A BLOCKCHAIN PROFILE FOR MEDICAID APPLICANTS AND RECIPIENTS

Institute for the Future
Blockchain Futures Lab[1]

Authors: Kathi Vian, Alessandro Voto, and Katherine Haynes-Sanstead

SUMMARY OVERVIEW

Blockchain technology has the potential to address many of the privacy, security, and interoperability problems that plague health IT and indeed health research. In this paper, we introduce a specific blockchain-based innovation: the **smart health profile**. This profile uses such blockchain tools as tokens, wallets, smart contracts, and oracle services as a foundation for rethinking the way that individual health and financial information is accessed and used across a wide variety of systems and applications. To introduce the smart profile, we focus on a solution to the specific problem of churning in the Medicaid program—that is, the constant exit and reentry of beneficiaries as a result of eligibility changes. However, as a sophisticated tool in the blockchain toolkit, the smart health profile can also prepare health IT and health research to take advantage of emerging artificial intelligence systems and may eventually lead to entirely new models of health care delivery.

INTRODUCTION

Blockchain technology is creating a new infrastructure for managing flows of money, information, and activity without a centralized database or administrator. It enables interoperable distributed systems that allow people and machines to use data without collecting it or even seeing it. It supports smart contracts that can automatically perform financial or other data transactions when specified conditions are met. Through so-called encrypted pseudonymous accounts, it allows individuals to control their own data and privacy needs, while providing a permanent and public transparent ledger that tracks the veracity of information.

The affordances of this new technology make it well suited to solving some of the most complex problems in health data, health financing, and health care. Consider specifically the following promises of blockchain solutions:

- ***Protection of privacy****:* A foundational idea in blockchain solutions is the *zero-knowledge proof*—that is, the ability to verify the data in a record without ever actually seeing the contents of the record. This ability makes it possible for people and machines to act on sensitive health, financial, family, and citizenship data without actually revealing it.
- ***Protection against fraud:*** The *immutability of records* is a well-known feature of blockchains. Blockchains run on networks of many personal computers (or other

[1] For more information about the Blockchain Futures Lab at IFTF, see http://www.iftf.org/blockchainfutureslab/

devices), and every record is held by multiple devices. If someone tries to alter a specific record—for example, to erase a medical test result or change the amount of a direct-deposit to an account—the record is immediately flagged as potentially fraudulent.

- ***Interoperability across diverse systems and data formats:*** Blockchains can reduce all kinds of data to a series of transactions that can be represented as *tokens*. Tokens can represent currency (as in the case of Bitcoins), but they can also represent data, such as YES/NO responses to questions like, "Does the person associated with this account qualify for benefits?" So-called *oracle services* can translate data from existing databases in a variety of formats into tokens that can then be tracked and accessed in the blockchain. No single grand scheme is necessary to assure interoperability.
- ***Control of access:*** Blockchains use *encryption keys* to access the records in the blockchain. Usually, there are two encryption keys—a private key and a public address. The public address makes the existence of the record visible. It might reveal, for example, all the instances of tests for hepatitis C. The private key might unlock the test results to the holder of the key. This basic formula creates great flexibility for controlling access to records and the data they represent.
- ***Pseudonymity:*** Anonymous data is often used in health research to compile the results of therapies or measure the extent of disease in a population, for example. It can be used to create relatively complex profiles that reveal correlations between diseases and behaviors or treatments and outcomes. However, if you want to use a profile to manage a specific individual's health care, a *pseudonymous profile* is better suited to act as a broker between the individual behind the profile and a host of services that interact with that profile.

Taken individually, each of these blockchain promises is clear enough. However, taken together, they open the door to an entirely new way of thinking. And this is what we propose to do with this paper—to suggest a new way of thinking about an individual's personal records that will ultimately create both opportunities and challenges for existing health institutions and markets of all kinds. At the heart of this new way of thinking is the concept of a **smart health profile**.

