A Blockchain-Based Approach to Drug Diversion Monitoring

Steven J. Branda, Randall A. Sendek

Mayo Clinic

Prescription drug monitoring programs are an essential element for controlling diversion of drugs for sale or abuse. Most US States have laws which institute drug monitoring programs, but current monitoring programs are generally not as widely-adopted or effective as the demand for drug management requires. This paper proposes a drug monitoring solution based on blockchain technology and Internet of Things inspired smart dispensing hardware, designed to address the limitations of current drug monitoring programs.

1. Problem Statement

"Doctor shopping" has traditionally referred to a patient obtaining controlled substances from multiple healthcare practitioners without the prescribers' knowledge of the other prescriptions. Prescription Monitoring Programs were supposed to be setup to help slow doctor shopping by patients.

Forty-nine States and the District of Columbia have laws which institute drug monitoring programs. As part of those laws they have set up centralized databases used to help track prescriptions of controlled substances to patients.

According to a new study from Johns Hopkins Bloomberg School of Health, only 53% of surveyed physicians use prescription drug monitoring programs, and less than three-fourths of physicians knew about their state's monitoring program. The study (Rutkow, Turner, Lucas, Hwang, & Alexander, 2015) shows that while physician adoption of prescription drug monitoring plans has increased rapidly in the last few years, there is still a lot of work to be done to make them more effective.

Prescription monitoring program use has shown slow growth. Many factors have been contributed to lack of adoption, including:

- Poor timeliness of data
- Poor accuracy of data
- Complexity of data and data retrieval
- Reliability of the database and connections to it

The second problem with current prescription monitoring program solutions is that there is no mechanism to track usage of the drug. We cannot generally determine whether a drug is being used as prescribed, only that a prescription is filled and or re-filled.

2. Proposed Use of Blockchain for Drug Monitoring

We propose a solution that would create a transparent mechanism which is shared, open, and easy to use. This mechanism would provide a way to track prescriptions from the inception of the order all the way to dosing of the drug.

The solution would provide a real-time mechanism of checking the current state of any patient's medications.

The solution would implement a tiered system of devices which would allow easy access to the data. These devices would include:

- Smart drug dispensers
- Smart phones
- Provider order entry systems
- Pharmacy order fulfillment systems

All these system would share a data store based on blockchain technology. The use of this technology helps resolve a number of issues in the current centralized database solution.

- Timeliness of data – how often does a pharmacy or provider load data into the centralized system? With blockchain technology all of the transactions are in the system immediately.
- Complexity of data and data retrieval – In the centralized database system retrieval of data and the assimilation of that data into the provider's standard system is a complex and arduous task. With blockchain technology the data is simple to access and easy to assimilate.
- Reliability of the database and connections to it – In centralized system connections can go down. With blockchain technology the solution is distributed and far more reliable.

Blockchain technology also brings an inherent transparency to the process. At every step of the process there are checks and signs offs to approve moving to the next step of the process.

For example, in our system, when a provider and patient meet and it is determined that a prescription is needed, the prescribing provider will check the blockchain for currently active prescriptions for the patient. This check will tell the provider if:

- There is currently an active prescription for the same drug within a certain time period.

- There is currently an active prescription for a drug from the same family within a certain time period.

If the blockchain returns an active prescription for the drug, the request is canceled. If there is no currently active prescription, the provider will contact the selected pharmacy with the order information. Upon seeing the order information come in from the provider, the pharmacist creates a buy order for the transaction of the requested prescription on the blockchain. The pharmacist invites both the provider and the patient into the transaction via encrypted messaging. The requesting provider and patient become required signatories on the transaction. At this point information for the prescription is appended to the transaction. This information will include:

- The doctor's identifying info
- The script information
- The patient's identifying info
- The timestamp of the order

This is similar to the information that is already collected under prescription monitoring programs.

The patient shows the pharmacist the relevant script information and the pharmacist finds the corresponding order. The patient then signs the transaction.

While the patient is signing the transaction, the provider will be contacted to sign the transaction with his/her key.

Upon seeing that the patient and doctor have both signed the transaction, the pharmacist then fills the prescription and signs the transaction. Once signed by the provider, the patient, and the pharmacist, the transaction is marked as complete.

At this point the blockchain solution we are proposing can go one step further than current prescription monitoring programs. This solution can help track misuse or overuse of the drug by the patient. By utilizing a smart dispenser connected to the blockchain by Internet of Things (IoT) technology, every dose can be accounted for on the ledger. As the patient takes a dose, the smart dispenser will check the blockchain for the last time the prescription was dosed to the patient. It will also check the original prescription to verify that the dose is due. If the dose is found to be valid, the smart dispenser will enter a ledger transaction to document the dispensing of the new dose of the prescription.

