It Is Time to Seriously Consider Personal Blockchains

Phil Laplante
Penn State

***Abstract*—Much has been written about the benefits of using blockchains for securing transactions in finance, healthcare, supply chain management and more, and some of these benefits are already being realized. But not nearly as much consideration has been given to use blockchains for records of personal transactions. That is, there is great potential for blockchains in certifying and securing the validity, time, and order of various life events, legal transactions, records of achievement, personal contracts, healthcare records, etc. In this article, the motivation for creating personal blockchains is presented. Then, various kinds of personal blockchain implementation possibilities, use cases, challenges, and solutions are briefly discussed. Personal blockchains offer many benefits but pose some challenges and create some concerns. The purpose of this article is to stimulate more discussion and research into these issues.**

In any social and legal construct, securing and validating all records pertaining to any event or transaction is extraordinarily important to protect both the individual and the relevant institutions. Birth, wedding and divorces, titles and patent filings for personal property, educational records, job histories, medical procedures, medications prescriptions, etc., provide a very comprehensive set of records for the life of an individual. The word cloud in Figure 1 illustrates some of the records and related artifacts a person might encounter in a lifetime.

Currently, these kinds of records for an individual are stored in a widely distributed, potentially unsecured way. For example, educational records are maintained by the various schools attended, medical records disparately held by hospitals, doctors' offices and insurance companies, personal and social records in local, state and federal government records offices, legal records in various courts etc. Mortgage applications involve official documents from banks, employers, creditors, taxing agencies, etc. Criminal records are stored on different local, state, federal, and international databases. Also, securing and validating the accuracy of these records are extremely important from legal, medical, ethical, privacy, and practical perspectives. Fittingly, the cloud in Figure 1 is amorphous and disorganized, much like the collective set of records for any individual, and even the person's own recollections of these events, which might be incomplete, out of order, or have incorrect dates.

Digital Object Identifier 10.1109/MITP.2020.2986910
Date of current version 11 September 2020.

Figure 1. Partial word cloud of a person's life events and associated records/artifacts.

For whatever legitimate purpose, trying to integrate and correlate all of these records is a difficult task, and also one that has the potential for error, discrepancy, and fraud. Typical errors include factual mistakes in recorded information, discrepancies in name, address, social security, and other material facts. These errors might not be easily discovered because of the diverse nature and diffuse storage of the records. When these kinds of problems are discovered, they are usually at very inopportune times, for example, when making a loan application, during a job hiring process, or as a red flag indicator that some sort of fraud has been or is being perpetrated. Therefore, it is very much in the interest of the individual, the public, and the government for a way to accurately, consistently, securely, and safely manage every recorded aspect of an individual's life. Here is where the blockchain enters.

BLOCKCHAINS

A blockchain is a collection of immutable records that are maintained across multiple entities. In its simplest form, the blockchain consists of a public transaction ledger and a set of rules for independent transaction validation. Figure 2 depicts a generic blockchain as a linked list of simple record blocks.

Each block is validated by a "nonce"—a number used to solve some cryptographic puzzle. The timestamp will be discussed shortly. The rest of the block data information is transaction dependent.[2]

The variations of blockchain implementations differ based on the type of entity in the network, transaction verification methodology, whether currency is involved in the transaction, and other factors. For example, there are models that permit any entity to participate in the blockchain, but let us consider only those where authorized (permissioned) entities can participate. Here, every permissioned transaction on the blockchain is added to the public ledger, stored in the blockchain, and is validated by other members of the network (let us call them "certifying authorities" or "CAs").

A transaction in such a blockchain could be simply storing information in the blockchain ledger, such as a new medical or educational record. Or, the transaction may be an exchange of assets of some type, for example, the sale of a home, purchase of stock, or payment of taxes. The transaction may be executing a step in a workflow/contract, signifying that the step/event has taken place, for example, birth, death, or marriage. Or, the transaction could trigger a financial event, such as the payment of a recording fee to the state.[2]

TIMING IS EVERYTHING

The term "timestamping" refers to marking the time when a certain event happened. Humans