THE SMART PROFILE: PSEUDONYMOUS APPROACHES TO A DISTRIBUTED IDENTITY

When we think of a profile in the traditional world of databases, we often think of it as a repository or a container of all the relevant information about an individual—like a web page on a social media platform or a Mint account that keeps your financial profile up to date by aggregating all your expenditures and sources of income in one place. That profile is uniquely linked to you, and even though it's password-protected, it is vulnerable to identity theft, hacking of the contents, or abuse by advertisers of every ilk.

In the world of blockchains, a profile is not really a repository. The blockchain is simply a distributed record of transactions. It's dynamic. It tracks flows of money or information. As such, it invites us to rethink our basic concept of a profile, not as a container of information, but as a service that provides on-demand access to specific information that

may reside anywhere. This information may be represented as transactions on the blockchain or as records in traditional databases. The services may be simple, as in the case of Bitcoin wallets that can transfer coins to your health care providers. Or they could be quite sophisticated, aggregating and verifying data from a wide variety of sources to respond to a specific question about whether or not you're currently qualified to receive Medicaid insurance.

At the heart of the blockchain profile is *a truly distributed identity*. It would be possible to set up the profile to aggregate the many blockchain markers of your identity in one place, but then it would then be vulnerable to all the same problems as a traditional database profile. However, *by thinking of the blockchain profile simply as a broker that can answer questions about you as the need arises*, your identity remains distributed. No one can ever see everything about you at once, including yourself.

What makes the profile smart is that the services it provides can be quite intelligent. It can make sophisticated queries and actually trigger an action when certain conditions are met. For example, suppose you had a smart drug dispenser that recorded every dose you take as a transaction on the blockchain. A profile service might check everyday to see if you've taken your pill and automatically order a refill when you've used up all the pills. Over time, however, an AI service might become much more sophisticated to use a combination of information about your vital statistics from your wearable device and population studies of people using the various medications for your condition and either recommend a different regimen to your physician or simply cut out the middleman and direct your pharmacist to deliver you a new prescription.

Note that your smart profile, acting as your broker, would never need to know who you actually are. In the scenario just described, it would simply send the new prescription to an encrypted address; only you and your pharmacist would have the private key to unlock the prescription. This is the practical meaning of a pseudonymous profile: it presents a face to the world on your behalf, a face that only you can claim.

To understand the specific technologies behind this smart profile—and its potential power as a fundamental building block in a blockchain solution to health IT and research—let's look at an example where the it could be implemented at a scale that might actually change the health outcomes for millions of people. Let's see how it would work to solve the problem of churning in the Medicaid program.

THE PROBLEM:
CHURNING IN THE MEDICAID PROGRAM

Unlike Medicare, Medicaid is a means-tested program in which eligibility is determined based on income thresholds and financial guidelines determined by state governments. As a result, millions of low-income adults struggle to maintain continuous coverage and continuity of care as a result of the rules of enrollment and re-qualification. A complex application process may require a waiting period of up to 45 days to verify eligibility. Depending on which state is administering the Medicaid program, eligibility may be certified for various periods up to a year, during which recipients must report changes in

income, dependents, residence, and other information that could alter their eligibility. If they become ineligible, even for a short time, they must reapply, and in any case, they must requalify when the certification period runs out. If they do not report changes or requalify in a timely manner, they must reapply again with the initial 45-day waiting period. As a result of this turnover—often referred to as "churning"—the average adult in the Medicaid system is covered for only about four-fifths of the year.[2]

The interruptions in coverage are costly across all the stakeholders in the Medicaid program. *For patients,* gaps in coverage can mean that they lose access to care that could prevent more serious illness and even death. The relationships they've established with existing health care professionals may be interrupted, and they may lose access to long-term prescription drugs. *For the health care professionals* who care for Medicaid beneficiaries, churning means that they need to continuously check for eligibility or potentially incur loss of income. *For the Medicaid program*, churning means higher average costs per person in the system. Studies show that the average monthly Medicaid cost per person drops by nearly 50% when coverage is continuous for even 12 months—from $597 to $345 per person per month. In addition, the reapplication process carries a high administrative cost for the program.[3]

