Blockchain-Based Scalable Network for Bioinformatics and Internet of Medical Things (IoMT)

Ned Saleh

Abstract The major problem in today's data creation and monetization is that the data creators (individual people trading, traveling, and interacting on social media) are not the data aggregators (the Googles, Facebooks, and Amazons of the world). As such, the full potential of the personal data value in the age of informatics has yet to fully materialize. This leads to constant conflict within the data ecosystem regarding who has the right to own and monetize data; the creators or aggregators. It has also led to a protracted debate on data sovereignty and expanded legislation for data privacy that we deal with every day when we navigate any website. The holy-grail solution for such a problem is vertical integration, i.e., integrating the data value chain by combining and ensuring that data creators and aggregators are the same in the data value stack. Until recently, this was deemed technologically impossible because individuals in society cannot be their own bank, e-commerce platform, their own search engine, and their own social media. However, the advent of miniaturized sensors driven by advancements in device engineering and miniaturization ushered in a new age of multifunctional sensors, often called the Internet of Things (IoT). In particular, the distributed miniaturized devices that measure the biological attributes of individuals are called the Internet of Medical Things (IoMT). This chapter describes an end-to-end ecosystem that offers a solution to this problem and the commercial pilot model it has implemented utilizing the nascent but promising blockchain technology.

Keywords Internet of Medical Things (IoMT) · Quantified wellness · Proof of identity · Homomorphic algorithms · Data monetization · Bioinformatics

N. Saleh (✉)
Synsal Inc, San Jose, USA
e-mail: ned.saleh@synsal.com

W. Charles (ed.), *Blockchain in Life Sciences*, Blockchain Technologies,
https://doi.org/10.1007/978-981-19-2976-2_3

1 Introduction

The major problem in today's data ecosystem harvested from individuals is creation, control, and monetization. A core component of the problem is that data creators (individual people trading, traveling, and interacting on social media) are not the data aggregators (e.g., Google, Facebook, Amazon, etc.). Because of this split, the full potential of the personal data value in the age of informatics has yet to fully materialize. This resulted in constant conflict within the data ecosystem of who has the right to own, control, and monetize data, the creators or aggregators, and led to a protracted debate on data sovereignty along with expanded, and sometimes conflicting, multi-jurisdiction legislations for data privacy that we deal with every day. Our approach to addressing this conundrum is the holy-grail solution represented in vertical integration, i.e., integrating the data value chain by combining and making the data creators and aggregators the same entities in the data value stack. Until recently, this was deemed technologically impossible since individuals in society cannot be their own bank, e-commerce platform, search engine, and social media. However, the advent of miniaturized sensors (through which individuals can create their own data) driven by advancements in device engineering and miniaturization ushered in a new age of multifunctional sensors, often called the Internet of Things (IoT). In particular, the distributed miniaturized devices that measure the biological attributes of individuals are called the Internet of Medical Things (IoMT). This manuscript describes an end-to-end ecosystem that offers the solution to this problem through a scalable network and the commercial pilot model in which it has been implemented.

1.1 Data Ownership

Data ownership is a complicated topic that has been recently addressed globally in academic, commercial, and legal circles. The European Union General Data Protection Regulation [1] and the California Consumer Privacy Act [2] are examples of legal frameworks intended to protect individuals' data. However, these regulations are complicated, challenging to enforce, and could be circumvented through loopholes that individuals do not realize [3]. This situation may be experienced several times a day as we navigate the internet and are asked to accept cookies, often with limited choices [4]. (As a tip, website cookies can be manually removed at any time from the site information icon in the URL field). Self-sovereignty is a concept that is almost entirely addressed in connection with identity and credentialing leading to a wide debate on Self-Sovereign Identity (e.g., [5]). However, within these elaborate debates, the essential question of who owns the data has not received much attention, even though there is an overarching assumption that individuals in society own their data (e.g., [6]). Within the context of life sciences research, three arguments are made. First, do researchers "create" data from individuals' devices? Second, do

individuals "control" their data? Finally, do individuals monetize their data? These concepts are analyzed below.

1.1.1 Data Creation

Data creation from IoMT is often defined as the digital rendering of a reality or actions taken by an individual. This capture or rendering usually involves proprietary technology, and the resulting data are stored or represented in a digital format [4]. For example, when epidemiology researchers plot disease outbreaks using Google maps mobile application, a digital route is generated using Google's proprietary technology (satellite-based GPS, software, algorithms, other sensors, etc.) and proprietary digital format [7]. As such, this digital route becomes the property of Google.

