KIDNER – A WORLDWIDE DECENTRALIZED MATCHING SYSTEM FOR KIDNEY TRANSPLANTS

Sajida Zouarhi

Orange Labs, 28 Chemin du vieux chêne - BP 98, 38243 Meylan Cedex, France, sajida.zouarhi@orange.com

Abstract

Individuals suffering from kidney failure today face significant challenges in order to obtain a transplant. They are placed on a waiting list and ranked by priority in hope that a kidney from a deceased donor is a transplant match. They do have another option: a living donor; someone they know, family or friend, willing to give them a kidney. These people may not be a transplant match, however there is a solution, a "Kidney Exchange" or a "Kidney Paired Donation".

In these programs, if two mismatched pairs (living donor and kidney recipient) can be grouped together so that they become transplant matches, both kidney failure patients can receive a kidney. While a great solution, these programs have a significant pitfall. They are limited to the specific registry regions participating in their program. The Kidner project was developed to help these exchange programs better detect life-saving opportunities and enable more people to access kidney transplants.

Keywords: transplant; kidney; privacy; security; blockchain.

Introduction

Background

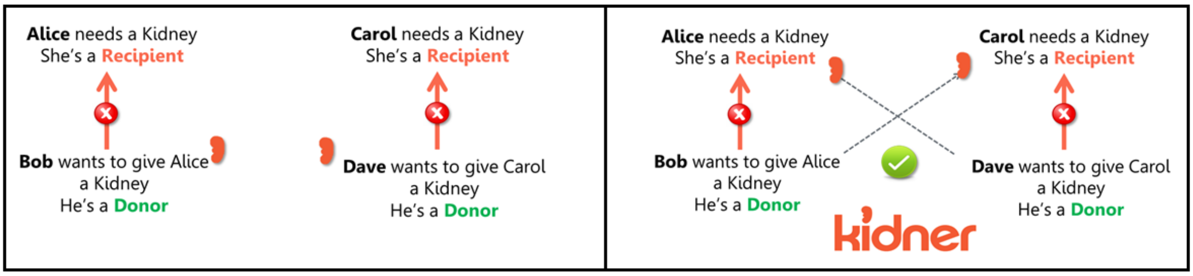
The average waiting time for a kidney transplant in the US is 3 to 5 years, [1] during this time patients have to go through a heavy process of dialysis at least 3 times a week, negatively impacting their normal social and work life balance. Being on dialysis is expensive, about 60 billion is spent in the US each year on kidney healthcare -

28% of Medicares budget, [2] and transplants are overall much cheaper than ongoing dialysis. Illness may worsen while waiting for a transplant and in the worst case, patients may die.

There is another option: a living donor; someone they know, family or friend that is willing to give them a kidney. Unfortunately, because many factors like blood type and HLAs need to be compatible, these people may not be a transplant match. To solve this “Kidney Exchange Programs” or “Kidney Paired Donation programs” (KPD), have been created. [3] In these programs two mismatched pairs (living donor and kidney recipient) can be grouped together so that they become appropriate transplant matches and both kidney failure patients can receive a kidney. Currently, KPD accounts for 10% of live kidney transplants in the United States. The pool of participants in KPDs face the same constraints as Traditional Cadaveric Kidney Transplant lists, they are limited to specific country or region. [4]

What would happen if we were to open the pool of participants in the Kidney Exchange Program to the entire world?

