Detrust: a Self-Credit Protocol

The Detrust Foundation

Version 1.1

Singapore
www.detrust.io

Table of Contents

Detrust: a Self-Credit Protocol 1

The Detrust Foundation

1 Preface 4

2 Protocol Framework 5

2.1 On-Chain IdAM and Off-Chain PISR 6

2.2 Off-chain Private Information Storage and Retrieval (PISR) 7

2.3 On-Chain Access Management: Distributed Identity Assess and Management (DIdAM) 7

2.4 Distributed Data Processing and Machine Learning 8

2.5 Privacy-preserving Smart Contract Execution 8

2.6 Cross-chain Protocol 9

3 Consensus Mechanism 9

4 Detrust Ecosystem 10

4.1 Data Level 10

4.2 Model Level 10

4.3 Application Level 10

4.4 Value level 11

5 Proposed Development Roadmap 13

6 Foundation 14

6.1 Governance Structure 14

Disclaimer 15

Terminologies 16

References 17

"My aim is to picture an ideal, to show how it can be achieved, and to explain what its realization would mean in practice."

— Preface of "The Constitution of Liberty"
by *Friedrich August von Hayek*

Abstract. This paper introduces Detrust, a protocol that aims at building a blockchain-based "personal digital value" ecosystem. The Detrust protocol departs from the current trust model that delegates ownership and access control of the data to a centralized trusted authority. Instead it empowers the users with data ownership.
Based on personal data, Detrust protocol provides privacy-preserving machine learning models and private smart contract supports that securely compute the sensitive individual's scores, e.g. credit score and health score.
Detrust is designed for distributed data streams processing. It enables a secure and resilient access control management protocol by utilizing blockchain as an auditable and distributed access control layer to the data storage and model computation layer. Detrust protocol is agnostic of the physical nodes and supports as well utilization of edge devices as cloud resources as storage and computation nodes.

1 Preface

Over the past years, blockchain-based Bitcoin[1] has shown us an secure and effective way of preserving digital assets without third-party credit system or physical endorsement. Asset ownership is firmly supported by the enormous computing power from Bitcoin network. The Internet, in tradition, cannot guarantee such properties as data breaches and infringements are common and growing, such as in financial areas. It is possible for us to solve the above-mentioned problems by utilizing distributed storage and p2p information interactive mode of blockchain. Therefore, we put forward Detrust protocol, that is, returning the ownership of personal data, storage, and disposal to data creators by blockchain encryption.

Nowadays, big data storage and calculation is wildly used in the calculation process to obtain, deal with and store personal data. The current system has expanded the application of big data of past years, leading to numerous isolated data islands and impacting comprehensive and multidimensional data analysis.

Current systems typically employ stove-piped architectures. Data is collected by specific applications and is stored on third-party data servers. The use of data is also often limited to the specific applications. It is difficult for the framework to synthesize various data sources. At the same time, users lose their rights to retain, use, or dispose the personal data they have generated.