Similar examples can be drawn from transacting with various commercial IoMT devices, so long as this digital rendering uses proprietary means. For example, Google purchased Fitbit, a consumer-grade fitness monitor, in 2021, resulting in Google's ownership of all Fitbit services and user data [8]. However, in other situations like capturing direct digital photography of a person, the images are owned by the photographer [9], medical images are often owned by healthcare facilities or providers [10]. The complicated ownership context suggests focusing more on privacy and control of IoMT and device data.

It should be noted that the absence of direct or active permission does not change the fundamental analysis that these technologies have knobs and controls that users can utilize to prevent data capture. Further, users benefit from interactive products and willingly agree to trade off data privacy for such free benefit [4].

1.1.2 Data Control from Devices

For individuals to exclusively control their data, there must be a protocol that ensures a secure chain of custody of the data from the point of collection or rendering to the endpoint where the data may be stored, utilized, or monetized in a marketplace. The author argues that the data collection technology used must also be part of the continuous chain of custody, owned and controlled by the individual, referred to as vertical integration of the total value stack [11]. Thus, in most cases and especially for bioinformatics, a hardware device or a "dongle" is most suitable for the inception of data at the point of interaction. The collected data must be tamper-proof and traceable, this condition is best served by a trusted network based on blockchain. Encryption can be integrated into the process to guard against data copying, especially in open (permissionless) blockchains. This security adds another layer of guaranteed control by the individual. Finally, for such a blockchain-based network to fully function as a truly decentralized network, a consensus protocol is needed, such as Proof-of-Identity (PoI). PoI requires the initial registration of biometrics to ensure that the user identity is confirmed before the hardware device collects bioinformatic data [12]. With PoI

securing the authenticity of the data, the entire blockchain-based network becomes trusted and self-sovereign, and the provenance of data is ensured.

1.1.3 Data Ownership from Devices

One exception to this analysis is medical/clinical data, which are regulated under different laws. The analysis above is not to be confused with DNA data and personal genome. These data are based on a body part (albeit nanoscale), and accordingly, the sequence is more about measuring the ingredients of human tissue. Using the aggregator's proprietary means, any digital rendering of reality becomes its sole property. No other party (including the person subject of data collection) has privacy rights to someone else's property.

Furthermore, different aggregators might simultaneously render reality in different yet proprietary formats. For example, for a person making purchases on an e-commerce platform using a credit card, both the credit card company and the platform will have different digital profiles using their own proprietary software. As a remedy to this significant problem, this chapter offers a solution based on a breakthrough device owned by the individual. Individuals collect data with a model that makes the owner both the creator and aggregator of their data. Further details are offered in the next section.

The final element in building a genuinely user-owned network beyond data control is the users' exclusive right to monetize the data. This element stems from the fact that if data are indeed considered private property, conditions in a free market imply that individuals have the right to transfer this property (or rent it) to another owner for compensation by fair market value. Irrespective of the scenarios that allow for data monetization, which will be addressed later, the fundamental right of ownership transfer follows immediately from true data ownership in a free society. As proposed in this manuscript, the concept of true data ownership makes the individual's data property and capital.

1.2 Data in Blockchain-Based Network

Like any individually owned property, data can only be traded if processes and standards for data valuation may fluctuate by supply and demand and retain a fundamental baseline. Data valuation remains one of the most intriguing business practices today. The initial approach to data valuation was in bulk data sales for advertising and marketing purposes (as Google and Facebook do). It then evolved as data inputs to artificial intelligence and machine learning algorithms. Data valuation recently became a rapidly expanding field in economics; there are several valuable treatises on this topic (e.g., [13, 14]), and there are attempts to create semi-automated personal data value calculators (e.g., calc.datum.org/, ig.ft.com/how-much-is-your-personal-data-worth/).

In this chapter, a blockchain-based data network—based on the vertical integration approach proposed—also benefits from the same principles of data valuation. Furthermore, if structured as a Decentralized Autonomous Organization based on these governance principles, such a network offers its participants the maximum data value return on their data collected vertically integrated within the network. The final point in this section involves handling encrypted data in the network described above. Homomorphic Encryption Algorithms (HEAs) are readily available and able to handle encrypted data, creating monetizable analytics that contribute to data valuation to the extent that the valuation models are still valid [15]. For example, in the Synsal network, an innovative miniaturized device [16, 17, 18] is accessed through a combination of retinal and fingerprint identity verification, satisfying the PoI requirement. The device directly collects bioinformatics, converts raw data to encrypted data, and uploads to a blockchain-based network. HEA-run analytics are sent back to the user or are monetized. More details about the Synsal network are described in the following section.

