Telecommunication Use Cases for Blockchain Technology

Volume 1

August 2019

EEA Telecom Special Interest Group Authors

Bashar Lazaar and Dr. Andreas Freund, ConsenSys
Darren Kress, T-Mobile
Inhyok Cha, Moojin Woo, and Jaehan Lee, SK Telecom
Takuya Sawadaand Kenichi Suzuki, KDDI Corporation

Editor

Ken Fromm, EEA (Editor)

Table of Contents

Use Case 1A: Blockchain-Based Telecom Call Roaming User Authentication 4
Introduction 4
Solution 4
Stakeholders 4
User Authentication Workflow 4
Architecture 5
Use Case 1B: Blockchain-Based Telecom Call Roaming Reconciliation 7
Background and Problem 7
Solution 7
Design Advantages 8
Technical Notes 8
Benefits 8
Challenges 9
Use Case 2: IoT Trust Attributes and Reputation Evaluation 10
Problem 10
Opportunity 10
Conceptual Design 10
Blockchain Benefits 11
Benefits to Transacting Parties 12
Application Examples 12
Challenges 12
Use Case 3: Data Privacy and Monetization 14
Background 14
Problem 14
GDPR Data Issues 15
Solution 16
User Stories 16
Benefits 17
Challenges 17
Use Case 4: Digital Contents Distribution Platform: Property Management and Distribution Market 18
Background 18
Solution 18
Stakeholders 18
Implementation Notes 20
Challenges 20
Use Case 5: CX in SDP Delivery Models 21
Problem 21
Aligning Business Goals around Business Outcomes 21
Solution 21

Constructing Economic Incentives for B2B Service Partnerships in the Telecom industry 22
Description of a Secure Economic Incentive-Driven Consensus Model to Align on Business Outcomes 23
Auditor Signalling 24
Auditor Voting 24
Vote Revealing 24
Objections 24
Benefits 25
Privacy, Security 25
Security-Related Challenges 25
Implementation Considerations 27
References 28
Use Case 6: Identity Attestation Flows for ISP Services and Components for Abstract API Creation 29
Abstract 29
Introduction 29
Example Use Cases 29
Message Objects 36
Glossary 41
Technical & Spec Implications 41
About the Enterprise Ethereum Alliance and Telecom SIG 42

Use Case 1A: Blockchain-Based Telecom Call Roaming User Authentication

Contributor: ConsenSys
Author: Bashar Lazaar, ConsenSys
Date: 21 August 2018

Introduction

The current signaling technology used by telecommunication operators to communicate on the authentication of roaming users is no longer as effective as it used to be. There are several reasons for this including authentication delays, security concerns, and cost. With respect to authentication delays, users will sometimes have to wait for periods of between 5 to 15 minutes until they get authorization for roaming service. In the age of near real-time response expectations, this delay is too long.

Furthermore – and ever more critical – is the fact that the existing encryption method used by the industry for roaming purposes – SS7 encryption – has been compromised. In fact, it was shown to be hackable via brute force over a decade ago. Obviously, a new and more secure approach is needed.

The third reason for upgrading roaming authentication is cost. Telecommunications companies are paying large monthly fees for their existing authentication services, but these services charges are not cost-effective, nor do they meet the requirements they were designed for.

Solution

A proposed solution is to make use of a blockchain-enabled communication network to facilitate the provisioning of services by telecommunication operators for users roaming between networks. This blockchain-based facility would be secured using modern encryption methods (SHA-3, for example) with each operator holding a public/private key pair. The idea is to create a registry of public keys for each operator on a permissioned basis so that each operator has access to other operators. This registry would thereby facilitate direct/encrypted communication of service authorizations for roaming requests – allowing for a common, secure, and traceable improvement from the current method.

Stakeholders

The primary stakeholders are the telecommunication operators whereas the beneficiaries are both the operators and their customers. The GSMA (Global System for Mobile Communications) is a global trade body that represents the interests of mobile network operators worldwide and would likely be one of the organizations to serve as a primary driver for mobile carriers.

User Authentication Workflow

Below is a chart that describes how the workflow would work for such as service.

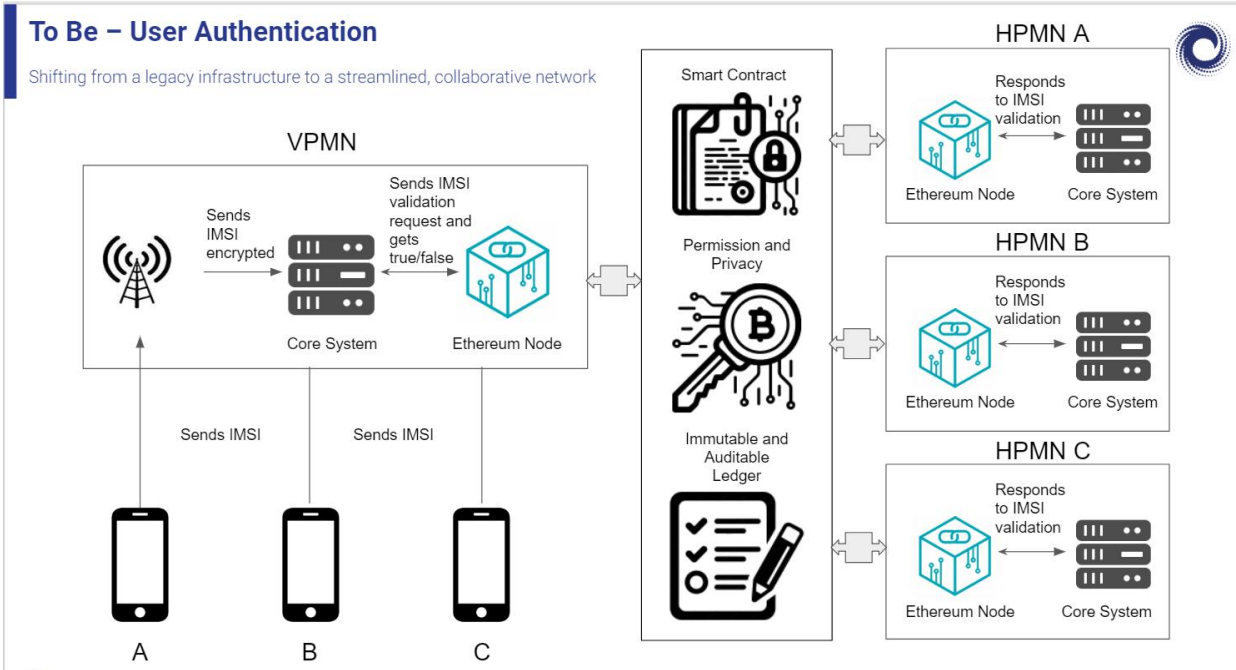
	1. User identifies itself to the VPMN	2. VPMN's VLR requests confirm. from HPMN's HLR	3. HPMN to confirm user's accessible services	4. HPMN confirms accessible services to VPMN
Process Step Description	a) The user turns his/her cell phone on while being in the visited country b) The cell phone communicates its IMSI number to the VPMN's Visitor Location Register	a) VPMN encrypts IMSI number b) The VPMN's VLR sends encrypted IMSI to the HPMN's HLR	a) HPMN decrypts IMSI number b) HPMN confirms within its database the services that its user should have access to while abroad c) HPMN encrypts the returned value for user's accessible services	a) HPMN sends encrypted user's accessible services to VPMN b) VPMN decrypts the accessible services propagated by HPMN
Actors	- User - Visited Public Mobile Network	- Visited Public Mobile Network - Home Public Mobile Network	- Home Public Mobile Network	- Home Public Mobile Network - Visitor Public Mobile Network
Network Participants / Consensus	- VPMN Node	- VPMN Node - HPMN Node	- HPMN Node	- HPMN Node - VPMN Node
Assets in Play	- IMSI Number	- Encrypted IMSI Number	- Encrypted IMSI number - Decrypted IMSI number - 1/0 per service requested by user - Encrypted values for user's accessible services	- Encrypted values for user's accessible services - Decrypted values ^
Business Rules (Smart Contract)	- Creation of record for user (consumer) - Identification of corresponding HPMN based on IMSI	- VPMN hashes the IMSI number - VPMN communicates encrypted IMSI to HPMN	- HPMN decrypts IMSI number - HPMN submits decrypted IMSI to off-chain database - HPMN maps user's accessible services - HPMN encrypts accessible services	- VPMN decrypts user's accessible services - VPMN confirms to off-chain database the services to be provided to user
Transaction on Ledger		- VPMN propagates encrypted IMSI number on ledger	- HPMN propagates encrypted accessible services	- VPMN confirms activation of user services

Architecture

To add to the workflow above, here is a high-level schematic that describes the interfaces and some of the underlying components. By using a blockchain-based solution, carriers benefit from shared schemas and standardized transaction processing (via smart contracts) that provide better security and faster response times than the current solution.

To Be – User Authentication

Shifting from a legacy infrastructure to a streamlined, collaborative network



Use Case 1B: Blockchain-Based Telecom Call Roaming Reconciliation

Contributor: KDDI and CLEAR
Author: Kenichi Suzuki, KDDI
Date: 29 January 2019

Background and Problem

Offering and supporting roaming telecom capabilities is an important service component for telecommunications companies but it must be profitable for the carriers in order to manage and maintain such services. Any such provisioning must also provide a seamless and low cost/no cost experience for mobile users.

Inter-carrier policies, along with the transaction and billing overhead involved with roaming, however, have become quite complex. This combination presents difficult challenges for carriers, especially when it comes to reconciling roaming services charges between operators.

The requirements for a global solution that might improve on the current approach are, not surprisingly, quite strict. Any provisioning and reconciliation solution must not only manage multiple relationships, it must also manage complicated financial relationships with varying laws and regulations in different countries and regions around the world.

From an internal carrier standpoint, supporting roaming capabilities with existing approaches has become quite difficult due to these financial and business workflow complexities, this is especially true when combined with the user expectations regarding service interoperability.

When looking at a new roaming reconciliation system, a number of concerns arise. A few of the more important concerns include:

1. Sharing sensitive business data with other companies
2. Protecting against spoofing and user fraud
3. Processing large volumes of data

Solution

To solve the problem, various companies involved with mobile roaming have formed a consortium that proposes to specify a telecommunications roaming service solution that can communicate and share sensitive data directly within a blockchain network.

