Med-Dev.io Technical White Paper (v1.3)

By Stuart Corby

December 2nd, 2017

Abstract The med-dev blockchain will provide integration and efficiency for product tracking record keeping compliance and inventory management for the global medical device industry.

This is achieved by controlled linking of the various stakeholders in the life of a medical device to maximize benefits for both their localized community and the global community of device users.

By managing localized sharing (among trusted individuals in teams) and creating permissioned sharing for the community as a whole, every stakeholder will gain utility while protecting their self-interest.

The med-dev blockchain will consist of a series of operating parts. Individuals will be able to access information provided by manufacturers and connect to regulator databases (via oracle nodes) for updates and listings of the devices they come into contact with. Those individuals will be able to join teams that can view their member's activities. Authorization nodes will allow the designation of these teams as representative of real world entities such as manufacturers, hospitals, clinics or regulators. Every interaction by an individual adds value to the chain hence they get to participate for free. As teams and designated entities gain value from managing their inventory, executing recalls and optimizing safe use of their medical products, they will pay for using the blockchain; tokens will be purchased by each team to grant access to the shared information for devices their members track.

The resulting blockchain will be able to manage the millions of transactions necessary to track and protect the world's medical devices. It will be able to interface with or act as regional regulator data-pools, while supporting both global and niche market manufacturers. Hospitals, clinics and doctors will be able to prove exactly which device was used and when, allowing them to protect patients by staying current with best use, getting instant notification of recalls or manufacturer advisories

The business of device management and how this industry can support the the blockchain economically is covered in more detail in Med-Dev: An introduction to the market by Stuart Corby.

Med-Dev and EOS.IO Our intention for Med-Dev is to implement it on the EOS.IO blockchain. EOS blockchain architecture is part of the latest iteration of blockchain technology and overcomes previous issues (which are described within this paper) of applying blockchain to the tracking of medical devices.

This whitepaper was re-written to follow the same terminology and a similar forma to the EOS.IO whitepaper to make it easier to follow. We recommend reading EOS.IO's documentation as well as our own - a suggested order for a 'cold start' would be:

1. Med-Dev: An introduction to the market
2. EOS: An introduction
3. EOS: Technical White Paper
4. Med-Dev: Technical White Paper (this document)

There is no business or prior relation between EOS.IO and Med-Dev or the author o this paper, although the principals in EOS.IO are part of the same community and known to the author.

Disclaimer

This document is for information purposes only. EOS system has not yet launched and implementation of Med-dev may vary based on our interactions with the EOS blockchain..

Background

Globally, regulators are increasingly requiring implementation of unique identification of every medical device. This is a response to both a growing number of recalls and to fight counterfeit products entering the market. Regulations differ b country and jurisdiction, but the general intent is that each manufacturer must uniquely label and then keep records of all devices made, they are then required to list product information with the relevant regulatory authority and keep distributior records that allow them to perform recalls in a timely manner. This forced application of unique identifiers to every medical device paves the way for other benefits across the whole industry. The largest potential for financial gains lie in supply chain optimization and accurate inventory management but unique ID's and a blockchain also facilitate the correct use of any device, the distribution of best practice documentation and the reduction of human error in identification. Ultimately the application of blockchain in conjunction with unique identification wi save lives by helping to avoid the incorrect end use of devices on patients.

The medical devices industry is the ideal market for the application of a low cost distributed ledger because of the millions of devices that need to be registered and tracked, and because stakeholders within the life of those medical devices have a wide variety of data needs that need to be satisfied.

Keeping an absolute transaction log and record of each device as it takes its journe from manufacturer to patient through multiple disparate parties, with different needs, will save lives, reduce costs and allow participants to remain compliant to regulatory rulings.

Unfortunately initial versions of blockchain, while promising in certain aspects, faile to provide transaction speeds, transaction volumes and transaction costs that were suitable to an industry which caters to extremely high value low turnover items as

well as consumable devices that are manufactured in the millions. Blockchain 2.0 with the introduction of smart contracts has made the technology viable. Now, as speeds have increased and mining costs reduced (and/or removed by proof of stake), blockchain can now be effectively applied.