As the dosing continues, the smart dispenser can determine that the prescription has fallen to a certain threshold. Once this threshold has been reached the smart dispenser will initiate a new prescription order by duplicating the original order placed by the physician. The will restart the

process, of necessitating the provider, the patient, and the pharmacist all to sign the new transaction.

3. Solution Design

A blockchain is a data structure that keeps track of state change in a system. As a system operates and generates events that change its state, these events are packaged up into blocks at a regular interval and added to the end of the data structure (Buterin, Ethereum White Paper: A NEXT GENERATION SMART CONTRACT & DECENTRALIZED APPLICATION PLATFORM, 2013). Each block contains the cryptographic hash of the previous block, making the newest block dependent on all blocks that came before it, thereby "chaining" them together. Thus the blockchain not only contains the entire history of state change events in a system, but also captures the order in which they occurred. This characteristic makes blockchain effective for implementing a ledger of transactions, and it is employed in crypto-currencies like Bitcoin.

Crypto-currencies are a specific example a decentralized peer-to-peer system. In such a system, multiple distinct parties can participate without a centralized authority, and yet come to agreement on the global state of the system. This agreement is facilitated by using a blockchain as a distributed trusted ledger of transactions, of which all participants can have a copy. In order to create this distributed trust, these systems introduce three behaviors around the blockchain. First, all participants in these systems are programmed to trust the longest, valid blockchain above all others. This provides a clear mechanism for resolving conflicts that typically make distributed trust difficult. Second, each block contains a value that validates the block as authentic. Bitcoin uses proof of work to provide block validation. A Bitcoin block is only valid under the following conditions

- It contains the SHA-256 hash from the previous block, which exists and is valid.
- All the transactions it contains are valid.
- The blocks timestamp is greater than the previous block, but by no more than 2 hours.
- It contains a computed nonce value that causes its SHA-256 hash to be below a certain value threshold.

This nonce value is the "proof of work" in the Bitcoin system because it can only be computed by brute force by repeatedly rehashing the block with a different nonce value until one provides an acceptable result. In Bitcoin, this process is called "mining" because participants are rewarded with new Bitcoins for generating a valid block, and it is costly in terms of time and energy. This cost deters and prevents malicious actors from creating a forged history.

Another form of block validation is called "proof of stake" (Buterin, What Proof of Stake Is And Why It Matters, 2013). Proof of stake algorithms randomly distribute the right to make the

next block amongst miners depending on their overall stake in the system. The fundamental unit of stake in any decentralized system is the unit required to participate in that system. For example, in the Bitcoin system, this unit is bitcoin. In order for users to participate in Bitcoin, they need to have a miner process their transaction into a valid block. Miners are incented to do so by the reward they get for generating a block, but also from a transaction fee the user can offer to process the transaction. When mining in a proof of stake system, miners will send units they hold to themselves as transactions in the block as their "proof of stake". The algorithm built into the system that determines block validity uses this proof of stake and current state of the system to determine if the block is valid. These algorithms are designed so that miners with a higher proof of stake are more likely to get the right to create the next block - thus the cost that deters malicious actors is the cost of obtaining a significant proof of stake, instead of the computational cost of proof of work. The key advantage of this approach is that it does not require the overall system to waste a lot of computational resources in order to create distributed trust. Also "proof of stake" can be mixed "with proof of work" to tune the security/cost ratio of the overall system.

Blockchain systems use public / private key encryption to anonymously identify individual users, and to prove the validity of transactions in the system that affects their resources. A user's public key effectively becomes their unique "name" in the system. When the user generates a transaction, they digitally sign it with their private key. All other parties on the blockchain can use the user's public key to verify this digital signature, proving the transaction was initiated by the user and not a third party.

The use of public / private key encryption is beneficial from a privacy perspective since private / public key pairs are made up of just two large randomly derived numbers. Neither of these numbers encodes any personally identifiable information, which allows activities on the blockchain to be attributed to a specific user without exposing any of their sensitive information publically. Users would still be required to register their public key with trusted authorities like health care and health insurance providers, since these entities would need to use them to identify the user on the blockchain. However, users would still retain control of the private key, so even if one of these trusted authorities is compromised, the attackers would not get the one thing they need to impersonate users in the system: the private key.

In addition to the features that create distributed trust, another very important feature of these decentralized systems is "smart contracts." Smart contracts are executable code that is stored as part of the transaction on the blockchain. In order for a transaction to be valid, which is necessary for a miner to generate a valid block, the executable code must be successful. Smart contracts are required by all decentralized peer-to-peer systems in order to achieve any level of general functionality. Bitcoin has a rudimentary capability for smart contracts, but systems like

Ethereum™ have more robust smart contract capabilities that can be applied to the healthcare space.