Ultimately the result of all these costs is poorer health outcomes for a significant portion of the poor adult population and a higher health burden on society as a whole. Clearly, an information infrastructure that could streamline the qualification, requalification, and interim coverage options for poor adults would greatly improve the overall functioning of the Medicaid system, improve the lives of millions of people, and even build greater productivity of the social economy.

At the same time, the obstacles to grand solutions are many. Chief among them is the distributed nature of the many records that feed the decisions of patients, providers, and Medicaid administrators. The qualification process must rely on financial information to be verified by banks and other financial institutions; on employment information to be verified by diverse employers; on medical information from patient records (for example, regarding qualifying disabilities); and on citizenship information from different government agencies, ranging from the Social Security Administration to Motor Vehicle Bureaus and others that can provide proof of residence. Furthermore, the burden for assembling this information and granting permissions to access it rests with applicants who are often ill-prepared to navigate the complex bureaucracy necessary for verification.

These obstacles—distributed data sources, a high need for simultaneous privacy and transparency, the requirements for verification, and the need for intelligent assistance in much of the process—are precisely the obstacles that a distributed blockchain solution like the smart health profile can address.

---

[2] Leighton Ku and Erika Steinmetz, "Bridging the Gap: Continuity and Quality of Coverage in Medicaid." School of Public Health and Health Services, George Washington University, September 10, 2013, p 1.

[3] Ibid., p 5.

THE FOCUSED SOLUTION:
A SMART HEALTH PROFILE FOR MEDICAID APPLICANTS AND RECIPIENTS

The smart health profile offers a robust solution to the problem of churning in the Medicaid system. As already explained, the profile is not a data repository. Instead, it's a series of services that access encrypted information about the recipient's age, citizenship status (including social security number and current residence), family income, and family composition, as well as medical information, such as disabilities. It makes this data available for specific purposes. Through a client application, the profile also provides user services, such as notifying the owner of the profile when his/her Medicaid status changes and automatically reapplying for benefits or insurance options.

We will describe the technological approach that assures privacy, interoperability, verification of all the necessary information, and immutability of the records below, but first consider three possible scenarios that such a profile might enable:

Scenario 1: Loss of benefits. If a person has been receiving Medicaid and increases his/her income, reduces family dependents, or recovers from a disabling illness, the pseudonymous profile automatically notifies the owner and the Medicaid qualification system of the change in qualification status. At the same time, the profile writes an insurance policy that is prequalified to maintain continuity of treatment with existing providers (if possible), that is affordable given the financial information available, and that optimizes for the kinds of illnesses the owner has suffered from in the past.

From the owner's point of view, there is a simple notification by text or mobile app that gives the owner the option to approve or disapprove the new insurance contract. *If the owner approves,* the profile forwards relevant, provable, and time-stamped data associated with the pseudonymous profile through end-to-end encrypted channels to the insuring agency, alerting the primary care physician of the change in insurance. All approvals are logged in an immutable record of coverage, which can be referenced in further inquiries. The profile effectively acts as a smart broker for health insurance. *If the owner disapproves,* the profile offers a series of options for P2P gap insurance or perhaps a P2P lenders fund where blockchain investors can invest in the profile, providing a fund for the owner to draw against for interim medical care.

Scenario 2: Reinstatement of benefits. In this scenario, the owner of the profile loses a job, takes on a new dependent, or is diagnosed with a medical condition that qualifies as a medical disability. The profile immediately notifies the owner, who can file for reinstatement with a simple YES response, or can decline Medicaid. If s/he declines, the owner has the option to continue the existing insurance or seek a new plan through a mobile app or web interface. If the owner approves the reinstatement action, the relevant, provable, and time-stamped qualifying information is forwarded to the Medicaid reinstatement system, and when it is approved, the existing health care insurance or lenders fund is discontinued automatically.