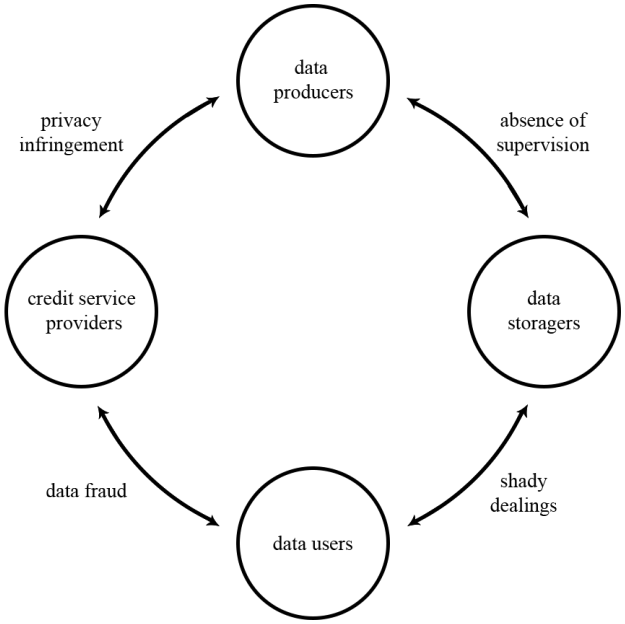


Fig. 1. Personal data is vulnerable and is being exploited

Users have to rely on trusted data storage service and its application providers. It is difficult for existing systems to solve various security issues in those scenarios (for example, auditable access privileged management, secure sharing, and secure computing). Although countries around the world are continuously establishing legislation to protect the security and privacy of personal data, personal private data breaching incidents are still emerging, rendering users helpless.

These restrictions urge us to reconsider our data storage and computing systems in a comprehensive way. Therefore, we put forward the Detrust protocol based on blockchain. Referring to Bitcoin, Bitshares and other design principles, we continue to improve those to meet the "Ockham razor" principle. Meanwhile, we enhance the scalability of Detrust future usage scenarios by improving its usability, security, and scalability.

Based on secure data storage and secure computing models, Detrust further empowers individual digital financial rights and raises the value of digital finance. In terms of digital rights, individuals on the network of Detrust can use comprehensive and multidimensional personal data to build accurate and customized models. These models may come from credit models, personal health models, and learning ability models.

2 Protocol Framework

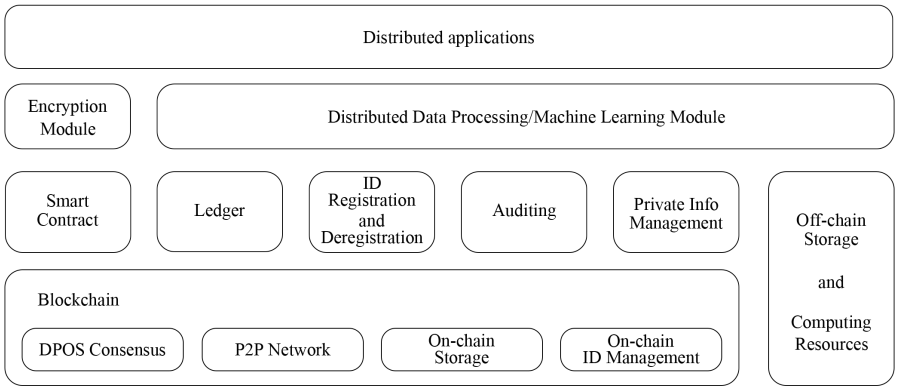


Fig. 2. Overview of the framework of the Detrust Protocol

In essence, Detrust protocol is a tamper-proof distributed ledger with off-chain storage and computation resources. It supports distributed data storage, identity access and management, ledger of transactions, distributed machine learning, and private smart contract. Upon Detrust protocol, users own their own data, and can easily and flexibly manage the access through the on-chain distributed Identity Access and Management module. Furthermore, personal data

are enriched through data preprocessing and feature engineering provided by Detrust protocol. Based on the wide spectrum of personal data, Detrust protocol further constructs the distributed machine learning models and private smart contract so that personal data can be utilized privately.

Specifically, Detrust contains following components:

1. Off-Chain data storage with on-chain identity access and management
2. Distributed data processing and machine learning
3. Private smart contract
4. Cross-chain exchange