2 Case Implementation of Internet of Medical Things (IoMT) with Real Ownership

This section demonstrates how the network described above is implemented in a realistic pilot commercial ecosystem. As shown in Fig. 1, the Synsal ecosystem [16, 17, 18]) starts with users accessing the device using biometrics necessary for the PoI protocol requirement. Data authenticity is guaranteed, as the Synsal device can only be accessed if the pre-registered user is interacting with the device. The device was engineered to make it challenging to maneuver around this step. For example, if the device is operated in a blood drop collection mode, a miniaturized proprietary cartridge is inserted into the device [16, 17, 18]. A micro-needle is mounted on the device upward so that a finger prick and fingerprint actions are performed simultaneously. Another example involves a sputum sample deposited in a cartridge when the user approaches the inserted cartridge. As shown in Fig. 2, a retina scanner on the device simultaneously verifies the user's identity. This level of engineering control

Fig. 1 Dr. Ned Saleh demonstrates how a user would interact with a prototype Synsal device

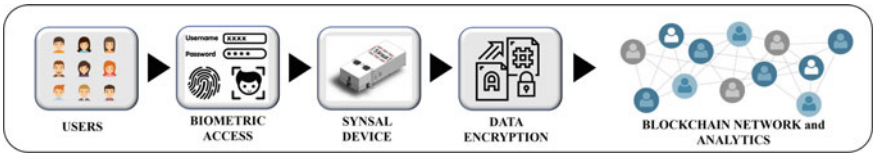

Fig. 2 The data process flow from users through the Synsal ecosystem

guarantees the fidelity of the data in the network and secures data ownership in the entire network based on the vertical integration approach discussed earlier.

The Synsal device is an engineering innovation that can handle several bodily fluids down to a few droplets (100 μl) thanks to breakthroughs in microfluidics engineering. The Synsal device is designed to be a non-invasive, general wellness Class-I medical device. It falls under the U.S. Food and Drug Administration (FDA) regulations related to Over The Counter and Direct-To-Consumer devices [19, 20]. Various assays (e.g., metabolic, cardiac, infectious, etc.) were validated on this device. The Synsal device creates a bioinformatics measurement from the electro-optical sensors in the device that analyze the pre-calibrated raw signal then encrypt it before it is transmitted to the network. The user-specific bioinformatics data enter the network encrypted. The network operators cannot access the encrypted data, nor can they decrypt it; only the original user can decrypt the data from a private key programmed at the initial unpacking and device set up. The user—and the user alone—is the data owner.

The data at this stage reside within the blockchain-based network, whether on-chain or off-chain, as in an InterPlanetary File System. The HEA can now access the data, perform analytics, and integrate these analytics with the rest of the network. It should be noted that the near-immutability attribute built-in in the blockchain architecture alone does not guarantee data ownership in a blockchain network. While the data are cryptographically tamper-free, it may still be transparent and visible to other users in the network—especially if the network is public and/or permissionless. Hence, encryption is necessary for exclusive control (and thus ownership) of the data. The ability of the user to decrypt their data and the analytics-based derivatives of the data generated by the network algorithms offers higher valuation of the users' data and unlock the maximum potential of monetization in the data marketplace connected to the network. It is also possible to program the encryption of the data to be portable and interoperable with other blockchain networks; this further maximizes the data value and offers more flexibility—especially in cases where dynamic consent is implemented. Fortunately, HEAs are themselves interoperable and can be implemented universally. Today we are witnessing a plethora of programmable blockchains and smart contract languages beyond Ethereum and Solidity that can sustain this level of flexibility (e.g., Casper, Polygon, etc.)

2.1 The Synsal Network

As stated in earlier sections, vertical integration of users' data stack relies on owning the initial aggregation layer, i.e., the hardware level that collects raw signals or a form of digital rendering of a specific attribute of the user-related reality. In that sense, one may question the availability of the technology, devices, or product practically accessible to the users to own, rent, or utilize in any other way that does not impact their exclusive ownership (including control and monetization) of their data. For example, suppose a person would like to perform an MRI and exclusively own and monetize his/her data. In that case, he/she would have to buy a next-generation portable MRI scanner such as Hyperfine that costs approximately $50k [21]. Incidentally, this is a remarkably inexpensive price point for an MRI device, yet it may not be accessible to most ordinary middle-class individuals.

The market for miniaturized IoMT now includes home ultrasound scanners at price points accessible to retail consumers and readily available on e-commerce platforms like Amazon. Even whole genome sequencers are now available in portable home devices priced around $1k thanks to advances in genomics technology like the Nanopore [22]. Furthermore, the market for home-based Point of Care (PoC) diagnostics and wearables is rapidly improving and covering vast areas of vitals measurement. In the age of the COVID-19 pandemic, PoC home testing now covers infectious diseases.

