many implementations of blockchains interpret data privacy as user's Private data privacy by pseudonymization. But data privacy is not just about user's Private data privacy, but also about the original transactional data privacy too. A lot of research is required to mitigate these risks, while handling transactional / Private data privacy.

At this moment, Monero and zCash are two prominent currencies , supporting privacy for Cryptocurrency transactions. But Monero does not support smart contracts as we speak. zCash launched Agoric support for JavaScript enabled smart contracts. Research can be done on this zCash technology stack, where Agoric JavaScript enabled smart contracts can be developed to store Private data of an individual of zCash. zCash has an opt-in privacy setting that can be enabled. After forking a branch and building a new Private data blockchain on top of zCash, the forked blockchain in in-built privacy settings can be used as a storage to store all Private data.

The Private data can be entered by individuals directly without any central party, by aligning to the philosophy of no central authority control in the blockchain. Each blockchain user can record a zCash transaction with a minimal cost in ZEC on the zCash blockchain. These Private data record transactions, once placed, can only be overridden by adding a new transaction. "Right for rectification" can be supported with revisions. Since blockchain entry is private to the individual himself / herself , who submitted the Private data, the Private data is accessible to himself/herself only.

Since the zCash transaction is verifiable through zkSNARKS, there is a privacy enabled verification process. This does not allow the leakage of Private data to even verifier as prover does not share the original Private data. Once the Private data is verified and recorded on the blockchain, there can be an API built that can verify Private data transactions any number of times. This API can be provided to all interested parties to validate the Private data of the prover any time with a fee for performing verification. That API layer can be built using the support of smart contracts and RESTFul APIs. This type of research not only handles data privacy, but also enables all privacy requirements. No external party needs to see the Private data because verification happens over zkSNARKS protocol. If there is a federated identity

solution built on this zCash Private data blockchain, that federated identity validation can serve as a mechanism for authentication for web 3.0 services. No web service using this Blockchain enabled Federated identity (BeFi) requires to see the Private data, rather rely on zkSNARKS for authenticating the users. This way, Private data on blockchain can be kept secure, serving the needs of relevant Private data for each verifier / external parties like enterprises for both validity of Private data and authentication purposes.

The other challenge is that privacy regulations are different across countries. They evolve independently bringing local differences. Since Blockchains operate at global level, there are no direct mechanisms within blockchains to customize the technology to meet local needs. Countries / states are here to stay. People (even those who are concerned about their privacy in countries with oppressive regimes) cannot disassociate easily from the concept of country / state that they are living in. Each person identifies himself / herself and nation / state is part of their identity. Blockchain features need to adjust to this fact and offer localizable blockchains to particular nations / states. This requires further research.

Many privacy focused currencies / blockchains are just focusing on basic building blocks of how to protect sender identity, receiver identity and transaction data. This level of privacy is bare-minimum and would not suffice to the needs like GDPR and CCPA. The amount of measures offered by even the best privacy focused currency , Monero, does not meet the GDPR, CCPA and other privacy standards. Blockchain technology community and operators operate in a trustless environment. So end users cannot risk personal / Private data storage on blockchains. Questions may arise about why to comply with local privacy regulations. Even Blockchain technology providers and communities are legally obligated to operate their business as per laws of the land. End users will expect the same level of privacy rights support from Blockchain technology platforms. So Blockchain technology providers and communities are not exempt from the law. Blockchain operators will be forced to seize / reduce operations, if the nations / states rule against their operations. China's ruling against bitcoin mining is such an example.

Blockchain technology solution providers also have to give due consideration and give respect to individual privacy needs and design technology solutions to enable self-service in privacy data handling, protection and verification. Selective verification of relevant Private data attributes based on specific business needs is another area of research. If a banking institution requires purely financial private data like PAN number in India, the blockchain technology should allow access only to such selective Private data and limit access to all other Private data like date of birth. No technology research is happening in this area. Many of the privacy related problems are still unresolved. zkSNARKS and Ring Signatures are definitely great advancements in supporting privacy, but not complete solutions.

The following are privacy rights proposed, well-understood, accepted and followed in many countries in the world. Blockchain cannot simply be ignorant of these rights of persons. Let us review how current technology research in Blockchain can help in supporting these rights. These are bare-minimum expectations of end users, who would be using blockchain technology. As no blockchain is focused on offering specific solutions for privacy related rights, More research is needed on how to enable support for these privacy related rights.

**The Right to Information :** With zkSNARKS, there is no Private data shared with external parties. So all Private information is in control of the owner. External parties are blocked from getting Private information. So zkSNARKS is a strong privacy control, putting power back into the individual owner's hands.