The first such capability allows smart contracts to be posted to the blockchain as an open call for some kind of exchange. For example, a user could post a smart contract that takes 10 coins, and returns the code for a $10 Amazon™ gift card encrypted with the public key of the user who sent the coins. This is just a simple example, and systems like Ethereum™ can support multi-party contracts, which are useful in the healthcare space.

The second such capability allows smart contracts to generate new kinds of tokens that can be used to fulfill smart contracts. For example, a smart contract can be generated that allows a manufacturer to register devices they just made to the blockchain. The smart contract would require input digitally signed with the manufacturer's private key, and would generate one token per device and assign those tokens to the manufacturer. Then when the manufacturer sells the device, they would transfer that token to the end user or distributor on the blockchain.

4. Technical Design

Our solution leverages blockchain in order to solve the problems we identified with the disbursal and use tracking of controlled substances. We propose a multi-level, decentralized peer-to-peer system managed by a distributed blockchain ledger of transactions. Since some of the peers in the proposed system are IoT devices, we will use the framework established by Samsung and IBM in their ADEPT proof of concept to categorize and describe the participants and capabilities required for our system (IBM Institute for Business Value, 2015).

The ADEPT paper proposes that a decentralized system capable of managing IoT devices needs three fundamental peer-to-peer capabilities: messaging, file transfer, and coordination. The ADEPT paper identifies existing open source systems that can provide the required messaging and file transfer capabilities, and proposed blockchain as the mechanism for coordination.

In order to make blockchain work across devices with significantly different levels of computational and storage resources, the ADEPT proposes classifying devices with a three level hierarchy.

1. **Light peers** are devices with the lowest level of processing and storage capability. These devices will be the most numerous in an Internet of Things, but they will also be dependent on high level devices for participation. The proposed "smart drug dispenser" would be considered a light peer.
2. **Standard peers** are devices with an intermediate level of processing and storage capability. It is unlikely they would be able to store the entire blockchain, but they could likely store the current block, which contains the entire current state of the blockchain.

This allows them assist light peers in achieving the three fundamental capabilities by acting as both a cache and a store and forward mechanism. A smart phone, tablet, or laptop would be considered a standard peer.

3. **Peer exchanges** are higher end devices with enough processing and storage capability to hold the entire blockchain. These devices create the backbone of the distributed trust system for a given scope (local, regional, global).

The top level of the proposed solution would be a nationally scoped blockchain maintained between drug manufacturers and prescription networks. Drug manufacturers will use smart contracts to create tokens that represent dosing units of a given drug at the point of production on the blockchain. When these dosing units are packaged the drug manufacturer uses another smart contract to generate a token that represents a shippable package of drugs. When these drugs are distributed to a pharmacy, these tokens will be transferred to the pharmacy using a smart contract. When the drugs are shipped out, the drug supplier will post a smart contract that will operate as such:

- Required Input
    - A count of all the drug units in the received shipment. This can be generated by the pharmacy's inventory system after the shipment is scanned in. Security can be increased by the drug company physically identifying each package of drugs with its associated token. In this case the smart contract would take a list of the package ids.
    - A unique identifier for the shipment that has been digitally signed by the private key of the pharmacy system, or the actual employee for additional security.
- Output
    - For every package or drug token sent to the smart contract, transfer that token to the pharmacy.
    - For any missing package or drug unit tokens, transfer that token to the address of the drug manufacturers stop loss program.

The prescription networks will operate similar to the drug manufacturers, and use smart contracts as the basis for their activity in the system. When a doctor sends a prescription through a prescription network, it will be published to the blockchain as a multi-party smart contract that will operate as such:

- Required Input
    - Patient
        - Coin transfer to cover the cost of the drug.
    - Health Insurer
        - Coin transfer to cover the cost of the drug.

    - Pharmacy
        - Drug dosing tokens that fulfill the prescription
        - Smart drug dispenser that will hold the drugs
- Output
    - Any overage of drug cost is refunded to patient. If the health insurer covers the full cost of the drug, then the total cost of the transaction will net to zero for the patient.
    - Coins transferred to pharmacy to cover drug cost.
    - Coins transferred to subscription network to cover fees.
    - Drug dosing tokens transferred to smart drug dispenser.
    - Smart drug dispenser transferred to patient.

