Цифровая личность (SSI).

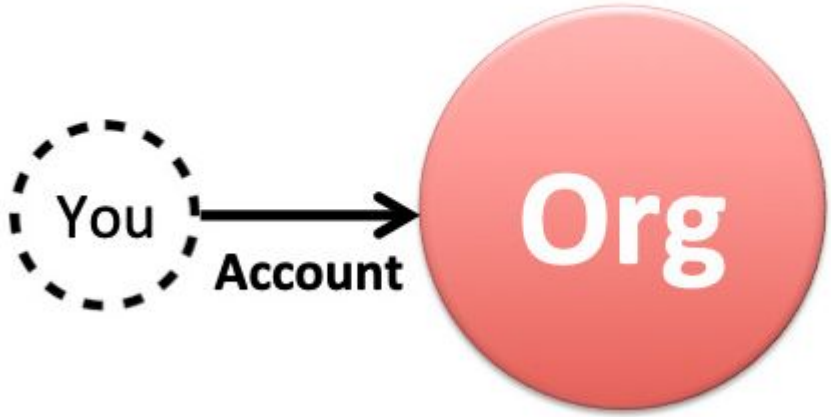
Блокчейн как решение проблемы цифровой идентичности

Алексей Воробей. Заместитель директора ООО “Брайтум”.
Председатель Совета Ассоциации “Технологии Распределенных Реестров”
Старший преподаватель юридического факультета БГУ

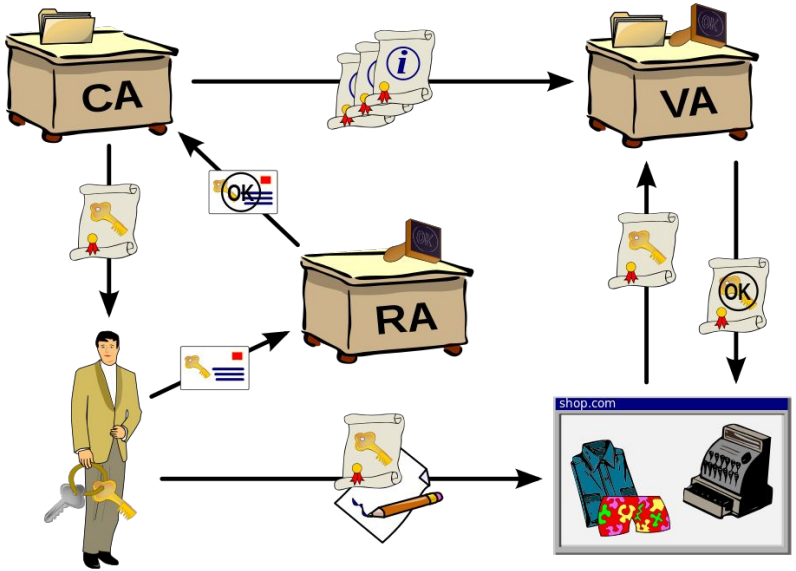
Структура лекции

1. Обзор текущего статуса индустрии цифровой идентификации.
2. Выявление ключевых проблем.
3. Концепт Self-Sovereign Identity.
4. Использование блокчейн-систем в качестве основы для реализации SSI.
5. Перспективы SSI и практическое применение.

Кто мы в цифровом мире?



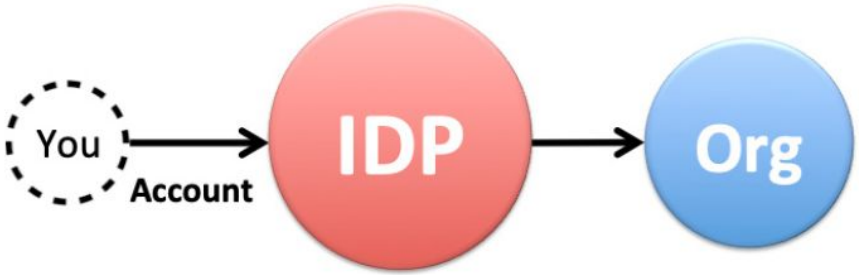
Как это работает?