**The Right of Access :** As Private data is only available to the individual owner , who puts his/her own Private data on blockchain, there are zero issues for access. As the blockchain like zCash maintains information privacy, no one else can access, as the data is not visible to other zCash users, including verifiers.

**The Right to Rectification:** Private data owner has the full control of the blockchain record and can keep amending the record and get it verified through zkSNARKS. Edited / Rectified records can be (re)verified. The verification of verifiers for Private data accuracy / integrity can only be achieved if a parallel verification is done by engaging the ID providers like a nation / state agencies. This requires further research for solutions.

**The Right to Erasure:** "Right To Be Forgotten"/ "Right for Erasure" is the biggest challenge for blockchain technology to support because immutable ledger is the backbone of blockchain technology. To support such use cases, Crypto-shredding solutions had to be researched and deployed on Blockchain. That way, the Private data once stored on blockchain can become completely irrecoverable. This requires further research for solutions.

**The Right to Restriction of Processing:** Private data owner has full control on whom to provide access to private data or not, how long on Blockchain. Each access grant has to be time-bound. And also, the access control can be dynamically changed by the Private data owner. This requires further research for solutions to implement on blockchains.

**The Right to Data Portability:** This right cannot be applied on blockchains currently because data is available directly on blockchain worldwide. So there would be no question of data portability. This may require further research for solutions because local regulations would consider this worldwide availability as breach of law / regulation. Instead of data portability, research is required on controlling data visibility.

**The Right to Object :** If a Private data owner comes across processing , which is objectionable, the Private data owner can simply suspend the access first. That way the Private data owner can block his / her Private data to be used in such processing. The objection can be raised off-blockchain and handled through legal / regulatory mechanisms outside Blockchain. This requires further research for solutions to generate evidence of objectionable processing of Private data from blockchain.

**The Right to Avoid Automated Decision-Making:** The Blockchain access control in the solution had to be granular for each use case / process so that the Private data owner gets a clear idea of how his / her Private data is being used in automated processing / decision making. Each external party ,seeking direct access to Private data of someone, has to be obligated to furnish full details of the processing, get a consent and access Private data, similar to cookie consent model in GDPR. This requires further research for solutions.

zkSNARKS is not a full solution because many business / legal / government processes require access to relevant Private data of end users in some form for its validity. For example, IT declaration in India requires PAN number to be furnished as on today along with declaration. So the research is required in handling such transactions without revealing PAN. Tokenization is one way to achieve this. Tokenization of Private data on top of blockchain storage as well can address such needs. So further research is required on how to overlay Tokenization on top of blockchain. A compliant solution for handling Private data will have to combine zkSNARKS , Self-service Access Control, Tokenization and Blockchain Federated identity to address use cases like verification of Privacy data accuracy, allow / disallow privacy data tokens for business /enterprise / government operational transaction processing, allow / revoke access to such tokens at the will of Private data owner and allow identification, authentication and authorization using Blockchain federated identity. As mentioned above, blockchain platforms are not immune to local laws. As the blockchain technology industry evolves, new research and solutions are required for compliance solutions. Given the state of the affairs where cyberthreats are growing at alarming pace, blockchains are prone to cyberattacks and can cause significant risks to privacy of its end users with large scale ramifications on human life. So it is essential that blockchain technology platforms need to revisit the current model of operations. The below table shows comparison various available privacy solutions, which are in their nascent stage, when it comes to handling data privacy.