In particular, the solution addresses the use of both Layer 1 (decentralized ledger) and Layer 2 (state channels) components, in order to provide both immutability and record keeping along with enhanced throughput and scale needed to support real-time global telecommunications.

Via this consortium, roaming contracts and business flows can be developed, propagated, audited, and enforced. These business flows and contracts are expressed via smart contracts within a blockchain solution. Among other transactional needs, the proposed smart contracts address the following areas:

- Matching the roaming call log with a fee list along with performing a service fee calculation
- Forwarding the call log of the user to the home carrier from the visited carrier

- Creating and sending an invoice for service charges and sending to the home carrier from the visited carrier
- Confirming receipt of invoice(s) and call logs by the home carrier
- Reconciling sent and received invoices and creating a balance of payments account with other carriers
- Making payment of open balances, carrying balances forward, and/or disputing any transactional elements

Design Advantages

With an improved roaming solution, Telco's will be able to better correlate a user's non-home carrier usage with a user's contract to provide greater transparency and faster service response and accommodation. The benefits for users are that they get great service flexibility and decreased service fees, which, in turn, will increase their usage. For telecommunication companies, the benefits include reduced costs, increased customer loyalty, and improved fraud prevention.

Technical Notes

- Network-related data and registry information can be exposed on a permissioned basis within the blockchain network whereas private transactions and data can be encrypted and processed via zero-knowledge proof algorithms.
- The consensus algorithm(s) used can be optimized to reflect the permissioned nature of the network as well as meet the needs of the contemplated throughput. The proposed algorithm is currently based on proof-of-authority consensus, which allows for only trusted parties to have roles in validating and verifying the transactions.
- Data processing can be minimized by transmitting only relevant data to roaming operator node.

Benefits

- **Transparency and Trust:** Trust between roaming partners will be secured by both the "mutual-monitoring" and "tamper-resistance" nature of a blockchain solution. Carriers can run and maintain nodes within the same network and therefore have a role in generating consensus for transactional records as well as validating and verifying each transaction block. Multilateral deals that incorporate and enhance with transparency and trust will also be possible.
- **Smart Contract Visibility:** Multilateral contracts can be executed and managed in a more transparent and faithful manner. Primary flows between parties will be automated and facilitated by smart contracts.
    - Visiting carrier: Getting user info in order to services → supply network service → write call-log to blockchain
    - Home carrier: Confirm call-log and invoice from visiting carrier → settle accounts and pay/receive payments

- **Real-Time Processing**: Another significant advantage of moving to a blockchain-based solution is the ability to process transactions in real-time and maintain more current roaming balances between carriers. (Although the performance of blockchain networks is often criticized, permissioned/private network in conjunction with the use of state channels are designed to handle the type of throughput contemplated here.) This real-time capability enables carriers to more readily know what is going on with cross-carrier traffic as well as stay on top of their business and revenue and expense forecasts and actuals.
- **Cost Reduction**: All the above benefits will allow carriers to reduce costs related to confirmation time, the adjustment process, and other post-transaction reconciliation that currently takes place. Doing the cost adjustments concurrently with the service provisioning will eliminate a significant amount of overhead and post-service activity. The commonality of the solution and the leverage gained by visible contracts expressed as executable code will also prove to be a significant savings for carriers.

Challenges

The proposed solution is not without challenges. A few of these include:

- **Legacy Systems and Internal Inertia** – Telecommunications system are complicated and contain a significant amount of legacy applications and packages. Change is not always easy to effect especially considering the internal structures and internal divisions along with existing relationships.

Use Case 2: IoT Trust Attributes and Reputation Evaluation

Contributor: T-Mobile USA
Authors: Darren Kress, T-Mobile
Date: 11 September 2018

Problem

The globally interconnected ecosystem has limited data to make informed trust decisions for IoT devices operating across a telecommunications network or otherwise interacting with services or other connected devices. In addition to limited data being available for trust decisions, the data used by one party to make a trust decision may not be the same criteria needed by another.

Where trust criteria are available for decisioning, it is often limited to data provided by a single entity. Not only does this provide a very narrow representation of trust, it also enables a single entity to have an enormous amount of control on critical trust decisions.

Opportunity

A way to address this problem is to enable a new era of trusted global communications with diverse technology operating at various levels of trust commensurate to the operational needs of the interconnected components.

We believe this solution can be realized through a blockchain-enabled mechanism that collects trust attributes from various entities and make this information available publicly for all ecosystem parties to allow each party to self-select the criteria needed for its decisioning process. One example data and source might be the device specifications as detailed by the sensor and/or device manufacturer and identified by the entity.

Additional attribution as to the identity of the sensor or device can be provided from additional sources to provide an additional level of validation or verification. An example of additional attestations might come from other nearby devices to correlate if the data provided by one device largely matches the data provided by the other device. (Temperature ranges for example or related fields of vision for overlapping cameras.) Each attributional statement or record can be made with secured authentication within a blockchain ledger. Depending on the nature of the transaction and level of trust required, if the available records prove enough trust, the device can then be engaged by the other device.

Conceptual Design

The design for such a solution would be as follows. A blockchain network would be used to collect and store trust attestations from various entities including OEMs, network operators, service providers, and other globally connected devices.

Attestations could include:

- Attributes from Trusted Partners
    - OEM
        - Verified Boot

        - Root of Trust
        - OEM Certificates that allow verification of model or device certificates
    - Network Operator
        - Security Assessment
    - 3rd Party
        - CTIA IoT Certification
        - Security Organization identifying potentially malicious activity
        - Peer Device
- Lifetime in Environment
- Number and Type of Trust Relationships
    - OEM
    - Operator
    - Service Partner
    - Consumer
- Known Valid Transactions
- Known Malicious Activity

Blockchain Benefits

The benefits of an IOT trust system executed via blockchain technologies are many. Here are just a few of the benefits.

- **Decentralized Ecosystem** -– Using a decentralized blockchain solution reduces the opportunity whereby a single party can establish or define trust within an ecosystem. Consensus algorithms along with an immutable ledger improves the collection of data as well as assures submitted information cannot be altered.
- **Open Ecosystem** – A solution via blockchain would likely by nature be more open, thereby allowing new parties to contribute criteria used for trust decisions. This openness would also allow for and facilitate dynamic changes in trust attributes.
- **Standard Protocols / Shared Data Formats** – The decentralized nature of blockchain technology means that all parties use the same protocols and data schemas and have access to the same data. This standardization is largely overlooked benefit in that integration and ETL work – which is common with interconnected systems – is largely eliminated.
- **Increased Longevity** – The decentralized operation of an IOT device trust network would conceivably increase the longevity of a solution in that it would be independent of any one party. Centralized hubs and registries are at the mercy of their owners and different incentives and motivations can alter the direction and purpose of a system. Decentralized systems are more adept at tempering single source motivations.

- **Reduced Attack Service** – A distributed network can in many cases reduce the attack surface for many types of security attacks. An example is Denial of Service (DoS). The more nodes in the system, the less effective a DoS will be.

Benefits to Transacting Parties

Transacting parties also gain additional benefits via the flexibility and open nature of the network and data. Any party that is making use of IOT trust attributes within the system can define what is trustworthy based upon their needs, the specifics of the transaction, and the identity of the other party. They can use any of the information that is available to them as they see fit, without necessarily relying on a central or authorizing authority. Now certainly there are possible downsides in that this flexibility may open up security issues for those less adept although we expect some standardization via smart contracts and other mechanisms that will set forth industry best practices for varying trust levels and authorities.

Application Examples

Here are a few examples of where an IOT trust network could be applied.

Home Network Control

Lisa is connecting her new door lock from AcmeLocks and goes through the installation steps with her home networking gateway. As part of these steps, she would initiate a sequence within the network gateway to verify and validate the new device. As part of the sequence, the Zigbee gateway would poll the device and read its make, model, and firmware version. The gateway would then search the IOT Trusted Device blockchain network for a certification record issued by the ZigBee alliance that would show the device is ZigBee certified.

Upon a successful validation, the user interface would confirm indicating certification, suggesting reliable operation. AcmeLocks would also be listed as manufacturer in the ZigBee certification record. Using this information, the gateway could find pending firmware updates that AcmeLocks posted to the ledger as well as a recent user manual. The gateway would give Lisa a choice to update the firmware as well as display or forward the manual for reading and review.

Additional Examples

- Mobile Device Network Access – This type of capability could be used to verify a mobile device's security level before trusting the device with network access, user credentials, or payment tasks. This device-level security check follows along closely with the Zero Trust security model in terms of verifying anything and everything trying to connect to a system prior to granting access.
- Malware Detection – This system could be used to verify the behavior of a sensor or device by comparing its behavior with what is perceived to be normal behavior from the same device or a similar/nearby device in order to identify malware or unauthorized access.
- Validate device certificate against registered manufacturer credentials for authenticity.

Challenges

Not surprising, there are a few challenges to address in order to arrive at a working solution. Here are a few at the top of the list:

- **Network Structure and Consensus** – One of the primary decisions would be how to structure the network – on a distinct permissioned blockchain, on a permissioned sidechain anchoring to a public chain, and/or some other type of hybrid approach whereby some data is public and used as a catalog/registry where other information is exposed on peer-to-peer basis. A related concern is the consensus algorithm to use and the node structure – first node operator, submitter, registrant, and verifier.
- **Third Party Access, Security, and Data Size** – Related to the point above – network structure and consensus – is how open the network will be to allow participation by new parties. It's one thing to access the data. It's another to be able to update information both with respect to security concerns as well as with data size and growth. The number of devices currently in use along with the estimates point to very large numbers. Adding additional attributes for each device increases the data size exponentially.
- **Record Attribution and Identity** – Another decision is how to establish trust in the submitted information with respect to the submitter's identity. Given the underlying cryptography, the submitter can be trusted to have the right credentials to post but there is and will be a question as to how to ensure the submitter is who they claim to be. This is no different than many current Web 2.0 solutions as well as blockchain solutions, just something that needs to be addressed – given the premise that records provided a "trusted" view of the device.
- **Network Incentives** – Rounding up the top list of challenges is how to create the right incentives for operating a network. A decentralized network is far different from a centralized hub when it comes to economic models, revenues, and costs. It's entirely conceivable that device manufacturers and network operators would support much of the costs for such a network either by funding development and/or maintaining nodes. Extending this operational capability to other parties (such as corporations who might want to use the data as part of their security authorization) would certainly extend the network reach and capabilities (assuming the inclusion of additional trust attributes). How the incentive and operational cost structure might work in this scenario is something that is not readily apparent and would need certainly need some study and attention.

