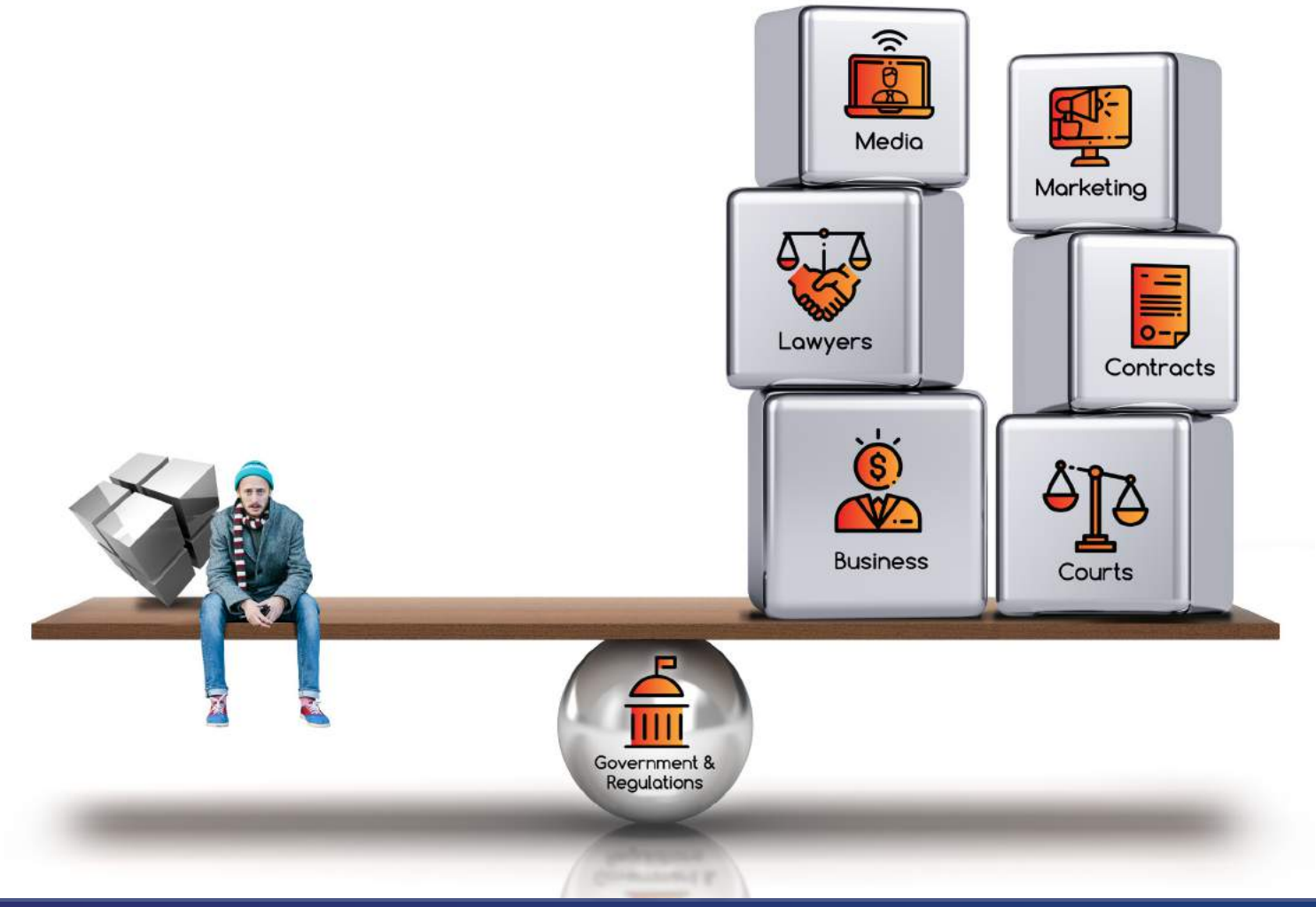
DECENTRALIZED DEMOCRACY



A Second Zero-to-One Invention on Blockchain

RICHIE ETWARU

Hu-manity.science

How blockchain technology can enable balanced agreements and open the door to decentralized democracy.