2.1 On-Chain IdAM and Off-Chain PISR

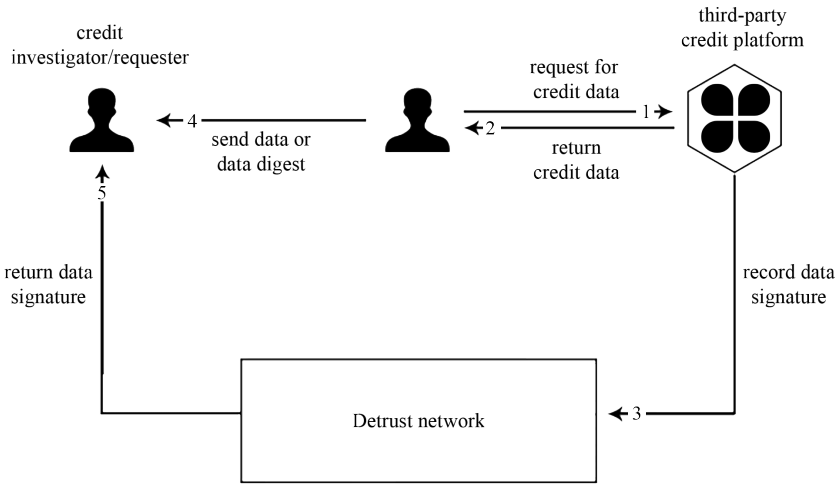


Fig. 3. Proposed self-controlled credit procedure

In the conventional stove-piped architecture, data is stored via special-purpose applications in a third-party data storage for further utilization. This conventional model has resulted into isolated data silos, where users have limited control over their data and how it is used. Users have to trust the third parties on their promises of security and accessibility. Although this model has enabled the bootstrap of the big data ecosystem, it is not necessarily the most suitable solution for the personal data management, as it neglects the ownership of data and mandates centralization through trusted third parties. These limitations necessitate a rethinking of the way to handle data. Instead, Detrust protocol are committed to constructing an independent and resilient data management system that ensures data ownership with the following two characteristics:

R1 Secure data storage (confidentiality, authenticity, integrity);
R2 Resilient, and auditable access control management (ownership and secure sharing).

Conventional model provides **R1**, but falls short in addressing **R1**. Recent decentralized storage startup efforts (Blockstack, Sia, Storj, Filecoin, Enigma[2], Enigma stores data access logs within the blockchain, without addressing the consequential scalability issues. Detrust is inspired by the above approaches, however, our focus on IoT data leads to a number of important design differences.

Detrust proposes a on-chain identity access and management (IdAM) to address **R2**. This provides us with an independent network that maintains a distributed ledger of access control permissions. Moreover, Detrust combines the blockchain with an off-chain data storage, for a scalable secure data storage to address **R1**. Detrust accommodates for personal data where only authorized services are granted access to. The built-in consensus mechanism underpinned Detrust allows the realization of an autonomous, self-sustaining decentralized storage ecosystem, where nodes are rewarded for providing the DIdAM function.

2.2 Off-chain Private Information Storage and Retrieval (PISR)

Detrust protocol proposes a blockchain network-based access rights management scheme to implement distributed access permission. At the same time, data storage can be stored on Detrust protocol under the chain to cope with expansion issues. After private information is stored in a decentralized file system, Detrust deciphers the private information and encrypts it at the terminal, splits and shuffles it, and stores it in a decentralized point-to-point distributed storage file system. Accessing personal privacy information stored in the file system by Private Information Storage and Retrieval (PISR), Detrust's secure multi-party computing system performs calculations after verification based on storage security. Secure multi-party computing and secure private information storage management make upper security application computing possible.

2.3 On-Chain Access Management: Distributed Identity Assess and Management (DIdAM)

Identity management and authentication is centralized in the Internet era with sensitive identity information controlling centrally by one or a few data nodes. The emergence of distributed ledgers (DLTs) has made it possible to implement distributed identity management systems.

Based on DLT technology, two types of decentralized identity management methods are implemented: decentralized trusted identity management and self-sovereign identity management[3]. The former stores the authentication information on the DLT after the user's identity is trusted for authentication, for subsequent access by third parties that need to be authenticated. Applications

are BitID[4]ID.me[5], etc. The latter does not rely on third-party verification to obtain its own trusted identity information, such as OneName[6], Sovrin[7], etc.

DIdAM is the cornerstone of Detrust's network self regulation. Individual users can use a trusted identity file (such as a government-issued ID, etc.) to create a Detrust ID and to authenticate on the chain without revealing personal sensitive information. Personally, identifiable information follows the principle of least exposure and only shares or participates in secure privacy calculations with a very limited number of trusted parties. This identity protocol supports uni-directional and multi-directional authentication with a reputation system based on zero knowledge proof.