The Med Dev Blockchain 'Tags'

The Med Dev block chain is not a crypto-currency. It uses random non-repeating 32 digit alphanumeric hash codes (tags) to represent each device that is being tracked. These tags are associated with any other identifiers that belong to the same physica device. A medical device can therefore only ever have one Tag, but can be found using any other unique code it is useful to link to it. For example a device may carry a GS1 datamatrix code and human readable code for compliance to the FDA, but sti be required to carry the manufacturer's own catalogue code for sale in other countries - in this case the Blockchain can query either result and get to the same parent tag and any associated information.

As any code is scanned by an individual it can request verification from various services.

The first verification is a check on the composition of the code, to classify and choose any further verification services that may be useful.

Once classified a code can be sent to the relevant oracle to check current external data on it. Oracle's can be used to interface with regulators, manufacturers or third party code generators.

Now the tag is identified and verified the individual user can be informed of any public information available for that code.

The cost of Individual interrogation of the blockchain is a time stamp, a geo-locatio and the anonymized identification of that individual (the blockchain can identify you if you return, but not who you are).

This data is locked within the Tag's own transaction log and only released to authorized parties.

Individuals can join teams. Teams authorize users within the team to share information with each other. Teams pay a minimum subscription fee to participate a a team on the Med-Dev Blockchain, for this subscription they receive as set amount of tokens which Tags consume when they are shared between team mates. 1 token allows one tag's (and therefore one device's) information to be shared between the whole team. There is no limit to the number of individuals that can join a team but any device scanned by a team member will use a token from that team.

The minimum subscription fee for teams is in place to support the ongoing operational costs of the services individuals call upon. The token charge is designed to prevent large teams, manufacturers or users of the system from being subsidized by the vast majority of small volume users.

Association services exist within the blockchain to allow teams to represent real world entities - for example a team can register as a manufacturer of a certain product. Where possible verification will be automatic. In the case of a US manufacturer, the FDA requests DI's be listed with a contact email address. As this address can only be added to a listing by manufacturers who have gone through FDA verification, the blockchain can validate the creation of a manufacturer team by contacting the registered email address and checking they are happy to authorize that team (and any individuals who are members or who its administrators choose to add in the future).

Now teams can be identified and individuals can share information, either within their team or to the manufacturer or from the manufacturer, smart contracts can be used to convey information, both on the device and on the devices status in a controlled manner throughout the blockchain.

Medical device users are subject to multiple levels of regulation, some of which is based around use of devices, some for storage of information about those devices. To be as flexible as possible the blockchain will permit token holders to export information to external storage in pdf format - thus allowing compliance with older regulatory requirements which require static documentation.

Transaction rates

The previous hesitation of using blockchain to record transactions for the medical device industry (or any industry) was the speed of writing and verifying those transactions and then the cost to do so using traditional Proof of Work.

The section below covers some of the calculations needed to estimate the transaction flow (and token use) of a fully functioning blockchain for the medical device industry:

Calculating the total number of transactions any platform will need to manage is highly subjective, instead we will simply prove that the number is large enough to warrant the use of the EOS.IO architecture.

Queries, updates on the status of a device, searches, recall events, messaging, requests for documentation links all hit the transaction logs. Products are often sold with other uniquely labelled peripheries, which manufacturers will also be able to list within the chain but for which they do not have to create a listing with a regulatory authority. This adds to the total number of product lines listed...

Example:

A leading Neuroscience manufacture has 22 device identifiers listed with the FDA,

they actively sell only 8 of these product lines and for each line they sell, on averag
12 unique devices a year. Their equipment is expensive and once installed lasts about 5 years. It is serviced once a year. Each registered item comes with 7 peripherals (power supplies, connector cables etc). There are user manuals associated with the devices that the operator should check quarterly.

Effective transaction rate for low usage high value medical device

8 DI * 7 Peripheries * 12 sold per year = New devices per year tracked
8 DI * 7 Peripheries * 12 sold per year * 4 years = Services tracked
8 DI * 12 sold per year * 4 years * 4 quarters = Read the instruction manual

Total = 14139 transactions per year for 8 product lines out of 22 listed

Extrapolation based on this example:

There are 1,557,354 devices currently listed on the GUDID database as sellable in the US.

