future internet

Article

Blockchain and the Tokenization of the Individual: Societal Implications

Monique J. Morrow [1] and Mehran Zarrebini [2,*]

[1] Vetri-Global, Klosbachstrasse 128, CH-8032 Zürich, Switzerland; monique.morrow223@gmail.com
[2] PFE International Inc., The Laurels, Saddlers Way, Long Marston, York YO26 8AW, UK
* Correspondence: mehran@zarrebini.com; Tel.: +2783-637-1270

Received: 27 July 2019; Accepted: 14 October 2019; Published: 22 October 2019

Abstract: We are living in a world where the very systems upon which trust is based are being challenged by new and exciting paradigm shifts. Centralization whether in the form of governments, financial institutions, enterprises and organizations is simply being challenged because of the lack of trust associated with data governance often experienced in the form of data breaches or simply a monetization of our data without our permission and/or incentives to participate in this emerging decentralization of structures. We see this trust deficit challenging the very institutions we have depended on including but not limited to financial institutions, private enterprises or government bodies. A new "social contract" is required as we continuously evolve into more decentralized and self-governing (or semi self-governing) entities. We will see more development in digital sovereignty with the caveat that a governance model will need to be defined. This position paper will present evidence that supports the premise that blockchain and individual tokenization could provide a new social contract.

Keywords: tokenization; blockchain; social; decentralization; monetization; waste management

1. Introduction

There are several key areas that will be driving decentralization and to some extent the creation of autonomous organizations; for example, the exponential growth of Fifth-Generation Technology (5G) and the Internet of Things (IoT)-connected devices that possess their own identities and data. They will communicate with each other without human intervention. The IoT industry is ripe for the next major wave of disruption through decentralized applications.

Examples of decentralization include supply chains, which are inherently complex, lack transparency and result in a duplication of tasks among stakeholders, impacting efficiency and cost. Other examples include energy companies that are also using digital assets in new and revolutionary ways and may usher in a new era of energy management worldwide such as the use of energy and an exchange of energy value amongst communities [1]. These assets could later be used to have some influence on how such projects are operated, allowing stakeholders to participate in key decisions that affect their communities [2]. Healthcare and tokenizing the asset of your health data such that they bring value to you will become important. This will perhaps challenge the very healthcare insurance entities that we know today. We are moving beyond a tokenization economy and rather witnessing the democratization of data at a societal level.

In this position paper, we explore the distinction between tokenization and encryption and the shift towards decentralization, specifically in the context of human data. We then explore the evolution of the social contract in a digital world where a digital citizen is the source of the social contract. Self-tokenization and data democratization are considered together with emerging solutions that seek to mitigate against data leakage and the protection of human data. Tokenization will impact the way organizations are governed in various ways, and regulatory models of corporate governance will need to be re-examined in light of the profound disruption to business caused by tokenization. We conclude the paper with a discussion on tokenization and waste management with specific emphasis on supply chains and autonomous/electrical vehicles.

2. Tokenization and Encryption

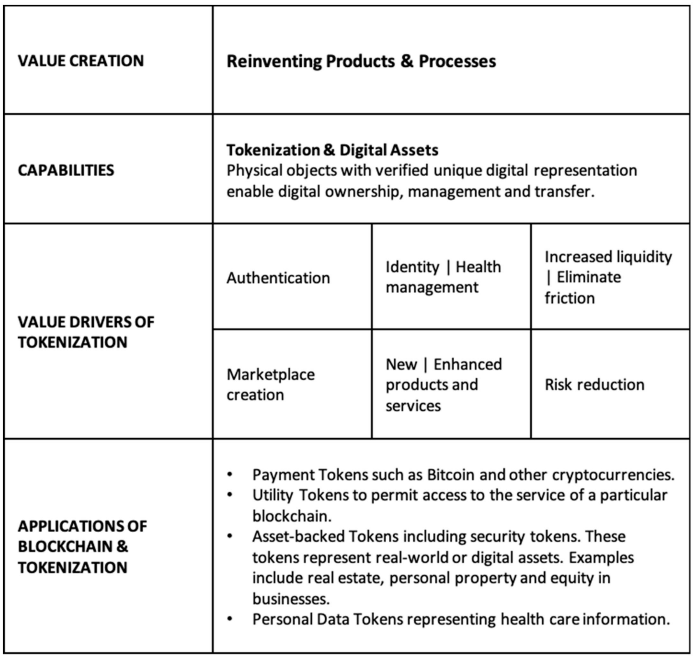
Digital transformation, "high tech" including AI and blockchains, has provided a multitude of opportunities for organizations to innovate by creating a leap in buyer value and delivering increased efficiencies across a wide cross-section of buyers. Individuals and businesses have therefore benefited tremendously from this transformation, but have also become susceptible to security threats and cyber criminality. In a study conducted by the Verizon Business RISK Team, more than 280 million payment card records were breached in 2008 [3]. The global financial market collapse not only created economic headwinds of unprecedented proportions, but also some of the largest data breaches in history also occurred in the same year. In fact, the study confirmed that if reasonable security controls had been in place at the time of the incident, the breaches could have been avoided in their entirety.