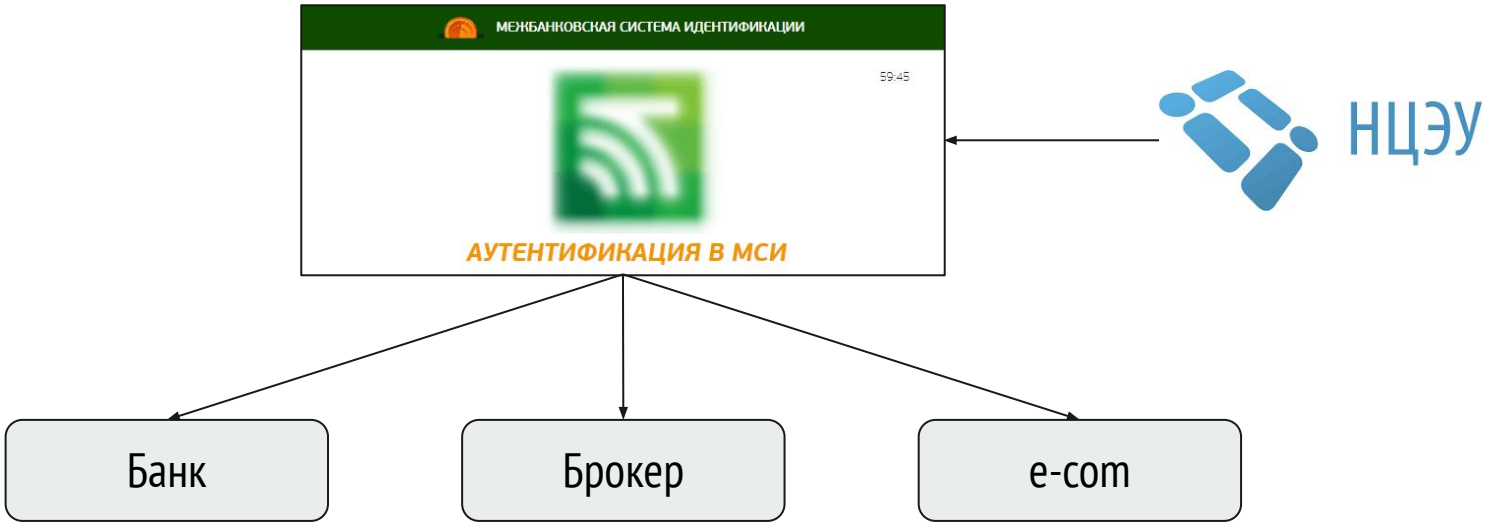
В чем проблема?

1. Отставание систем от потребностей рынка.
2. Проблемы с взаимным признанием удостоверяющих центров.
3. Идентификация по IP-адресу не означает идентификацию лица и авторизацию на совершение определенных действий.
4. Подписанные документы не решают проблемы полноты и актуальности данных.
5. Авторизация на базе принципов shared secrets несет риски компрометации базы паролей.

Федеративная идентичность - решение?



Отечественные банковские реалии



Что получили?