Figure 1. Kidney Paired Donation between two incompatible pairs



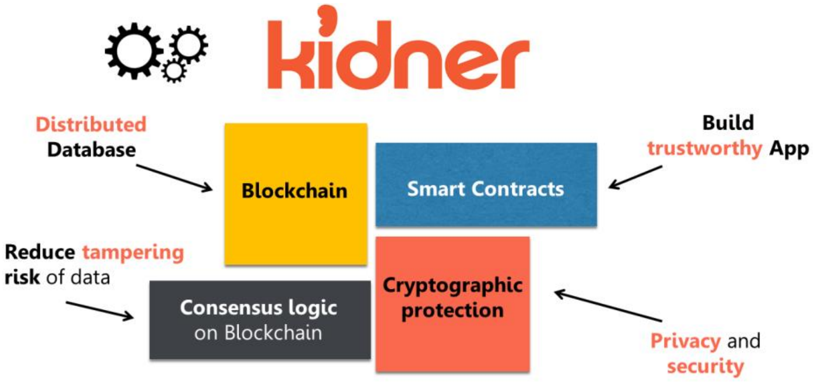
Kidner Solution

Our goal is to make the current transplant system more efficient, more secure and more efficacious. To do so we realized that we need to increase the data volume by involving more hospitals in the process and asking them to share their data to create a bigger and more relevant pool. Such an effort requires us to address governance and trust among systems, as well as offer transparency for all actors in the system. This is why a blockchain architecture is the best way to create a multi-parties ecosystem of hospitals and healthcare actors that want to achieve a common goal: a better and safer care for the patients.

Overview of the system architecture

1. General overview

Figure 2. Main components of the Kidner solution



Blockchain **-** It's a distributed ledger (database) that can only be updated by consensus among the peers that compose the network. [5] [6] Each peer stores the ledger locally and the ledger is identical among the peers. The peers communicate in a distributed fashion to update the ledger with no need of central authority. The protocol is designed to ensure the traceability and non-repudiablity of the transactions and to discourage or resist attacks or malicious behavior on the network.

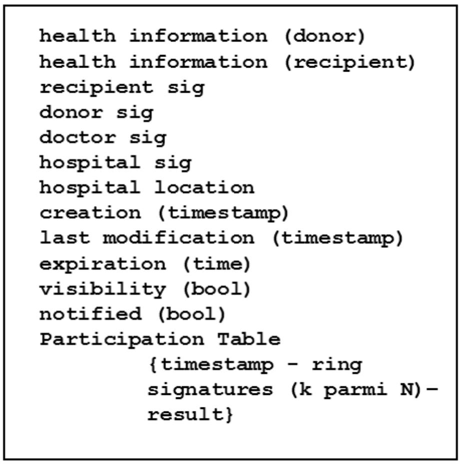
Smart contracts – A smart contract is a collection of rules which are deployed on a blockchain, and shared and validated collectively by a group of stakeholders. A smart contract can automate business processes in a trusted way by allowing all stakeholders to process and validate contractual rules as a group. [6] [7]

Benefits of the blockchain for this use case

- Past transactions or blocks in the chain cannot be modified: when a piece of information is recorded it is never deleted so it is a proof that can be used and verified to prevent corruption and abuse.
- It's a powerful tool for traceability and transparency which are keys to many administrative issues in healthcare – for example the billing process. It reduces disputes between actors of the ecosystem.
- An actor can not claim to be fully in charge of the entire process and ask every other actors of the ecosystem to trust it as a third part. Central organization or authorities are however part of the operational solution which will give them an efficient tool for audit.

We can build a fair and transparent matching mechanism that generates non-repudiable ***proof of match*** because the computation is done by multiple nodes managed by various hospitals.

Figure 3. High-level overview of a *Certificate* Structure



```
health information (donor)
health information (recipient)
recipient sig
donor sig
doctor sig
hospital sig
hospital location
creation (timestamp)
last modification (timestamp)
expiration (time)
visibility (bool)
notified (bool)
Participation Table
        {timestamp - ring
        signatures (k parmi N)-
        result}
```

Private, Public and (Un)Permissionned ledgers

Requirements for blockchains vary greatly across different use-cases; there will not be a one size fits all solution. [7] Hyperledger opensource protocol is being designed to be highly modular, with pluggable options to suit different needs [8] - from open unpermissioned ledgers (e.g. Ethereum or Bitcoin) to private permissioned ledger (e.g.Bankchain). [9]