Compliance to security standards is a resource-intensive challenge to all businesses irrespective of size. Despite the enormous efforts and vast expenditure of businesses to secure their data, hundreds of millions of records have been breached and continue to be. For instance, in 2008, the Verizon Business RISK team highlighted that retail, financial services and food and beverage accounted for three-quarters of the 2008 breaches. The majority of the records were compromised from servers and applications [3]. In 66 percent of the cases, the breach involved data that the organization did not know existed on their servers. Data breaches have continued to plague numerous industries since 2008. In 2018, an unprecedented number of breaches occurred, varying in severity. Hacking groups injected malicious code into poorly-secured web pages of British Airways, which exposed the data of 380,000 customers, and in India, an ID database managed by the Indian Government was compromised, exposing the identity details and private information of 1.1 billion individuals [4].

Two technologies utilized in the protection of data is encryption and tokenization. Tokenization and encryption are often mentioned together, and their definition is used interchangeably. While both are utilized as data obfuscation technologies, there are clear distinctions between the two. Both technologies can be utilized to secure data under varying circumstances, and in some instances, such as end to end payment facilitation, both encryption and tokenization are used together.

Encryption is the process of using an algorithm to transform plain text information into a non-readable form called ciphertext. An algorithm and an encryption key are required to decrypt the information and return it to its original plain text format. In symmetric key encryption, the same key is used to both encrypt and decrypt the information. In asymmetric key encryption, two different keys are used for encryption and decryption. Therefore, the private key can decrypt messages sent to an individual, but cannot decrypt what is sent to another part, as that is encrypted with another key pair. Today, secure sockets layer (SSL) encryption is commonly used to protect the information as it is transmitted on the Internet. Using the built-in encryption capabilities of operating systems or third-party encryption tools, millions of people encrypt data on their computers to protect against the accidental loss of sensitive data in the event their computer is stolen. Data encryption can be expensive and a resource-intensive proposition.

Tokenization, on the other hand, is the process of converting a piece of data into a random string of characters known as a token. Tokenization protects sensitive data by substituting non-sensitive data. The token serves merely as a reference to the original data, but cannot be utilized to determine those values. A credit card number, for example, is replaced within the merchant's storage environment by a token value generated in such a way that it cannot be linked back to the original data element [5]. The token value can, therefore, be used in numerous applications, some of which are considered in this paper, as a substitute for real data (see Figure 1). The advantage of tokens is that there is no mathematical relationship to the real data that they represent. The real data values cannot be obtained through reversal, and hence, a breach renders the information invaluable.



VALUE CREATION	**Reinventing Products & Processes**		
CAPABILITIES	**Tokenization & Digital Assets** Physical objects with verified unique digital representation enable digital ownership, management and transfer.		
VALUE DRIVERS OF TOKENIZATION	Authentication	Identity | Health management	Increased liquidity | Eliminate friction
	Marketplace creation	New | Enhanced products and services	Risk reduction
APPLICATIONS OF BLOCKCHAIN & TOKENIZATION	• Payment Tokens such as Bitcoin and other cryptocurrencies. • Utility Tokens to permit access to the service of a particular blockchain. • Asset-backed Tokens including security tokens. These tokens represent real-world or digital assets. Examples include real estate, personal property and equity in businesses. • Personal Data Tokens representing health care information.		

Figure 1. Blockchain and tokenization value framework.

Tokens are being increasingly used to secure varying types of sensitive information. In particular, personal identifiable information such as healthcare information, email addresses and account numbers are such examples. From a security perspective, tokenization significantly reduces risk based on the fact that sensitive data cannot be breached if it is not there in the first place. However, there are a number of other use cases where tokens create value such as the tokenization of traditional financial assets where liquidity creates barriers to entry, and tokenizing these assets, for instance, using blockchain to convert rights into a digital token backed by the asset itself can solve this problem. We are likely to see an increase in the number of tokenized real assets including but not limited to real estate, where investors are able to own portions of real estate and collectibles such as art [6]. The future will result in an environment of greater personalization and customization. In both instances, the token represents distributed ownership of the underlying asset's value, but not the asset itself, democratizing the process of ownership.

A new "tokenized" economy offers tremendous potential for creating a more efficient and inclusive environment in which tangible and intangible assets can be traded through greater liquidity, accessibility, transparency and faster and cost-effective transactions [7]. Furthermore, tokenization in essence allows you to compartmentalize personal data and manage them across different users simply and effectively. That data can therefore only be accessed by an entity who has the correct token. The information is secure and completely portable since the personal data is controlled by the individual and shared with permission, a stark difference to data that are being utilized currently.

3. The Shift towards Decentralization

In addressing the shift towards "decentralization", it is important to define nomenclature and context. For example, the question for clarification is: what is meant by "decentralization" in comparison to "distributed" and "peer-to-peer" constructs? Distributed within the context of organizations has been the topic of a body of research specifically around the study of organization computing [8]. The underlying network and IT applications facilitate collaborative communications. The peer-to-peer or P2P architecture refers to the foundational network of nodes where the clients do not share any of their resources such as storage capacity, computing power, network connection, bandwidth and content [9]. Within this paper, decentralization may assume the use of distributed and P2P capabilities. At a societal level, the shift towards decentralization has various sources such as the financial crisis of 2008, the numerous breaches of citizen data in the form of hacks and the lack of privacy by design [10].