Scenario 3: Change of state of residence. In this scenario, the owner of the profile moves to a new state where the rules for qualifying are different and Medicaid recipients need to reapply. To manage this situation, the profile flags any change of address transaction and prequalifies the profile owner under the new rules. It alerts the owner with a simple text or mobile app interface that s/he either qualifies or doesn't. If the owner qualifies, s/he can simply respond YES, and application is activated. In the gap between application and acceptance, the profile offers a series of options for P2P gap insurance or a P2P lenders fund where blockchain investors can invest in the profile, as in Scenario 1.

In none of these scenarios is the Medicaid office or the insurance company ever privy to the actual identity of the recipient. They are transacting entirely with the pseudonymous profile, which serves as a confidential broker between all the services, both private and public. The medical record carries a flag that indicates the insurance/Medicaid status of the patient, and the flag is updated by a periodic pull from the profile, but the medical professional or health care organization never sees the complete profile. In fact, the owner does not ever see the entire profile either.

Technically, this solution might be enabled by a three key blockchain components: a highly deterministic (HD) wallet, one or more smart contracts, and an oracle service. Let's look at each of these in turn.

The HD wallet. In the world of blockchain transactions, a wallet is a service that helps a user manage ownership and transfer of their virtual assets. In order to verify ownership of these assets and authenticate transfers, the wallet must establish an identity for the user. To do so, it provides a pseudonymous identity comprised of two cryptographic components: a public key and a private key. The public key serves as a publicly shared address to which other people and machines can send virtual assets and queries about those assets. The private key is kept secret, but can be combined with the public key to validate actions taken on behalf of the user, including transfer of funds or submitting data.

A Bitcoin wallet, for example, verifies the owner's bitcoin balance and transfers bitcoins (tokens) according the owner's instructions, once the private key is provided. It provides a simple interface for Bitcoin owners to track and spend their coins. But a wallet could just as easily hold virtual "tokens" representing validated data from an application form, for example. A token, in this case, might indicate whether or not someone has been diagnosed with a chronic condition like asthma by a certified docator. If the condition is certified, the person would receive a token representing this condition, just as they might receive a bitcoin. These validated bits of data could then be transferred between the owner and parties with whom the owner is interacting, including healthcare providers and financial institutions.

Early blockchain wallets created a single static address as the public key. This presented a security concern, as analytical tools could track ongoing public use of the profile, to construct a high-level picture of the account user and their relationship to

other account holders. An HD wallet enhances the security and privacy of these early wallets by using a single seed to algorithmically generate a new address for each transaction. This offers the ability to maintain ownership and privacy of the wallet if one of the owner's transactions are de-anonymized or otherwise compromised. More important for our Medicaid scenarios, it assures that all the data transactions managed by the wallet are never visible as a whole (even to the owner), while they can still be exchanged with so-called zero-knowledge proofs for validation.

This means that "tokens" linked to the wallet can be spent—or more conceptually, the information in the profile can be verified—without anyone, including the owner, ever seeing the totality of the data that is linked to the wallet (that is, the profile). For example, the profile can verify that the owner has a unique and valid social security number without revealing the actual number. A profile could verify that a user's blood pressure is above a certain threshold, without seeing the blood pressure reading itself.

The smart contract. The second enabling technology of the profile is the smart contract. Smart contracts were implemented in more recent blockchain systems, most notably by Ethereum. They allow code instructions, as well as data inputs and outputs, to be held, verified, and executed by a network of computers, rather than one trusted computer. In its simplest form, a smart contract executes a transfer of tokens when one or more conditions are met. In our profile scenario, the smart contract might be used to execute the following types of transactions:

- If a valid and unique social security is number is linked to the profile, send a YES token to the prequalification service.
- If a direct deposit account is linked to the profile, send a YES token to the prequalification service.
- If income in the direct deposit account decreases, send a YES token to the prequalification service.
- If a medical record is linked to the profile, send a YES token to prequalification service.
- If a qualifying disability exists in the medical record, send a YES token to the prequalification service.
- If the owner of the profile is pre-qualified for reinstatement, send a YES token to the owner notification service.

