Exploring privacy challenges of blockchain-based supply chain in the pharmaceutical industry

Research Project (CSE 3000) by Jean Gal | Supervised by Tianyu Li & Zekeriya Erkin | July 1st, 2021 | j.c.r.gal@student.tudelft.nl

1 - Research Question

How to preserve privacy in healthcare supply chains based on distributed ledger technology?

- From *2015 to 2019*, 76% of data breaches happened in Healthcare Services.
- Protect healthcare data → Dark Web, Ransoms, Financial & Identity fraud.
- What are the privacy challenges of blockchain based supply chain? What techniques can preserve user privacy in pharmaceutical supply chains?

2 - Definitions

Supply Chain (SC) → Process of making and selling goods. Includes all the stages from the supply of materials to the distribution/sale of goods.

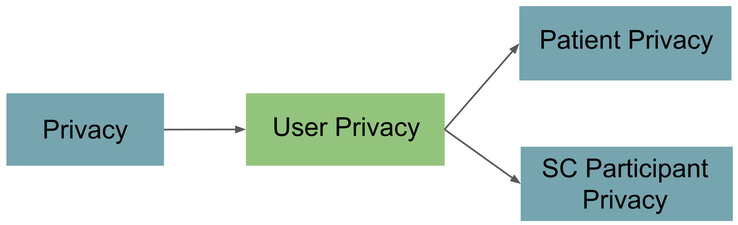
Supply Chain Management (SCM) → Optimization of supply chain flows: **Information**, Material & Financial.

Blockchain → A shared and immutable ledger for recording transactions and information.

PPE → Personal Protective Equipment

GDPR → General Data Protection Regulations

Privacy → Someone's right to keep their personal data secret.



Privacy targets

3 - Research Method

Literature Survey: World Wide Science & Google Scholar tools to find research papers. The research steps are:

Step 1: Research Blockchain and Supply Chain concepts. Read about applications of blockchain in SCM.

Step 2: Research privacy requirements of SCM. Investigate on blockchain privacy.

Step 3: Find SC applications in Healthcare. Research where privacy is important.

Step 4: Establish major privacy challenges and research solutions. Find cryptographic technique.

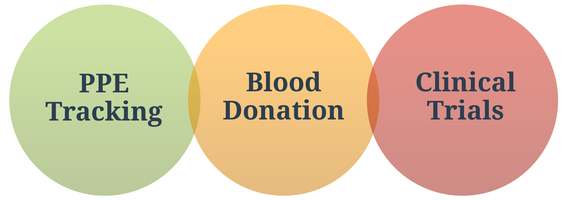
4 - Challenges

Blockchain characteristics:

Transparency	Transactions can be transparently viewed.
Immutability	State or quality of being incapable of mutation.
Traceability	Ability to trace all the stages that led to a particular point in a process that consists of a chain of interrelated events.

1) Provide **Privacy** in a **Traceable** blockchain
2) Preserve **Privacy** from **Transparent** transactions [2]
3) Provide **Privacy** in an **Immutable** blockchain
4) Ensure patient's **Anonymity** and their **Accountability**

5 - Pharmaceutical Supply Chains



6 - Techniques

Pseudonymisation	Pseudonyms to hide the identity of users
Zero Knowledge Proofs	Verify transactions without access to their content
K-Anonymity [1]	Reduce risks of re-identification through transactions
Mixing Services [2]	Blur relations between transaction participants
Group Signature [2]	Sign transactions on behalf of a group and mask the individual identities
Ring Signature [2]	Absence of tracing authority → Complete anonymity

7 - Conclusion

- Techniques can preserve patient privacy through **anonymity** and **unlikability** and guarantee **accountability**.
- For future work, explore privacy threats of centralized services.

8 - References

[1] Sweeny, L. (2002). K-Anonymity: A model for protecting privacy. International Journal Of Uncertainty, Fuzziness And Knowledge-Based Systems, 10(05), 557-570. https://doi.org/10.1142/s0218488502001648

[2] Feng, Q., He, D., Zeadally, S., Khan, M., & Kumar, N. (2019). A survey on privacy protection in blockchain system. *Journal Of Network And Computer Applications*, *126*, 45-58. https://doi.org/10.1016/j.jnca.2018.10.020