Compared to Ethereum or Bitcoin where the network and the ledger are open by design to anyone, Hyperledger network is only accessible to authenticated members (permissioned) and the ledger can only be read and used by the members (private), it is design for consortium or critical ecosystems, moreover some transactions can be encrypted on the ledger to preserve confidentiality. [8]

Security and resiliency

As presented in the overview, Kidner works in a distributed fashion with a high resiliency and integrity, and has no single point of failure. To ensure PHI - protected health information - stays protected, details surrounding the patients are anonymized by additional mechanisms before being stored in the ledger. It makes it impossible for a person to look at the medical data and to know the identity of the patient, while making it possible for the algorithm to find matches in an automated and reliable way and to notify the doctor. Only then can the doctor find the corresponding patient file on his local database.

Proof-of-Concept

We worked on a public opensource blockchain called Ethereum to illustrate in a simple way the Kidner concept and the patient journey. The front end and blockchain smart contracts described below were developed by the hackathon team of **Chainhack 2015**. For the proof of concept we used the Ethereum [6] platform to implement a basic matching system through a smart contract (solidity file: https://github.com/sajz/kidner).

Kidner process

Describe here is a patient centric view of the process:

1. **Prerequisites**

Prerequisite 1: the hospital is a safe place where healthcare professional can help the patients and provide a guarantee that there is not pressure or on going traffic into the kidney donation process.

Prerequisite 2: the hospital information system is secured, the database can’t be breached by an attacker to steal patients data and the network is private so that no one else can listen or interfere with the internal network and critical data that are transmitted and stored.

2. **Filling the *Certificate***

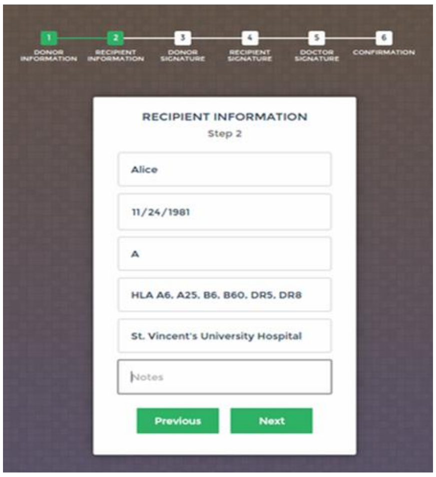
Donor, Patient and Doctor meet at the Doctor's office. They are connected through the doctor's computer on the hospital private network with direct access to the hospital database which is secured (see prerequisite 2). Information about the Donor and Recipient are filled automatically from the file or by the Doctor. They then, each at a time, sign a *certificate* that states 3 things:

- Donor is willing to give a kidney
- Recipient is willing to accept the kidney

- Doctor agreed that Recipient health is good and that it is safe for him or her to have a transplant, same assessment regarding the Donor health.

The Doctor and the patients will sign this form with a private key (multi-signature), triggering the *certificate* to be anonymized, encrypted locally, and sent to the blockchain via an internet connection.

Figure 4. Step 1 Donor information, Step 2 Recipient information, Step 3-4-5 Donor, Recipient and Doctor signatures



RECIPIENT INFORMATION
Step 2

Alice

11/24/1981

A

HLA A6, A25, B6, B60, DR5, DR8

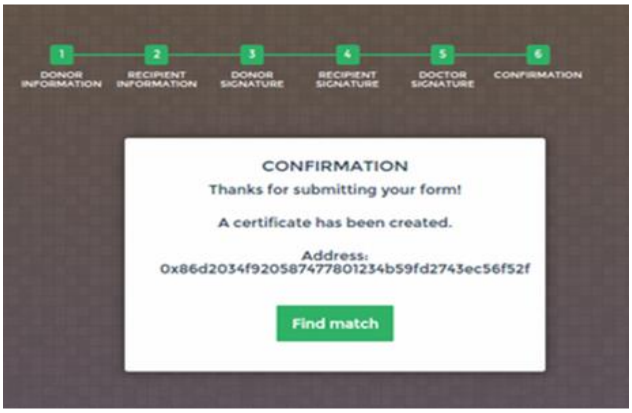
St. Vincent's University Hospital

Notes

3. **Successful update of the blockchain ledger**

At the end of the process, the *certificate* is issued and can be found at its address on the Ethereum blockchain.