The thesis is that the centralization of citizen data is subject to abuse. This centralization can take the form of government and commercial entities where the governance model is questionable due to these abuses. The exhortation that "data is the new oil" only amplifies the value of citizen data and the interpretation that such data is indeed a tokenized asset [11]. The Satoshi Nakamoto white paper describing Bitcoin as a "P2P Electronic Cash System" is a manifestation of decentralization at a societal level that offers a frictionless exchange of value [12]. This notion of decentralization goes further to include the creation of "Decentralized Autonomous Organizations" or DAOs where smart contracts create business and organization logic as to provide governance in the absence of centralization [13]. A smart contract is a computer program code that is capable of facilitating, executing and enforcing the negotiation or performance of an agreement using blockchain technology. The first experiments with DAOs and smart contracts clearly showed that these solutions function in an arena that is almost entirely unregulated, and attempts to experiment with DAOs have not gone without controversy and have in themselves stimulated research in this space [14]. Whilst technology possesses no agency and therefore cannot prevent miscreant actors from exploiting its intentional use, there is a chasm developing between intentional/unintentional surveillance by central authorities and the balance of what may be best for society [15,16].

This observation begs the question as to how this chasm may be resolved and by which entities. What kind of social contract is required for the digital world we share? How is trust defined, and what is the role of trust towards decentralization? Social contract theory can be best defined as shaping policy consensus between designated authorities, e.g., government entities and citizens. There is an implication that values and ethics are shared [17]. In the 21st Century, fostered by the use of social media and the Internet, social contracts have been evolving to identity politics and the notion of multiple identities especially when referring to IoT and to the Internet of Everything and Everyone. Dignity and the struggle for recognition are provoking the requirement for a new social contract that can function in a digital world [18]. Given the pattern of decentralization or a hybrid therein, a novel and relevant social contract must put the citizen in the centre of the digital universe as an active player. A citizen can be defined as an individual who selectively and knowingly asserts his/her rights in a digitally-driven world. Therefore, a citizen does not necessarily mean an individual who belongs to a particular nation state, nor is a world citizen implied here. A digital citizen whose data is valuable must be the source of the social contract between he/she and the entities that he/she "trusts" preferably in decentralized modalities. This is a new assertion given that 21st Century social contracts have been evolving to include universal basic income to the right of guaranteed employment under Industry 4.0. There is still a dependency on government entities where social contracts involve the instrument of taxation that is required to provide a "collective welfare" for nation-state citizens [19]. Who creates the rules and how such rules are implemented may be a function of a societal smart contract that is developed by the digital citizen.

The blockchain has been evolving over the past 10 years to include adoption by enterprises and in some cases governments. However, the missing link has been a digital citizen-driven social and smart contract. There is an assumption that the digital citizen possesses a priori knowledge in both the development and use of these emerging mechanisms that foster the creation of a new social contract. This assertion may be true; therefore, further exploration on the type of training and education and by which entities is recommended.

4. Trust in a Centralized World and Emerging Solutions for the Protection of Human Data

There is a body of research that seeks to define "trust", which is a complex sociological, psychological concept and the basis for human interactions [20]. As the old adage goes, "Trust takes years to build, seconds to break, and forever to repair" (source unknown). Given the data breaches and misuse of individual/citizen data described in Section 3, trust in a centralized world is problematic as the governance model assumes self-regulation by the central parties. This fact is described in the Netflix documentary entitled, "The Great Hack," where privacy and abuse of individual/citizen data is the tip of the iceberg of a calculated strategy to both take data and control away from the individual [21]. An observation has been that the "outrage" from this data abuse has not come from individual/digital citizens, but rather from nation-state governments and privacy, as well as human rights organizations [22]. This fact begs the question as to whether or not the individual is immune to such data abuses that involves his/her data. Perhaps the response to this hypothetical question may be the degree of perceived or actual abuse, e.g., personal bank account and funds stolen vs. identity fraud vs. data leakage with no "direct harm" as a result of an organizational breach. If the degree of perceived or actual abuse is greater than "no direct harm," then the question is whether or not the egregious act has resulted in the individual behavioural change from passive to active digital citizen. There is an abundance of research in human hacking, but in terms of empirical and behavioural analysis that confirms a change as a result of such abuse, the research is lacking at least at the macro level [23]. This particular question may be difficult to ascertain because individuals (collectively) may be disinclined to share the fact that they have been victims. Therefore, the postulation is that behavioural change is possible when correlated with the severity of the abuse.

However, trust can manifest itself in a Thomas Hobbes-like Leviathan where a central authority like a government entity operates in the background to assure that society behaves according to the rules that have been developed by the central authority [24]. As a social psychologist, Thomas Tyler observed that rules will be followed if the citizens perceive procedural fairness [25]. At the opposite end of this trust spectrum is peer to peer (P2P) trust, which is based largely on relationships and shared ethical norms. P2P trust may be interpersonal as experienced amongst families, friends or via a shared set of operating principles, for example the Internet. Furthermore, the modality of the engineers who develop protocols and architectures to evolve the Internet (The Internet Engineering Task Force or IETF) is "rough consensus and running code" and "we reject kings, presidents and voting" [26].