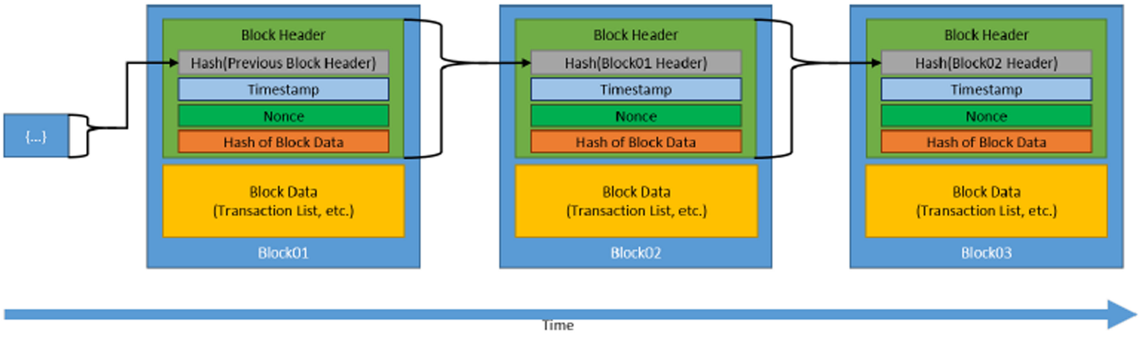

Figure 2. Generic blockchain.[8]

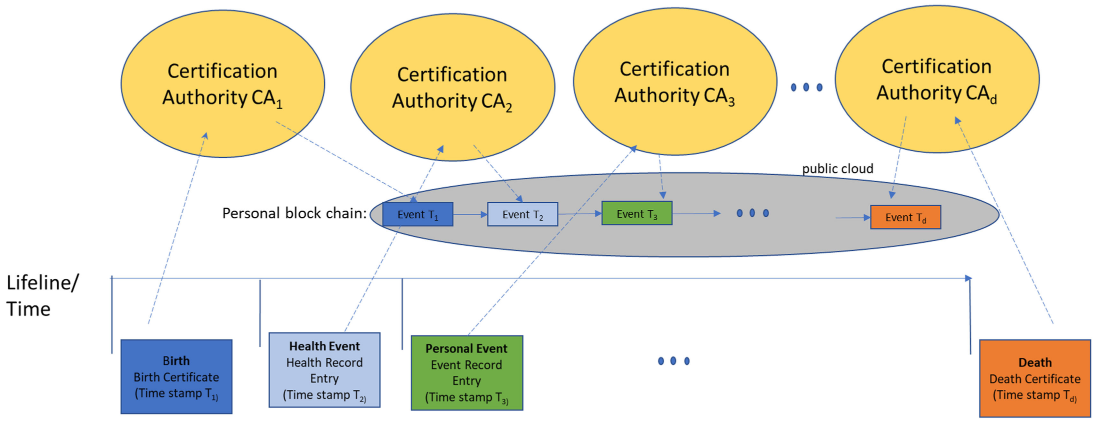

Figure 3. Representation of a generic lifechain—A personal blockchain.

have recognized the importance of marking time from its use in navigation and coordination of human activities for thousands of years. Today, timestamps are still used to associate a date and/or time to important events. Timestamping is important in many activities from process control, supply chain management, finance, and computing. In any personal transaction or event, timing and order matter. Birth, wedding, divorce, title and patent filing dates, etc., are all used to establish precedence and legitimacy. For example, the first born in a family lineage, the date of conception, or sequence of events in intellectual property rights, all have important legal and financial implications.

When errors or discrepancies in these sequences are discovered, significant problems can arise. Time-based discrepancies might include records indicating a person was born and married on the same day or making some legal decision before the age of majority. For our personal well-being timing also matters—dates and times of medical procedures, with respect to insurance coverage, the sequencing of medication administration, and so forth. Of course, deliberate falsification or malicious corruption of any records creates other kinds of difficulties. But all of these problems would be mitigated by storing the transactional information accurately and securely with timestamps in a blockchain.