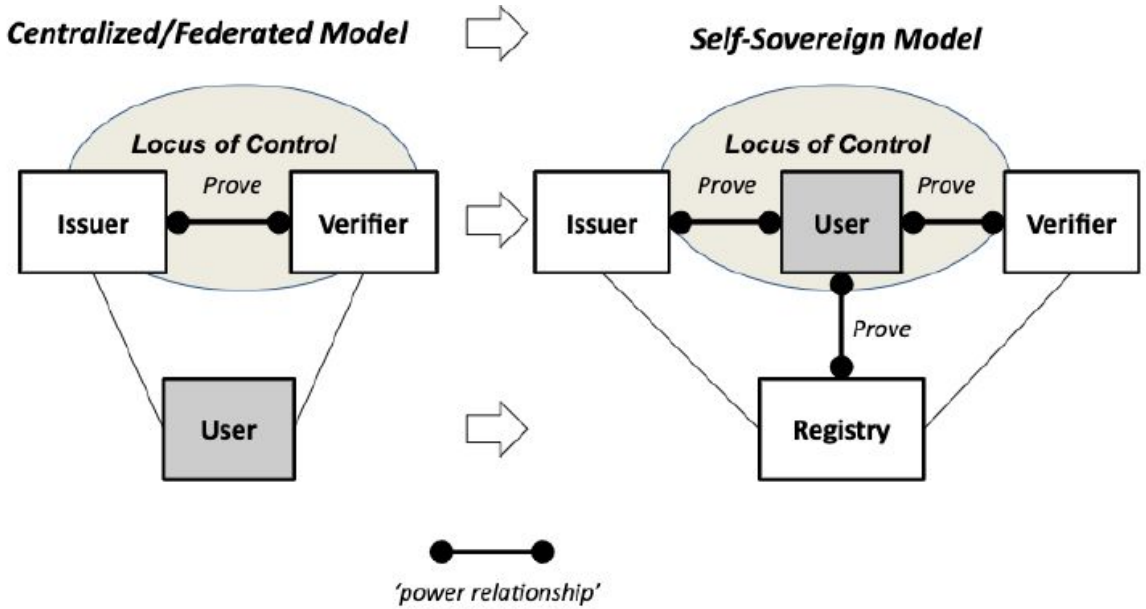
1. Увеличение копирования информации и, как следствие, увеличение риска их утраты.
2. Рост влияния крупных корпораций.
3. Нецелевое использование персональных данных.
4. Снижение уровня сквозного проникновения цифровой личности в условиях паноптикума информационных систем.

Что будем делать?