2.4 Distributed Data Processing and Machine Learning

In Detrusts framework, distributed artificial intelligence (DAI) includes a machine learning network constructed by machine learning and secure computing modules. Detrust's open distributed artificial intelligence API will be the heart of information processing in the upper intelligent ecosystem. The distributed artificial intelligence framework of Detrust adopts a Byzantine-Tolerant Machine Learning scheme for P2P-based computing network may fails sometimes. This scheme can avoid a single point of failure, and in the case of multi-point failure, this solution proves that the model results converge to the true value.

2.5 Privacy-preserving Smart Contract Execution

Intellectual property protection and privacy is one serious concern when adapting current blockchain technology. Smart contract engines such as Ethereum Virtual Machine, have to make public its contract code, so that the execution of the contract can be publicly verified. The openness of an open-source virtual machine environment guarantees the ability of public verification, yet it has no way to avoid hackers to compromise proprietary properties of the contract by reverse engineering. Such limitation prohibits personal or sensitive data storage or processing on blockchain.

People have proposed solutions to preserve private information on a trustless network. Solutions such as Enigma[2] adds an encryption layer on top of the computation layer to preserve data privacy. Detrust plans to support the implementation of third-party encryption protocols. Detrust is committed to data breaching prevention. It will not compromise on intellectual property, and sensitive data protection.

Aside from privacy preservation, Detrust's smart contract environment plans to support various features and extensions including but not limited to the following:

- integration with offline file systems and database systems,
- queries from Oracle services such as *Oraclize*,
- contract governance,
- multiple high-level languages,

- multiple execution environments,
- formal verification

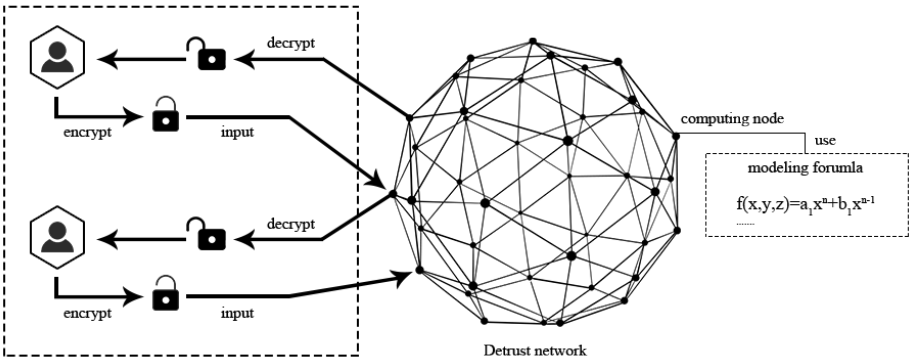


Fig. 4. Distributed Computing Model

2.6 Cross-chain Protocol

Detrust will support both cross-blockchain messaging (digital asset transfer between blockchains) and atomic cross-blockchain swap (exchanging assets without an exchange). A cross-chain protocol is the key in bridging different value networks. Detrust will support both cross-blockchain messaging (digital asset transfer between blockchains) and atomic cross-blockchain swap (exchanging assets without an exchange). It is planned to support cross-chain protocols to connect with other blockchains such as Cosmos[8]. Its implementation is supported using smart contract environment.

3 Consensus Mechanism

There is not a "best" consensus algorithm to rule them all. A trade-off has to be made in a specific application scenario. Gilbert et. al[9] proved the "Brewer's CAP theorem" which states that it is impossible for a distributed data system to simultaneously provide more than two out of the following three guarantees: availability, Consistency and Partition Tolerance. Detrust is not going to propose a silver bullet mechanism, but rather, utilizes existing Delegated Proof-of-Stake (DPoS) algorithm.

Though Proof-of-Work's (PoW) sovereign-grade protection are designed to withstand nation-wide attacks[10], its security level is overkill for the majority of the decentralized applications. The DPoS consensus mechanism, compared with PoW, is weaker in terms of security level. However, it is a reasonable choice for a credit network due to its efficient architecture design.