LIFECHAINS

Life is an implicit sequence of timestamped events, that is, every person's life can be represented by a unique chain of events with timestamps—birth, vaccinations, religious ceremonies, courses taken, graduations and degrees earned, sicknesses, procedures, treatments, job history, marriage, divorce, votes, passport activity, even criminal convictions, and certainly death. In order to preserve and protect the efficacy of this chain of events, I believe that every person should have their own personal blockchain storing and protecting the dates and data of these events. I like to call such a personal blockchain a "lifechain."

By creating and maintaining this timestamped, blockchain record structures every person can have a secure and trusted record of every life event—one that is easy to examine (with appropriate permissions) and validate. Here a timestamping authority (another CA) could establish a common timescale for the system that would guarantee transaction order and verify the accuracy and validity of the timestamps.[6]

Figure 3 shows the architecture of a lifechain—it is private but stored in a distributed fashion in a public cloud.

The lifechain is a permissioned blockchain with a distributed ledger stored in a public cloud. The "owner" of the lifechain is the individual or, in the case of a minor or some other disabling condition, the legal guardian of the individual. Here, the CAs are permissioned hospitals and physicians' offices, school boards and educational institutions, government agencies, employers, financial entities, etc. A further discussion on the characteristics of CAs follows in a later section.

Table 1. Role-based permissions for a lifechain.

Role	Create record	Read record	Make changes	Authorize CA
Individual/guardian	No	Yes, all data as permitted by law	No	Yes, nongovernment CAs
Government certification authority	Yes, as permitted by law	Yes, only those authorized by individual	No	Yes, other government CAs and certain nongovernment CAs as permitted by law
Nongovernment Certification authority	Yes, as permitted by law	Yes, only those authorized by individual	No	No
Timestamping authority	No	Yes, only timestamp information	No	No

While government CAs will have permission to access to all records in the lifechain and can authorize (give permission to) other government or nongovernment CAs (as permitted by law), most nongovernment CAs must be authorized by the owner to conduct transactions in the lifechain, and then only to certain data in each block. Thus, a potential employer might be given authorization only to access certain parts of educational records, military service records, and criminal records, but no other types of data in those records nor other kinds of records (such as financial information). Owners are only allowed to authorize CAs and to read data in the lifechain (as permitted by law)—not add records. This feature is necessary to prevent fraud, deception, and incorrect entries.

The timestamping authority is only authorized to read timestamping information for the purposes of participating in the consensus decision and to ensure accuracy. In the event of an error, the timestamping authority would notify the owner and relevant CAs. Table 1 summarizes the role-based permissions for a lifechain.

As is characteristic of a blockchain, in the present model, no entity is permitted to make changes to neither records nor data in the _blockchain. Since this represents a practical shortcoming in the lifechain model, further discussion on making changes in the lifechain is needed and follows shortly.

The idea of such a personal blockchain is not new. For example, IBM patented a design for a "personal ledger blockchain,"—a generic, localized encrypted public blockchain (multiple access) with timestamps for storing different kinds of personal records.[3] This invention does not mention certification authorities but relies on public–private key encryption for access, however. Others have proposed a personal (localized) blockchain for academic/training records[1] or healthcare information.[5] I am simply endorsing and proposing an extension of these ideas—A universal structure for storing everything about a person but using CAs and a timestamping authority for additional security and authenticity.

SOME LIFECHAIN VIGNETTES

Your lifechain is a unique "social DNA" recording personal, business, financial, employment, educational, and health and all kinds of other events and transactions.

Consider the following descriptive vignettes of various transactions in the lifechain of one person, Pebbles, the daughter of Fred and Wilma. In each case, the addition of a block must go through the permissioning of the CA and consensus process and only permissioned CAs can access (authorized) data in a block. The timestamping authority is also involved in the consensus process for all block additions.

Vignette 1: Upon the birth of their child, Fred and Wilma authorize the hospital and county department of records to create a public blockchain ledger (lifechain) for Pebbles. Her birth certificate and medical information are entered into her lifechain. A social security number is requested from the social security administration and is entered into her lifechain. As Pebbles grows, she obtains vaccinations, and other medical procedures are performed on her. Her family doctor, authorized by Fred and Wilma (jointly—all future transactions must be so), adds these medical records to the lifechain. As she completes preschool, elementary school, and middle school, her transcripts are placed in the lifechain by the (authorized) area Board of Education. Each time a record is placed in the lifechain, it is validated by the other participants, and any exceptions trigger some form of notification to all of the participants, and Pebble's parents. Note if anywhere during this period, the status of Fred and Wilma changes such that they no longer have joint authority (divorce, death, or abandonment), an appropriate legal jurisdiction transfers the authorization right to one or the other parent.