Additionally, reputation graphs can reflect P2P trust relationships [27]. The blockchain has often been referred to as "trustless trust", an assertion from Reid Hoffman and evidenced by the operational nature of the blockchain, e.g., "in proof we trust" [28]. Within the context of this paper, there is evidence to suggest that the digital citizen is evolving towards a hybrid approach between P2P and Leviathan trust where the result is the removal of intermediary actors and the requirement for transparency in Leviathan trust models [29]. There are emerging solutions that seek to mitigate against data leakage and the protection of human data. With privacy by design as a tenet, in regulation, the European Union General Data Protection Regulation (GDPR) has defined data protection specific to enterprises. Failure to adhere to GDPR compliance will be expensive for enterprises [30]. GDPR further poses the question as to what constitutes actual data, for example hashing of personal data within the blockchain could be problematic. One recommendation has been to avoid hashing personal identifiable information (PII) as a practice [31]. There has been consideration for the use of zero knowledge proof (ZKP) mechanisms to mitigate against data leakage where range values can be applied in lieu of actual human-personal-digital citizen data. Commercialization of such capabilities is in progress [32]. Additionally, there is a continuous dialogue between academics and enterprises as to use cases and standardization of ZKP mechanisms [33]. Secure multiparty computation (SMPC) is currently being applied for privacy-enforced computation, the on/off chain within the blockchain context [34]. The Sir Tim Berners-Lee Project, Solid, is taking a step further in re-designing the web where the individual can be in control of his/her data [35]. Bryan Ford at EPFL in Switzerland has established a Decentralized and Distributed Systems Lab (DEDIS) with "no single trusted party" [36]. David Chaum has been in the privacy space for decades and is now implementing Elixxir [37].

This list of emerging solutions is in no way a comprehensive one, but confirms rather the trends towards digital-citizen control of his/her data and the implementation of human data privacy overall. There is room for additional research so as to assure selective disclosure and control for the digital citizen.

5. Governance and Regulation in a Tokenized World

Tokenization will impact the way organizations are governed in various ways. Basic notions inherent in corporate governance will be transformed such as accountability, responsibility, transparency and trust [38]. There is an opposing view that there is no urgent need to put digital technologies on the regulatory agenda as the practice of governance will not be disrupted by technologies such as distributed ledgers, blockchain and IoT. Clearly, the products and services of these organizations will be affected, but traditional regulatory models are robust enough to deal with such disruption [39].

There is an emerging view that extant regulatory models of corporate governance will struggle and need to be re-examined in light of the profound disruption to business caused by tokenization [39]. Tokens can be created to develop a link between the token and economic or non-economic ecosystem such as personalized data and can also be created to record or transfer this data via computer code on the distributed ledger. The general topic of tokenization is less than three years old, and that of self-tokenization a relatively new topic. The digitalization of all kinds of both tangible and intangible assets and of the creation of new types of rights raises substantial governance issues. It has been shown that with the tokenization of tangible assets such as securities, the new corporate stakeholders or token holders could potentially affect the balance of power within organizations [40]. Furthermore, a new form of trust, digital trust, based on mathematical algorithms and machines is being developed as the reliance on intermediaries and third parties diminishes. The rapid pace at which the development of the distributed ledger and blockchain is taking shape reinforces the dependency on digital trust. Digital trust has therefore an impact on how we interact with other entities and society in general. People will increasingly trust decentralized forms of governance in the future [41]. Libra aims to create a reliable digital currency and infrastructure that can deliver on the promise of the "Internet of money". To make the mission of Libra, a stable cryptocurrency governed by an independent association tasked with evolving the ecosystem, a reality, a governing entity, the Libra Association [42], has been designed to facilitate the operation of the Libra blockchain. The association will develop and adopt a comprehensive charter and a set of bylaws for the association on the basis of the currently proposed governance structure. The association will ultimately develop a path toward permission-less governance and consensus on the Libra network.

Blockchain technology has the potential to solve principal-agent issues that flourish in the area of regulation and governance. Individuals would be able to verify and regulate access to and use of personal data. Legislation would have to adapt in order to define clearly data ownership and the use of non-consensual data. In the area of personal data, there is a trade-off between the claim that private data ownership would enhance privacy protection and sovereignty over one's own data and the public's need for data access in instances such as enhancing researchers' access to data for clinical care, public health and research [43].

Increased transparency has the potential to protect individuals. Personal data storage on the blockchain will allow people to own and maintain personal data, granting and rescinding access and enabling it to be used, shared or deleted as necessary. Each user has complete transparency over what data is being collected and how it is processed [44]. Disintermediation would simplify the process of authorizing access to personal data, which would streamline processes and increase efficiency. With increased mobile application usage, a set of permissions is often granted upon download or sign-up. While opting-out is generally the only way to relinquish continued access to data, the improvement of the existing permission dialog in mobile applications, access control policies will be stored on the blockchain where the user has rights to modify them or revoke access to previously collected data.

6. Tokenization in Waste Management, Electrical and Autonomous Vehicles

A circular economy is an industrial system that is restorative or regenerative by intention and design [45]. The "end of life" concept is replaced with the concept of restoration and strives for waste elimination through the innovative design of materials, products, systems and the introduction of novel business models. Through numerous technological advances, recycling has become increasingly more viable through the deployment of technology such as radio frequency identification (RFID) and IoT. The deployment of these technologies has created greater efficiency with respect to logistics, knowledge sharing and tracking of materials [46].

More recently, various circularity initiatives have begun leveraging blockchain technology for verification purposes. RecycleToCoin [47] looks to increase participation through recycling waste in the United Kingdom. Users of the RecycleToCoin application are incentivized to take their recyclable plastic and aluminium cans to participating stores. They are then given tokens in a secure digital wallet based on the quantity of recyclable material deposited, which can then be turned into digital currencies (Bitcoin or Ethereum) or gift cards via GiftPay [48] or donated to PlasticBank [49]. PlasticBank has created recycling systems in many global locations providing fair value for waste collectors and supporting digital transactions through the employment of a permissioned blockchain. In order to achieve scalability and incorporate other technologies such as analytics and visual recognition, PlasticBank has employed blockchain on IBM LinuxONE [50].