Use Case 3: Data Privacy and Monetization

Contributor: SK Telecom
Authors: Inhyok Cha, Moojin Woo, Jaehan Lee, SK Telecom
Date: 07-Sep-2018

Background

Telecom operators across the world have been facing increasing challenges to their traditional business models. These challenges include increasing costs for infrastructure and data spectrum due to the exponentially increasing consumer demands for more data and fierce competition among telcos along with increased scrutiny from both the public and the authorities regarding telecommunication business practices.

One of the more recent challenges is due to growing awareness from the public as well as stricter regulatory stances by authorities regarding privacy and property rights of data that either belong to subscribers or may originate from subscribers. A few examples of this include:

- Data that subscribers own may include the subscribers' documents, images, videos, as well as information about the subscribers' identities, all or part of which subscribers may choose to store on telco-operated cloud services.
- Data where subscribers are the sources of generation may include SMS texts, locations, time, and contents of activities, stated likes, preferences, interests, and/or opinions, service usage patterns, purchase and/or payment histories, and more.

In almost all cases, telcos would only use data that they have been given explicit consent to use from the subscribers. The situation is more complicated, however, when one considers that many telcos are increasingly applying advanced data analytics, often backed by massive and centralized big-data infrastructures and use of advanced machine-learning (ML) methods such as Deep Learning and other similar techniques to extract ever more 'insights' about their subscribers.

This profiling is often done on an individual basis but is also performed in various 'groupings' or 'categories' as well. Such analyzed insights may include highly accurate estimates of people's characters, preferences, emotions, hobbies, political and other social inclinations, family and other social relations and networks, and behavioral and transactional predictions.

Many telcos are nowadays capable of analyzing each subscriber it serves in hundreds of 'categories' and forming integrated, comprehensive 'profiles. In many cases, telcos then could use such insights to optimize its business practices and processes, including optimization of its infrastructure construction and adaptive usages, as well as enablement of highly targeted digital marketing campaigns towards individuals and groups of individuals.

Problem

The reality of the situation is that even if subscribers have given direct and comprehensive consents for data usage to their telcos, they may not be very clearly informed of the breadth and depth of the insights that companies can extract from consented data. Also, in most cases, subscribers do not get direct monetary benefits from such insights in any way, although they often provide most of the data streams that are needed and used in the generation of such insights.

Meanwhile, in the outside world, consumer awareness about the ‘value of data’ and the ‘importance of data privacy’ is becoming more heightened. Recent outcries against data and privacy handling practices by global OTT services such as Facebook and Google YouTube suggest that telcos, who are similar handlers of massive amounts of data about their subscriber consumers, may be subject to an equivalent risk of public outcry.

Also, in the regulatory environment, the adoption of GDPR in EU is projected to cause increasing levels of hitherto unseen challenges to data handling organizations. The GDPR regimen contains significant measures regarding consent or other legal grounds for lawful processing, about data subject rights, privacy and putting back the control of personal data in the hands of people. Any compliance, therefore, clearly requires a perspective that addresses exposure and risk across broad reaches of data processing, storage, and transmission.

Voices from NGOs and even law firms advocating ‘MyData’, referring to data owners’ rights to not just derivative benefits but also to direct benefits from the data value-creation chain, are becoming heard in public spaces as well. Clearly, telcos are well advised to carefully study how they may best the situations by contributing to ease concerns from consumers as well as authorities while at the same time delivering innovative services to the subscribers while also helping to improve the corporations’ business performances.

GDPR Data Issues

The General Data Protection Regulations (GDPR) address three primary issues with respect to personal data. They include how to track personal data, privacy by design, and the right to be forgotten.

1. **How to Track Personal Data** – Personal data resides in many applications that span servers, data centers, geographies, internal networks, and cloud service providers. GDPR holds parties accountable for that data regardless of where it is stored. It also requires parties to be able to access, report, and remove personal information from all those systems when required by consumers or regulators. Tracking this flow of data and reporting on its use is still an ad hoc process and can benefit from formalization.

2. **Privacy by Design** – With respect to putting data privacy and proper and lawful use of individuals’ data at the heart of all the business, GDPR requires firms to take an approach known as "privacy by design". Under the privacy by design approach, data controllers must consider the privacy risks and data protection compliance from the start of a project involving personal data. Such projects might include the building of new IT systems, developing new financial products, drafting new policies, and sharing data with third parties. As such the opportunity is present for novel industry-wide approaches.

3. **The Right to be Forgotten**– The "right to be forgotten", as it has become known, allows individuals "to obtain from the controller the erasure of personal data concerning him or her without undue delay" if there are specified grounds to do so. The first (and most widely known) of these grounds is that "the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed". Another relevant ground is where the individual "withdraws consent on which the processing is based…and there is no other legal ground for the processing". Addressing this right in a way that does not conflict with the notification and reporting aspects outlined above can be complicated but certainly within the realm of new architectures.

Solution

Blockchain technology promises to enable a variety of decentralized services where the participants do not have to have to create or establish prior trust toward other participants. Ethereum in particularly via its support of Turing-complete smart contracts may be well suited to bring about solutions to the data-related challenges facing telecommunication providers.

When it comes to privacy by design, GDPR addresses pseudonymization and anonymization techniques. As any data stored on blockchain may constitute personal data, developers and companies which are likely to be subject to GDPR must limit the kind or amount of personal data stored on blockchain, and come up with new methods to anonymize data by utilizing some state-of-the-art technologies such as Zero Knowledge Proofs for the minimization of possible conflict with GDPR.

In terms of “the right to be forgotten”, personal data related to subscribers should be kept separate from the blockchain in an “off-chain” data storage because of the immutability characteristic of blockchain, with only its cryptographic hash value or evidence on blockchain platform. By doing so, personal data can be erased in case of subscribers’ request or specified grounds for deleting their information without impacting the integrity of the blockchain.

User Stories

Blockchain networks can be used to establish a record of data events and transactions. While the data of the event itself (i.e. the user, the particular use or notification) may not be included in the transaction record, a notation as to its occurrence might establish an immutable record its existence.

For example, a telecommunications service provider might generate and store ‘customer insights’ about individual and/or groupings of their subscriber customers – after collecting, processing and analyzing data provided by subscribers. In the course of this offering, they would notify individual or groups of customers of the availability of the new insight and offer to ‘return’ or ‘send’ such insight to the customers. These notifications might then be recorded into the Ethereum blockchain as having taken place at a time – with a link to permissioned records that would provide specific details on the notifications and their derivation.

Subscribers could either accept or decline such offer, where such indication might also be recorded on the blockchain as an event. If an offer is accepted, the telco service provider would send the insights, along with transaction metadata, to the respective customer. The sending mechanism may be by way of use of mobile phone text messages, in text or file formats, customer’s emails, cloud-based service accounts, or other mechanisms. The insight information is then stored in encrypted format in a repository – such as the mobile phone, SIM card, any other online or offline device, or a cloud storage – using the subscriber’s public key as the lookup key.

When an individual wish to ‘read’ the insight data, they would access the insights via the key, decrypt it using their private key (which would have been pre-installed or otherwise a prior provisioned to the individual), and privately consume it. (This access and decryption event might also be recorded on the blockchain.)

Any individual may wish to sell or trade the whole or part of the insight information to a third party or may wish to simply share it with a friend or other party. The individual’s indication of their wish to share, sell, or trade their insight information, along with some metadata describing it for the purpose of discovery by a third party, would also be recorded as an event. Such an indication could also be broadcast or similarly shared in a blockchain-based ‘marketplace’ like system.

If any individual or a third-party institute who participates in the blockchain-based ‘data marketplace’ finds a description of insight information that it may be interested in, a sharing-request, buy-signal, or trade-

signal may emanate and run through the marketplace. All such signaling may also be recorded via a blockchain record.

There may be third-party aggregator or broker who may aggregate insight information from multitudes of subscribers and sell or trade aggregated such information on behalf of the subscribers who offered up their insight information as well as any third party in demand of such insight information. The telco service provider may act as such an aggregator or a broker. Any share, sell, or trade activities are all recorded into the blockchain. The telco service provider may not directly sell the insight information in decrypted format. It may only direct the prospective customer to a link whereby the customer would be able to retrieve the stored insight information.

Benefits

In the scenario described above, individual subscriber may benefit by 1) becoming better informed about their own self (characteristics, preferences, behavioral tendencies, actual activities, etc.), and 2) being able to share such information either freely to selected parties or at a profit to parties who have demand for such insight information.

Blockchain technology may be used as a way of giving the ownership of the data or the value originating from it back to subscribers or users, which is impossible in the centralized architecture that has been dominant in internet services for the past decades.

The telco service provider may benefit by 1) forming a new relationship with its subscriber where the subscriber may feel better served, 2) thereby expecting to compete more effectively against its competitors, and 3) directly drawing newer revenues from transaction fees charged to customers of insight information in the marketplace. The authorities may benefit by being ensured that telco service subscribers' data privacy and property rights may be upheld in more transparent and immutable ways than before.

Challenges

Technical challenges include scalability and storage. Using a layer 2 solution (i.e. side channel or permissioned Ethereum-based ledger) could help solve the scalability issue as transaction throughput would be faster. Storage could also be handled via an offline solution that anchors records and data sets to the blockchain. This approach would reduce duplication of data as well as improve performance and data storage scalability. Pinning the data to the blockchain would preserve its authenticity by allowing verification of the data by users and third parties who have explicit permission to the data.

Use Case 4: Digital Contents Distribution Platform: Property Management and Distribution Market

Contributor: Takuya Sawada and Kenichi Suzuki, KDDI Corporation
Date: 10-Sep-2018

Background

Recently, telcos are facing fierce competition among MNOs and against MVNOs. Telecom services are now commoditized and under pressure to reduce service fees. Some governmental authorities are also putting pressure on telcos to lower prices for their services. Under these circumstances, telcos are looking for ways to increase customer loyalty and, thereby, reduce churn rate. They are looking for new revenue opportunities outside of traditional telco services.

Distributing digital content such as videos, audiocasts, images, even books distributed through telecom networks and consumed by their customers would be one way to generate revenues and provide increased value to customers. The amount of digital content to be consumed on digital devices (including primarily the phone is projected to grow dramatically, thereby representing a huge opportunity. New digital content distribution mechanisms can benefit from blockchain technology. Here's how.