Vignette 2: Pebbles graduates high school (the records having been inserted and validated into the lifechain) and she reaches the age of 18 (the age of majority in many countries). The state department of records (or other appropriate CA) transfers the lifechain authority from Fred and Wilma to Pebbles. Pebbles decides to join the Navy to earn tuition upon completion of her service. Her official military records are entered and maintained (by the Department of the Navy, which is made a CA with her permission) into her lifechain, through her honorable discharge from the Navy after four years of service. Pebbles decides to use her tuition benefits to apply to public university (PU) to study engineering. The application process is relatively simple since, by authorizing PU to access her blockchain (educational, financial, and service information only), PU can pull together all of the necessary information to needed to make the academic decision and any decision to provide financial aid. After four years of study, Pebbles graduates with her bachelor's degree in electrical engineering. She has already obtained a fantastic job—during her senior year, she autosubmitted several applications (including her complete educational, military service, and part-time work records) to potential employers.

Vignette 3: Over the course of her life, Pebbles experiences many pleasures and challenges including marriage, losing and finding employment, getting tickets for speeding and illegal parking, and diagnosis and treatment for cancer. Along the way, she and her husband apply for and get a loan for a new home. After 30 years in their home, the mortgage is retired; a few years later, Pebbles and her husband retire. For each of these life's events, appropriate amendments are made to her lifechain. Sadly, two years after retirement, Pebbles is diagnosed with cancer again, and after a long treatment, she passes away. Each of the medical diagnosis, procedures, and treatments were recorded in the lifechain, as was her death certificate.

Abuse Vignette

When I was in my late 40s, the county certification authority in the jurisdiction that issued my birth certificate was discovered to have been corrupted and had fraudulent birth certificates issued in the last few years. Since there was no way to *prima facie* distinguish a fraudulent from a valid birth certificate, the only fix was for all birth certificates issued by the authority dating back to the 19th century had to be reissued. A lifechain structure would have prevented the fraudulent birth certificate from being created through the consensus process. But even if the consensus process had somehow been defeated (e.g., by some sort of multiagency conspiracy), when later discovered, the legitimate birth certificates could have been revalidated by other certifying authorities in an individual's lifechain.

In a similar way, could the US Office of Personnel Management, US Defense Information Systems Agency, and Equifax records data breaches have been prevented by lifechains? Would the cross checking by CA of the lifechain for each individual has protected against these breaches and other kinds of fraud? There is no way to know for sure, but in any case, lifechains will be capable of preventing or mitigating many other kinds of identity fraud, title fraud, and other forms of criminal activity.

CERTIFICATION AUTHORITIES

The lifechain owner gives permissions to a CA based on some level of trust. Trust for governmental agencies varies greatly from one individual to another, and some persons distrust no matter how many assurances, oversite, or auditing is provided. Hospitals, financial, educational, and other institutions participating in the lifechain can hold various forms of licensure or certification from relevant commissions or oversite bodies and be subject to audit. But again, trust is a personal matter. So what benefit is giving permission if the individual cannot completely and continuously trust the CA?

One possibility, in addition to domain specific certification by relevant oversite bodies, is for the CAs to continuously certify each other through the blockchain decryption process. That is, throughout the block addition consensus process, any CA that is consistently wrong in its evaluation is subject to review or audit. CAs checking in on and auditing each other continuously protects against spoofing and malware injection. In addition, each CA could also use separate blockchains for securing their records, increasing confidence in them. Fraud would require a vast conspiracy across certification authorities rather than within one of them.