In this design, services might be conceived as smart contracts, formalizing their processes as automated computer code. For example, the pre-qualification service might be a series of algorithms that process the tokens to determine if the profile qualifies for reinstatement, in which case, the service might simply send a YES token to the notification service to activate a series of interactions with the owner of the profile. However, the profile (and its smart contracts) may also need to interact with non-blockchain processes or databases in order to execute their transactions. Interoperability between blockchain and non-blockchain services thus requires our third enabling technology: oracle services.

Oracle services. The third important enabling technology for the profile in this solution is the oracle. The oracle validates information needed for the smart contracts, pulling from a diverse set of data sources. It draws both from databases through API's and from in-person interactions (like blood pressure levels during a doctor's visit). The oracle is a trusted third party, either human or algorithmic, that makes sure information is provided without corruption from either the user or validator. Importantly, oracles allow the profile solution to work without complete interoperability of the many systems the profile must monitor.

The oracle introduces a key point of vulnerability into the profile solution, however. What if it returns the wrong result? What if the data source itself is not trustworthy? What if the oracle itself (or an outside hacker) deliberately tampers with the data? The solutions to this kind of vulnerability involve building a consensus of multiple data sources and a consensus network of oracles.

The smart contract can use formulas that set a standard of consensus among multiple oracles for any particular data point (token). This standard need not be 100% agreement in all cases. While we would want 100% agreement that a given social security number is valid and is being used by one and only one individual, we might be more tolerant of a 90% agreement on the birth city. This tolerance would allow for a degree of flexibility when the contract is faced with mistakes in existing historical records. To assure the honesty of the oracles themselves, we might leverage so-called *M-of-N multi-signature transactions* to create a consensus network of oracles. Multiple oracles would be called by the smart contract, each with just one private key that can be used to sign the data transaction. Because these oracles are competing in the marketplace, they would have an incentive to provide the most accurate and honest data to the smart contracts.

Oracle solutions are at the cutting edge of efforts to build interoperable and integrated blockchain solutions, and innovations in this technology are likely to rapidly improve the security and verifiability of blockchain.

The functional advantages of the blockchain profile solution for Medicaid qualification are many. The profile provides a **single-point interface** to what in reality is a distributed identity, without creating the kinds of vulnerabilities or potential for abuse of centralized databases. The profile removes the burden on the individual of managing an increasingly complex digital identity without compromising the individual's privacy.

Such a profile is also able to provide a wide range of verified and essential data to **a multitude of extensible services** (smart contracts) that further reduce the risk and burden on personal health insurance management. It not only streamlines the complex bureaucratic (and often hampering) processes currently involved in securing Medicaid and other health insurance products; it enables a set of user-friendly products, such as mobile apps, that can proactively assist Medicaid applicants and recipients in managing their health insurance.

The profile further supports the potential for **new kinds of peer-to-peer insurance and health financing products**. By linking the Medicaid information to other health insurance opportunities, it can create an on-demand market for **custom-tailored health insurance products**. For example, it could theoretically configure a plan that provides the best coverage for a nontraditional family with one or more outstanding health requirements—and offer it as an investment opportunity across a wide network of non-traditional insurers. At the same time, it directly addresses the problem of continuity of coverage between Medicaid and other health insurance plans.

In addition, because the profile is also linked to medical records, it can help in the **discovery of the best providers** when medical conditions change or when the owner moves to a new location. It can even facilitate initial choice of new primary care physicians and set up orientation appointments. For impoverished health care recipients, this kind of support would greatly reduce the health care burden on individuals, presumably leading to much improved health outcomes and lower overall costs to the Medicaid system.