We are witnessing a blurring between wearables, home PoC diagnostics, and home (semi-)clinical devices, including home hemodialysis [23]. Despite all the home-based IoMT and PoC devices, no data ownership model is designed structurally to guarantee absolute control and security of user data, this is especially true if these devices are connected to databases or networks for data analysis straight to medical records. The realm of patient clinical data ownership or medical records remains outside the scope of this manuscript. However, it suffices to mention that a complicated web of laws regulates the ownership of patient data and medical records, which vary from one state to another within the USA and from one country to another. The Health Insurance Portability and Accountability Act (HIPAA) regulates health care providers' patient records privacy and permissions. However, there are no legal provisions on medical data monetization, especially if the data are deidentified [24].

Furthermore, disease reporting laws may override the HIPAA provisions per state or federal law [25] under the U.S. Centers for Disease Control and Prevention. To the best of the author's knowledge, there are no known networks to date that involve IoMT or home devices collecting clinical data or bioinformatics that comprise *simultaneously* engineering (as opposed to administrative) guarantee of legal ownership (dynamic control and monetization) and maximum potential for collective and individual analytics. Additionally, without explicit data encryption, blockchain-based networks alone do not guarantee absolute ownership of user data—even in private and permission-based networks. There remain risks of identity disclosure through differential privacy [26] or zero-knowledge proof loopholes [27, 28]. As shown in Fig. 3, a vertically integrated bioinformatics network is architected to achieve real

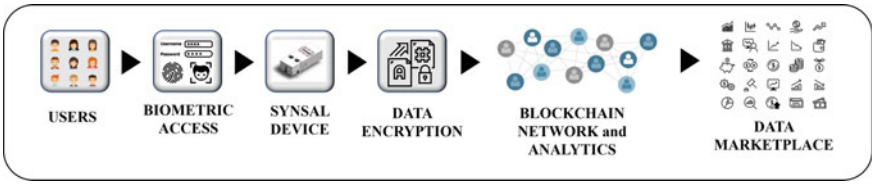

Fig. 3 The creation and protection of data value through the Synsal Network

ownership of data where users exclusively control their data from the point of inception by guaranteed engineering encryption. The data reside on a blockchain-based network with the maximum potential of data monetization through HEA that unlocks the maximum potential of data value. If this network is connected to a marketplace, it constitutes an end-to-end ecosystem for data ownership and monetization, a Data As A Capital model.

2.2 Sensors, Device Engineering, and Scaling in the Synsal Network

This section offers some technical glimpses into the Synsal device engineering [16, 17, 18]. The device addresses an essential aspect of the true miniaturization of a home-based or decentralized analytical test lab. The approach taken in engineering the device is not a "brute-force" miniaturization [29], where all device elements are mechanically scaled-down and cramped in compact space. Such an approach only scales down the physical sub-modules but does not scale down the raw sample handling—especially if the samples are only a few drops of bodily fluid (blood, tears, etc.). In addition, such an approach does not proportionately scale down mechanical tolerances and thermal loading and becomes not feasible from the system engineering design analysis. Proper scaling of an analytical home-based device must also include scaling-down of the sample handling chemistry. Without such technological breakthrough, the device will eventually have to analyze a diluted sample of the input fluid. The biomarker concentration will drop significantly and will likely be below the detection limits of any known sensor. The Synsal device is designed to implement the miniaturization and scale down on the microfluidics level, thanks to the breakthrough in the proprietary surface activation technology [30, 31] that leads to micro-splitting of fluids samples while preserving the biomarker concentration [16, 17, 18]. Specifically, the technology allows for creating programmable selective fluid flow due to the ability to create different polarities of surface energy. When interacting with lyophilized assays, this makes for natural chemistry scaling down. The Synsal device is equipped with electrochemical and optical sensors designed and validated for 1picoAmp-1pmol with high frequency ultrabright LED illumination

to perform particle counting/cytometry and time/frequency-domain optical signal processing, with usable signal-to-noise ratio.

Besides the ability to be programmed to measure various assays, the device can also perform Nucleic Acid Amplification Tests, which are critical for viral detection assays. However, unlike Polymerase Chain Reaction protocol, the device uses a well-known isothermal protocol called Reverse Transcription-Loop-mediated isothermal AMPlification (RT-LAMP). The device also has a biometric activation input user interface and built-in encryption chips [32].

3 Tokenization and Value Scaling in the Blockchain-Based Network of Hardware Devices

This section illustrates how a blockchain network can be tokenized to maximize user-owned data valuation. The Synsal network is designed to implement the true ownership model discussed above based on vertical integration of the data value stack. Furthermore, data are processed to create maximum potential value from analytics and monetizable reports. This model uses an innovative and proprietary network effect based on Reed's modified law in scaling [16, 17, 18]. Figure 4 displays the scaling properties when following Reed's modified law in scaling [33].

