future internet

MDPI

Article

Artificial Intelligence Implementations on the Blockchain. Use Cases and Future Applications

Konstantinos Sgantzos [1,*] and Ian Grigg [2]

[1] Department of Computer Science and Biomedical Informatics, University of Thessaly, 35100 Lamia, Greece
[2] YangSec Ltd, MST9051 Mosta, Malta
* Correspondence: sgacos@gmail.com; Tel.: +30-693-657-6979

Received: 30 June 2019; Accepted: 31 July 2019; Published: 2 August 2019

Abstract: An exemplary paradigm of how an AI can be a disruptive technological paragon via the utilization of blockchain comes straight from the world of deep learning. Data scientists have long struggled to maintain the quality of a dataset for machine learning by an AI entity. Datasets can be very expensive to purchase, as, depending on both the proper selection of the elements and the homogeneity of the data contained within, constructing and maintaining the integrity of a dataset is difficult. Blockchain as a highly secure storage medium presents a technological quantum leap in maintaining data integrity. Furthermore, blockchain's immutability constructs a fruitful environment for creating high quality, permanent and growing datasets for deep learning. The combination of AI and blockchain could impact fields like Internet of things (IoT), identity, financial markets, civil governance, smart cities, small communities, supply chains, personalized medicine and other fields, and thereby deliver benefits to many people.

Keywords: blockchain; cellular automata; AGI; convolutional neural networks; intelligence augmentation; deep learning; IoT; identity; decentralized governance; personalized medicine

1. Introduction

One of the biggest puzzles of humanity is the preservation and expansion of knowledge. Humans strive to provide future generations with accumulated technological and scientific achievements through immutable records. In ancient times, civilizations have used oral tradition, cave paintings and stone carvings, before settling on the leaves of papyrus, better known today as paper. Well-made paper can survive a long time, including centuries and could be copied on demand [1]. Unfortunately, papyrus is not invulnerable to destruction by fire. Alas, the destruction of the Library of Alexandria led to perhaps the greatest loss of recorded knowledge in history. As has been observed of history itself, the destruction by fire of recorded knowledge is repetitive; in 2018 a disastrous fire destroyed a great deal of recorded indigenous knowledge held in the Brazil National Museum [2].

It has been suggested that digital recordings of disks, files and the Internet would be a better solution, but the record so far is patchy: Disk failures, file system failures and lost websites make digital storage a non-trivial exercise. We now have a new technology promising to solve all these problems, called blockchain [3].

Yet humanity has no particular desire to record knowledge for its own sake, rather knowledge is recorded so knowledge can be expanded as an evolutionary survival strategy. The recent advances in machine learning within the field of artificial intelligence have not only created a new model for general computation, they have opened the possibility for the expansion of knowledge beyond the direct agency of the human mind.

In this paper, we present the hypothesis that a blockchain can not only maintain the datasets on chain for input into AIs, it can also host an AI advanced enough to work with its own data and achieve the siren call of independently advancing knowledge—the artificial general intelligence (AGI). We also explore the possible advancements of such an implementation through the years to come. This is a controversial proposal, and more so in a decentralized context in which all users will be able to access and benefit from its computational abilities. It is our belief that this proposal will become a reality within a decade, give or take.

2. On the Construction of an AI on a Blockchain

On the face of it, blockchain does not suggest itself easily as a platform for AI. Nevertheless, presenting an immutable storage medium that incorporates a high level of cryptographic security and at the same time features, which are not available elsewhere in the relevant technologies (e.g., centralized data centers and supercomputers), we suggest it may become the prominent platform for AI in the future [4].

2.1. The Blockchain as a Transaction Platform

Blockchain was first introduced in Bitcoin [3] as a fully shared ledger that would be globally visible to all parties when a transaction was recorded on it without any presence of a trusted central authority. In each transaction, the previous owner signs, using the private signing key corresponding to her public key, a hash of the transaction in which she received the Bitcoins and the public key of the next owner [5]. The blockchain consists of a set of sequential blocks, where each block embeds verified transactions. As transactions are processed and verified by miners, they are accepted into future blocks. Transactions in each block are hashed, paired and hashed again in a Merkle tree until a single hash is obtained, which is the Merkle root [6]. The Merkle root is stored in the header for the block. Each block header also includes the hash of the of previous block header, which results in a chain of blocks. The basic structure of blockchain is given in Figure 1 [7].

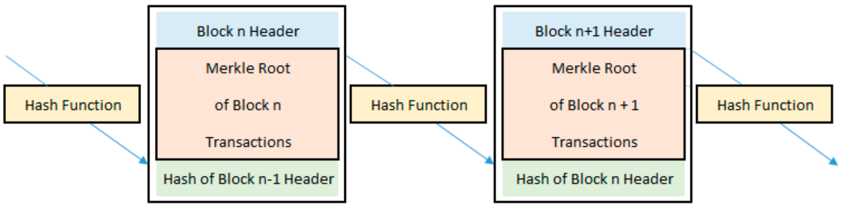


Figure 1. The basic structure of the blockchain [7].