This usage of smart contracts on both the supply and demand side of the system has some clear advantages. First, pharmacies will be compelled to participate in the supply side of the system because it is the only way they can receive the drug dosing tokens they need to fill prescriptions. Secondly, smart contracts can also encode the number of refills and the minimum number of days between them which can prevent someone from filling the same prescription twice. Pharmacies will have no motivation to disburse the drugs unless the smart contract is successful.

The participants of the proposed system are mainly comprised of peer exchanges and light peers. The peer exchanges are the systems managed by the drug suppliers, prescription network, health insurance providers, and the pharmacies. Peer exchanges may not, however, all be equal: drug suppliers, prescription network, and health insurance provider will probably be scoped at a national level, and contain the entire blockchain, while the pharmacies will mostly operate at the regional scope, and only store the blocks relevant to their regional peers. This will decrease the cost of the more numerous peer exchanges that would be installed in pharmacies, so that each brick and mortar store can have one. This allows the regional capacity for processing for managing the blockchain grow proportionally with the regional supply and demand for controlled substances. Proof of stake can be used at both the global and regional levels of the blockchain to decrease the computational cost of block mining, so that the peers can also operate as the miners.

The main light peer will be the smart drug dispenser. This device will be supported by the peer exchange at the time of drug disbursement and by a standard peer, like a smartphone or smart TV, once it has been transferred to the patient. The smart drug dispenser will keep track of when it is actuated to dispense a dose. Whenever a dose is dispensed it will place a transaction on the blockchain to transfer the drug dosing token from itself to the patient. These spent

doses can be required in addition to previously described prescription inputs in order for a prescription smart contract to process a re-fill.

Another advantage discussed in the ADEPT paper is the ability for light and standard peers to self-associate with each other to improve the overall system. In the proposed system the smart drug dispenser might notice that its owner also has a smart watch (light peer) or smart phone (standard peer) registered to a local or regional block chain. It could initiate a trust relationship with either of those to generate reminders or messages when the patient should take a dose of drugs. Also, in the case where the drug is treating a chronic condition, it can generate a reminder to get a refill, or even process the refill itself. This could be accommodated by the patient posting a smart contract to the blockchain that allows its standard peer to send coins and drug dosing tokens on their behalf to the smart contract that re-fills the prescription. The refill can be automatically mailed to them or they can receive a notification from their standard peer that it is ready to be picked up.

The prescription smart contract can also use the state of the blockchain to determine the patient's current supply of a given drug, vis-a-vis drug tokens assigned to dispensers currently held by the patient and drug dosing tokens currently held by the patient that have not been spent to re-fill the prescription. If the tokens are over a certain threshold the smart contract can assume the patient is filling multiple prescriptions for the same drug simultaneously and fail.

A final note is that the proposed mechanism describes many instances where one peer needs to know about a smart contract posted by another peer. Smart contracts are posted to the block chain, but it is not always practical to scan all the smart contracts in the block-chain to determine which ones apply. For the most part we can expect the peers involved to use peer-to-peer messaging to notify each other when the smart contracts are posted to the blockchain.

5. Summary

Prescription drugs diverted from legitimate medical application for sale or abuse are a significant problem in the US health care system. The complexity of monitoring and controlling the distribution of such drugs is amplified by the significant diversity of providers, payers and pharmacies in the US system, and the lack of a common, trusted mechanism for monitoring prescription fulfillment and use. We propose a shared, trusted mechanism based on blockchain technology and taking advantage of nearly ubiquitous connectivity to use smart, IoT dispensing devices, that addresses these difficulties in a novel fashion, that has incentives for participation by all elements of the drug delivery chain.

Works Cited

Buterin, V. (2013). *Ethereum White Paper: A NEXT GENERATION SMART CONTRACT & DECENTRALIZED APPLICATION PLATFORM.* Retrieved 08 08, 2016, from Blockchain News: http://www.the-blockchain.com/docs/Ethereum_white_paper-a_next_generation_smart_contract_and_decentralized_application_platform-vitalik-buterin.pdf

Buterin, V. (2013, 08 26). *What Proof of Stake Is And Why It Matters.* Retrieved 08 08, 2016, from Bitcoin Magazine: https://bitcoinmagazine.com/articles/what-proof-of-stake-is-and-why-it-matters-1377531463

IBM Institute for Business Value. (2015). Empowering the edge: Practical insights on a decentralized Internet of Things. Sommers, NY: IBM Institute for Business Value. Retrieved 08 08, 2016, from http://www-935.ibm.com/services/multimedia/GBE03662USEN.pdf

Rutkow, L., Turner, L., Lucas, E., Hwang, C., & Alexander, a. G. (2015, March). Most Primary Care Physicians Are Aware Of Prescription Drug Monitoring Programs, But Many Find The Data Difficult To Access. *Health Affairs*, pp. 484-492.