In a classical database where network effects are absent, each additional user contributes to the growth of the network depending on the size of the network (Sarnoff

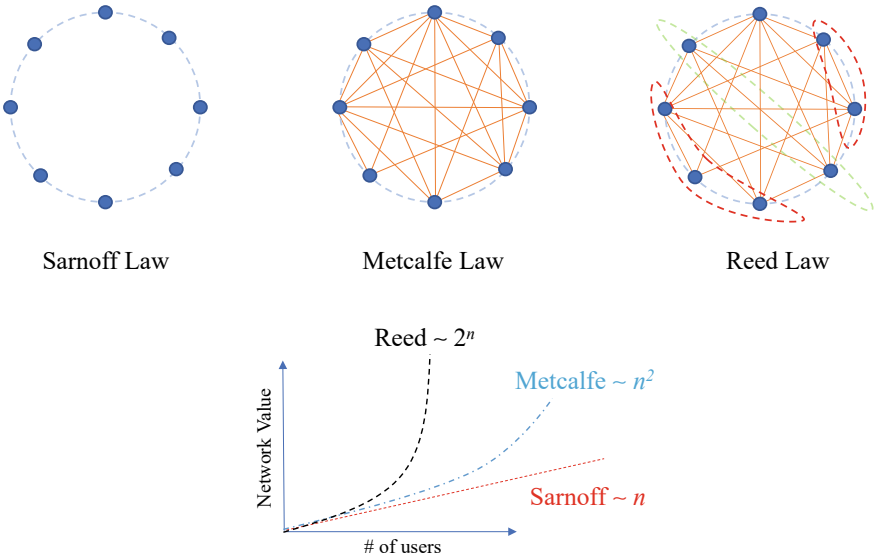

Fig. 4 Differences in scaling properties when using Reed's Law versus other laws used to predict value in scaling

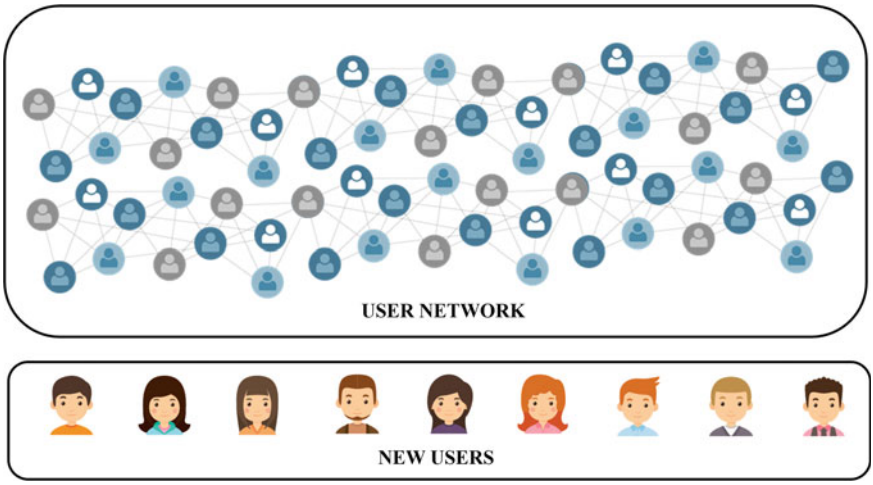

Fig. 5 A depiction of the relationship between users and the total Synsal Network

Law). An additional small group of users increases the value of the network by a factor proportional to $\Delta n/N$, where n is 'number of users added' and N is the total number of users in the network (Fig. 5). The network's scaling follows a logarithmic pattern with the integration of such increments according to the formula:

$$\int_{N}^{n+N} \frac{dn}{N} = \log \frac{N+n}{N}$$

Accordingly, the network value increases logarithmically, but its growth stagnates as it becomes larger. For example, the value of the data in a network of siloed users (as in a network of protected medical records) follows such a logarithmic trend. However, suppose the user's data can be processed collectively. In that case, the network effect will kick in and drive the value of the network higher than the logarithmic scaling, depending on the way the users are clustered in inter-related groups. There are various ways to model network effects discussed in the literature (e.g., [33]), the details of which are outside the scope of this manuscript. It is of *paramount* importance to notice that if the identity of the users is protected, then the clustering actually cannot happen. The maximum value of the network remains logarithmic. However, for the network to scale under the network effects depicted in Fig. 4, the identity of the users must be known to the network operators. In most practical cases, the network operators have access to the user's identity and become the beneficiary of the data valuation. This is very common in social media platforms where the users' identity is known to the data aggregators (owners or operators of the network) who are the ultimate beneficiaries of the network value, as in advertising revenue.

To recap, the dilemma is that the network cannot simultaneously scale the value of the data utilizing the network effects and keep the identity of the users protected. One

way to resolve this dilemma—perhaps the only way possible—is using encryption like HEA to cluster users in interrelated groups. In this case, the network operators (data aggregators) could not monetize the data. However, the network can be set up as is the case in the Synsal Network so that the individual users, and only the individual users, can monetize the data and yet benefit from network effect driven scaling since they can decrypt their profiles.