One of the major criticism DPoS mechanism received is its vulnerability to attacks, especially DDoS (Distributed Denial-of-Service) attacks. Attackers has to only take down some of the delegate nodes to completely shutdown the blockchain. Detrust recognizes such weakness and relies on third-party services to maintain its availability.

Detrust also employs the DAO (distributed autonomous organization) for its network self-governing. DAO is capable of performing full-network voting, dispute arbitration, and consensus management, without being controlled by individuals. It is not only an effective complement to the existing DPoS consensus mechanism, but also the core carrier to promoting community self-governance in the future. In view of this, Detrust incorporates DAO into the consensus system.

4 Detrust Ecosystem

4.1 Data Level

There are multiple dimensions of personal data: basic personal data, consumption data, learning data, social media data, health data, etc. The data generation and appraisal parties include various institutes and companies such as governments, hospitals, schools, banks, e-commerce companies, and Internet social platform, etc. Individuals can firmly control data ownership in their own hands by Detrust protocol. Meanwhile, individuals can easily authorize others to use his data at ease so that data can be used effectively and protected in privacy.

4.2 Model Level

Based on distributed machine learning, Detrust provides rich models for personal data while ensuring data privacy and security. The Detrust model layer is the core technology aimed at preserving privacy for multiple users in a distributed network composed when computing. Personal information is used in various models provided by distributed machine learning to achieve personal digital value. At the same time, Detrust has strong scalability. In the future, it can quickly access other public-linked data through various cross-chain protocols to serve the blockchain ecosystem.

4.3 Application Level

Personal credit agreement system based on multi-dimensional value measurement is at the core of Detrust ecosystem. In this system, relying on community

Name	Service	Business
credit investigation	Credit investigation builds credit scoring model aiming at lending, behaviors or commonweal. It Synthesizes and evaluates based on mass personal information.	Real name authentication of users, anti-fraud, filing and verifying privacy.
lending	Lending include small cash loans, credit loans, social security loans, housing fund loans, academic background loans, skills loans, academic degree loans, commonweal loans, interest loans, etc.	user authentication, anti-fraud verification, lending examines and approves risk control model, etc.
financial management	currency fund,digital assets,credit asset management, etc.	user authentication,, anti-fraud, financial product investment model, etc.
crowdfunding	project crowdfunding, activity crowdfunding, etc.	user authentication, anti-fraud, crowdfunding product investment model, etc.
investment	Stock right, digital assets, project investment, etc.	user authentication, anti-fraud, product investment model, etc.
digital assets transactions	the whole transaction process	user authentication, anti-fraud, transaction risk model, etc.
mutual insurance	accidental self- insurance, serious illness self- insurance, self-property insurance, etc.	user authentication, anti-fraud, actuarial model, etc.

Table 1. Examples of applications enabled by self-credit protocol

networks and data networks, Detrust supports developers to develop a variety of Self-financial applications by supporting multi-party distributed computing technologies and personal artificial intelligence engines.