Food waste throughout the world is an increasing problem due to its impact on the environment, natural resource scarcity and significant contribution to global warming and climate change. One third of all food produced is lost or wasted. The United Nations Sustainable Development Goals (SDGs) aim to include a target to halve per capita global food waste at the retail and consumer level and reduce food losses along production and supply chains, including post-harvest losses by 2030 [51]. In Europe, food waste is an increasing concern. The production, distribution and storage of food use natural resources, and the discarding of food, especially that which is still edible, increases these impacts. One company in the United States is aiming to tackle food waste in order to solve food insecurity and also resolve an estimated USD 40 billion in tax credits for businesses that remain unclaimed annually. Goodr [52] is utilizing blockchain technology to track an organizations' surplus food waste from collection to donation, enabling tax deductions for organizations fully compliant with the Internal Revenue Service (IRS) in the United States, reducing greenhouse gas emissions and creating social good by moving edible surplus to communities in need.

Blockchain technology can also be used in other waste management industries and plays a pivotal role in ensuring that recyclables do not end up in landfill. Digital tracking of data allows for deeper analyses of supply chains. Utilising this technology with IoT devices and RFID, greater efficiencies can be gained and roque activity marginalised. Such activity has been prevalent in the tire recycling industry across the globe. Each year, 1.6 billion new tires are generated, and around one billion of waste tires is generated [53]. The collection and recycling of tires and prevention from landfill, sensitive habitats and abandoned areas remain a challenge for the industry globally. The tire supply chain consists of the production of raw materials, the production of tires, the distribution of tires, the use of tires and then the collection, sorting and recycling of end of life tires (ELTs). ELTs are processed into rubber granulate and energy recovery.

There are therefore a number of stakeholders involved in the industry, which include raw material producers, tire manufacturers, buyers and sellers, waste collectors, recyclers, logistics companies and the government, who oversees the recycling industry from a regulatory and governance perspective. In the supply chain, the raw materials constitute the basic unit out of which a tire is produced. This is the basic material from which a tire is created. The tire manufacturers could therefore tokenize the raw materials. The token would represent a digital twin that is a depiction of the raw materials in the form of a token utilised to trace the raw materials throughout the supply chain. This allows stakeholders to follow the newly-defined asset throughout the supply chain.

There are a number of ways to digitalize the raw materials in a tire. The raw materials could be deemed a non-fungible asset, an asset in the form of a token, which through cryptography would help to prove verifiably the ownership and authenticity of the asset. Another option is to have the asset defined as a fungible asset; the asset can therefore not be interchanged. Therefore, if a specific batch of raw material is required to be traced throughout the supply chain, then this approach would be more feasible. In this instance, the raw materials will be assumed to be non-fungible. The raw material producers therefore generate tokens, which are then supplied to the logistics companies. The logistic companies take the raw material and the equivalent amount of tokens that are representing the amount of raw materials in weight and transport or ship them to the tire manufacturing plant. The manufacturing plant receives both tokens and raw materials and produces tires. The tire producer can therefore continue with the token that represents the weight, or the token can be converted to represent the actual number of tires produced.

The raw material tokens can therefore be spent in the exchange of a tire token that will be issued by the manufacturing plant. Another option would be to create a batch token that represents the weight of raw material utilized to make a batch of tires. This batch of tires, once manufactured, is moved to a warehouse. A seller of the tires has both a batch of tires for sale and the equivalent number of tokens that represent the batch of tires. As tires are sold, a quick response code could be scanned to verify the authenticity of the tires in the supply chain. Additionally, the buyer of the tire could be provided with the token that verifies the authenticity of the tires purchased. As the tires are replaced in the future and ELTs transported to waste tire processors, there is full visibility and traceability along the entire supply chain. The tokens therefore represent the validation of the genuineness of the product itself.

With multiple stakeholder involvement including multiple raw material manufacturers, tire producers, logistics companies and recycling companies, the privacy of information would be of great concern. The privacy of each stakeholder could be controlled through the private issuance of tokens utilizing ZKPs [32]. Certain information could be kept private in order to protect different stakeholders, and visibility can be granted to entities on a need-to-know basis. Ownership of blockchain assets can be transferred without revealing the confidential transaction details, while still ensuring regulatory compliance according to custom-defined business rules. In the event that a government requires oversight of the supply chain, it could be provided an auditor role utilizing viewing keys in order to gain industry insights into the network. Such insights would include knowledge of productivity, manufacturing outputs, prohibition of the resale of waste tires and output validification from recyclers to determine processing subsidies. The provision of end-to-end visibility into multiple enterprise supply chain networks utilizing blockchain technology enables multiple stakeholders to track and trace end of life tires, creating trust by recording indisputable transactions on the distributed ledger.