Certifiers have a duty to be honest and faithful but are also liability to the efficacy of the lifechain if they are not. This trust concern occurs because certification is difficult and often causes conflict. But the certification of CAs such that trust is pervasive remains an open problem.[7]

FIXING ERRORS/UPDATING LIFECHAINS

It is certainly possible that the information stored in the lifechain could be discovered to be incorrect. One of the hallmarks of blockchain oriented-solutions is their immutability—this feature makes, for example, financial records highly resistant to forgery, alteration, and mischief. But with respect to personal records, it is possible that errors could be made and later discovered—and these must be corrected; for example, a correction to an error in an educational transcript or other artifact. Social security numbers have been known to be falsified, issued to two different persons, or accidentally cancelled—all serious problems. In such cases, the strength of traditional blockchains provides an obstacle.

Fortunately, a special, reversible form of blockchain, called a “block matrix” has been developed. This data structure supports “the ongoing addition of hash-linked records while also allowing the deletion of arbitrary records, preserving hash-based integrity assurance that other blocks are unchanged”.[4] This kind of approach to lifechains would allow for the correction of inevitable errors or changes needed to an “immutable” record.

What about the possibility of CAs colluding to create a fictitious person by false birth certificate and social security number? Or what about accidentally declaring a person dead by removal of their social security number? Potential for these problems is real and has occurred, but would be entirely preventable via lifechains since only certain CAs can make fixed changes as permitted by law and with approval of the owner and other CAs.

Artificial intelligent agents (built into certain CAs) could help to audit blockchains and provide more efficient/adaptive consensus algorithms. Intelligent CAs could also be used to detect and prevent fraud and certain attacks (e.g., denial of service) on the lifechain or its supporting infrastructure.

CONCLUSION

I do not claim that I have worked out all the details of creating and maintaining personal blockchains. The use case examples I presented have numerous “what if” conditions that need to be explored. For example, there are issues with standards compliance, certification authorities, owner state of mind, etc. In addition, there are technical implementation details to be worked out. Finally, there are surely legal issues that can only be resolved with state and local legislation. But from an operational standpoint, the overall concept for lifechains is there; it could work and have numerous benefits.

Of course, this proposal is also very controversial as there political, social, ethical, and legal considerations to be discussed. Privacy advocates may differ on the value or even feasibility of this approach. Also, there will be political objections—since the federal government is not the central hosting authority, the distributed hosts and certification authorities (e.g., hospitals, doctors, churches, local and state governments, educational institutions, etc.) must act as checks and balances to the system.

But I am convinced that through role-based access control a distributed ledger/blockchain with timestamping provide maximum security and confidence for securing all forms of personal records. Lifechains will make identity theft harder to commit and will make all kinds of social transactions such as applying for a mortgage, having a medical procedure or complex financial transactions easier. Despite the details to be worked out and the concerns, the potential benefits of lifechains are so great that they need to be explored much further.

REFERENCES

1. Z. Chen and Y. Zhu, "Personal archive service system using blockchain technology: Case study, promising and challenging," in *Proc. IEEE Int. Conf. AI Mobile Services*, 2017, pp. 93–99.
2. T. Costello and P. Laplante, "Blockchain for automation: Assessing and seizing the opportunity," *Cutter Bus. Technol. J.*, vol. 32, no. 2, pp. 6–12, Mar. 2019.
3. D. N. Dillenberger, "Personal ledger blockchain," U.S. Patent 10,013,573, Jul. 3, 2018.
4. R. Kuhn, D. Yaga, and J. Voas, "Rethinking distributed ledger technology," *Computer*, vol. 52, no. 2, pp. 68–72, 2019.
5. A. Roehrs, C. A. da Costa, and R. da Rosa Righi, "OmniPHR: A distributed architecture model to integrate personal health records," *J. Biomed. Informat.*, vol. 71, pp. 70–81, 2017.
6. T. Saidkhodjaev, J. Voas, R. Kuhn, J. DeFranco, and P. Laplante, "Aggregating atomic clocks for time-stamping," in *Proc. IEEE Int. Conf. Service-Oriented Syst. Eng.*, to be published.
7. J. Voas and P. A. Laplante, "IoT's certification quagmire," *Computer*, vol. 51, no. 4, pp. 86–89, 2018.
8. D. Yaga, P. Mell, N. Roby, and K. Scarfone, "NISTIR 8202. Blockchain technology overview," 2019, *arXiv:1906.11078*. [Online]. Available: https://doi.org/10.6028/NIST.IR.8202