Solution

To incentivize both content production and distribution, telcos could issue credits for use as rewards within distribution networks, thereby allowing the creation of new value chains. From a rights holders' standpoint, illegal copying and distribution of digital content is a huge problem, representing the loss of revenue as well as the potential compromise of authorized distribution channels.

It is also difficult to get revenue from secondary markets. With blockchain technology, smart contracts, and non-fungible tokens, it may be possible to resolve a number of these issues. Primarily it could help define mechanisms and workflows whereby revenues could be shared and distributed equitably to fairly reward content producers as well as promoters and distributors in secondary/non-traditional markets.

Note that, in these contexts, 'digital content' is not limited to video, audiocasts, music, or books. Many kinds of things in the world can be digitized and distributed. For example, event tickets, which is the right to see the event, is an area that could benefit from an incentivized distribution system.

Stakeholders

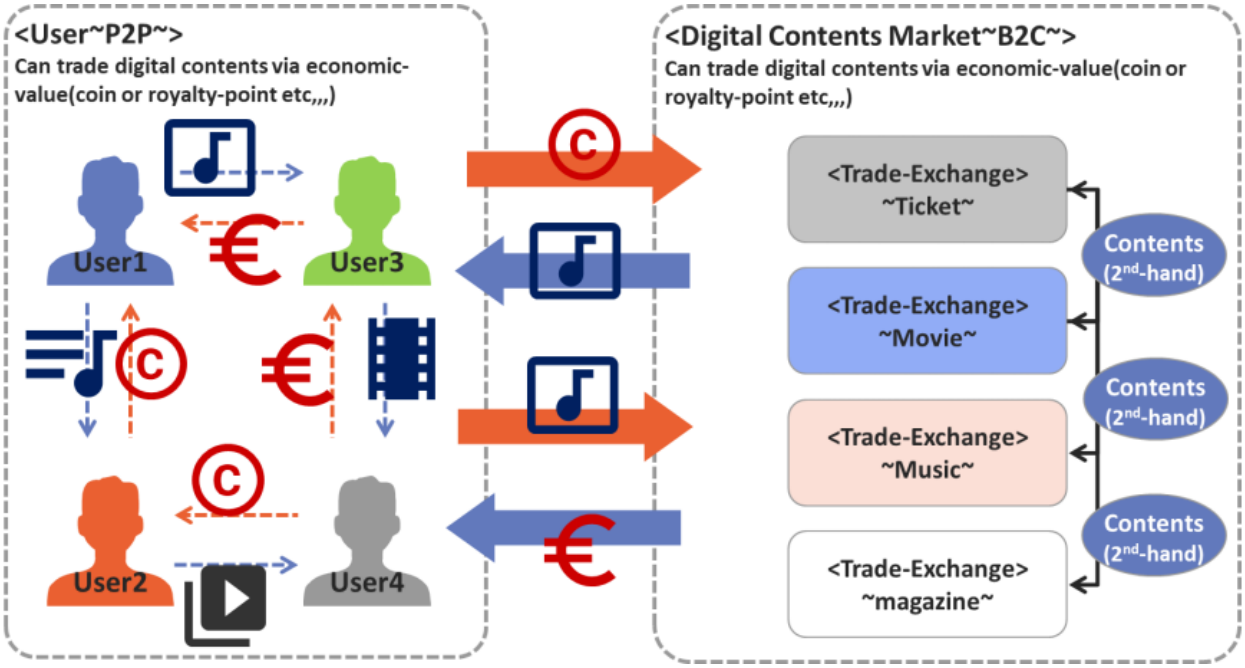
There are several stakeholders and beneficiaries in this type of model. Here's a breakdown of a few of them.

- Platforms
- Content Creators
- Content Owners
- Content Aggregators

- Users
- Promoters/Influencers

Here is a description as to how a content distribution platform might work using blockchain technology:

- Create mechanisms for registering and providing unique IDs for content via a nonfungible tokens (NFTs) or other digital ID formats.
- Support other types of distributable/promotable property that can benefit from a trackable and incentivized distribution system.
- Create smart contracts that support transfer of ownership rights (all or partial) and for other rights including distribution, promotion, creation of derivative works and other traditional IP rights. (The NFTs will allow for tracking and usage attribution.)
- Create smart contracts that calculate the distribution of royalties and other revenues between content creators, owners, distributors, promoters, and others in the value chain.
- Support mechanisms to aggregate royalties and allow for payment via cryptocurrency and/or other acceptable currency forms.
- Provide credits to consumers for consuming and/or rewarding content along with ways for users to increase their credits.
- Create mechanisms for tracking implicit rewards (i.e., attention/views/responding to surveys) as well as explicit rewards (tips, bonuses, direct fees, etc.)



Implementation Notes

- Telcos can use existing cryptocurrencies and/or tokens as the digital currency that would be used in the system.
- Telcos can provide methods for content registration and authentication, rights transfer, usage payments along with payment distribution, reconciliation, and settlement.
- Digital content could be stored in telco-managed storage networks in a secure manner with copy protection.
- Ethereum and similar blockchain platforms that support tokens and smart contracts can be used for registering content via tokens along with recording transfers, usage, and other actions for that token within the system.
- Ethereum can provide smart contract which can be used to support a variety of intellectual property transactions including transfer, copy, limited counts of access, limited length of access, and many more.

Challenges

- Ethereum by itself cannot guarantee the copy protection of the contents as it manages only the rights associated with the token when the content is associated with the token. Content could get separated from the token (by copying it directly from the user device and then introduced into the content stream as an unauthorized copy). Fingerprinting and content analysis could help reduce unauthorized content.
- Scalability will also likely be an issue although as with other use cases, improvements to the Ethereum mainnet as well as Layer 2 solutions shows promise in resolving this concern in the not too distant future.

Use Case 5: CX in SDP Delivery Models

Contributor: Consensus Systems (ConsenSys)
Authors: Dr. Andreas Freund, ConsenSys
Date: 31-Aug-2018

Problem

Quality issues in inter-carrier service relationships in the telecom industry are both legion and legend. Although modern technology has brought great improvements in this area, the root cause – misaligned business goals between untrusted counterparties – remains unaddressed.

Telecom service providers are often more economically incentivized to provide cheap and fast service rather than fast but higher quality service at reasonable prices. This has been the case for the last 50+ years because the necessary mechanisms to provide the proper quality control and its enforcement are for the most part very (human) resource intensive.

The advent of blockchain technologies, however, is starting to shift since one can for the first time execute functional contract terms in an automated, tamper-proof, and collusion-resistant manner. This technical shift opens the door to combine blockchain's consensus mechanics on the state of a business event along with game theory and incentive economics to align and encourage business partners to provide good and fast service at reasonable prices.

Aligning Business Goals around Business Outcomes

Behavioral psychology shows us that improperly structured economic incentives and self-interested behavior of participants often leads to unintended and economically bad consequences. For example, Staples had an incentive program in place in 2012 where in-store associates only received full commission credit for selling a computer with at least $200 worth of accessories (Temkin, 2012). The consequence: Staples store associates only sold computers if the customer wanted to buy at least $200 worth of accessories. This led to massive drops in computer sales until the incentive program was stopped.

Something similar is happening throughout the telecom industry. Only low costs and speed are directly economically incentivized, whereas quality is often not. It is assumed that there is high or at least sufficient quality and only failure to provide quality is penalized but most often in no proportion to the economic incentives given to speed and costs. Furthermore, the process of applying penalties is cumbersome and often costly due to required litigation.

Consequently, the Telecom industry has significant quality issues in B2B service partnerships where quality cannot be as easily ascertained as through a non-functioning wifi router from a hardware vendor.

Solution

The question to be answered, therefore, is how we can align business goals of all telecom ecosystem participants. The answer is surprisingly simple, yet its implementation has been difficult up until now. The solution is for the service recipient to receive the same type of value incentive as the service provider. This means both parties would receive both rewards and penalties to be automatically enforced in a collusion-resistant and tamper-proof manner through blockchain smart contracts (Wood, 2015).

Constructing Economic Incentives for B2B Service Partnerships in the Telecom industry

Constructing economic incentive models is difficult (Carpenter, J. et al., 2009 and references therein). Crowding out of desirable behavior in different forms occurs due to economic incentives and enforcement of incentive rules requires a good understanding of the underlying population of participants. Whereas the latter is hard for large ecosystems, in a business setting, it is significantly simplified since there are incentives to do business with one another: All parties have things other parties want and typically informal relationships for a majority of business relationships are long-lasting establishing a significant "trust" factor.

However, this "trust" factor is only at the executive level of the pyramidal hierarchy and not at the operational level where it matters. This means that trust is formally only established at the legal contract level and not at the operational level, even within companies. This very fact leads to significant business goal misalignments amongst companies and even within companies.

Given the above, let us construct a simple, yet generally applicable incentive model that will meet our needs for the Service Provider and the Service Recipient:

1. Upon self-verified completion of a service task with a well-defined business outcome such as installing and activating a new receiver in a home, a service provider is paid X% of a previously agreed service fee $Z in real-time, with X > 50%, or < 50% depending on the nature of the service and business relationship. No price discount is provided by the service provider to the service recipient for Net + 0 payment terms. Y% of the service fee such that X% + Y% = 100% is put into an escrow function to account[1] for a period of A days, where A days represents a normal payment period such as 30 days, or 90 days. After the A day period is passed, the escrowed amount is paid out to the service provider through a token to fiat exchange function. The percentage Y of the service is called the economic stake of the service provider and the percentage X is the stake of the service recipient[2] .
2. The service recipient receives the completion of the service task in the agreed-upon KPIs such as MTTR, Complaint Rate, etc. and agrees to the above payment terms.

In addition, as we will see below, we need the function of a Business Outcome Validator or Auditor. Auditors function as independent validators of business outcomes. The Auditor population should be large and anonymous, or at least pseudonymous, to the business ecosystem participant.

The use of auditors can be triggered by a variety of business conditions related to the state of a business outcome. However, in a service scenario, they will be used either if a complaint about a service task has been filed or a completed service task is audited as part of a service provider agreement.