ABSTRACT

If two parties to an agreement are equal in the strength of their positions, the agreement reached between them will be balanced. If they are unequal, the agreement will favor the stronger of the two. Unfortunately, even in our current representative democracy there exists the high likelihood of an individual having no choice but to accept an agreement with an organization, such as a health care provider, that is unbalanced in favor of the organization. This is because many of the laws passed by elected representatives are sufficiently broad in scope that powerful organizations can interpret them in their favor, and because a large organization can readily afford to lose one customer who refuses the agreement as long as many others acquiesce. Blockchain technology can be used to level the playing field by allowing individuals to come together and engage in collective negotiation with large organizations, achieving balanced agreements through strength in numbers. For example it can help redefine personal data as personal property and ensure that regulations, which will always be broad in scope, are interpreted more fairly for all. Above all, it can change how we make agreements, thereby creating a less flawed version of democracy, which we call decentralized democracy.

It is well accepted that if two participants in a transaction are equal in the strength of their positions, then the resulting agreement is likely to be balanced.

If the two participants are unequal, the agreement is likely to be unbalanced and to favor the stronger party.

There can be many reasons why one participant — Party A — is in a stronger position than the other — Party B — and therefore able to create an unbalanced agreement.

Party A may have more time than Party B, who is in a hurry to make the agreement. For this reason, Party A is in a stronger position. He or she can afford to delay and extract better terms.

Party A may be physically stronger than, and able to intimidate, Party B. For example, Party A could be the schoolyard bully who takes your lunch money, thus forcing you into an unbalanced agreement. (It's called an agreement because you agree to give up your money in exchange for not being beaten.)

Party A may have the advantage of being able to choose between offers made by Parties B, C, and D, forcing the winning party to accept an unbalanced agreement.

Party A may have the advantage of the law, which — for whatever reason — gives them more rights and more leverage than it does to Party B.

These are all familiar situations. The question is, why would Party B ever consent to an agreement that wasn't balanced? After all, each of us is a free human being, and when offered a transaction we can choose to enter into an agreement or not. This would be the argument of libertarianism, which emphasizes freedom of choice, individual judgment, and voluntary association. If you don't like something, you can walk away.

But in everyday life, we often choose to enter into unbalanced agreements. We do this both knowingly and unknowingly.

We knowingly enter into unbalanced agreements for various reasons.

Convenience — Sometimes we suspect an agreement is unbalanced, but if the stakes are low and we're in a hurry or just don't have the energy to quibble, we go along. For example, we click on the terms of service statement on a website or sign a car rental form without reading every word. Why do we do this? Because everyone else does it, it seems harmless, and lawyers write these things, so that's just the way the world works.

For an individual consumer, negotiation with the corporate entity is not an option; and therefore when faced with an agreement that seems unbalanced the choice is to sign or walk away — which means not joining Facebook or not patronizing that particular car rental office and having to find another. But many large corporations are virtual monopolies, at least in terms of the real-life choices faced by the average consumer. Yes, you could seek out another social media platform or car rental office, but is that realistic?

Necessity — Sometimes we suspect an agreement is unbalanced, but the stakes are high and the price for not agreeing is prohibitive. When your child is lying on the gurney in the emergency room of the only hospital within a fifty-mile radius and the admitting nurse puts a piece of paper in your hand and tells you to sign, you're going to sign it. As you hand it back, you hope that the government and the politicians for whom you voted have enacted laws that oversee how hospitals operate and the forms they make you sign.

In the labor market, the individual worker needs a job to feed his or her family. When jobs are scarce — either by reason of poor economic development or a downturn in the economy — the individual worker is at a disadvantage because he or she is competing with many other workers for the same job. When labor is cheap, the owner of the means of production can therefore offer an employment agreement that is unbalanced and results in less wealth going to the worker and more to the owner. The worker, who has a family to support, has no choice but to accept the unbalanced agreement.

Compulsion — Sometimes we knowingly enter into agreements that are unbalanced, and we do this because the force of law is weighted

in favor of the other party. For example, the power of eminent domain gives the government the right to compel you to sell your property so a highway can be built. The military draft can compel you to join the Army. Paternity laws can compel a biological father to support his child. These are all transactions that are legally weighted in favor of the strong — in this case, the government. The price for noncompliance may be prison.

Sometimes we *unknowingly* enter into an unbalanced agreement.

We unknowingly enter into an unbalanced agreement when the full scope and description of the agreement has been hidden from us — not entirely out of sight, which would violate contract law, but buried under a mass of distracting text that we could read word-for-word but don't. The vast majority of users of social media platforms including Facebook and LinkedIn haven't read the terms of service because they seem to be nothing more than a legal formality included only to please the company's lawyers, and because any negative consequences of acceptance seem distant and unlikely. What harm could come of agreeing to the terms of service — haven't millions of other people already agreed? How could the terms possibly injure me?