Figure 5. Step 6 Confirmation



CONFIRMATION
Thanks for submitting your form!

A certificate has been created.

Address:
0x86d2034f92058747780l234b59fd2743ec56f52f

4. **Last step: Disclosure**

A search is launched when the Doctor of Alice & Bob submit the *certificate*. If a match is found, the Doctor will receive the hash of the address of the *certificate* of Dave & Carole pair. He will then use this ***proof of match*** and the contact details provided by Kidner to reach out to the other Doctor. Dave & Carole's Doctor will verify the ***proof of match*** by checking it against the local database of the hospital and confirming that it maps to an existing patient file on his side.

Future work

The next step of our roadmap is to create a consortium of actors interested by the solution described here and to have pilot centers to deploy the network and test it at a national scale and then between countries with similar quality and cost of care (e.g. UK and Ireland and France).

We are working on a version of the Kidner software which will be based on Hyperledger – a blockchain protocol different from Ethereum and more suited to this use case.

Conclusion

Kidner is a collaborative project that was developed to address the financial and security challenges that face cross border transplantation.

It aims at creating a KPD that extends the mismatched live donor-recipient pool through a decentralized non-profit system deployed world-wide which makes possible analysis and matching of patients while providing them complete anonymity.

We hope the development of this system will lead to the first kidner-based surgeries, enabling increased renal transplants per year.

Acknowledgments

Author warmly thank: Dr Mathew Rose from the Royal College of Surgeons in Ireland for his contributions, David Curran and our Hackathon team that developed the proof-of-concept, and the Kidner community (list of contributors and slack access available on www.kidner-project.com).

References

[1] National Kidney Foundation, 2014. [online]. Available: https://www.kidney.org/news/newsroom/factsheets/Organ-Donation-and-Transplantation-Stats. [accessed january 2017].

[2] PKD Foundation, «Kidney disease by the numbers,» [online]. Available: https://pkdcure.org/wp-content/uploads/2016/05/kidney-disease-by-the-numbers.pdf. [accessed january 2017].

[3] T. S. M. U. Ü. Alvin E. Roth, «Pairwise kidney exchange,» *Journal of Economic Theory,* vol. Volume 125, Issue 2, p. 151–188, December 2005.

[4] A. E. Roth, Who Gets What — and Why: The New Economics of Matchmaking and Market Design, 2015.

[5] S. Nakamoto, «Bitcoin: A Peer-to-Peer Electronic Cash System,» 2008. [online]. Available: https://bitcoin.org/bitcoin.pdf. [accessed january 2017].

[6] V. Buterin, «Ethereum white paper,» 2013. [online]. Available: https://github.com/ethereum/wiki/wiki/White-Paper. [accessed january 2017].

[7] Hyperledger, «White paper,» 2016. [online]. Available: https://wiki.hyperledger.org/groups/whitepaper/whitepaper-wg. [accessed january 2017].

[8] C. Cachin, Architecture of the Hyperledger Blockchain Fabric, Zurich, 2016.

[9] UK Government Chief Scientific Adviser, «Distributed Ledger Technology,» [online]. Available: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/492972/gs-16-1-distributed-ledger-technology.pdf. [accessed january 2017].

Author details

Sajida Zouarhi is an engineer and a PhD student in Computer Science and Network since 2014 with Orange labs and LIG (computer science laboratory of Grenoble). Her research work is about Blockchain-based solutions and "Quality of service of complex and heterogeneous systems for critical data transmission" especially in Healthcare and Internet of Things.