Similar incentive rules that are applicable to a service provider and a recipient are also applicable to the Auditor:

1. The Auditor will be compensated for their service through a token reward. The size of the reward depends on the value-at-risk; however, should be significant enough to incentivize participation, e.g. one could either make a living off this service or significantly supplement an already existing income source. There are two available options to realize this:

[1] Tokens in a Blockchain smart contract representing the appropriate fiat currency amount e.g. 50 tokens = $50 AUD

[2] Note the stakes are treated differently. The service recipient stake is the real time payment and cannot be clawed back automatically, whereas the service provider stake is the escrowed funds that can be taken away if malicious action is detected.

a. Service recipient and provider contribute in equal parts tokens that are tied to fiat currency to an escrow function. In this case, it is recommended that both parties provide a percentage of the annual value of a service contract.

b. Each time an auditor is rewarded, the token reward is "minted" by the platform. We will discuss what we mean by the platform when we talk about implementations.

2. For Auditors to have "skin in the game", they will have to escrow a token stake that is significant enough, on the one hand, to deter malicious behavior by the auditor, on the other hand, low enough that it does not deter participation. There will be several instances, see the next section, where Auditors will have to escrow a token stake to economically participate in the business ecosystem.

Care must be taken such that the rewards and stakes/penalties of the incentive system are set in such a way that they do not incentivize the wrong behavior as happened in the case of Staples. This will require some experimentation through pilot studies to find the right configuration of the above model before applying such an incentive model more broadly in a business ecosystem.

Description of a Secure Economic Incentive-Driven Consensus Model to Align on Business Outcomes

After having discussed the economic incentive model, we now need to discuss the behavioral enforcement mechanism. On the surface, this is rather simple, if all participants behave honestly and have the right processes in place such that the contractually agreed upon KPIs are met, then there are no issues and we have achieved the goal of high or good quality service at reasonable prices in a reasonable amount of time.

However, in order to discourage malicious behavior such as lying about completed service tasks, colluding with other service provider or auditors, we need a rule enforcement process that can be trusted by all participants. For this to hold the process needs to be tamper-proof and collusion resistant. We will discuss this feature in our security analysis. The enforcement process is modeled as a consensus process for Auditors validating either a claim of poor quality of a business outcome or malicious behavior or a randomly selected business outcome that has completed and can be described as follows:

Auditor Signaling

- At the beginning of the predefined time period, called an epoch, say three months, an Auditor signals through a token stake[3] if they want to be a business outcome auditor. Participants who are not staked cannot be Auditors.
- Business outcomes that require validation based on outcome specific rules agreed upon by the impacted business partners are assigned a random set of an uneven number of auditors from the set of signaling auditors. The assignment is done "in the blind" such that auditors do not know who else has been assigned to a specific audit task to avoid collusion
- Signaling auditors determine how many outcomes they want to validate in a given epoch. A signaling Auditor has to participate in validation processes they have chosen. If they do not choose any assigned validation processes, their initial stake will be slashed through the burning of the staked tokens. Signaling Auditors will be automatically unbonded at the end of an epoch unless they are involved in an unresolved outcome validation process. See discussion below.

[3] Corresponds to a certain value in fiat currency e.g. 1 Token = $1 AUD

Auditors can, however, choose to stay bonded. A signaling Auditor cannot unbound the stake during the epoch he or she signaled to participate in validation processes.

- Auditors need to stake each outcome they want to validate with an additional token amount as a security deposit

Auditor Voting

- After inspection, the selected auditors vote on the assigned business outcome during the voting period given in the number of epochs which is determined ahead of time by the counterparties to the business outcome
- The auditors in the consensus majority on an outcome to be validated receive in equal parts the stake of the auditors that were in the minority in addition to any other rewards assigned to them such as contractual agreement rewards as discussed in the previous section
- If the auditors agree with the outcome, the stake of a participant such as the service recipient or service provider who wanted an outcome validated or disputed an outcome is returned minus a validation fee to be equally distributed amongst the auditors who formed the majority vote. If not, the stake of the participant is distributed in equal parts to the auditors who formed the majority vote
- If a selected auditor did not participate in the outcome validation to which they were assigned, the actor will lose their posted stake at the end of the voting period for a validation event

Vote Revealing

- Votes by auditors are submitted as cryptographic commitments in order to avoid gaming the vote
- After the voting period for a validation event is over, the participating auditors who have submitted votes, need to reveal their commitment by submitting the hiding key of the commitment and open the vote. If an auditor does not reveal their commitment(s), they will lose their stake (tokens are burned) at the beginning of the next epoch.
- If the vote on an outcome is a tie through no-votes or no-reveal, the validation process repeats at the beginning of the next epoch with a random selection of signaling auditors.
- The stake of the auditors is not returned but rather added to their outstanding stake to further incentivize participation.

Objections

- Any participant such as a service provider or service recipient can raise an objection to the auditor consensus in the epoch during, E, or immediately after, E+1, the auditor consensus was reached by requesting a 2nd round of validation by another set of randomly selected auditors during the epoch, E+1. In order to raise an objection, a participant needs to provide a stake for the objection in order to avoid spurious objections spamming the system. The size of the required stake is determined as a percentage of the value-at-risk of the business outcome
- If the new set of auditors agree with the objection, then the participant raising the objection receives the stake plus a percentage reward from the original stake associated with the business outcome as well as the stake of the initial set of auditors. The new set of auditors receives the remaining stake of the initial auditors who were contradicted by the second set of auditors. The

exact percentages need to be specified either within a platform or on a case-by-case basis. In both instances, the consensus process parameters are determined by the consensus of the participants in the business ecosystem.

- If the new set of auditors disagree with the objection, then the objecting participant loses its stake. The stake is distributed in equal parts amongst the auditors that confirmed the conclusion of the original auditor set.

The above process requires that each Auditor has a unique digital identity that has been validated by an agreed-upon set of participants in the business ecosystem to be able to hold individual entities accountable through their economic stakes.

Benefits

- **Economic & Customer Experience Benefits:** We have constructed an incentive model and consensus algorithm, that aligns business goals of B2B service partnerships in the Telecom industry around specific business outcomes that are independently verifiable in a tamper-proof and collusion resistant manner. We believe this model to be a significant improvement for the Telecom industry to achieve significantly higher quality service outcomes at lower costs than before.
- **Security Benefits:** We have performed a game-theoretic security analysis of the economically incentivized consensus model and shown this model to be a highly secure process. In addition, we discussed platform security in the same game-theoretic analysis framework. Lastly, we gave implementation considerations in terms of high-level requirements to implement the model on a permissioned Blockchain platform with economically incentivized consensus and capable of support business logic through smart contracts.
- **Regulatory Benefits:** The economic benefits and improved customer experience, in turn, will likely ease regulatory burdens currently in place due to the systemic quality issues in the industry.

Privacy, Security

- DIDs are pseudonymous not fully anonymous. However, as long as no PII is used in the above use case and no mnemonics are derived from PII, the privacy of individuals and institutions data is guaranteed.
- Security is based on standard cryptography for encryption and authorization protocols such as OAUTH or DID-AUTH.

Security-Related Challenges

There are several types of attacks against possible against the above described incentivized consensus process. We will discuss them one by one and how the above system and possible implementation either avoid such scenarios or make them economically unattractive.

1. **Business Ecosystem Collusion Attacks:** Service Providers or Service Recipients can collude to bribe Auditors or Auditors can collude together to for example extort service providers or service recipients or to maximize their collected fees/rewards. The defense against such type of attacks are:

a. Auditors are randomly selected in the blind and with short voting windows, a large auditor pool[4] and the possibility to detect collusion and submit it as a malicious action by any participant which would lead to a significant economic loss (burning or redistribution of the stake), the probability of such attacks is low. In order to ensure a continued high level of security, during pilots and in production the grievance factor[5] should be >> 1.

b. Service Providers have even higher stakes than individual auditors and similar arguments as applied to Auditors apply to this actor group as well.

c. Service Recipients have stakes in the validation of business outcomes they request and are, therefore, incentivized to behave honestly as well. In order to ensure enough economic "skin in the game", the stakes for submitting a validation requests for a business outcome, unless it is an agreed-upon audit event, should be high enough to discourage collusion with Auditors since, if found out, the stake would be lost including those of the colluding Auditors.

2. **Extortion Attacks[6]:** Since neither service providers, service recipients nor auditors will have an influence on one another to submit a transaction and cannot process transactions, transaction censoring is not possible. Therefore, extortion of economic gains through transaction censoring is not possible from these participants. Transaction censoring by platform nodes with the aim to extort, however, is possible, but through the usage of the right economic consensus model for platform nodes such as Proof-of-Stake with Slashing conditions such as Casper FFG (Buterin, 2017) for Ethereum, can be very costly economically, if discovered. Other forms of extortion attacks by service providers, service recipients or auditors use economics means to fall under the category of collusion attacks which we have discussed already.

3. **Discouragement Attacks[7]:** In our scenarios, such an attack can only be launched by Auditors and platform nodes. As described above, we are slashing the stake of Auditors who are trying to delay or obstruct the voting on a business outcome through non-voting. And inconclusive voting triggers another round of voting until a conclusion on an outcome has been reached with the stakes of all Auditors and participants rolling over into subsequent epochs. Non-participation in outcome validation processes after signaling participation also leads to a loss of stake. Platform nodes can go offline in order to make reaching consensus impossible in a proof-of-stake consensus model[8] or censor transactions as already discussed. Again, there exists economic consensus models with a mathematical proof of security such as Casper FFG that can be employed to make such an attack economically too costly.

[4] The larger and the more diverse the auditor pool is the less likely it will be they can coordinate amongst one another successfully -- law of large numbers

[5] The grievance factor of an incentivized consensus algorithm is defined as the ratio of the sum of penalties of malicious actors to the sum of penalties of honest actors in case of a consensus failure

[6] An actor set A of size > ½ of the total set of actors participating in a consensus process such as running a Proof-of-Stake protocol of a Blockchain or another economic action in which actor set A can censor, charges an extortion fee, f, to participants and censors those who do not pay the fee, f.

[7] An attacker set A acting maliciously within an economic consensus model in order to reduce other validators value gain, even at some incurred value loss to themselves, in order to encourage the attacked actors to drop out of the consensus model

[8] For Proof-of-Work consensus models such an attack is not possible.

