Децентрализованная идентификация: «законы идентичности».

Технология распределенных регистров (DLT[distributed ledger technology]), основанная на blockchain привела к появлению новых подходов к управлению идентификацией (IdM) [1]. Личность предоставляется централизованной службой, которая выполняет проверку подлинности пользователей на основе существующих проверенных учетных данных (например, паспорта) и записывает удостоверения личности в DLT для последующей проверки 3-ми сторонами. Три конкретные схемы IdM на основе DLT: uPort, ShoCard и Sovrin, выбрали, в частности, потому что именно они служат образцами как преобладающих дизайнерских решений так и обнаруженных проблем[2-4,6]. Кроме того, они предоставили самую подробную техническую информацию об их схемах, подкреплены значительными онлайн сообществами и имеют значительное финансирование венчурным капиталом. Окончательного критерия схем IdM не существует. Поэтому используют систему оценок, известную как «законы идентичности» [4], которые служат для определения удач и отказов цифровых систем идентификации. Эта широко известная структура представляет полный спектр проблем IdM, охватывающих как безопасность и конфиденциальность, так и пользовательский интерфейс. Кроме того, «законы» обеспечивают необходимую гибкость, которая идеально подходит для применения на гетерогенных и ранних стадиях развития технологии распределенного управления DLM на основе технологии распределенных реестров DLT [5-7]. Сами «законы» заключаются в следующем:

1 - Пользовательский контроль и согласие. Информация, идентифицирующая пользователя, должна быть раскрыта только с согласия этого пользователя.

2 - Минимальное раскрытие информации для ограниченного использования. Идентификационная информация должна собираться только по принципу «необходимо знать» и храниться на основе «необходимости сохранения».

3 – Стороны с правом доступа. Идентификационная информация должна распространяться только сторонам, которые имеют законное право доступа к информации о личности в транзакции.

4 - Направленная идентификация. Необходимо публично или более осторожно поддерживать совместное использование информации об идентификаторе

5 - Дизайн плюрализма операторов и технологий. Решение должно обеспечивать возможность взаимодействия различных схем идентификации и учетных данных.

6 - Человеческая интеграция. Пользовательский опыт должен соответствовать потребностям пользователей и ожиданиям, чтобы пользователи могли понять последствия их взаимодействия с системой.

7 - Постоянный опыт в разных контекстах - Пользователи должны иметь возможность ожидать последовательного опыта в разных контекстах безопасности и технологических платформах [4, 5].

[1] Kim Cameron, 'The Laws of Identity'. Microsoft Corporation, 05-Nov-2005.

[2] 'Travel Identity of the Future – White Paper'. SITA; ShoCard, May-2016.

[3] 'Not-so-clever contracts', The Economist, 30-Jun-2016.

[4] Dhamija and Lisa Dusseault, 'The Seven Flaws of Identity Management: Usabilty and Security Challenges', IEEE Secur. Priv., vol. 6, no. 2, pp. 24–29, Mar. 2008.

[5] Paul Dunphy and Fabien A. P. Petitcolas, 'A First Look at the Usability of Bitcoin Key Management'
https://www.researchgate.net/publication/300925188_A_First_Look_at_the_Usability_of_Bitcoin_Key_Management

[6] http://bitid.bitcoin.blue/

[7] http://btcdesk.ru/ms/novaya-sistema-dlya-transgranichnyx-platezhej-na-osnove-corda-dlt.html