**State of the art vs Existing works - a comparison (by identified privacy attributes)**

| Privacy Aspect | zkSNARKS (zCash) - State of the art | RingCT (Monero) | OASIS | Beam | Verge | Dash |
|---|---|---|---|---|---|---|
| To Prove to verifier that privacy data is accurate without revealing privacy data for legitimate purposes | This is supported. zkSNARKs research implementation in zCash is strong. Provers can leverage zkSNARKS for verification without sharing original data with verifiers. | Ring signatures and single use addresses offer privacy. This approach also hides private data. | Secure Enclaves are used for Trusted Execution Environments | Beam offers levels of confidential addresses, assets and transfer models. But verifiers will have to still validate the provers inputs. | Not supported because this uses TOR network and stealth addresses.. So original data has to be shared and verified. Verifiers and Provers will be on the TOR network. | Uses CoinJoin to mix up transactions and privateSend. But not fully privacy supporting. Original data required to be shared with the verifier. In fact, Dash is no longer considered as a strong privacy enabled blockchain. |
| To Protect privacy data from unauthorized access | This is supported as the entire data like sender , receiver and amount are kept private | Stealth addresses and RingCT protects data from external parties. #1 in privacy | No additional privacy features to protect data. | Supported through confidential addresses, assets and maximum privacy transactions | TOR network protects unauthorized access from external parties, but not from insiders. | No special hiding features. CoinJoin creates ambiguity. Unauthorized access may eventually be done if CoinJoin is broken. |
| to know what personal / private data is being collected / sold / disclosed and refuse such operations | Not applicable, is private data is not shared at all | Not applicable. Private data is not visible to senders and receivers as well | No support once data is revealed. | No support once data is revealed. | Not applicable. Stealth addresses provide anonymity to users. | Risk of privacy data being collected / sold / disclosed is present, if coinJoins are broken, |
| to request that a business delete any personal data / stop profiling | Businesses cannot access data | Businesses cannot access data | Businesses cannot access data | Businesses cannot access data | Businesses can access sender / recipients data by profiling | Businesses can possibly infer Private Data with profiling. |
| Right be forgotten / Erasure | Not supported directly | Not supported | Supported | Not Supported | Not Supported | Not Supported |
| Right for Rectification | Partially Supported | Partially Supported | Supported | Not Supported | Not Supported | Not Supported |

## Real world project deployments by government and industries - Monero

In this section, Monero is taken up as an example, as it is the market leader in valuation as privacy enforcing crypto-currency, even though not all privacy controls are in place for this currency to comply with any regulations.

Monero is a decentralized cryptocurrency. It uses a public distributed ledger with technologies which enhance privacy that make transactions in such a way that it promotes anonymity of end users. Observers cannot decipher addresses trading Monero, transaction amounts, address balances, or transaction histories. The protocol is open source and based on CryptoNote. The developers used this concept to design Monero, and deployed it in 2014. Monero uses ring signatures, ring CT, secret addresses, and IP addresses to make transactions which are unclear to the outside world.

Monero has the third-largest developer community among cryptocurrencies. Its privacy features have attracted many cyber criminals. It is increasingly used in activities such as money laundering, darknet markets, ransomware, and cryptojacking. The United States Internal Revenue Service (IRS) has posted bounties for individuals that can develop technologies which trace Monero transactions. Developers also implemented a zero-knowledge proof method, which guarantees a transaction occurred without revealing its value. Monero recipients are protected through secret addresses generated by users to receive funds, but untraceable to an owner by a network observer.These privacy features are enforced on the network by default, though users have the option to share a private key to permit third party auditing their wallet, or a transaction key to audit a transaction. Monero uses a proof-of-work algorithm, RandomX, to validate transactions. The method was introduced in November 2019 to replace the former algorithm CryptoNightR. Both algorithms were designed to be resistant to ASIC mining.

## Federal policies and regulations - Monero

One of the most important aspects of cryptocurrencies from a civil liberties perspective is that they can provide privacy protections for their users. The government authorities are setting up the regulation for cryptocurrencies as below: But EFF(Electronic Frontier Foundation) is concerned that the U.S. government has been increasingly taking steps to weaken the anonymity of cryptocurrency transactions and incorporate the financial surveillance of the traditional banking system to cryptocurrencies. The Department of the Treasury's Financial Crimes Enforcement Network (FinCEN) announced a Proposed regulation that would require entities such as exchanges to collect identity data about people who transact with their customers using self-hosted cryptocurrency wallets or foreign exchanges. Although EFF is still reviewing the proposal,there are several concerns as below.

1. The regulation would mean that people who store cryptocurrency in their own wallets would effectively be unable to transact anonymously with people who store their cryptocurrency with entities such as exchanges.
2. For some cryptocurrencies, transaction data—including users' addresses—is permanently recorded on a public blockchain. That means that if you know the identity of the user associated with a particular address, you can obtain information about all of their transactions that use that address. Thus, the proposed regulation's requirement that exchanges collect identifying information associated with wallet addresses means that the government may have access to a massive amount of data.
3. The regulation could hamper broader adoption of self-hosted wallets and technologies that rely on them, or at least make it difficult to integrate these technologies with intermediaries like exchanges.

In the case of Monero, the transactions are currently impossible to trace back, so this cryptocurrency is popular with cyber criminals. Due to this it has influenced some exchanges not to list it. Exchanges in South Korea and Australia have delisted Monero and other privacy coins due to regulatory pressure.