We unknowingly enter into an unbalanced agreement when we purchase a drug that may have significant side effects whose severity has either been deliberately hidden by the drug manufacturer or buried within a mass of fine print that the drug company knows the consumer isn't going to read. A 2016 study that tracked consumers as they viewed a website for an allergy medication found that most of them didn't read the risk warning information. Of twelve potential side effects mentioned in the text, the average participant correctly recalled just one. Why didn't they read the warnings more carefully? Part of the problem, noted the researchers, was that drug warnings are ubiquitous and the participants, all of whom had allergies, assumed they knew the risks, even though they had never before seen the fictitious medication described on the website.[1]

The Limitations of Representative Democracy

The problem of unbalanced agreements is nothing new. For most of human history, agreements between the powerful and the powerless were routinely unbalanced, and the weaker party had no choice but to accept the will of the stronger. Kings ruled over their subjects, and while in some societies there existed a veneer of impartial law in the form of documents such as the Code of Hammurabi, the Ten Commandments, and much later the Magna Carta, the vast majority of human beings lived according to the whims of their rulers. Some kings owned all the land in their realm, making their subjects nothing but tenant farmers with few rights. The king could conscript citizens for war or tax them to pay for his new castle. Like a wagon wheel, the king was the hub, and his realm revolved around him.

One problem with this system was that even the wisest of absolute rulers has a way of becoming corrupt and striving to amass power. Being human, even a benevolent king is simply incapable of making balanced agreements in any sustained way.

In 1776, in the newly formed United States of America, the great experiment in democracy was designed to rectify this problem. On one designated day every two years, vast political power was granted to a large class of citizens (at the time, white, land-owning males). With their votes cast on that one day, they could elect representatives who would then assume legislative power and craft laws that were fair to the majority.

But make no mistake: During the terms that legislators served in office — two years for representatives, four years for the president, and six years for senators — the voters had little recourse. They had to accept whatever laws their representatives passed, pay the taxes demanded, and serve in wars the president declared.

If the citizens didn't like it, their power consisted of voting the bums out of office at the end of their terms. Voting was a way for people to share evidence of their agreement around the state of something — in this case, their elected officials.

In some towns, the newly minted citizens of the United States practiced direct democracy, which is where every eligible citizen votes on every new law and regulation. In a few towns this still exists, as well as in Switzerland, a rare example of a nation with direct democracy at the levels of the municipalities, cantons, and federal state. Swiss citizens vote four times a year on a wide variety of issues, such as the building of a new street, financial approvals of a school, or on constitutional changes.

At its very best, for the first time in history the system of representative democracy provided a voice for ordinary people in the crafting of the laws under which they lived. For example, consumer protection laws, enacted by representatives, make it more likely that an agreement between an individual consumer and a corporate food producer will be balanced, in the sense that the law provides penalties for processed food producers who sell food that's tainted or mislabeled, or otherwise seek to mislead consumers.

But despite its clear improvement over the old single-ruler system, representative democracy has significant shortcomings.

Implicit vs Explicit Laws

When voters send a representative to their state capital or to Washington, they're sending someone who has advertised himself or herself as holding certain political beliefs. It's the assumption of the voter that once in office, the politician will be true to those stated beliefs. But there's no guarantee that any politician will create laws the voters whom they represent will endorse.

Because no law can possibly describe every potential scenario, regulations tend to be broad-based and subject to interpretation. They are *implicit* rather than *explicit*. Consequently, the courts are tasked with interpreting laws that are challenged by lawsuits. Laws are challenged in court for either of two reasons:

1. The plaintiff believes the law, while clearly written, is unjust. For example, in the 1965 case Griswold v. Connecticut, the US

Supreme Court struck down a Connecticut law banning the sale of contraceptives. The law was clear and needed no interpretation, only repeal.

2. The plaintiff believes the law needs clarification. In the 2010 case Citizens United v. Federal Election Commission, the Supreme Court re-examined a series of earlier campaign electioneering laws and rulings, and, in siding with the plaintiff, interpreted the First Amendment right to free speech to include corporate spending on political issues.

Because laws often contain "loopholes" permitting actions that can, directly or indirectly, achieve the same result as a prohibited action, people and organizations who are wealthy or powerful can find "workarounds" to achieve their goals. For example, nowhere is this more clearly seen than in campaign finance laws. No matter how many campaign finance laws are passed, wealthy people manage to funnel their cash to organizations supporting those politicians whom they want to see elected.