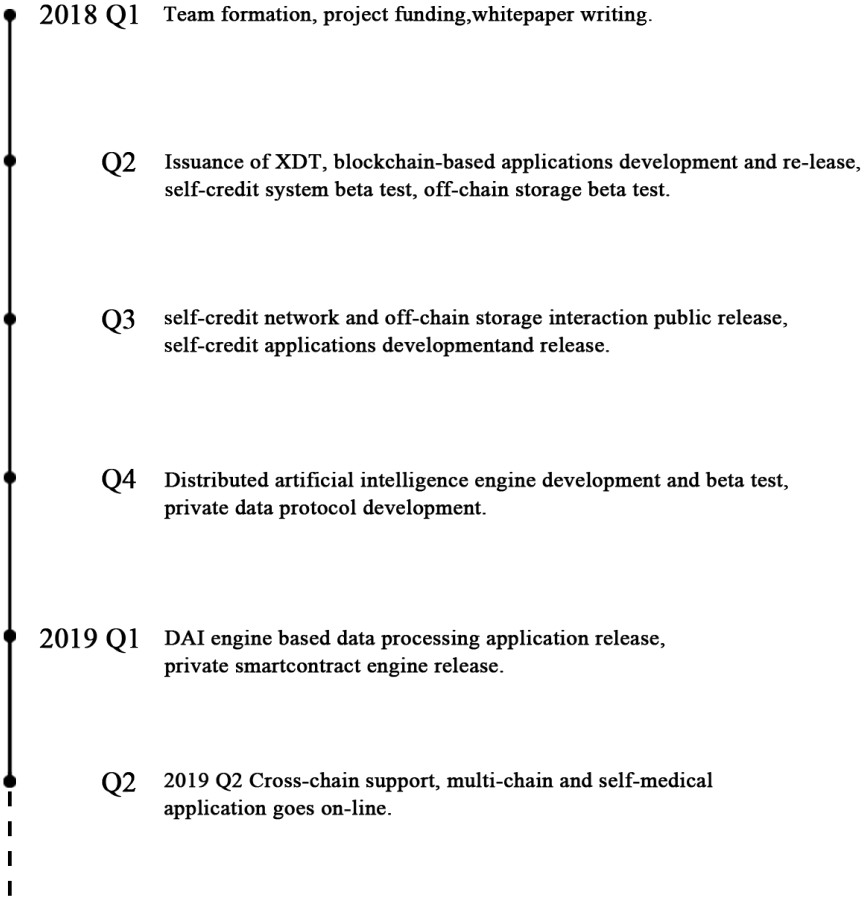
Developers can build various applications (as shown in Table.1) based on the multiple personal financial AI model in Detrust's application ecosystem. At the same time, they can help maximize the benefits of the best products through intelligent matching between applications.

4.4 Value level

The core of the blockchain is to provide value transfer. Individual values can be quantified and transferred across time and space with high efficiency and equity based on Detrust protocol. Through data layer, model layer, and application layer of Detrust, individuals can begin to measure value from the date of birth.

The value measurement system constantly updates and iterates over individual timestamps through smart contracts and cross-chain operation protocols.

5 Proposed Development Roadmap



6 Foundation

6.1 Governance Structure

The foundation Detrust has set up in Singapore is an independent, democratic governing body for all members of Detrust shared economic ecosystem. The project team will work with members of angel advisors to build Detrust Foundation and maintain the daily operations and reporting affairs.

After its foundation, it will begin to select the appropriate community to join the Detrust Foundation's functional committee, where they will make decisions and promote Detrust ecosystem development, operation and promotion.

The functionalities of the Foundation includes but not limited to:

- Work with other ecosystem partners to govern of their resources in an open way
- Develop a digital economy with shared ecological mechanisms and safeguard the interests and values of each party in the mechanism;
- Provide more developers with an open and sustainable platform and ecosystem

As time goes by, the Foundation may be replaced by other more innovative governance methods, but its essential to build formal governance institutions in the beginning for all innovative governance methods.

In the future, the Foundation will invest resources in research, development and governance. Meanwhile, it will hire a development team to promote this work, improve the technology of the entire ecosystem and continue to maintain open source code base. Therefore, all members of the ecosystem will continue to benefit.

The Detrust Foundation's initial vision for governance is to adopt a combination of professional committees and functional departments to respond to daily work and special issues. The Foundation will set up various functional committees (including strategic decision committees, technical audit committees, remuneration and nomination committees, public relations committees, etc.). Referring to the company's institutional framework, the foundation establishes daily operations such as the units of human resources, administration, finance, marketing, research and development (or laboratory), etc.