## Environmental, Social, Business implications - Monero

**Environmental Implications:**
For each cryptocurrency, it uses tons of energy to mine, hence it has a huge negative environmental impact, as many of the privacy focused currencies use proof-of-work and promote usage of ASIC infrastructure. But Monero PoW is ASIC resistant. So Monero usage is quite prevalent, making it more adopted by communities. This attribute makes Monero attractive to hackers worldwide too.

**Social Implications:**
Monero is considered more of a privacy token and allows cyber criminals greater freedom from some of the tracking tools and mechanisms that the bitcoin blockchain offers. Monero, in particular, is increasingly the cryptocurrency of choice for the world's top ransomware criminals. Hackers have embedded malware into websites and applications that hijack victim CPUs to mine Monero.

**Business Implications:**
The incentive for the attackers shifts decisively towards making their malware as silent and low-impact as possible, so as to maximize the duration of their mining operations on compromised systems for maximum profit.

Below are the differences in Monero compared to other cryptocurrency
1. On each of the public bank statement papers (all chained together), the names of the sender, receiver and amount being transferred are redacted.
2. The chains used to link each of these papers together are made out of a different type of metal.

In Monero the chains are made of "CryptoNight," a metal that can only be worked with by hand, and thus super factories cannot mass produce it.

Currently Monero does not support Smart contracts. Hence the impact of Monero is mostly limited to its Cryptocurrency user community.

## Discussion on Economic /Tokenomics aspects

Tokenomics determines two important aspects of any cryptocurrency - the incentives that define how a token will be distributed and the utility of the tokens that influences the token's demand. Ring Signature is the core behind Monero transactions. It is a digital signature that one user or a group can create a Key, but it is not possible to identify users from the generated key. This uses stealth addresses so that transactions can't be traced or linked to the sender or receiver. Ring confidential transactions hide sender information, allowing the recipient only to see the actual amount only. CryptoNote is an application layer protocol that can obscure transactions at the protocol level while allowing third parties to do validations.

Stealth Addresses allow senders to create one-time public keys or addresses for every transaction. On behalf of the recipient, The sender generates a new address to send the XMR tokens with additional data. The address owner uses these bits of data to create private keys that unlock the funds in that address. Since each sender generates a new stealth address, Transactions cannot be linked to any wallet.

In 2018, Bulletproof protocol was introduced in Monero to reduce the transactional data size and speed up confidential transactions. This protocol ensures that the privacy features work optimally while making transactions faster and achieving low transaction fees on the chain.

In 2020, Dandelion++ is introduced to eliminate the risk of exposing IP addresses of Monero nodes. Dandelion++ uses proxy nodes to broadcast and distribute information to confuse hackers trying to get information.

Monero uses a proof-of-work (POW) algorithm which is ASIC-resistant and CPU-friendly. ASICs are efficient for mining, or creating new tokens but very costly and not many can afford them. So, A small number of people control a significant portion of the network, which poses a security threat to the Monero network. Monero employs an algorithm to limit the efficiency of ASICs. Monero mining can be done on desktops and other handheld devices, allowing anybody to participate in the mining ecosystem without expensive equipment, as the ASIC-resistant algorithms introduce everyone to the same level

The Monero price as of Nov 9, 2022, is $128.27. XMR has a live market capitalization of $2.3B and a circulating supply of 18,198,458.973 XMR. The initial supply of XMR was supposed to be capped at 18,300,000 XMR. In order to incentivize miners to continue to validate transactions on the Monero blockchain, there is a tail emission of 0.3 XMR per minute.

The second largest privacy-focused currency, zCash has institutional acceptance and is far more compliant with regulators/laws than Monero. Developers have a good reputation in their fields which Institutions prefer over projects which have anonymous developers like Monero. zCash has optional privacy with a view key, which fits far better with governments.

zCash uses a proof-of-work mining algorithm where Miners verify transactions and secure the network. zCash has a 2.5-minute block average and offers a block reward that is 4X of Bitcoin. zCash uses transaction expiry to minimize the impact of any non-mined transactions. If it is not mined after 50 minutes or 40 blocks, a transaction expires and funds remain unencumbered.

ZEC can be mined using an ASIC mining rig or a computer with a capable graphics card. Most Linux-based operating systems support zCash mining. zCash recommends using an ASIC mining pool or miner as the network difficulty for PC mining has become so high that it is not profitable anymore.

zCash was designed similarly to Bitcoin and has a total supply of 21 Million coins which can be mined till 2032. As a deflationary measure, zCash blocks are halved every 4 years. As of Nov 9, 2022, zCash's price is $38.61 and has a circulating supply of 13 Million ZEC coins with a Market Cap of 601.4M.