(1,557,354/22)*8 = actively sold devices = 566,311

566,311*14139 = 8,007,064,802 transactions per year

31,536,000 seconds in a year

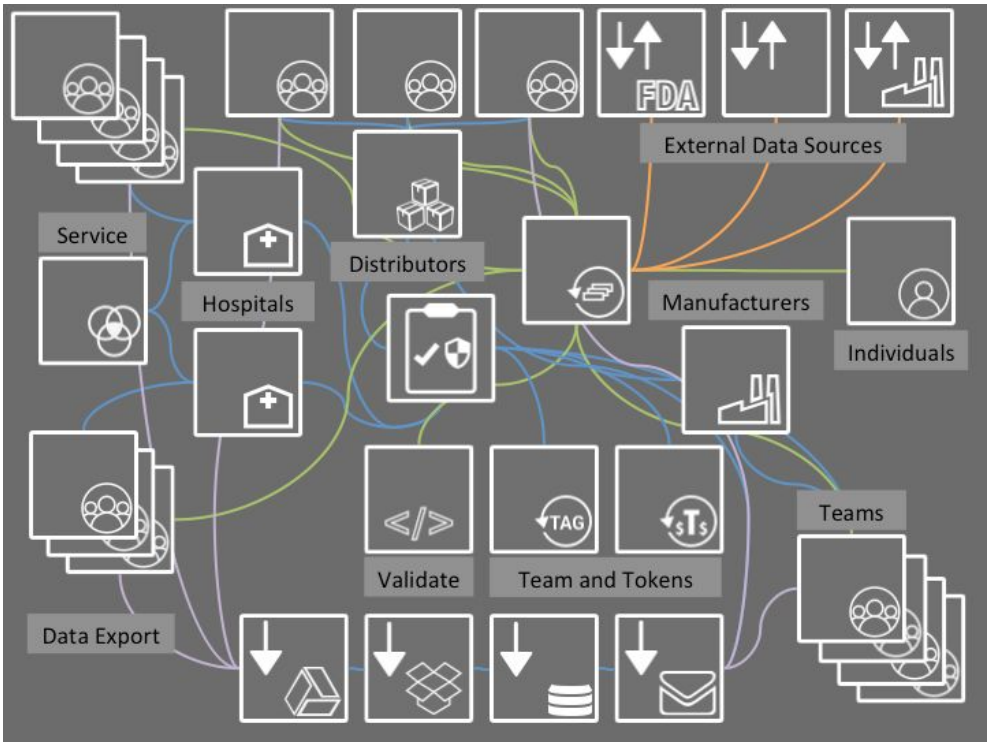
Therefore 8,007,064,802 / 31,536,000 = 254 transactions per second

If every medical device manufacturer selling into the US were like this one then the blockchain would be required to operate at 254 transactions per second.

While it is unlikely that every manufacturer will sign up to the Blockchain, it is important to note that the above covers only the US market, is limited to listed devices and excludes peripheries, and is based on a small turnover high value item, as opposed to a high volume consumable device, which also make up a high proportion of the devices sold.

It is safe to assume that any implementation must be able to scale to thousands of transactions per second.

The Med-Dev BlockChain



Summary Medical devices carry specific requirements, they exist in a complex regulatory regime, with demanding labelling requirements that vary both within and between regulatory regimes. To facilitate uptake individuals mus be encouraged to use the system by exchanging their activity for the potential to receive advisories for devices from regulators and manufacturers and by checking the providence of the items they are using. I falls then to teams, who gain value from the aggregation of data and from the better management of their inventory to be the billable parties in the Med-Dev blockchain.

Implementation Implementation will be based by creating the above services and adding them into the EOS.IO architecture. The Med-Dev foundation will fund the creation and ongoing running of services by issuing revenue return tokens.

The foundation will ICO 20% of revenues within the blockchain to finance the building of the Med-Dev blockchain. Ie 20% of all revenue from the sale of tokens on the blockchain will be distributed to the participants of the ICO.

Some of the ICO tokens will be pre-sold at a discount of 30% to recognize the risk

Technical Requirements

The following section goes on to look at implementation based on the EOS.IO architecture and follows the same pattern as their white paper.