4. **Value Extraction Attacks**[9]**:** Such attacks are not possible in our business scenario since we are in a closed business ecosystem where the exchange mechanism between tokens and fiat currency is tightly controlled.
5. **Time-Based and Transaction-Ordering Attacks:** Since neither service providers, service recipients nor auditors will have an influence on one another to submit transactions and cannot process transactions, transaction ordering attacks are not possible. However, they are possible for platform nodes. Yet, this can be circumvented using Trusted Execution Environments such as Intel-SGX that allows one to do a random transaction ordering that cannot be tampered with from the outside since it is a black box and comes with a cryptographic proof of correctness. This effectively takes away the ordering attack vector. Time-based attacks for platform nodes are also no longer possible with such a trusted ordering service for each node. In addition, time-based attacks are only possible for Auditors during voting. However, since we are employing blinded votes, any timing-based attack on a visible vote count is not possible.
6. **Transaction and Data Tampering Attacks:** These types of attacks are virtually impossible in decentralized processing platforms employing Blockchain technology that also use economic consensus models such as Bitcoin's Proof-of-Work or Proof-of-Stake. The only known form of this type of attacks is the so called 51%-attack, where 51% of either the compute power or the economic stake is controlled by a malicious set of platform nodes. This would allow for creating an alternate Blockchain with altered transactions and data. Such an attack is very costly and has not been successfully executed against any larger Blockchain network.

Implementation Considerations

Given the above security analysis, we can now give implementation requirements:

1. **Platform:** In order to ensure tamper and collusion resistance, a Blockchain stack that allows for business logic execution through smart contracts and has an economically incentivized consensus algorithm with a mathematical proof of security. We recommend a Proof-of-Stake consensus algorithm since the platform nodes should be permissioned, in contrast to for example Bitcoin or Ethereum, through the platform itself should be open.
2. **Digital Identity:** We recommend integrating a proven Decentralized Digital Identity Provider such as uPort, Sovrin, Blockstack or Microsoft for to provision platform identity and, in order to reduce complexity, leverage the Decentralized Identity Foundation's Identity Hub reference implementations[10] for identity integration. To reduce the platform failure points, we recommend a decentralized access control system by leveraging the aforementioned identity systems as an access control layer.
3. **Incentive Model:** The incentive model can be created through a smart contract system built upon a Blockchain stack that allows one to freely define tokens and their value based on the business needs and easily build any desired business logic.
4. **Consensus Model:** The consensus model can be created through a smart contract system built upon a Blockchain stack that allows one to freely define consensus rules and easily build any desired business logic. The model can leverage the provided digital identity system integration to enable unique identification of participants.

[9] An actor set A is intentionally extracting value from an ecosystem in order to subvert its function or in order to collapse the ecosystem by exploiting an open value process such as through a token exchange without value reciprocation such as through revenue sharing through another value process

[10] To be released soon and currently under development by the Decentralized Identity Foundation

5. **Exchange Facility:** Since we are dealing with economic value, there needs to be an exchange facility built using smart contracts that allows one to exchange tokens to fiat currencies and vice versa leveraging escrow accounts at banks that require a multi-signature approach to unlock funds related to platform token stakes. This facility needs to be defined and controlled by the platform governance body and should best be run by a 3rd party such as a bank.

References

Temkin, B. (2012). “Why Staples Refuses to Sell Computers to Customers”, Retrieved from: https://experiencematters.blog/2012/12/05/why-staples-refuses-to-sell-computers-to-customers/

Wood, G. (2015). “ETHEREUM: A SECURE DECENTRALISED GENERALISED TRANSACTION LEDGER”, Retrieved from: https://ethereum.github.io/yellowpaper/paper.pdf

Carpenter, J., et al. (2009), “Strong Reciprocity and Team Production: Theory and Evidence.” Journal of Economic Behavior & Organization, vol. 71, no. 2, 2009, pp. 221–232., doi:10.1016/j.jebo.2009.03.011.

Buterin, V., Griffith, V. (2017) “Casper the Friendly Finality Gadget.” Ethereum Foundation, Retrieved from: https://github.com/ethereum/research/blob/master/papers/casper-basics/casper_basics.pdf.

Use Case 6: Identity Attestation Flows for ISP Services and Components for Abstract API Creation

Contributor: Consensus Systems (ConsenSys)
Authors: Dr. Andreas Freund, ConsenSys
Date: 12 September 2018

https://hackmd.io/Ij5bT35sTwWolJ0qeirQMg

Abstract

In this document, we define a set of user flows and describe the associated Message Objects that support an agent-centric approach to the request, issuance, presentation, verification, and revocation of interoperable attestations. Such attestations can then be used in, for example, identity access management, service access management, account management, etc.

1. Introduction

In the digital world, identity needs to be able to prove that some data is true to another entity that requests it. The attestations discussed here are the method of proof. The requester may be software, and the response may or may not require the involvement of the individual/identity who the proof is being made against. These examples and flows depict how attestations are requested and resolved. We use Identity as it relates to the concept of decentralized identifiers (DIDs) and their associated document objects as per the W3C specification, see details below.

2. Example Use Cases

We use examples here to give guidance/suggestions for how attestations can be used with real-world telecom examples. The overall use case is a person, Alice, who registers for an ISP provider account using a process that includes using an attestation she possesses to prove she holds the required proofs to the claims that are required to open an account such as a driver's license or a credit card. After the account opening, Alice requests an attestation from the ISP that she is now a customer of the ISP provider, and presents that attestation to another telecom provider to, for example, access a service or purchase a specially discounted product.

Agents

We use the term "User Agent" (UA) to refer to an app on a smartphone or other device that has access to DID-linked keys and the power to do things on behalf of a DID owner (Alice). Similarly, we use the term "Enterprise Agent" (EA) to refer to the comparable component representing an Organization – e.g. an ISP provider. A UA and EA are conceptually the same, but while the UA is likely a personal device such as a laptop, a tablet or a phone, an EA is likely a service that processes requests based on business rules and data held in back-end systems. Note that an EA might need input from a specific member of the

organization to complete the processing of a request. In that case, the EA might contact that user through that person's User Agent (although there are many other possibilities).

Sites

In the examples below, "Sites" are assumed to be Web or Mobile Site – user interfaces that allow a user (Alice) to trigger the start of a process. Naturally, there are many other ways to trigger the start of such a process.

Decentralized IDs (DIDs), Documents and Attestations

Each of Alice's Decentralized Identifiers (DIDs) referenced in the scenarios are generated and held by her user agent (UA) and used for a specific purpose - for example, her relationship with the ISP. Her DIDs are not necessarily correlated to any other identifiers that make up her identity. Per the W3C DID Specification, a DID Document is associated with a DID that contains information about the public keys and service endpoints for that DID. Thus, given a DID and DID Document for another Identity, an entity has a mechanism to resolve and communicate with the Identity Owner of the DID. DIDs may be public and stored on a publicly available Distributed Ledger, with their associated DID Document found via a mechanism such as the DIF Universal Resolver, or might be pairwise private DIDs, where two Identities directly exchange DIDs/DID Documents using a message service.

An attestation is something (such as a Verifiable Credential) issued by an entity to a holder (often the subject of the attestation). The holder can then prove to others that they hold the attestation.

Interface Guidelines

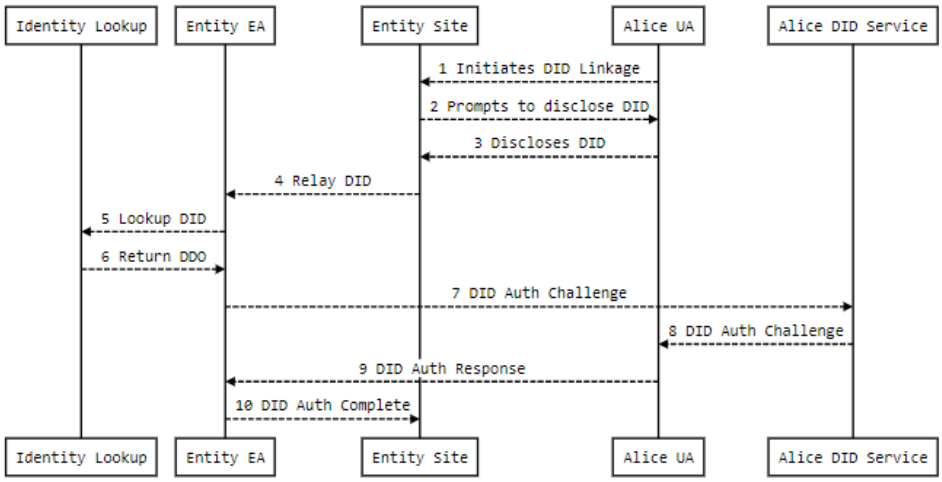
Some basic guidelines can be defined such as:

- Private keys are accessible only to Agents (User and Enterprise), thus any encrypting or signing of information must be done by an Agent.
- In general, services used by identities are addressable using the service pointers located in a DID Document, and Agents are addressed via user-aware services. The only exception is the invocation of a User Agent through direct mechanisms such as a deep link on a mobile site, a QR code on a Web site scanned by a User Agent, or a Bluetooth/NFC data exchange.

2.1 Alice Links to an Entity

In order to communicate a request for attestation to an entity (in our examples, Alice to an ISP), a user will first need to establish a connection between her user agent and the entity she will interact with. This is necessary for all follow-on scenarios.

Alice wants to transact with the entities described in the scenarios with the intent to receive or exchange attestations. First and foremost, the entity must verify that Alice is the owner of the decentralized identifier she claims is in her control. In order to find Alice's user agent, a service such as the Decentralized Identity Foundation's (DIF) Universal Resolver (UR) has to exist to look up Alice's Decentralized Identifier (DID), and subsequently retrieve her DID Document Object (DDO). The keys located in Alice's DDO are used to authenticate Alice's ownership or control of the DID and to determine access to Alice's identity hub and user agent.