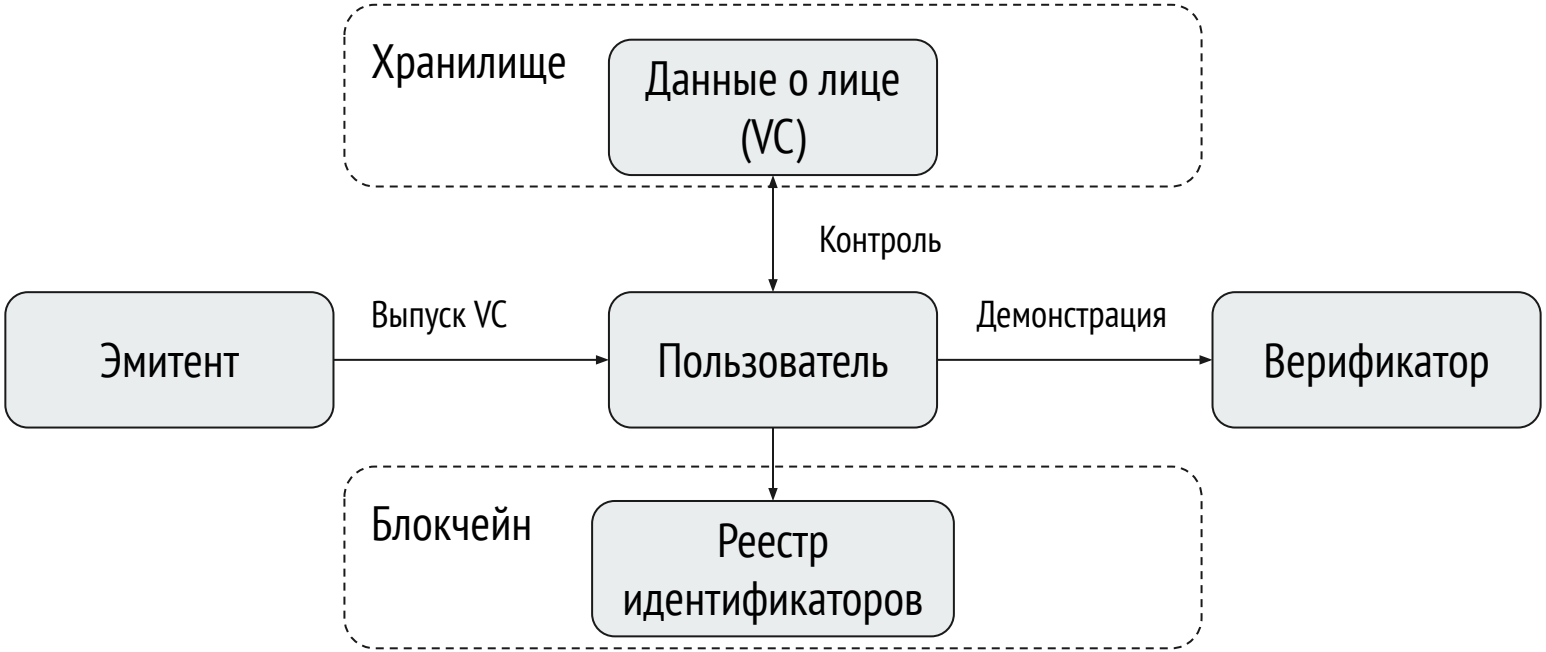
Требования к системе

1. Универсальные идентификаторы, признаваемые в различных юрисдикциях.
2. Контроль за предоставлением собственных данных.
3. Интероперабельность технической платформы в контексте взаимодействия с другими информационными системами.

SSI - изменения локуса контроля



Базовые элементы SSI

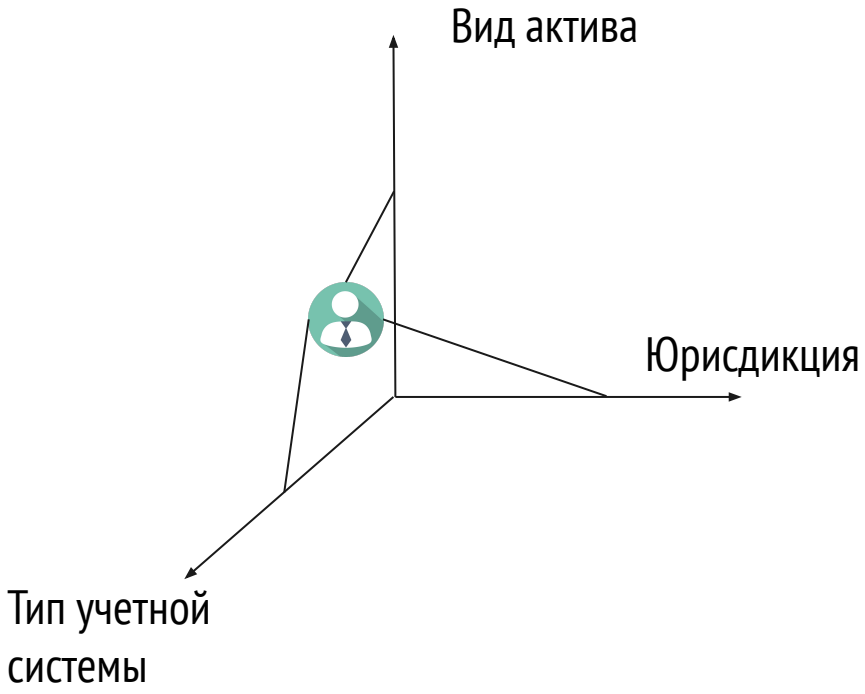


Для чего необходим блокчейн?