Disclaimer

1. This document is only used to convey information; the above information or analysis does not constitute investment decisions. Moreover, this document does not constitute any investment advices, intentions or abetting investment.
2. This document does not compose of or be understood as purchase and sale agreement, or any solicitation to sell or buy securities, nor contract or commitment in any form;
3. Investors should have clear understanding of risks of Detrust; the investment involvement indicates they know and accept the project risks, and are willing to assume corresponding results or consequences by themselves;
4. The Detrust team does not undertake any direct or indirect losses of assets involved in the Detrust project;
5. The fund-raising objects of this project are only persons with legal investment qualification; based on the different attitudes and policies toward virtual currency, please consult your local lawyer before participating in the project pre-sale to avoid violation of national law. If your local laws prohibit you from participating in virtual currency related activities, please immediately stop your relevant actions; otherwise, all the risks arisen are at your own risks.
6. Relevant applications or products dont reach the expected risks of Detrust itself or the buyers. Detrust application is currently in the development stage, and there may be relatively large changes before releasing the official version. It could not reach the expected anticipation or imagines, which the Detrust itself or buyers have on Detrust application or Detrust tokens functions or forms (including behaviors of the participants). Any wrong analysis or changes in underlying design and others are likely to lead to this situation.
7. The rapid development of vulnerability risks, cryptography or the development of other related technologies, such as the development of quantum computers may crack the encrypted tokens and Detrust platforms, leading to the loss of Detrust. Any encrypted digital currency may return to zero. Investors must be aware of this risk.

Terminologies

Delegated Proof of Stake (DPoS) leverages the stakeholder voting mechanism to resolve the consensus problem in a democratic manner. Block producers are voted by participants of the blockchain network. Elected delegates are authorized to set the parameters, from fee schedules to transaction sizes.

Sandbox is a security mechanism of running applications in a restricted secure environment in an effort to mitigate network vulnerabilities. By disabling or restricting access to memory, system files, and settings, sandbox achieves safely executing unverified or untrusted programs or codes, without risking the hosts.

Feature engineering refers to the process of structuring unstructured data using domain knowledge, which is necessary before machine learning process. It increases the predictive power of machine learning algorithms by creating features from raw data that help facilitate the machine learning process.

Identity Access and Management (IdAM) refers to the process and policies involved in managing the Identity information and attributes. It is for securely initiating, storing, and managing user identities and access permissions. Two main functions of IdAM are authentication (ensure users are who they say they are) and authorization (users can access the the applications and resources they have permission to use).

Private Information Storage and Retrieval (PISR) is a privacy-enhancing technique that allows users to safely access information of storage system on the condition that users communication and information secret are kept.

Distributed Machine Learning refers to multi-node machine learning algorithms and systems that are designed to improve performance, increase accuracy, and scale to larger input data sizes. Increasing the input data size for many algorithms can significantly reduce the learning error and can often be more effective than using more complex methods. Distributed machine learning allows companies, researchers, and individuals to make informed decisions and draw meaningful conclusions from large amounts of data.

Private Smart Contract refers to the smart contract system with the ability for counterparties of a transaction that prevents other participants from knowing certain facts or detail about the transaction.

Cross-chain Protocol allows users to conduct cross-chain transactions without the necessity of third-party exchanges. It expands the existing double-chain atomic asset exchange agreements, allowing multiple participants to exchange assets on different blockchains and ensure consistency and atomicity of the entire transaction.

References

1. Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system, 2009.
2. Enigma scalable privacy for every blockchain. https://enigma.co. Accessed: 2018-04-01.
3. Paul Dunphy and Fabien A. P. Petitcolas. A first look at identity management schemes on the blockchain. *CoRR*, abs/1801.03294, 2018.
4. bitid: Bitcoin Authentication Open Protocol, April 2018. original-date: 2014-03-31T14:16:56Z.
5. Id.me wallet. https://id.me. Accessed: 2018-04-01.
6. Onename.
7. Sovrin: Identity for all. https://sovrin.org. Accessed: 2018-04-01.
8. Cosmos network. https://cosmos.network. Accessed: 2018-04-01.
9. Seth Gilbert and Nancy Lynch. Brewer's conjecture and the feasibility of consistent available partition-tolerant web services. In *ACM SIGACT News*, 2002.
10. Arvind Narayanan and Jeremy Clark. Bitcoin's Academic Pedigree. *Queue*, 15(4):20:20–20:49, August 2017.