Electric vehicles represent the fastest growing sector of vehicle sales globally, with sales increasing by 64 percent in 2018 and Tesla's Model 3 Sedans the biggest seller in the second half of 2018. In China, sales of electric vehicles increased by over 500 000 units to 1.2 million in 2018, by far the largest contributor to electric vehicle sales [54]. At the end of 2018, the global fleet of light vehicle plug-ins was 5.4 million with an estimated sale in 2019 of 3.2 million vehicles [54]. Power Ledger and Silicon Valley Power [55] have recently completed a blockchain trial that monetizes electric vehicle charging infrastructure, creating the potential for tokenized carbon credit trading. Power Ledger's blockchain-backed platform was trialled to track and manage the Low Carbon Fuel Standard (LCFS) credit generation from solar panels and electric vehicle charging infrastructure, as well as credit trading. The solar and charging data produced from the Tasman infrastructure was recorded as smart contracts on the blockchain platform, which then created a digitized LCFS certificate. This certificate contained a cryptographic hash of the information calculated in real time, which was then sent to Silicon Valley Power's wallet, enabling Silicon Valley Power to monetize their electric vehicle charging infrastructure, thereby creating a secondary market for tokenizing and trading LCFS credits.

The rise of autonomous vehicles is set to be transformational as the market is set to reach USD 42 billion by 2025 [56]. While ethical challenges with respect to split-second decision making remain a major concern, greater understanding of the ethical guidelines artificial intelligence (AI) will follow will need to be understood in great depth. When driving, individuals learn from their own mistakes. They rarely learn from others, collectively making the same mistakes over and over again. AI, on the other hand, evolves differently. When an autonomous vehicle makes an error, all of the other autonomous vehicles are able to learn from it. In fact, new autonomous vehicles will inherit the complete skill set of their ancestors and peers; so collectively, these cars can learn faster than people. If this data is recorded on the blockchain, new autonomous vehicles essentially evolve at a rapid pace since the data is available immediately via the distributed ledger.

It is inevitable that in a short period of time, autonomous vehicles will manoeuvre along roads in conjunction with human-driven cars. Sophisticated AI tools and distributed ledger technology will empower individuals to better learn from the experiences of others. The increased use of autonomous vehicles is ultimately premised on trust. The individuals who buy or use them have to trust the technology and must be comfortable using that technology for its true value to be realized. In order to build this trust and acceptance, autonomous vehicle manufacturers must ensure the technology is safe, secure and creates a leap in value for consumers. The machine world and social world will therefore operate in unison. Humans will therefore emulate the superior learning processes of the machine. The machine hive will become a role model for a new human hive in which we march in peaceful unison toward a world free of mistakes and accidents [15].

7. Conclusions

In summarizing this research, the authors explored the application of tokenization to the individual and assessed its societal implications in the form of defining a new social contract; articulating the security, privacy in terms of encryption and identifying further mechanisms as to secure further digital citizen data and assert control. It was shown that at the societal level, blockchain technology is being used in the waste management industry in combination with IoT devices to reduce waste, greenhouse gas emissions and create social good. It was demonstrated that blockchain technology can play a pivotal role in ensuring recyclables such as tires do not end up in landfill. Digital tracking of data allows for deeper analyses of complex supply chains where multiple stakeholder involvement is inherent in the supply chain. The review covered the monetization of electric vehicle charging infrastructure with the advent of global growth in sales of electric vehicles. The application of IoT and blockchain was extended to autonomous vehicles, which rely on machine learning and pattern recognition, approaches from the field of artificial intelligence. Blockchain will facilitate the learning approach, requiring an extensive learning strategy and trust where vehicles will be exposed to a large number of complex situations.

Trust architecture models whether Leviathan in nature or P2P will more than likely be hybrid in nature, as will the related governance models. There are emerging solutions about whether the commercialization of ZKP mechanisms or David Chaum's Elixxir should be followed. The assertion "we are valuable" implies that the digital citizen must be an active player for selective disclosure and control. There is room for empirical research to confirm the results of this assertion. John Cheny-Lippold's book, We Are Data, Algorithms and the Making of Our Digital Selves [57], is a step in this direction when discussing "data about data". Identity is foundational in this discussion, whether referring to an individual, IoT or connected cars.

In summary, this specific research topic "tokenization of the individual and societal implications" is still nascent. The authors believe that this position paper can be a framework for further research.

Author Contributions: Writing, original draft, M.J.M. and M.Z.; writing, review and editing, M.J.M. and M.Z.

Funding: This research received no external funding.

Conflicts of Interest: The author declares no conflicts of interest.