In addition, laws can quickly become out of date. For example, consider property laws. In ancient times, property was defined as land and the tangible things you owned: your horse, your boots, your sword. (Your soul belonged to God, and when you were done with your earthly body, he wanted it back.) The concept of intellectual property did not exist.

But as time went by, people began to realize that intellectual property — a book you wrote or a picture you made — had value and could be owned. In the West, the first references to intellectual property don't appear until 1624 in the Statute of Monopolies, an act of the Parliament of England that was the first statutory expression of patent law.

In 1710, Parliament passed the Statute of Anne, the first law that protected the copyrights of books and written materials. This law was enacted a full two hundred and seventy years after Johannes Gutenberg first printed his Bible with movable type and opened the floodgates to mass-produced books. Progress on the protection of intellectual property continued to be slow. As late as the mid-nineteenth century, Charles Dickens, whose books were published

in the United States without his knowledge or consent, complained bitterly about the lack of international copyright laws. He wrote in his 1839 novel *Nicholas Nickleby*, "Now, show me the distinction between such pilfering as this, and picking a man's pocket in the street: unless, indeed, it be, that the legislature has a regard for pocket-handkerchiefs, and leaves men's brains, except when they are knocked out by violence, to take care of themselves." (By the way, I can freely quote Dickens because the copyrights on his books have long since expired.)

And today, with the global explosion of the internet, copyright infringement has become a contentious topic. In the United States, the relevant federal law is 17 U.S. Code § 506, which states in part, "Any person who willfully infringes a copyright shall be punished as provided under section 2319 of title 18, if the infringement was committed — (A) for purposes of commercial advantage or private financial gain…" and then, "For purposes of this subsection, evidence of reproduction or distribution of a copyrighted work, by itself, shall not be sufficient to establish willful infringement of a copyright."

This leaves a lot of room for interpretation. If you copy an audio file of a Beatles song and send it to your friend as a gift, is that illegal? (Probably no.) What if your friend responds by sending you a Rolling Stones song, which means that now you have profited from the exchange? (Probably yes.)

Over time, the interpretation of laws bends toward the wealthy and powerful. Even in a representative democracy, the individual is much more likely to end up with an unbalanced agreement that benefits the stronger party — the government, a corporation, a wealthy person.

The Growing Value of Personal Data

Throughout history, as long as intellectual property had little monetary value, any discussion of the classification of intellectual property was merely academic. There was no point in protecting something that was seen to be worthless. A horse or a piece of land had real value and could not be taken from the owner, whereas a poem you wrote was just an idea that anyone could copy for free.

Slowly, society began to value things like ideas even though you couldn't touch them or hold them in your hand.

It took England two hundred and seventy years after the invention of the printed book to affirm that printed materials were intellectual property worthy of legal protection. It's not that books didn't exist before Gutenberg; they did — at its height in the first century BCE, the Great Library of Alexandria housed between 40,000 and 400,000 scrolls. But before the printed book, you couldn't copy and sell books for much of a profit. There was no money in it. But with manufactured popular books, you could print them and sell them by the thousands. Suddenly, pirated books were depriving authors like Charles Dickens of significant amounts of income.

Likewise, for centuries your personal data — your medical history, the type of food you grew, the type of wagon you drove — had no market value. It was difficult to collect and there was no use for it. After the dawning of industrialized era, companies such as insurers traded in the basics, such as your date of birth and your income, and the census collected demographic information. Mailing list companies had files of addresses and other basic data, such as the names of magazine subscribers. (If you subscribed to *Field & Stream*, a store that sold fishing rods wanted to know.) But these things had very modest commercial value.

The revolution of digital data and the internet has changed that.

Within the past thirty years, personal data has become very valuable. Why? Because, on a mass scale, we now have the technological capability to:

1. Collect it.
2. Store it.
3. Analyze it and prioritize it.
4. Apply it to a question or business goal.

To whom is your data valuable?

Here are some examples.