3.1 Tokenization and Value Scaling

This section offers additional means that the data value in the network can be further scaled if the value is captured in the form of a token, typically and more suitably a Utility Token (UT). In a blockchain-based network, the UT can be created using smart contracts that are built-in automated code in the network that can offer users more functionality and control and, perhaps most importantly, carry parameters of dynamic consent. The tokenized data can be tightly or loosely tethered to the UT, which can be traded on a platform or interoperably on a secondary market. The UT must be carefully programmed in the smart contract regarding its utility rights. If the UTs are finite while the number of new users is not, a condition of scarcity can be created that drives the valuation of the UT in addition to the rules of network effect that continue to apply to the UT. An additional feature unique to the Synsal Network (and any other network based on acquiring a piece of hardware to participate in the network) can be added. The device can be purchased using a value-based token considered a Security Token (ST) similar to a stable coin. The advantage of incorporating an ST is that network can operate with a dual token. This is particularly important to stabilize the UT—especially if the latter is finite, making it otherwise prone to speculations often called "pump-and-dump" actions. The coupling of the ST to the UT adds stability to the network. This chapter does not, however, address the technology and regulatory requirement to operate such a dual token network.

3.2 Basic Stabilization Tokenomics

Finally, it is important to provide some guidance on the token economics (tokenomics) of the dual token system described above, making for a stable and scalable blockchain hardware-based network of bioinformatics data. It is fair to state that many or most of the Initial Coin Offerings in the past several years irrecoverably lost a significant portion of their initial value due to a lack of certain tokenomic guardrails and bootstrapping mechanisms. It is exceptionally challenging to recover value once the native UTs slump on a trading platform. To make a UT representing a network like the Synsal Network, there should be some or all of the following factors:

(1) Intrinsic value creation and growth mechanism from data created by users. UT value is tethered to data
(2) Value creation from a single user in the network without scaling from the network effect
(3) Security Token coupled to the UT to offer robust UT stabilization mechanism, and liquidity exit
(4) UT participation is mandatory by users and data buyers, leading to high UT velocity
(5) UT derivatives on the platform (options, futures, swaps) to be used when applicable to offer another layer of valuation.

4 Future Directions

Engineering miniaturized IoMT devices improved on the heels of the COVID-19 pandemic. Home monitoring of vitals and other wellness needs provides crucial indicators of underlying conditions behind elevated COVID-19 illness; telemedicine also makes strides within the same context. Also, clinical, wellness, and medical data are expected to accumulate significantly [34]. With increases in data volumes, we will likely witness broader debates on data privacy, ownership, and monetization. There are also questions regarding the rights of governments and medical health record keepers to share data in semi-real-time to get insight on possible outbreaks of a new pandemic—especially if new Coronavirus variants or other viruses may be more contagious than the variants we witnessed in the course of the pandemic.

We also are witnessing expansion in the blockchain domain and utility-based cryptocurrency offerings. Examples include Algorand (algorand.com/; [35], Avalanche (https://www.avax.network/), Solana (solana.com/), Harmony (harmony.one/), and in particular, BurstIQ (burstiq.com), a HIPAA-compliant blockchain network. This massive momentum in Blockchain is also taking place as virtual reality applications are moving to a new plateau with the emergence of the Metaverse [36]. Alongside this momentum, we are also witnessing world governments, including the U.S. federal and state governments [37], trying to stay abreast with the legislative demands to keep the U.S. as a jurisdiction friendly to innovative blockchain companies and venture capital to operate and grow. In total, it is hoped that all this momentum will help materialize and widen the adoption of vertically integrated blockchain hardware-based networks similar to the one described in this manuscript by Synsal. Life sciences, clinical research, and market analysts will benefit as more bioinformatics data, quantified wellness, and analytics reports are generated thereof from such networks.

5 Conclusions

This chapter addressed a rapidly increasing topic of importance in the age of bioinformatics and IoMT, namely, data ownership and monetization. In order to guarantee true ownership of data (privacy, control, and monetization), vertical integration of the full data stack is needed. As such, the initial point of data aggregation usually involves hardware. This chapter presented a case study of the Synsal Network, where an innovative device collects data from a network of participating users. The device acts as a "dongle" to participate in the network. The network uses encryption and algorithms to maintain ownership of the data and maximize the scaling of data value to the users' interest. As an added benefit, data tokenization can accelerate data valuation and liquidity—especially when a data marketplace is part of this end-to-end ecosystem.