1. Блокчейн используется в качестве доверенной среды для фиксации фактов
2. Блокчейн может быть использован в качестве системы управления ключами пользователя
3. Блокчейн может быть использован в качестве среды для запуска DID-модуля

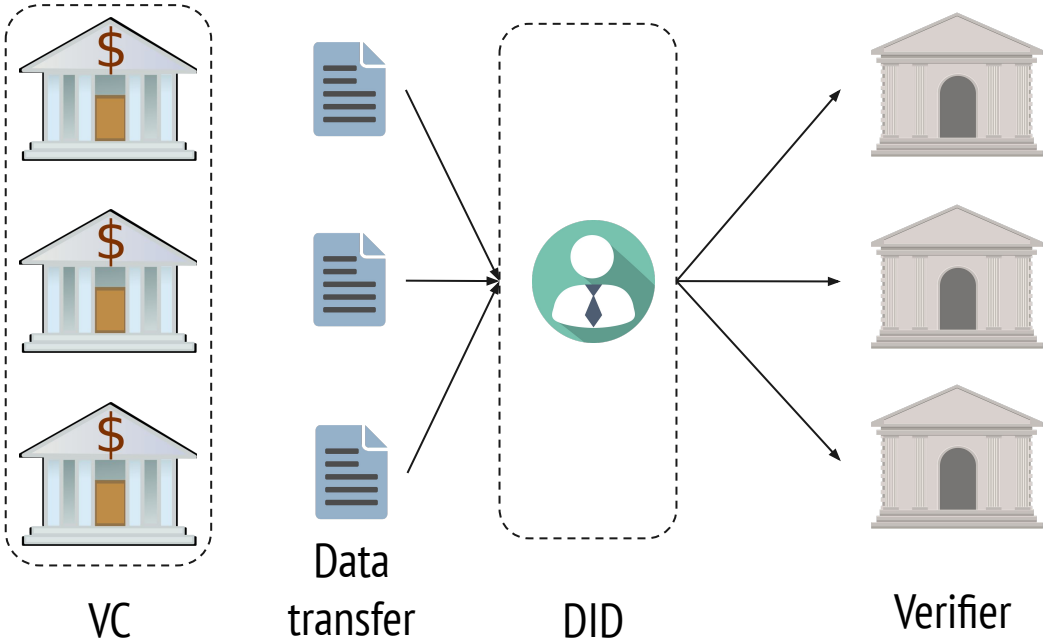
Применение SSI

Эволюция доверия в финансах



Транзакционные издержки на всех этапах

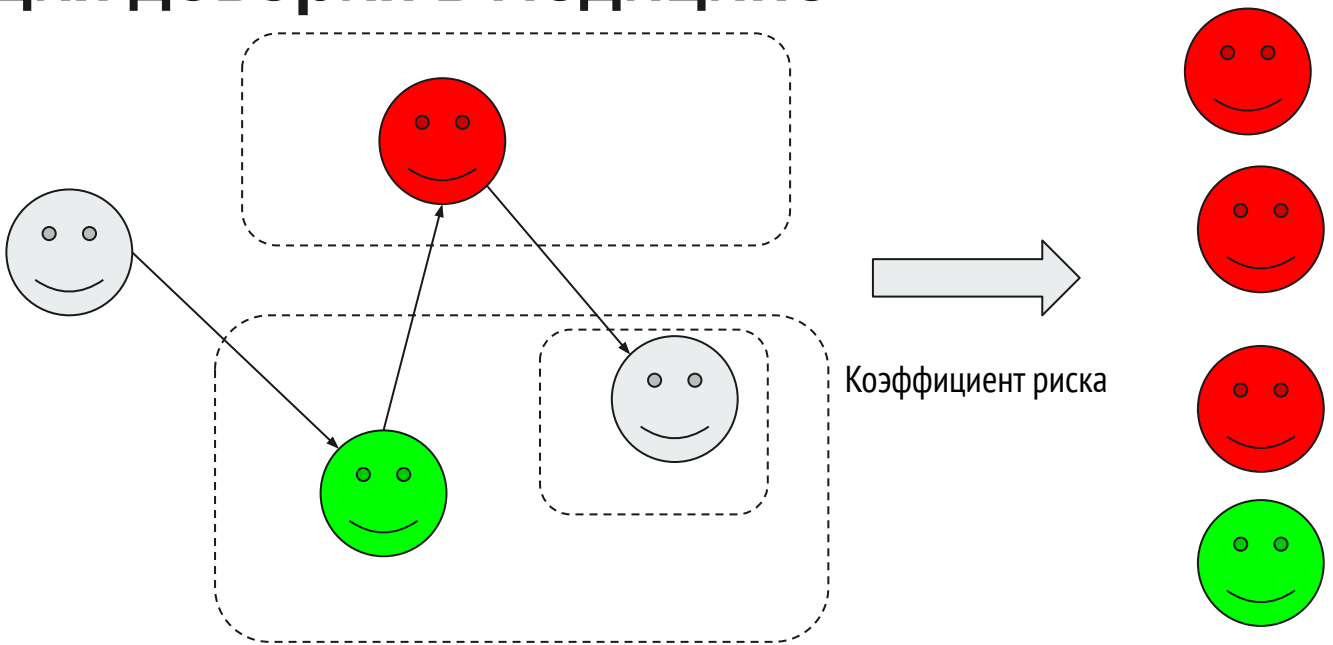
Что можно сделать?