In the article "How Much Is Your Data Worth? At Least $240 per Year. Likely Much More," the author, Wibson (the name of a blockchain-based decentralized marketplace empowering individuals to monetize their data), calculated how much your personal data was worth on Facebook and its associated platforms, including Instagram. Facebook utilizes user data including age, social relationships, interests, location, and browsing history to develop precision digital advertising strategies on its own properties including Facebook, Messenger, and Instagram, as well as sites and applications in its broader third-party network. The goal is to show you only the ads that are most closely aligned with your interests. Wibson wrote that according to Facebook filings with the US Securities and Exchange Commission, "in 2016 the company generated nearly $27 billion in revenue through its advertising products, which amounts to approximately $20 per monthly active user or MAU per year." The value to advertisers of the Facebook data is not just the data itself but how it's distributed — it's only useful when it can be used to precisely target potential customers.[2]

Using various calculations, including a study entitled "Consumer Privacy Choice in Online Advertising: Who Opts Out and at What Cost to Industry?" from the Simon School of Business, Wibson came up with a figure of $47 for the value to Facebook of the average user's behavioral data in 2016.[3]

It may not seem like much, but when multiplied by an estimated 2.19 billion monthly active users, it amounts to a significant amount of money.

Facebook says that it does not sell the data it collects from its users. Rather, it uses the data to help its advertisers target only the exact consumers they want, which makes Facebook advertising more valuable than advertising on other platforms. In April 2018, Facebook founder Mark Zuckerberg testified before a joint meeting of the Senate Judiciary and Commerce Committees. He said, "What we allow is for advertisers to tell us whom they want to reach, and then we do the placement. So, if an advertiser comes to us and says, 'All right, I am a ski shop and I want to sell skis to women,' then we might have some

sense, because people shared skiing-related content, or said they were interested in that, they shared whether they're a woman, and then we can show the ads to the right people without that data ever changing hands and going to the advertiser."

But it's not that simple, because in the past Facebook has allowed third parties to access Facebook user data. In an April 4, 2018 blog post entitled "An Update on Our Plans to Restrict Data Access on Facebook," Mike Schroepfer, Facebook's chief technology officer, admitted that at least 87 million Facebook users had their data used without consent by Cambridge Analytica, a political firm intending to influence the 2016 US presidential election. And when discussing a data "scraping" method involving Facebook's search and account recovery features, because of the activity of "malicious actors" he admitted, "we believe most people on Facebook could have had their public profile scraped." The company says that it has closed loopholes that allowed third parties to scrape data from its users.[4]

While these activities were going on, Facebook users had no idea their data was being scraped and used for political purposes.

A libertarian would argue that Facebook is a free service supported by advertising, just like old-fashioned terrestrial radio and broadcast television. Therefore you cannot expect that your data won't be gathered and exploited. It's the price you pay for enjoying the free service.

That position may be debatable, especially because Facebook is now a global monopoly (no other platform offers what Facebook does), and therefore the argument could be made that it's become a public utility with the attendant responsibilities of a utility.

How about health care, a service for which you pay dearly? When you go to the doctor, you make an agreement for the exchange of value: You pay a fee (either directly or through your insurer) and the doctor provides a service. The agreement will also say, either tacitly or implicitly, that in order to provide his or her services, the doctor will need to collect and analyze your personal health data: The diseases you have, the prescriptions you take, the nature of your current complaint. The doctor may even take images of the inside of your body and have

an analysis performed of your DNA to detect a genetic component to your illness. He or she may also make a mental health evaluation.

Fifty years ago, other than to insurance companies, all of this information had little commercial value. We just didn't have the data processing power to collect it, store it, analyze it, and exploit it on a mass level.

Now we do, and today every patient is linked to his or her electronic health record (EHR), a dataset of all the health-related information about that individual. A copy of the patient's EHR may exist in any office where the patient ever sought treatment or was tested. It may also have been sold to a data broker.

Is there any regulatory control over a patient's EHR?

An implicit agreement between you and your doctor exists in the form of the Privacy Rule of the 1996 Health Insurance Portability and Accountability Act (HIPAA), which establishes standards that work toward protecting patient health information. As the government says, "The Rule requires appropriate safeguards to protect the privacy of personal health information, and sets limits and conditions on the uses and disclosures that may be made of such information without patient authorization. The Rule also gives patients rights over their health information, including rights to examine and obtain a copy of their health records, and to request corrections."