Tokenomics play an important role in enhancing compliance of these privacy focused blockchains. But many blockchains are yet to deploy tokenization for privacy compliance purposes.

## Future prospects

There are a lot of interesting projects that are being built on top of Monero which makes Monero one of the better prospects in the crypto world. Ring signatures are gaining popularity in the blockchain space as a special type of digital signature and allow for a group of people to transact with each other, and with third parties, without revealing the link between an individual signature and an individual’s public key.

zCash protocol, which extends the Bitcoin protocol with more advanced cryptographic algorithms, enables people to execute direct payments, without disclosing any details related to transactions. Confidential transactions rely on advanced cryptographic techniques in order to provide a means for people to keep the actual amount of their transactions private, while nonetheless allowing the public networks to verify the transactions. When combined with technologies such as CoinJoin, these tools could preserve privacy both at the content level and metadata level.

Haveno is a platform that exchanges Monero for fiat currencies like EUR, GBP and USD or other

cryptocurrencies, like BTC, ETH, BCH. All communications in Haveno will be routed through Tor, to preserve privacy. Trades on Haveno will happen between people only, there is no central authority. Haveno provides arbitration in case something goes wrong during the trade. Transactions between traders are secured by non-custodial multi-signature transactions on the Monero network. The revenue generated by Haveno will be managed by an entity called Council, composed by members of the Monero community, not the Haveno Core Team and will be used to fund Haveno and Monero development.

Modern cryptographic techniques ensure that transaction data remains confidential by default and is not necessarily incompatible with the notion of transparency. Users can choose to uncloak transaction data to third parties in order to disclose relevant information to third parties in a certified manner.

## Conclusion

Personal data and sensitive data should not be trusted in the hands of third parties, where they are susceptible to attacks and misuse. Users should be able to own and control their data without compromising on security. Users should not be required to trust any third party and be aware that data is being collected about them and is being used. Blockchain recognizes the users as the owners of their personal data and companies can focus on utilizing data without being overly concerned about properly securing and categorizing them. With a decentralized platform, making legal and regulatory decisions about collecting, storing, and sharing sensitive data should be simpler. Laws and regulations can be programmed into the blockchain itself so that they are enforced automatically. A Blockchain ledger can also act as legal evidence for accessing data since it is tamper-proof.

Transparency is a necessary condition to implement a trustless system that does not rely on any trusted authority or intermediary; but private data has to be protected with additional controls in the interest of blockchain users as well as to comply with regulatory requirements. While some transparency is required to validate transactions, modern cryptographic techniques can be used to prove that a particular transaction is legitimate, without having to disclose the source, the destination, or the actual content of the transaction. Some of these techniques are already well understood, and others are not yet fully mature and are still in course of development, but it is only a matter of time and engineering to perfect them. Decentralized blockchain technologies are paving the way for new forms of disintermediation which, depending on the uses that are made of them, might either increase or decrease people’s ability to protect their privacy and data confidentiality.

It only takes one major privacy data breach on blockchain for legal / compliance authorities to start forcing blockchain platforms to implement GDPR/CCPA and related privacy controls. So it is best if blockchain implementations start proactively working towards technology solutions for compliance and also keep end users feel safe on blockchains.

## References


- Tokenization- https://blog.softwaremill.com/asset-tokenization-on-blockchain-will-disrupt-the-asset-management-landscape-befbd71639b1
- OSPEAD - https://ccs.getmonero.org/proposals/Rucknium-OSPEAD-Fortifying-Monero-Against-Statistical-Attack.html
- Haveno - https://haveno.exchange/faq/
- Zyskind, G., O. Nathan and A. S. Pentland (2015) "Decentralizing Privacy: Using Blockchain to Protect Personal Data", in Security and Privacy Workshops (SPW) 2015. IEEE, pp. 180-184.
- Non-interactive zero-knowledge proof
- Blockchain Technology: Data Privacy Issues and Potential Mitigation Strategies
- The privacy paradox in blockchain: best practices for data management in crypto
- z-Cash - How It Works
- zk-SNARKS and privacy on blockchain
- ZSL: zk-SNARKs for the Enterprise
- zk-SNARKS discussion by zCash team
- BEAM
- VERGE
- Privacy coins like zCash, Monero and Dash Explained
- Privacy Coins and zkSNARKS
- Privacy coins and the law of privacy - a paradoxical relationship?
- Data Protection Laws Around The World
- US Govt targeting Cryptocurrency for financial surveillance
- Wikipedia for Monaro