References

1. European Parliament and Council of the European Union (2016) General Data Protection Regulation 2016/679. https://gdpr.eu/
2. California Consumer Privacy Act (2018) Title 1.81., Sections 1798.100—1798.199.100. https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?division=3.&part=4.&lawCode=CIV&title=1.81.5
3. Check Hayden E (2013) Privacy loophole found in genetic databases. Nature. https://doi.org/10.1038/nature.2013.12237
4. Vezyridis P, Timmons S (2021) E-Infrastructures and the divergent assetization of public health data: expectations, uncertainties, and asymmetries. Soc Stud Sci 51(4):606–627. https://doi.org/10.1177/0306312721989818
5. StClair J, Ingraham A, King D, Marchant MB, McCraw FC, Metcalf D, Squeo J (2020) Blockchain, interoperability, and self-sovereign identity: Trust me, it's my data. Blockchain Healthc Today https://doi.org/10.30953/bhty.v3.122
6. Banterle F (2018) Data ownership in the data economy: a European dilemma (No. 3277330). SSRN. https://doi.org/10.2139/ssrn.3277330
7. Monir N, Abdul Rasam AR, Ghazali R, Suhandri HF, Cahyono A (2021) Address geocoding services in geospatial-based epidemiological analysis: a comparative reliability for domestic disease mapping. Int J Geoinformatics https://doi.org/10.52939/ijg.v17i5.2029
8. Frew J (2021) Should you worry about your health data now that Google owns Fitbit? MUO. https://www.makeuseof.com/google-owns-fitbit-health-data/
9. Lewis A (2021) Who owns a photograph in the social media age? JD Supra; Fenwick & West LLP. https://www.jdsupra.com/legalnews/who-owns-a-photograph-in-the-social-9457360/
10. Who owns medical records: 50 state comparison (2015) Health Information and the Law Project. http://www.healthinfolaw.org/comparative-analysis/who-owns-medical-records-50-state-comparison http://www.healthinfolaw.org/comparative-analysis/who-owns-medical-records-50-state-comparison
11. Orszag P, Rekhi R (2020) The economic case for vertical integration in health care. NEJM catalyst 1(3). https://doi.org/10.1056/cat.20.0119
12. Cerezo Sánchez D (2019) Zero-knowledge proof-of-identity: Sybil-resistant, anonymous authentication on permissionless blockchains and incentive compatible, strictly dominant cryptocurrencies. SSRN Electron J. https://doi.org/10.2139/ssrn.3392331

13. Bendechache M, Limaye N, Brennan R (2020) Towards an automatic data value analysis method for relational databases. In: Filipe J, Smialek M, Brodsky A, Hammoudi S (eds) Proceedings of the 22nd international conference on enterprise information systems. SciTePress, Science and Technology Publications, Lda, pp 833–840. https://doi.org/10.5220/0009575508330840
14. Robinson SC (2017) What's your anonymity worth? Establishing a marketplace for the valuation and control of individuals' anonymity and personal data. Digit Policy Regul Gov 39:88. https://doi.org/10.1108/DPRG-05-2017-0018
15. Catak FO, Aydin I, Elezaj O, Yildirim-Yayilgan S (2020) Practical implementation of privacy preserving clustering methods using a partially homomorphic encryption algorithm. Electronics 9(2):229. https://doi.org/10.3390/electronics9020229
16. Khalid W, Saleh N, Saleh F (2017) Standalone microfluidic analytical chip device (United States Patent Application). https://pimg-faiw.uspto.gov/fdd/64/2017/38/033/0.pdf
17. Saleh N, Khalid W, Saleh F (2017a) Apparatus and method for programmable spatially selective nanoscale surface functionalization (United States Patent Application). https://pimg-faiw.uspto.gov/fdd/80/2017/80/033/0.pdf
18. Saleh N, Khalid W, Saleh F (2017b) Self-flowing microfluidic analytical chip (United States Patent Application). https://pimg-faiw.uspto.gov/fdd/98/2017/38/033/0.pdf
19. U.S. Food and Drug Administration (2019) General wellness: policy for low risk devices—Guidance. Center for Devices and Radiological Health Guidance. https://www.fda.gov/regulatory-information/search-fda-guidance-documents/general-wellness-policy-low-risk-devices
20. U.S. Food and Drug Administration (2020) Classify your medical device. Overview of Device Regulation. https://www.fda.gov/medical-devices/overview-device-regulation/classify-your-medical-device
21. O'Connor M (2020) FDA clears "world's first" portable, low-cost MRI following positive clinical research. Health Imaging; Innovate Healthcare. https://www.healthimaging.com/topics/healthcare-economics/fda-clear-worlds-first-portable-mri
22. de Rojas C (2020) Portable sequencing is reshaping genetics research. Labiotech.eu; Labiotech. https://www.labiotech.eu/in-depth/portable-sequencing-genetics-research/
23. Home hemodialysis (2015) National Kidney Foundation. https://www.kidney.org/atoz/content/homehemo
24. Sharma R (2018) Who really owns your health data? Forbes. https://www.forbes.com/sites/forbestechcouncil/2018/04/23/who-really-owns-your-health-data/
25. Reportable diseases. (2022) Medline Plus; National Library of Medicine. https://medlineplus.gov/ency/article/001929.htm
26. Nissim K, Steinke T, Wood A, Altman M, Bembenek A, Bun M, Gaboardi M, O'Brien DR, Vadhan S (2017) Differential privacy: a primer for a non-technical audience (Grant No. 1237235). Center for Research on Computation and Society, Harvard University. https://privacytools.seas.harvard.edu/files/privacytools/files/nissim_et_al_-_differential_privacy_primer_for_non-technical_audiences_1.pdf
27. Al-Aswad H, El-Medany WM, Balakrishna C, Ababneh N, Curran K (2021) BZKP: blockchain-based zero-knowledge proof model for enhancing healthcare security in Bahrain IoT smart cities and COVID-19 risk mitigation. Arab J Basic Appl Sci 28(1):154–171. https://doi.org/10.1080/25765299.2020.1870812
28. Tomaz AEB, Nascimento JCD, Hafid AS, De Souza JN (2020) Preserving privacy in mobile health systems using non-interactive zero-knowledge proof and blockchain. IEEE Access 8:204441–204458. https://doi.org/10.1109/access.2020.3036811
29. Nourse MB, Engel K, Anekal SG, Bailey JA, Bhatta P, Bhave DP, Chandrasekaran S, Chen Y, Chow S, Das U, Galil E, Gong X, Gessert SF, Ha KD, Hu R, Hyland L, Jammalamadaka A, Jayasurya K, Kemp TM, Holmes EA (2018) Engineering of a miniaturized, robotic clinical laboratory. Bioeng Transl Med 3(1):58–70. https://doi.org/10.1002/btm2.10084
30. Saleh N, Sahagian K, Ehrlich PS, Sterling E, Toet D, Levine LM, Larne M (2014) Maskless plasma patterning of fluidic channels for multiplexing fluid flow on microfluidic devices. Lab-on-a-Chip, Microfluidics & Microarray World Congress Agenda, San