References

1. Finance 4.0. Technical Report. 2018. Available online: https://www.research-collection.ethz.ch/handle/20.500.11850/286469 (accessed on 5 May 2019).
2. IISD. Tokenization of Infrastructure. A Blockchain-Based Solution to Financing Sustainable Infrastructure. 2019. Available online: https://www.iisd.org/sites/default/files/publications/tokenization-infrastructure-blockchain-solution.pdf (accessed on 5 May 2019).
3. Verizon. Data Breach Investigations Report, Verizon Business RISK Team. 2009. Available online: https://enterprise.verizon.com/resources/reports/2009_databreach_rp.pdf (accessed on 5 May 2019).
4. DashLane. Data Breaches 2018: The 20 Biggest Breaches of the Year. 2018. Available online: https://blog.dashlane.com/data-breaches-2018/ (accessed on 8 May 2019).
5. First Data. Data Encryption and Tokenization: An Innovative One-Two Punch to Increase Data Security and Reduce the Challenges of PCI DSS Compliance. 2009. Available online: https://www.firstdata.com/downloads/thought-leadership/fd_encrypt_token_pci_whitepaper.pdf (accessed on 8 May 2019).
6. Hargrave, J.; Sahdev, N.; Feldmeier, O. How Value Is Created in Tokenized Assets. *SSRN Electron. J.* **2018**. [CrossRef]
7. Deloitte. The Tokenization of Assets Is Disrupting the Financial Industry. Are You Ready? 2018. Available online: https://www2.deloitte.com/content/dam/Deloitte/lu/Documents/financial-services/lu-tokenization-of-assets-disrupting-financial-industry.pdf (accessed on 10 May 2019).
8. Podolny, J.M.; Page, K.L. Network Forms of Organization. *Annu. Rev. Sociol.* **1998**, *24*, 57–76. [CrossRef]
9. Schollmeier, R. A Definition of Peer-to-Peer Networking for the Classification of Peer-toPeer Architectures and Applications. In Proceedings of the First International Conference on Peer-to-Peer Computing, Linkoping, Sweden, 27–29 August 2001; pp. 101–102. [CrossRef]
10. Morlino, L.; Quaranta, M. What is the impact of the economic crisis on democracy? Evidence from Europe. *Int. Political Sci. Rev.* **2016**, *37*, 618–633. [CrossRef]
11. Hirsch, D.D. The Glass House Effect: Big Data, the New Oil, and the Power of Analogy. *Maine Law Rev.* **2014**, *66*, 373.
12. Nakamoto, S. Bitcoin: A Peer to Peer Electronic Cash System. 2008. Available online: https://bitcoin.org/bitcoin.pdf (accessed on 10 July 2019).
13. Jentzsch, C. Decentralized Autonomous Organization to Automate Governance Final Draft-Under Review. Available online: https://lawofthelevel.lexblogplatformthree.com/wp-content/uploads/sites/187/2017/07/WhitePaper-1.pdf (accessed on 12 July 2019).
14. Hacker, P. *Corporate Governance for Complex. Cryptocurrencies? A Framework for Stability and Decision Making in Blockchain-Based Organizations*; Forthcoming in: Regulating Blockchain. Techno-Social and Legal Challenges; Oxford University Press: Oxford, UK, 2019.
15. Zuboff, S. *The Age of Surveillance Capitalism, The Fight For. A Human Future at the New Frontier of Power*; Hachette Book Group: New York, NY, USA, 2019.
16. Brunton, F. *Digital Cash, the Unknown History of the Anarchists, Utopians, and the Technologists Who Created Cryptocurrency*; Princeton University Press: Princeton, NJ, USA, 2019.
17. Jos, P.H. Social Contract Theory: Implications for Professional Ethics. *Am. Rev. Public Adm.* **2006**, *36*, 139–155. [CrossRef]
18. Fukuyama, F. *Contemporary Identity Politics and the Struggle for Recognition*; Profile Books Ltd.: London, UK, 2018.
19. Sharma, M.; Chapman, T.; Saran, S. *A New Social Contract for the Digital Age*; The Future of Work and Education for the Digital Age: T20 Argentina; CIPPEC: CABA, Argentina, 2018.
20. Robbins, B.G. What is Trust? A Multidisciplinary Review, Critique, and Synthesis. *Sociol. Compass* **2016**, *10*, 972–986. [CrossRef]
21. The Great Hack. Available online: https://www.netflix.com/hk-en/title/80117542 (accessed on 26 July 2019).
22. Isaak, J.; Hanna, M.J. User Data Privacy: Facebook, Cambridge Analytics and the Privacy Protection. *Computer* **2018**, *51*, 56–59. [CrossRef]
23. Okenyi, P.O.; Owens, T.J. On the Anatomy of Human Hacking. *Inf. Syst. Secur.* **2007**, *16*, 302–314. [CrossRef]
24. Hobbes, T. *Leviathan: Or the Matter, Forme, and Power of a Common-Wealth Ecclesiasticall and Civill*; Cambridge University Press: Cambridge, UK, 2010.