But the world of medical information is rapidly changing, and in this environment, the agreement is sufficiently vague as to allow those in possession of your personal health data to work around the law and sell your data. As Adam Tanner wrote for The Century Foundation in his article "Strengthening Protection of Patient Medical Data," when a patient leaves the doctor's office or hospital, "pharmacies, insurers, labs, electronic record systems, and the middlemen connecting all these entities automatically transmit patient data directly to what is, in effect, a big health data bazaar. This trade — which has nothing to do with the individual's treatment or insurance processing — is allowed by HIPAA privacy rules only if the patient's name is removed." This health data bazaar is growing exponentially — according to a market intelligence

report by BIS Research entitled "Global Big Data in Healthcare Market-Analysis and Forecast, 2017-2025," the data market in healthcare was estimated $14.25 billion in 2017, and is estimated to grow over $68.75 billion by the end of 2025.[6]

Let's assume that your anonymity is preserved. Even so, the agreement you have with your healthcare provider is *unbalanced* and *unfair* because the harvesting and sale of your data isn't spelled out in the agreement, and you have no way to "opt out" of the system. You cannot "shop around" for a health care provider who doesn't sell your data because 1) they all do it, and 2) the sale of your data isn't explicitly described in your agreement with your doctor, so from their point of view there's nothing for you to object to.

But to make it worse, anonymity is increasingly *not* guaranteed. While your name and address may be stripped from the data your healthcare provider sells, data miners and brokers can now circumvent HIPAA's privacy protections by matching anonymized patient files with freely available identified consumer data, creating highly accurate profiles.

Again, the individual healthcare consumer has no way to opt out of this unbalanced agreement, and — to counter the libertarian's argument — the only way to keep your data from being harvested and sold is to *not get health care*. That's not a viable solution to the problem.

It doesn't help that HIPAA laws are complex, vague, and open to interpretation. As Warner Slack, a Harvard Medical School professor and one of the pioneers in developing electronic health records, told Adam Tanner in an interview, "HIPAA is so complex that I don't know anyone who understands it."[7]

In addition, HIPAA controls only what are called "covered entities" — in general, they are direct healthcare providers and health insurance companies. Providers of products and services that are not governed by healthcare laws can collect and sell whatever data they want. These ungoverned providers, including social media sites, medical equipment and supplement sellers, fitness centers, health apps, can legally buy and sell your information without your permission.

The question of ownership of your healthcare data is the central issue.

Do you own your healthcare records — the property that is the byproduct — form a transaction which you've paid?

In 49 out of 50 states, the answer is "no."

According to Healthinfolaw.org, of the 50 states, only one stipulates that the patient owns his or her health records: New Hampshire.

Healthinfolaw.org notes that "many states have specific laws addressing how providers must maintain, protect, and dispose of records, as well as laws giving patients, providers, and others access to medical records, regardless of ownership status. In addition, patients in all states have many rights with respect to their medical records under the HIPAA Privacy and Security Rules."[8]

Nevertheless, 21 states have laws specifying that the hospital and/or physician owns the medical records of a patient. You've paid for those records, and yet the hospital owns them.

The remaining 28 states have no law identified conferring specific ownership or property right to medical records.

Between patients and health care providers in the United States, there now exist hundreds of millions of unbalanced agreements. What can an individual patient do to keep their records out of the vast healthcare data marketplace? If they want to keep seeing a doctor for any reason, there's nothing they can do to opt out.

Blockchain technology provides users with the tools to claim exclusive ownership of their data. As Radhika Iyengar-Emens wrote in her 2018 article "Blockchain in Healthcare: A Data-Centric Perspective," in the blockchain community a central tenet is that "individuals should be able to control and monetize any information connected to their digital identities." Ultimately, blockchain-based EHRs can "accelerate the transition to patient-centric healthcare by putting the patient and the patient's data at the center of the healthcare ecosystem."[9]

Yes, but how would we go about doing that? Our imaginary friend Satoshi Nakamoto's zero-to-one whitepaper inspired an avalanche

of use cases where blockchain is used to have large networks agree on what something is. Instead, we have built a second zero-to-one invention on blockchain, one that enables large networks of humans, companies, governments and machines to agree on how something should work. For example, how should a regulation manifest itself into balanced contracts between business and consumers, specifically our first proof of concept addresses how HIPAA should manifest itself into balanced agreements governing the ownership, buying, handling, and selling of our personal healthcare data.

Blockchain: Tilting the Balance of Power

What can the individual do to level the playing field when making agreements with powerful governments or corporations? Is there any recourse at the moment when you're presented with a terms of use agreement and you feel as though it's weighted in favor of the company, but you can't afford to hire a lawyer and you really want the service? Do you have to click "I accept" and cross your fingers and hope you haven't agreed to something that could hurt you or take from you something that belongs to you?

A solution is at hand.