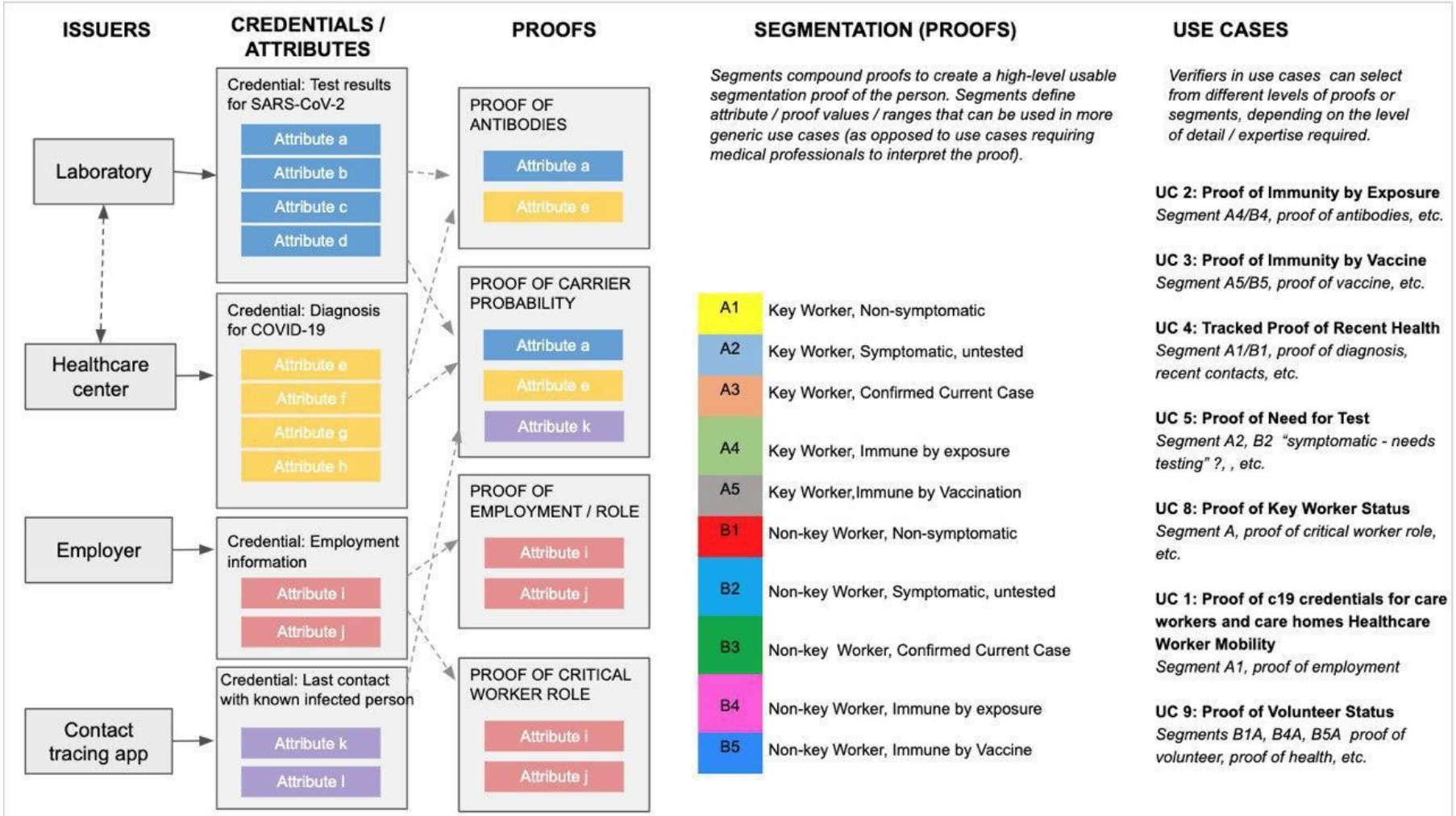


Что решает SSI и DLT?

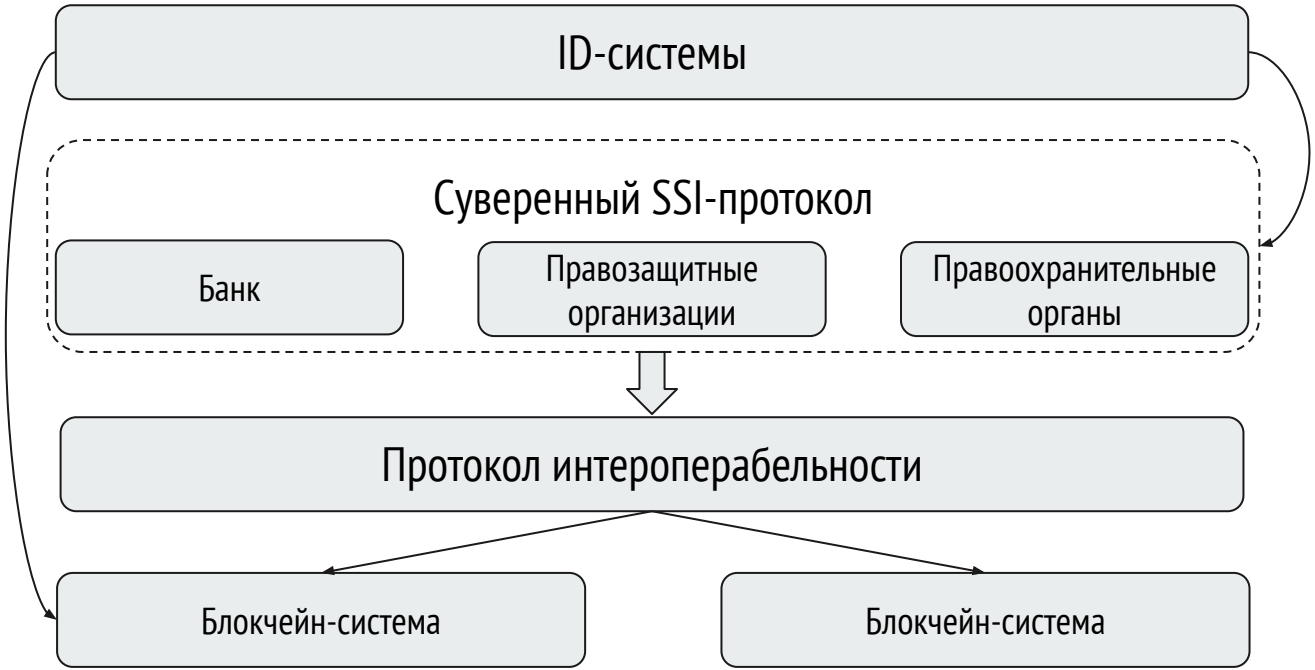
1. Универсальный процесс идентификации ❌
2. Устойчивая и интероперабельная система авторизации ✅
3. Фиксация отношений внутри организаций ✅
4. Процедура принятия решений ❓
5. Процедура проверки решений ✅
6. Процедура делегирования полномочий ❓
7. Процедура проверки полномочий ✅