One of the key advantages of the blockchain profile-as-broker solution is **interoperability of data**. In the near term, the profile offers the ability to solve a specific problem like churning in the Medicaid program without having to guarantee interoperability across the many divergent data systems that currently define what we might think of as a patient's **Medicaid identity**. In the longer term, however, it also lays the foundation for a much more comprehensive solution to a distributed health infrastructure.

THE COMPREHENSIVE SOLUTION: A DISTRIBUTED INFRASTRUCTURE FOR HEALTH

It should be clear from this description of advantages that the smart health profile is not simply a solution to the specific problem of churning in the Medicaid system. It is actually a template for building out a distributed infrastructure for health. A smart pseudonymous profile could become a basic building block for people to manage their health and health care, supporting the following innovations:

Integration of intelligent algorithms: As a collection of digital services, organized around access to information and smart contracts that can activate functions based on that information, smart profiles can lay the foundation to take full advantage of a wide range of custom-tailored applications that make personal health management and health care services easier to provide and easier to access, likely leading to better health outcomes. The AI prescription generator mentioned earlier is an example.

Accessible health records: Access to medical records currently varies widely across the country. While the ability to obtain copies of specific medical records is a basic right at present, the rules and processes for getting those records can vary from state to state and even institution to institution. And while some states currently have enabled exchange of electronic medical records across providers under some

conditions, the systems are not integrated in many states. Users must often explicitly request transfer of records, sometimes using burdensome procedures. Smart profiles, coupled with user-facing applications, could enable real-time authorization of records transfer or even real-time user querying of records for specific information, such as, "When was the last time profile X had a thyroid test and what was the result?"

Virtual medical consultant: With the advent of the internet, online sites have become important (if sometimes misleading) tools for people who are trying to interpret their symptoms, their test results, or their risks for certain diseases. Without ever compromising the user's medical privacy, a smart profile could match symptoms with medical records and other user data to provide personalized rather than generic medical advice. Combined with intelligent voice interfaces, this basic building block could become the basis of a voice-activated virtual medical assistant, allowing users to ask questions like: What is my current risk for diabetes? Should I consider alternative thyroid treatments at this time? The assistant could even draw on Auger-like prediction services to compile answers to these kinds of questions. These answers might likewise become part of a user's medical profile, alongside more traditional medical records.

New models of health care delivery: Already, many of the sectors of the economy have been disrupted by on-demand models that match service providers with service users in real-time. Matching doctors with patients with specific symptoms in real time is clearly a more complex and privacy-sensitive task than matching drivers with riders or other gig workers with tasks. However, with a smart pseudonymous profile, it would be possible for providers to pre-check the patient records to determine their own ability to respond and for patients to check ratings of doctors, also drawn potentially from a pseudonymous profile.

Medical pattern recognition: Smart profiles could support new medical and epidemiological research practices. Again, without creating vulnerable collections of personal medical data linked to a particular individual, researchers could query millions of profiles to gain high-resolution views of patterns of illness and response to therapies. These queries could include not only medical data, but also all the financial, family, residence, and age information that could reveal a much more complex picture of the correlations among these factors and health outcomes. Some of these patterns could be tracked in real time to manage epidemics.

Clearly such innovations would ultimately reorganize the health and healthcare sector in the profound ways that we're already seeing in other sectors where automation is streamlining services, creating new kinds of workers, and undermining traditional institutions. Theoretically, all of these changes could occur without the blockchain. But the smart pseudonymous profile, with its zero-knowledge proofs and its ability to tap into diverse data streams that are verified through consensus oracle networks, provides a core building block. This building block might be analogous to the html web page that launched the Internet revolution, and might similarly just as rapidly and as extensively launch widespread system change in health and health care.