Where the individual is powerless, the group can wield great power and restore balance to agreements. Blockchain technology, which many people associate with cryptocurrencies such as bitcoin, can provide a vehicle for organizing and aligning vast numbers of individuals around a specified issue or agreement, so that the power of the group can be leveraged to affect change.

While cryptocurrencies such as bitcoin allowed great numbers of people to agree on what something was — a unit of currency — the next step in the advancement of blockchain technology is to allow great numbers of people to agree on how a regulation should be interpreted.

Historically humans have acted in numbers in various ways to change how something works. Marches, riots, petitions, collective bargaining (unions), and class action lawsuits are all examples of where humans have changed how something works by acting as a large group. Each of

these methods of collective action requires significant time, resources, and in some cases can take decades if not centuries for a change to occur. Blockchains can be used to pool large groups together, capture and store immutable legal evidence and documentation for each person, ensure that organizations, governments and machines can see the collective immutable legal evidence and documentation in real time, and facilitate the coordination of a large group to renegotiate or notify an entity where there is an imbalanced contract based on a predatorial interpretation of a regulation. Change the how.

While petitions, riots and marches have been somewhat successful historically at fixing some of the flaws in our democracy where corporations or industries had us captured in unbalanced contracts, the distributed ledger technology and asymmetric cryptography of a blockchain reduces the time and effort needed and increases the effectiveness of collective action. We can use blockchain to agree on how things should work, in a balanced form.

Towards a Less Flawed Democracy

The key to an individual's control of their personal healthcare data — and by extension, any set of personal data including financial and consumer — is their ability to opt-out of an unbalanced agreement, and propose a set of go-forward opt-in conditions that are balanced and equitable.

A solution that includes blockchain makes these choices possible.

As we know, if an individual consumer opts out of an unbalanced agreement, the more powerful entity (in this case, the data broker) will merely shrug and carry on with business as usual. In a data set comprising millions of individuals, the loss of one individual contributor means nothing. The only loser is the solitary individual who opts out.

But if many millions of individuals choose to opt out of an unbalanced agreement, then the opposing party has no choice but to negotiate better terms and/or change behaviors.

For example, let's say that fifty million individuals agree that their medical data is their personal property, and if a data broker wants access to it, this must be done under certain conditions and at an agreed-upon price. Because the fifty million individuals collectively have leverage, the data broker will be forced to negotiate or acquiesce to a better and more balanced deal.

This is a form of *decentralized democracy*. Under such a system, the privacy regulations passed by elected representatives will be interpreted closer to the original intent of the lawmakers we elected to represent us. The loopholes and workarounds in laws such as HIPAA will be less advantageous to the wealthy and powerful, and individuals of ordinary means won't have the court system — which is expensive — as their only recourse. By pooling our decentralized power, starting with HIPAA we can collectively renegotiate how regulations in our democracy are interpreted fairly and equitably one at a time.

At Hu-manity.co, using blockchain technology we've built a model of how individual consumers can unite and engage in the collective negotiation of any agreement, starting with agreements covering the buying, handling or selling of personal healthcare data.

We use blockchain to assemble a digital package of five *legal artifacts* for each individual. This gives them (with Hu-manity.co, acting as their proxy) the evidence to negotiate with corporations who wish to buy, handle or sell the individual's personal data. Briefly, these five artifacts are:

1. The language of the regulation that confirms the individual's ownership of his or her data and permits the negotiation or notification.

2. The form that the regulation specifies has to be sent to the organization notifying the organization that the individual is removing the assumption that there is no need for explicit consent and authorization to be captured for the use of their data (this is the "opt-out").

3. A title to one's digital-self classifying human data as property, with a unique ID that can be used to refer back to the relevant consent

and authorization of the property management and monetization choices around one's digital-self. This is the bridge that facilitates the opt-in to new terms.

4. The proposed new terms of an agreement between the individual and the organization (the "opt-in"), which is balanced and recognizes the value of the personal data being bought, handled or sold as human property.

5. The fifth artifact consists of several pieces including a consent form, explicit authorization, and the monetization preferences around the individual's digital property such a lease terms, preference of donation, and wills and estate instructions around the digital property.

Once each person has a digital legal package that gives them the legal corridor to renegotiate or notify of their desire to opt-out of the unbalanced assumption of "how" the regulation (such as HIPAA) should work, Hu-manity.co then assembles individuals into a large group to collectively notify the organization they are not in agreement with how they interpret HIPAA.