Эволюция доверия в медицине




ISSUERS
CREDENTIALS / ATTRIBUTES
PROOFS
SEGMENTATION (PROOFS)
USE CASES
Laboratory
Healthcare center
Employer
Contact tracing app
Credential: Test results for SARS-CoV-2
Attribute a
Attribute b
Attribute c
Attribute d
Credential: Diagnosis for COVID-19
Attribute e
Attribute f
Attribute g
Attribute h
Credential: Employment information
Attribute i
Attribute j
Credential: Last contact with known infected person
Attribute k
Attribute l
PROOF OF ANTIBODIES
Attribute a
Attribute e
PROOF OF CARRIER PROBABILITY
Attribute a
Attribute e
Attribute k
PROOF OF EMPLOYMENT / ROLE
Attribute i
Attribute j
PROOF OF CRITICAL WORKER ROLE
Attribute i
Attribute j
Segments compound proofs to create a high-level usable segmentation proof of the person. Segments define attribute / proof values / ranges that can be used in more generic use cases (as opposed to use cases requiring medical professionals to interpret the proof).
A1 Key Worker, Non-symptomatic
A2 Key Worker, Symptomatic, untested
A3 Key Worker, Confirmed Current Case
A4 Key Worker, Immune by exposure
A5 Key Worker,Immune by Vaccination
B1 Non-key Worker, Non-symptomatic
B2 Non-key Worker, Symptomatic, untested
B3 Non-key Worker, Confirmed Current Case
B4 Non-key Worker, Immune by exposure
B5 Non-key Worker, Immune by Vaccine
Verifiers in use cases can select from different levels of proofs or segments, depending on the level of detail / expertise required.
UC 2: Proof of Immunity by Exposure
Segment A4/B4, proof of antibodies, etc.
UC 3: Proof of Immunity by Vaccine
Segment A5/B5, proof of vaccine, etc.
UC 4: Tracked Proof of Recent Health
Segment A1/B1, proof of diagnosis, recent contacts, etc.
UC 5: Proof of Need for Test
Segment A2, B2 "symptomatic - needs testing" ?, , etc.
UC 8: Proof of Key Worker Status
Segment A, proof of critical worker role, etc.
UC 1: Proof of c19 credentials for care workers and care homes Healthcare Worker Mobility
Segment A1, proof of employment
UC 9: Proof of Volunteer Status
Segments B1A, B4A, B5A proof of volunteer, proof of health, etc.

Государственное управление с использованием SSI



В сухом остатке

Преимущества

1. Самостоятельный выпуск “цифровой личности”.
2. Контроль за правами доступа к аккаунту
3. Контроль за доступом к данным

Недостатки

1. Проблемы восстановления паролей
2. Вопросы признания SSI
3. Вопросы управления базовым блокчейн-протоколом

Что мы считаем необходимым?

1. Создать рабочую группу по изучению опыта исследований консорциума W3C.
2. Провести теоретические и прикладные исследования по вопросу актуальности внедрения принципов SSI в экономику Республики Беларусь.
3. Сформировать пул предложений по совершенствованию национальных дорожных карт по развитию цифровой доступности.
4. Осуществить пилотных проектов для проверки гипотез по внедрению SSI

Рекомендуемая литература

1. Verifiable Credentials Data Model 1.0
2. Decentralized Identifiers (DIDs) v1.0
3. Self-Sovereign Identity, Decentralized Digital Identity and Verifiable Credentials. *Alex Preukschat and Drummond Reed*
4. Engineer's Guide to Financial Internet Kindle Edition. *Pavel Kravchenko, Bohdan Skriabin and Oleksandr Kurbatov (Author)*
5. Decentralized Public Key Infrastructure. A White Paper from Rebooting the Web of Trust
6. SSI Meetup channel

Спасибо за внимание!