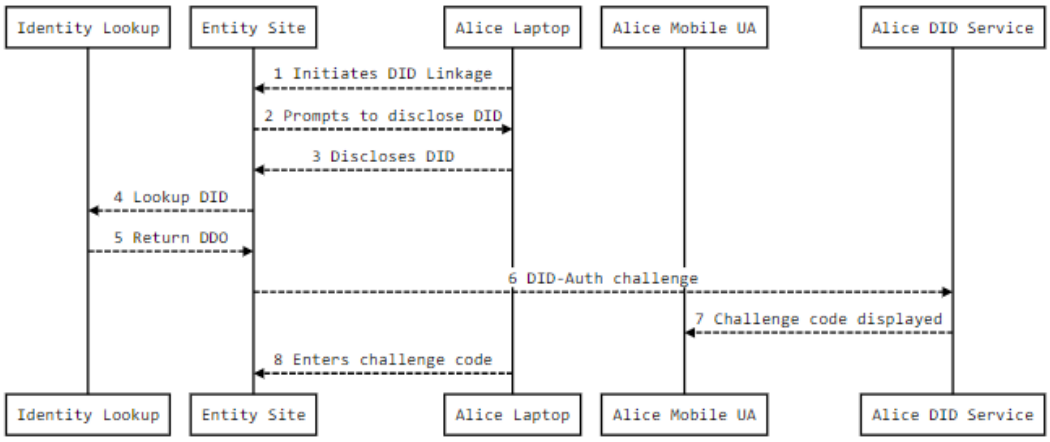


1. Alice navigates to an entity's website and clicks a link to initiate a DID linkage with the entity. The content received from clicking the link includes DID information about the Entity that Alice should use for the relationship.
    - Alice may have to use a DID Service such as the DIF Universal Resolver to access the DID Document associated with the DID.
2. The entity prompts Alice to disclose a DID that represents her digital identity.
    - If the website was accessed via a laptop/desktop, the website typically displays a QR Code, and Alice uses her mobile wallet app to scan the QR. If the website was accessed via her mobile device, a protocol handler raises Alice's UA app.
3. Alice selects an existing DID or creates a new DID for this relationship and sends the DID to the Entity Site.
4. The Entity Site passes the DID to the Entity's Enterprise Agent to initiate the DID Authentication (DID-Auth) response.
5. The EA uses the Universal Resolver (UR) to request retrieval of the DID Document that matches the provided DID.
6. The DID Document is returned to the EA.
7. The EA initiates the DID-Auth process by issuing a challenge to Alice's Identity Hub.
8. Alice's Hub passes the DID-Auth challenge to Alice's User Agent for signing.
9. Alice's User Agent proves her identity with a signed response to the DID-auth challenge.
10. The Entity's Identity Hub confirms the response and notifies the Entity Site of the successful establishment of a relationship such as a login.

Two Factor Authentication (2FA) without a User Agent

A second identity linking scenario to consider is when Alice is registering with the site using a device that is not a UA, yet she still wants to use her UA to establish the connection. In this case, Alice discloses a DID connected to her UA to the site, the site contacts the UA and the mobile

device containing the UA and displays a code for Alice to use. Alice enters the code into a form on the site, proving that she controls the DID.



1. Alice navigates to an entity's website and clicks a link to initiate a DID linkage with the entity.
2. The entity prompts for Alice to disclose a DID that represents her digital identity.
3. Alice selects an existing DID and sends the DID to the Entity Site.
4. The Entity's EA uses the DID Service to request retrieval of the DID Document that matches the provided DID.
5. The DID Document is returned to the Entity's EA.
6. The EA initiates the DID-Auth process by issuing a challenge to Alice's DID Service.
7. Alice's DID Service passes the DID-Auth challenge to Alice's UA for signing.
8. Alice's UA processes the challenge and displays a code expected by the Entity Site on the mobile device.
9. Alice enters the code on her laptop and the Entity Site confirms the response, resulting in a successful login.

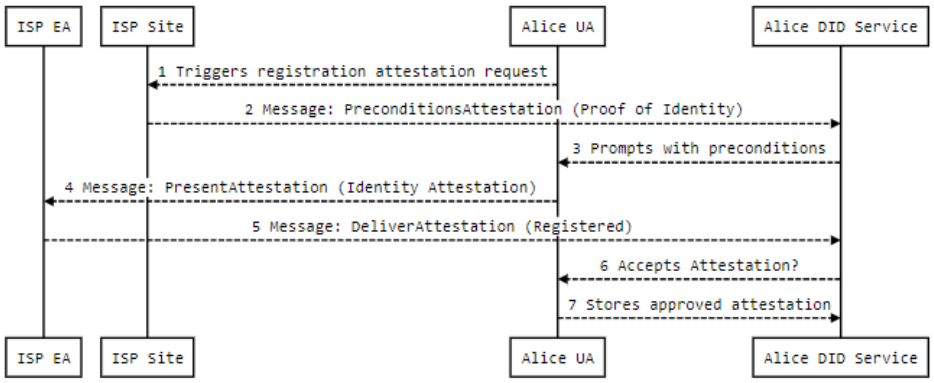
2.2 New Account Opening for Alice

Alice is attempting to open an ISP account and her DID is not linked to the ISP. In this example, she must first link her DID to the DID of the ISP and then present proper proof of identity from another trusted source such as a bank or another telecom provider.

Assumptions

- Alice has a DID Service accessed via an application on her mobile device.
- Alice has a verified digital attestation for her identity from a trusted identity provider.

Alice performs a DID Authentication as described in section 2.1 to link her DID to the DID of the ISP. After this has been completed, Alice proceeds with the account opening process.



1. Alice initiates a Registration request on the ISP site.
2. The ISP's EA determines that there are preconditions for Registration: she must prove she has a valid proof of identity. The ISP's EA initiates a request for presentation of the preconditions.
3. Alice is prompted by her UA to provide the preconditions.
4. Alice selects the correct attestation to use and her UA sends them back to the ISP's EA.
5. The ISP provider EA processes the preconditions and sends a Registered Account attestation to Alice's DID Service.
6. Alice accepts the request to accept/store the account attestation.
7. Alice's DID service stores the account attestation and broadcasts it to her connected devices.

Referenced Action Objects

- PreconditionsAttestation
- PresentAttestation
- DeliverAttestation

2.3 Alice wants to reopen an account

Alice is attempting to open an ISP account and her DID is already linked to the ISP (old customer for example). In this example, she must prove that she previously has received appropriate account attestations.

Assumptions

- Alice is linked to the ISP via her DID.
- Alice has a DID Service accessed via an application on her mobile device.
- Alice has a verified digital attestation for her previous account with the ISP.

1. Alice initiates a Registration request on the ISP site.
2. The ISP's EA determines that there are preconditions for Registration: she must prove she has the proof for the old account. The ISP's EA initiates a request for presentation of the preconditions.
3. Alice is prompted by her UA to provide the preconditions.
4. Alice selects the correct attestation to use and her UA sends them back to the ISP's EA.
5. The ISP's EA processes the preconditions and sends a Registered Account attestation to Alice's DID Service.
6. Alice accepts the request to accept/store the reopened account attestation.
7. Alice's DID service stores the reopened account attestation and broadcasts it to her connected devices.

Referenced Action Objects

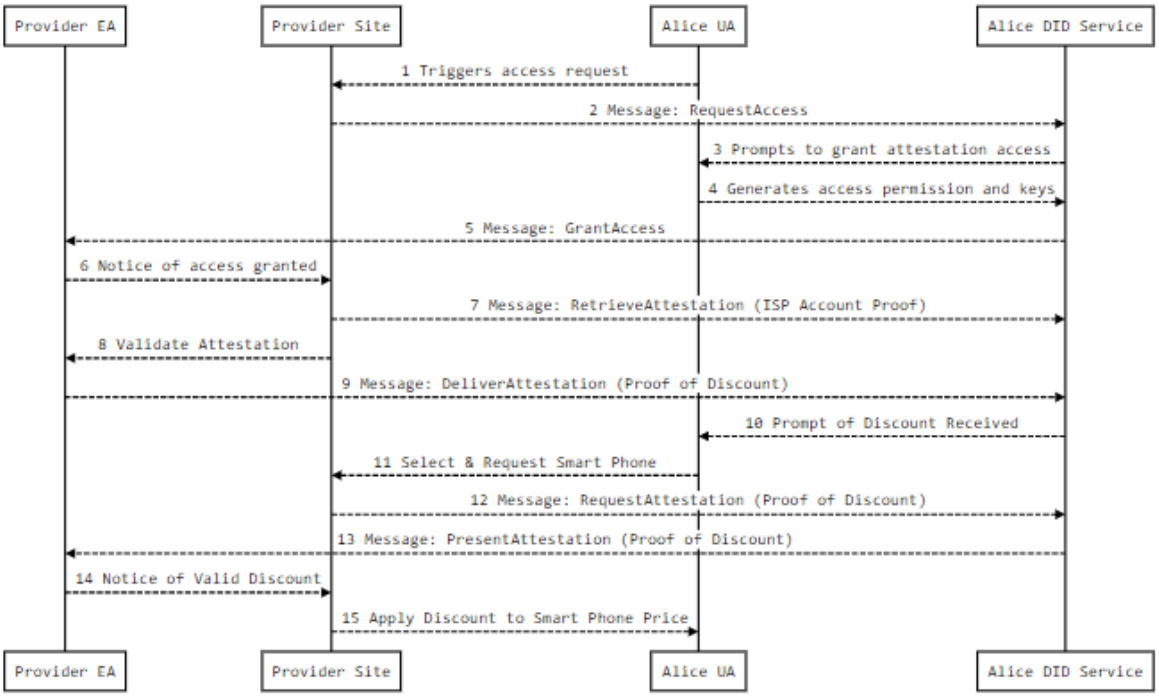
- PreconditionsAttestation
- PresentAttestation
- DeliverAttestation

2.4 Alice accesses a Service or Benefit with Her ISP provider account attestation

Alice possesses an account attestation from her ISP, and she wants to buy a discounted smartphone from another telecom provider that is part of her ISP's partner program.

Assumptions

- The provider site has linked Alice to her DID via DID Auth.
- Alice has a DID service accessible via an app on her mobile device.
- Alice possesses an account attestation from her ISP.



1. Alice navigates to the provider site and initiates the flow to request access to a discounted smartphone.
2. The website sends a RequestAccess Message to Alice's DID Service.
3. Alice's DID Service relays the request to Alice's UA, which prompts her to grant/deny access permission.
4. Alice grants permission to access her ISP's account attestations by pushing a signed permission object and DID-specific keys to her DID Service.
5. Alice's DID Service stores the keys she generated for the provider site and relays a GrantAccess Message to the Provider EA to provide notice that its permission request has been granted.
6. The provider site is notified by its EA that the access permission has been granted to Alice's DID Service.
7. The provider site sends a RetrieveAttestation Message to Alice's DID Service which returns the ISP provider account attestation to the provider site.
8. The provider site requests that the EA validates the attestation.
9. The provider EA validates Alice's attestation and delivers the Discount attestation to Alice's DID Service through a DeliverAttestation Message.
10. Alice's DID service prompts Alice in her UA that the discount has been delivered.
11. Alice selects and requests a smartphone on the provider's website.
12. The provider's site sends a RequestAttestation Message to Alice's DID service to retrieve the discount attestation to be applied to the smartphone purchase.