Consensus Alogorithm DPOS	Utilizing EOS's DPOS transaction will be confirmed with 99.9% certainty within 1.5 seconds.
Accounts	Individuals will be able to assign their own user name
	Usernames can be associated with email accounts to allow invitations to be sent or employees of entities to be identified
	Usernames can be associated with multiple domains. This allows one individual to be associated with multiple teams.
Messages & Handlers	Each account will be able to send and receive messages Messages can be automatic. Messages can be user generated. Message handling scripts will be held in the private database of each account.
Role based Permission Management	Weighted hierarchies will be used to manage permissions within each organisation giving multi user control over token use within the Med-dev blockchain. Hierarchies are based on the following classifications
Individual	All users must have an individual account
Team	A team has its own individual account. A team must have individuals, but an individual does not need to join a team
Company	A company has its own individual account. A company may have many teams, but a team can only have one company
Regulator Team	A regulator team must have individuals, but an individual does not need to join a regulator team
Regulator	A regulator may have many regulator teams, but a regulator team can only have on regulator
Service	A service must be owned by a team. A service can represent many teams, many individuals or a combination of both.
System	The system will issue Tags (to represent other forms of unique ID's). Any machine readable code can be scanned and it, along with its tag, will be stored on the blockchain - the code scanning activity will still be recorded (and a tag assigned) nc matter the format of the code.
	Validation will look run analysis of all codes being presented and consider temporarily or permanently suspending individual nodes if they repeatedly send data that is not useful to the community. This process will exist to prevent spamming activity.
Named Message Handler groups	A key requirement of Med-dev is to efficiently disseminate information on transactions between teams, companies and regulators.
	for example - a device has been marked as used and destroyed by a hospital. The hospital team needs to know this to manage their inventory and ensure they have a device on hand for the next life saving operation, the manufacturer should be informed to understand how long their stock is being held and increase efficiency i

	the system, the distributor might then be informed to replace stock as quickly as possible. Named message handler groups exist to allow contracts to know, and to efficiently inform, relevant parties of the actions their individual has made.
Permission mapping	This allows individuals to take actions on behalf of a team - for example issue a recall. The origin of the recall can be found within the company or regulatory team, but to all other users of the system, the recall comes from (and can be verified in th block as coming from) the team
Evaluating permissions	EOS.IO can evaluate permissions in parallel and understands hierachy in order to assess if permissions are valid. For More details see their technical paper
Messages with Mandatory Delay	Certain actions can carry a forced delay to allow other owners to countermand them. One such action could be a recall notice. There were 30 million recall events by the US FDA in 2015 - recalls are costly, and issuing one in error can cause considerable patient distress and cost.
Recovery of stolen keys	Individuals will select partners to allow them to reset their accounts (equivalent of requesting a new password) - the partner will have to agree to reset account - creating a strong protection against hackers. Team access will be suspended on reset and will need to be reauthorized by a correctly permissioned team member.
Minimizing communication Latency	To allow accounts to exchange records rapidly (sub 3 seconds) and thus confirm information about the product being scanned and, if relevant, its status, messages utilize block cycle threads, transactions Receiver and Notified accounts process so that transactions generated in one cycle can be delivered to any other block cycle. This is discussed in full in the EOS whitepaper.
Partial Evolution of Blockchain state	Some full nodes will only run specific applications. As an example the oracle node for interface and reference with the FDA's GUDID database data set will not run any other services. In fact multiple oracle nodes may be utilized to allow fast transmission of headline information about a Device Identifier (Company name, product name, product catalogue number. Product recall status) as opposed to the full GUDID listing, which carries considerably more data).
Conclusion	There is a some risk in using an unproven blockchain technology, but as existing chains are not viable for Med-Devs purposes, it is preferable to use a pre-funded community recognized chain as opposed to reinventing the underlying architecture for one market vertical. Creating the med-dev blockchain on the EOS.IO platform overcomes previous technical barriers to entry. It keeps costs low for community members and allows the proper allocation of those costs within the community. The advantages of the med-dev blockchain for utilizing unique identifiers to their full potential will reduce costs all along the supply chain and most importantly improve patient outcomes and save lives.