Diego, CA. https://www.academia.edu/42946895/Maskless_Plasma_Patterning_of_Fluidic_Channels_for_Multiplexing_Fluid_Flow_on_Microfluidic_Devices
31. Saleh N, Sterling E, Toet D (2015) Non-contact current measurements for AMOLED backplanes using electron-beam-induced plasma probes. Dig Tech Pap 46(1):118–121. https://doi.org/10.1002/sdtp.10306
32. Silicon Valley startup produces device for detecting Coronavirus (2020) Business; Bloomberg. https://www.bloomberg.com/press-releases/2020-03-21/silicon-valley-startup-produces-device-for-detecting-coronavirus
33. Currier J, NFX team (2018) The network effects bible. Guides Publishing. https://guides.co/g/the-network-effects-bible/121715
34. Pastorino R, De Vito C, Migliara G, Glocker K, Binenbaum I, Ricciardi W, Boccia S (2019) Benefits and challenges of big data in healthcare: an overview of the European initiatives. Eur J Public Health, 29(Supplement_3):23–27. https://doi.org/10.1093/eurpub/ckz168
35. Chen, J., & Micali, S. (2016). *Algorand* (arXiv:1607.01341). http://arxiv.org/abs/1607.01341
36. Jeon H-J, Youn H-C, Ko S-M, Kim T-H (2021) Blockchain and AI meet in the metaverse. In: Fernández-Caramés TM, Fraga-Lamas P (eds), Blockchain Potential in AI [Working Title]. IntechOpen. https://doi.org/10.5772/intechopen.99114
37. Botella, E. (2021, June 28). Wyoming wants to be the crypto capital of the U.S. Slate. https://slate.com/technology/2021/06/wyoming-cryptocurrency-laws.html
38. Highest intensity focused laser (2008) Guinness World Records. https://www.guinnessworldrecords.com/world-records/highest-intensity-focused-laser

Dr. Ned Saleh is the Founder of Synsal, Inc. He received his engineering doctoral degree from the University of Michigan in 2004 under the supervision of Prof. Gérard Mourou, who won the Physics Nobel prize in 2018. Dr. Saleh's academic work played an important role in bringing this award to the world front stage when the laser system he developed with a handful of scientists was cited in the Guinness Book of World Records for the "Highest Intensity Focused Laser" in 2008 [38]. Dr. Saleh's career afterwards took him to a series of senior academic and industry positions, including Berkeley Lab, Intel, IBM, Applied Materials and Apple, and others in the Silicon Valley.