13. Alice's DID Service sends a PresentAttestation message to the provider's EA.
14. The provider EA sends a notice of a valid attestation to the provider site.
15. The provider site applies the discount to the smartphone price.

Referenced Message Objects

- RequestAccess
- GrantAccess
- RetrieveAttestation
- RequestAttestation
- DeliverAttestation
- PresentAttestation

Message Objects

Identity Hub attestation handling relies on the passage and recognition of common Message types that DID Services, User Agents, and consuming apps/services understand. In order to ensure that the flows related to attestations are precise and maximally descriptive of their intent. These objects are extensions of the Schema.org Action object, the schema origin of which shall be schema.entethalliance.org. These objects are strictly a shared means of communicating and facilitating the various activities related to attestations; they do not infer or require a specific type of proof format or material be used within them.

The following is a description of the list of objects (more complete – not included in the above limited examples) and examples that encompass their structure and properties:

RequestAttestation

The Holder requests an attestation from an Issuer.

- Type of attestation wanted
- List of tag strings to describe the attestation
- Detailed, human-readable description of the attestation being requested (mostly for UAs to display to users)
- Who is the attestation for?
- What format do you need it in?
- Enable passing of preconditions
- Option to set a deadline for issuance/fulfillment

```
{
  "@context": "http://schema.entethalliance.org/",
  "@type": "RequestAttestation",
  "identifier": UNIQUE_ID,
  "for": ["did:foo:123-456"],
  "format": CLAIM_FORMAT,
  "expiration": EPOCH_TIME,
  "description": "California Driver's License",
```

```
  "tags": ["license", "driving", "permit", "DL", "driver's license"],
  "preconditions": ARRAY_OF_PRECONDITION_PROOFS (optional)
}
```

DenyAttestation

In response to a request for an Attestation, a Verifier/Issuer informs a Holder that the attestation cannot be provided. This Message inherits from schema.org's RejectAction.

- Linked attestation action ID
- Reason for refusing the Request Attestation Action.

```
{
  "@context": "http://schema.entethalliance.org/",
  "@type": "DenyAttestation",
  "identifier": UNIQUE_ID,
  "purpose": "We cannot open your account, you have presented insufficient proofs."
}
```

PreconditionsAttestation

In response to a request for an Attestation, a Verifier/Issuer informs a Holder a list of Pre-Conditions that must be met before the requested Attestation can be issued.

- Linked attestation action ID
- Specify a set of preconditions, each with their own descriptors

```
{
  "@context": "http://schema.entethalliance.org/",
  "@type": "PreconditionsAttestation",
  "identifier": UNIQUE_ID,
  "preconditions": ARRAY_OF_PRECONDITION_DESCRIPTORS
}
```

OfferAttestation

In response to a request for an Attestation that cannot be issued because that type is not available, provide to the Holder a list of attestations that ARE available.

- For each attestation type available to the requester:
  - Type of attestation
  - List of tag strings to describe the attestation
  - Detailed, human-readable description of the attestation being requested (mostly for UAs to display to users)
  - Formats available for the attestation

```
{
  "@context": "http://schema.entethalliance.org/",
  "@type": "OfferAttestation",
```

```
  "identifier": UNIQUE_ID,
  "availableAttestations": ARRAY_OF_ATTESTATION_DESCRIPTORS
}
```

DeliverAttestation

Used by any party that delivers a finalized attestation to a target entity. This Message inherits from schema.org's SendAction.

- Linked attestation action ID
- Payload of the proof material
- Format of the proof material
- Time delivered

```
{
  "@context": "http://schema.entethalliance.org/",
  "@type": "DeliverAttestation",
  "identifier": "UNIQUE_ID",
  "object": ATTESTATION_PAYLOAD,
  "description": "California Driver's License",
  "tags": ["license", "driving", "permit", "DL", "driver's license"]
}
```

PresentAttestation

This Action is the envelop used to present an attestation to an inspecting party.

- List of tag strings to describe the attestation
- Detailed, human-readable description of the attestation being requested (mostly for UAs and EAs to reason over and use in display)
- Format of the attestation payload
- The attestation payload

```
{
  "@context": "http://schema.entethalliance.org/",
  "@type": "PresentAttestation",
  "object": ATTESTATION_PAYLOAD,
  "description": "ISP Account",
  "tags": ["ISP_DID", "ISP_Name", "Customer_DID", "Account_Type", "Account_Status"]
}
```

SignAttestation

A party sends an Action to a target prompting them to sign the provided attestation payload. This Message inherits from schema.org's EndorseAction.

- Linked attestation action ID
- Payload of the proof material
- Format of the proof material
- Time delivered

```
{
   "@context": "http://schema.entethalliance.org/",
   "@type": "SignAttestation",
   "identifier": UNIQUE_ID,
   "object": ATTESTATION_PAYLOAD,
   "description": "ISP Account",
   "tags": ["ISP_DID", "ISP_Name", "Customer_DID", "Account_Type", "Account_Status"]
}
```

RevokeAttestation

The party that previously supplied an attestation sends a notice to the attestation owner/holder that issuing party has revoked the attestation. This Message inherits from schema.org's DeactivateAction.

- Attestation ID
- Revocation code - array of revocation codes (look for an existing standard)
- Reason for revocation - array of human-readable descriptions of the reason, or URI

```
{
   "@context": "http://schema.entethalliance.org/",
   "@type": "RevokeAttestation",
   "identifier": UNIQUE_ID,
   "object": ATTESTATION_PAYLOAD
   {"description": "ISP Account",
   "tags": ["ISP_DID", "ISP_Name", "Customer_DID", "Account_Type", "Account_Status"]}
   "result": REVOCATION_RECORD,
   "purpose": "Your account was revoked."
}
```

AmendAttestation

Used to update an attestation. Requires past ID, optionally including previous attestation. This Message inherits from schema.org's ReplaceAction.

- Attestation ID
- Change delta of some kind
- Reason for amendment - array of human-readable descriptions of the reason, or URI

```
{
   "@context": "http://schema.identity.foundation/",
   "@type": "AmendAttestation",
   "identifier": UNIQUE_ID,
   "object": ATTESTATION_PAYLOAD
   {"description": "ISP Account",
   "tags": ["ISP_DID", "ISP_Name", "Customer_DID", "Account_Type", "Account_Status"]}
   "purpose": "Your account has been reopened"
}
```

RequestAccess

Request permission for access to a DID's Identity Hub data. This Message inherits from schema.org's AuthorizeAction.

- Access Permission being requested
- Intended use of data being requested

```
{
  "@context": "http://schema.entethalliance.org/",
  "@type": "RequestAccess",
  "object": PERMISSION_OCAP,
  "purpose": "Display and filtering on a professional network",
}
```

GrantAccess

The party that allows a permission sends a notice to the requesting party to let them know the permission has been granted. This Message inherits from schema.org's AcceptAction.

- Access Permission being requested
- Intended use of data being requested

```
{
  "@context": "http://schema.entethalliance.org/",
  "@type": "GrantAccess",
  "object": PERMISSION_OCAP
}
```

DenyAccess

The party evaluating the permission request does not grant the permission and sends the requesting party a notice of the denial. This Message inherits from schema.org's RejectAction.

- Access Permission being requested
- Intended use of data being requested

```
{
  "@context": "http://schema.identity.foundation/",
  "@type": "DenyPermissionAction",
  "object": PERMISSION_OCAP,
  "purpose": "I do not want to allow you access at this time",
}
```

RetractAccess

The party that has previously issued a permission granting access sends a notice to the affected party to let them know the permission has been retracted. This Message inherits from schema.org's DeleteAction.

- Access Permission being retracted

```
{
   "@context": "http://schema.entethalliance.org/",
   "@type": "RetractAccess",
   "object": PERMISSION_OCAP,
   "purpose": "I no longer want you to have access to my attestations",
}
```

RetrieveAttestations

Used by any party that has been granted permission access to a set of Attestations via the GrantPermissionAction to retrieve a set of Attestations.

```
{
   "@context": "http://schema.entethalliance.org/",
   "@type": "RetrieveAttestations",
   "identifier": "UNIQUE_ID",
   "object": ATTESTATION_PAYLOAD,
   {"description": "ISP Account",
   "tags": ["ISP_DID", "ISP_Name", "Customer_DID", "Account_Type", "Account_Status"]}
}
```

Glossary

- **Decentralized Identifier**: Decentralized Identifiers (DIDs) are a new type of identifier for verifiable, “self-sovereign” digital identity. DIDs are fully under the control of the DID subject, independent from any centralized registry, identity provider, or certificate authority.
- **DID**: Decentralized Identifier
- **DID Auth**: Authentication of an Identity by verifying the Identity’s control of its DID
- **DID Document**: The control document that specifies keys, service endpoints, and other basic details about a DID.
- **DDO**: Abbreviation for a DID Document
- **EA**: Enterprise Agent: a HUB-aware service that integrates with an Enterprise’s backend systems and representatives to process HUB requests. Conceptually equivalent to a person’s UA, but for an organization.
- **UA**: Abbreviation for User Agent
- **Universal Resolver**: A mechanism of getting the DID Document associated with a DID across any (supported) DID implementation from the Decentralized Identity Foundation
- **UR**: Abbreviation for Universal Resolver
- **User Agent**: a smartphone-based digital wallet, browser

Technical & Spec Implications

- For the DID Service /permission spec: add an optional timeout for access permissions.

About the Enterprise Ethereum Alliance (EEA)

The Enterprise Ethereum Alliance (EEA) is a global standards organization that is creating and maintaining an open, standards-based architecture and specification for accelerating the adoption of Enterprise Ethereum. The goal of the EEA's Enterprise Ethereum Client Specification and forth-coming testing and certification programs is to ensure interoperability, multiple vendors of choice, and lower costs for its members. Contact the EEA Member Support team at membership@entethalliance.org for more information.

About the Telecom Special Interest Group (SIG)

The EEA Telecom Special Interest Group (SIG) is exploring ways that Ethereum can be used to drive efficiency and new capabilities in the telecommunications industry. The SIG's work includes educational calls, development of detailed use cases, and work sessions that promote collaboration and adoption of best practices for blockchain development.

Here are a few of the advantages of joining the EEA and becoming a member of this industry group.

- Learn and collaborate with other Telecom members
- See how your business can adapt and make use of innovative technologies
- Help build blockchain requirements and specifications to power changes in the industry
- Influence the changes in regulations that needed to secure this future