25. Tyler, T. *Why People Obey the Law*; Princeton University Press: Princeton, NJ, USA, 2006.
26. IETF. On Consensus and Humming in the IETF. 2014. Available online: https://tools.ietf.org/html/rfc7282 (accessed on 17 July 2019).
27. Liu, L.; Xiong, L. Peer Trust: Supporting Reputation-Based Trust for Peer-to-Peer Electronic Communities. *IEEE Trans. Knowl. Data Eng.* **2004**, *8*, 843–857.
28. Werbach, K. *The Blockchain and New Architecture of Trust*; The MIT Press: Cambridge, MA, USA, 2018.
29. Adam, I.; Fazekas, M. Are Emerging Technologies Helping win the Fight Against Corruption in Developing Countries. 2018. Available online: http://www.govtransparency.eu/wp-content/uploads/2019/02/ICT-corruption-24Feb19_FINAL.pdf (accessed on 16 July 2019).
30. Data Protection. Rules for the Protection of Personal Data Inside and Outside the EU. 2018. Available online: https://ec.europa.eu/info/law/law-topic/data-protection_en (accessed on 19 July 2019).
31. Blockchain-Consortium. How does the EU's GDPR Apply to Hashed Data on the Blockchain? 2018. Available online: https://legalconsortium.org/uncategorized/how-does-the-eus-gdpr-view-hashed-data-on-the-blockchain/ (accessed on 20 July 2019).
32. Qedit. A Privacy Layer For. Your Blockchain Network. 2019. Available online: https://qed-it.com/ (accessed on 20 July 2019).
33. ZKProof. Zero Knowledge Proof Standardization. 2019. Available online: https://zkproof.org/ (accessed on 20 July 2019).
34. Shrobe, H.E.; Shrier, D.L.; Pentland, A. *New Solutions for Cybersecurity*; The MIT Press: Cambridge, MA, USA, 2017.
35. Solid. How Solid Realizes the Web as it was Originally Envisioned, in Layman's Terms. 2019. Available online: https://solid.inrupt.com/how-it-works (accessed on 20 July 2019).
36. EPFL. DEDIS. 2019. Available online: https://dedis.epfl.ch/ (accessed on 25 July 2019).
37. Elixxir. Introduction. 2019. Available online: https://elixxir.io/introduction (accessed on 25 July 2019).
38. Fenwick, M.; Vermerlen, E.P.M. *Technology and Corporate Governance: Blockchain, Crypto and Artificial Intelligence*; Lex Research Topics in Corporate Law & Economics Working Paper No. 2018-7; European Corporate Governance Institute (ECGI)-Law Working Paper No. 424/2018; Social Science Reaserch Network: Paris, France, 2018.
39. Zagar, T.M. A New Chapter for ICONOMI: Transformation of Corporate Governance and Issuance of Equity Tokens. 2018. Available online: https://medium.com/iconominet/a-new-chapter-for-iconomi-transformation-of-corporate-governance-and-issuance-of-equity-tokens-dc603df2272b (accessed on 25 July 2019).
40. Blemus, S.; Guegan, D. Initial Crypto-asset Offerings (ICOs), Tokenization and Corporate Governance. Tokenization and Corporate Governance. 2019. Available online: https://ssrn.com/abstract=3350771 (accessed on 26 July 2019).
41. Libra. White Paper. 2019. Available online: https://libra.org/en-US/white-paper/ (accessed on 20 July 2019).
42. Libra. Section 05 The Libra Association. White Paper. 2019. Available online: https://libra.org/en-US/white-paper/#the-libra-currency-and-reserve (accessed on 20 July 2019).
43. Evans, B.J. Much Ado About Data Ownership. *Harv. J. Law Technol.* **2011**, *25*, 69–130.
44. Zyskind, G.; Nathan, O.; Pentland, A. Decentralising Privacy: Using Blockchain to Protect. Personal Data. MIT Media Lab. 2015. Available online: https://web.media.mit.edu/~{}guyzys/data/ZNP15.pdf (accessed on 28 May 2019).
45. Ellen-MacArthur. Towards the Circular Economy. Economic and Business Rationale for an Accelerated Transition. 2013. Available online: https://www.ellenmacarthurfoundation.org/assets/downloads/publications/Ellen-MacArthur-Foundation-Towards-the-Circular-Economy-vol.1.pdf (accessed on 28 May 2019).
46. The Circular Economy and Developing Countries. *A Data Analysis of the Impact of a Circular Economy on Resource-Dependent Developing Nations*; COE-Resources Issue Brief 3; Centre of Expertise on Resources: Hague, The Netherlands, 2019.
47. RecycleToCoin. Introduction. 2019. Available online: https://www.the-blockchain.com/2017/11/13/can-blockchain-revolutionise-third-sector-introducing-worlds-first-recycling-intiative/ (accessed on 30 May 2019).
48. GiftPay. Solutions. 2019. Available online: https://www.giftpay.co.uk/business/solutions.aspx (accessed on 30 May 2019).

49. PlasticBank. What We Do. 2019. Available online: https://www.plasticbank.com/what-we-do/ (accessed on 30 May 2019).
50. IBM LinuxONE. IBM LinuxOne. 2019. Available online: https://www.ibm.com/it-infrastructure/linuxone (accessed on 30 May 2019).
51. United Kingdom Parliament Briefing. Food Waste: Key Facts, Policy and Trends in the UK. 2016. Available online: https://researchbriefings.parliament.uk/ResearchBriefing/Summary/CBP-7552 (accessed on 14 July 2019).
52. Goodr. Feed More. Waste Less. 2019. Available online: https://goodr.co/about-us/ (accessed on 14 July 2019).
53. Global Tire Recycling Market. Global Tire Recycling Market. Analysis: Opportunity, Demand, Growth and Forecast. 2016–2024. Available online: https://www.goldsteinresearch.com/report/global-tire-recycling-industry-market-trends-analysis (accessed on 14 July 2019).
54. EV Volumes. Global EV Sales for 2018-Final Results. 2019. Available online: http://www.ev-volumes.com/country/total-world-plug-in-vehicle-volumes/ (accessed on 23 July 2019).
55. PowerLedger. Power Ledger and Silicon Valley Power Trial to Turn Electric Vehicles into Mobile Atms. 2019. Available online: https://www.powerledger.io/article/power-ledger-and-silicon-valley-power-trial-to-turn-electric-vehicles-into-mobile-atms/ (accessed on 17 July 2019).
56. Snell, R. The Rise of Autonomous Vehicles and Why Ethics Matter. 2019. Available online: https://www.digitalistmag.com/improving-lives/2019/04/02/rise-of-autonomous-vehicles-why-ethics-matter-06197534 (accessed on 18 July 2019).
57. Cheney-Lippold, J. *We are Data, Algorithms and the Making of Our Digital Selves*; New York University Press: New York, NY, USA, 2017.