This is the *collective opt-out*, which could stifle the flow of data to the organization. We are using blockchain to get large groups of people to assert (and act, via renegotiation or notification) their position on how an agreement should work and become balanced.

We will not do an opt-out only, as the potential stifling of the data flow will help neither humans nor organizations. We believe data should flow *under equitable conditions*.

The new terms of the opt-in have two parts: 1) The company must add the unique ID found in the title of ownership of the individual's digital-self so that anyone buying, handling, or selling that individual's data has a low-friction method to find and respect the owner's property management and monetization preferences. 2) Instructions that the company must adjust their contracts to reflect that they are now buying, handling or selling "human property," and hence the data has all of the protections of property downstream.

Hu-manity.co uses the blockchain to store immutable legal evidence of each person's interpretation of *how* a regulation should be interpreted, and then coordinates large numbers of individuals, each equipped with a digital legal package, to engage in collective renegotiation with corporations who have offered imbalanced contracts or have taken predatory assumptions on our rights, as laws tend to be broad and ambiguous.

With blockchain technology, individuals can act collectively to restore balance to unbalanced agreements and advance democracy one step closer to perfection.

CONCLUSION

Over many centuries, the concept of human property rights has been steadily evolving. We now stand at the cusp of another great breakthrough: the recognition of personal data as personal property.

At Hu-manity.co, we believe that our set of 30 human rights adopted by the United Nations in 1948 and bestowed to every human at birth needs to be expanded by one more: Human right #31, a decentralized human right declared as, “Everyone has the right to legal ownership of their inherent human data as property.”

Blockchain technology has made it possible for our culture to correct a flaw in our democracy and enable individuals, acting collectively, to engage in balanced agreements with any organization or corporate entity.

Hu-manity.co has developed proprietary technology that identifies existing legal corridors in privacy regulations and has designed new *collective-action-contracts* on blockchains, which humans can use to negotiate new terms of consent and authorization with corporations so that inherent human data can be respected as legal property. While the use in healthcare relative to HIPAA has been the focus of this paper as an illustrative example, many unbalanced sets of agreements between large groups of individuals and corporations can be approached for rebalancing similarly.

We envision a world where the next generation of human rights and policies emerge from a balance of centralized power and decentralized technological empowered communities. Marches and riots are of the past, we are entering the world of blockchain backed collective renegotiations to rebalance some of the imperfections in representative democracy.

ENDNOTES

1. Hoy, Mariea Grubbs and Levenshus, Abbey Blake. “A mixed-methods approach to assessing actual risk readership on branded drug websites.” Journal of Risk Research, Volume 21, 2018. Published online: 27 Aug 2016.

2. Wibson. “How Much Is >Your< Data Worth? At Least $240 per Year. Likely Much More.” Accessed on Medium.com.Wibsom. July 21, 2018.

3. Johnson, Garrett; et al. “Consumer Privacy Choice in Online Advertising: Who Opts Out and at What Cost to Industry?” Simon Business School Working Paper No. FR 17-19. Posted: August 21, 2017.

4. Schroepfer, Mike. “An Update on Our Plans to Restrict Data Access on Facebook.” Newsroom.fb.com. Published April 4, 2018.

5. Tanner, Adam. “Strengthening Protection of Patient Medical Data.” The Century Foundation. January 10, 2017.

6. BIS Research. “Global Big Data in Healthcare Market: Analysis and Forecast, 2017-2025 (Focus on Components and Services, Applications, Competitive Landscape and Country Analysis).” 2018.

7. Tanner, Adam. Ibid.

8. Health Information & the Law Project. “Who Owns Medical Records: 50 State Comparison.” Last updated 08/20/15. Accessed July 22, 2018.

9. Iyengar-Emens, Radhika. “Blockchain in Healthcare: A Data-Centric Perspective.” CryptoOracle (DoubleNova Group), 2018.

About the Author

Richie Etwaru (born January 2, 1976) is an American business executive, author, global keynote speaker, adjunct professor and patent holder who specializes in the next era of commerce termed “Trusted Commerce”.

He has held c-level roles at Fortune 500 companies for two decades, and serves as advisor to venture capitalists, startups, governments, academia, and large organizations on transitioning to Trust Companies.

Richie’s book Blockchain Trust Companies, Every Company is at Risk of Being Disrupted by a Trusted Version of Itself (2017) is used by universities, consulting organizations, and governments, and his TEDx talk Blockchain Massively Simplified has been viewed over one million times.