2.2. The Blockchain as a Computing Platform

Blockchain can be considered as a general purpose computing platform at two levels—of the transaction, and of the system. Unlike prior systems in financial cryptography that specified exactly the semantics of the transaction, Bitcoin introduced the transaction as a small program in computer code written in Script [8], a derivative of the FORTH language.

Although opening up the possibility of sophisticated programs such as 'smart contracts,' there are constraints. Transactions in a block are charged for on a byte-by-byte basis, and therefore space is at a premium. Each transaction has to be verified by every node, including in the face of the halting problem, or the impossibility of knowing that an arbitrary program will terminate. These constraints suggest a minimal, efficient language without looping, thus challenging the notion of universal computing as well as imposing penalties on users for any inefficient calculations. Script can be seen as Turing complete through the use of two stacks, forming a two-push-down-automaton. In this arrangement, loops are unrolled in Script with the help of the extra stack [9].

As a system, blockchain can be considered as an unbounded Turing tape exhibiting write once, read many (WORM) characteristics, where transactions within successive blocks can be linked computationally, using explicit validating rules to ensure replication. Using Script and a proper "read and write" head it forms a Wang B machine, being in essence, a special case of a probabilistic total

Turing machine that is controllable in code. Such an implementation is now not only proven to exist, but also available generally in Bitcoin style blockchains [10]. Moreover, the blockchain as a storage medium, or an unbounded Turing tape, offers probably the perfect petri dish for implementation of evolutionary processes such as genetic algorithms.

2.3. The Genetic Algorithm as a Direction for Machine Learning

A genetic algorithm (GA) emulates the way natural evolution has over billions of years used division, random mutations and trillions of replications and recombination [11,12]. A typical GA consists of an algorithm, called a neuron, that feeds back on itself with from 0.02% to 2% chance of mutating the inputs to achieve fitness. Unlike a classical computing algorithm approach, which results in a deterministic, unique solution, the replication and mutability of neurons results in a population of randomly varied instances that, swarming towards higher performance mediated by fitness, forms a neural network [13].

2.4. The Cellular Automaton as the Neuron of Genetic Algorithms

The cellular automaton represents the smallest, tightest and general atomic computational unit to act as a neuron within a genetic algorithm, which makes it singularly suitable for blockchain and its very constrained transaction size.

Cellular automata were first introduced by John von Neumann in 1951 as a discrete model of a simple two-state, one dimensional grid of cells that can be either on or off [14]. In the 1970s, John Conway introduced a two-state, two-dimensional cellular automaton named "Game of Life" [15]. In the 1980s, Stephen Wolfram conducted a systematic study that organized von Neumann's cellular automata on specific set of rules [16]. Mathew Cook showed that one of Wolfram's rules, the CA110, is Turing-complete. Their work has been published in 2002 in the bestselling book "A New Kind of Science" [17]. William Gilpin establishes that a cellular automaton can be used to construct a convolutional neural network if and only if it is Turing complete (Figure 2) [18].

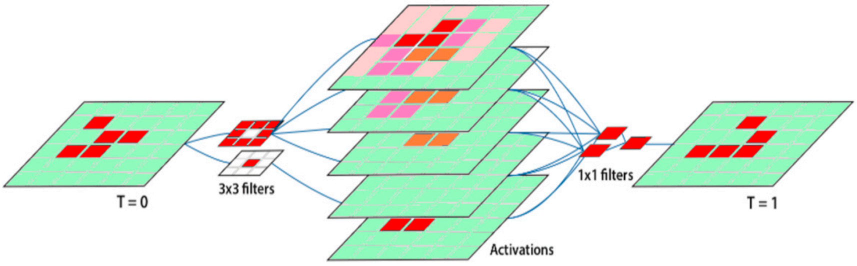


Figure 2. Conway's Game of Life as a convolutional neural network. Two convolutional filters identify the value of the center pixel and count the number of neighbors. These features are then scored and summed to generate a prediction for the system at the next time point.

As an extension to the above notion, if such an automaton is formed, then a swarm of cellular automata of similar origin could possibly form what is described as a Church-Turing thesis [19]. Furthermore, above a certain point of computational evolution, they could form what is described by the Church–Turing–Deutsch principle, which states that a universal computing device can simulate every physical process [20,21].

The fundamental paragon of the topological locality as a result of a dynamical update rule on a cellular automaton, which consequently certifies that the rule domain is minimal, sets an upper bound on the rate at which information propagates across space. This locality makes cellular automata explicitly analogous to a convolutional neural network (CNN), the de facto standard neural network architecture for the analysis of images or high-dimensional data [18,22]. The aforementioned study [18] supports our theoretical approach [4].

2.5. Implementing GAs on Blockchains

We show the task of implementing a GA on a blockchain in two ways: By theory and by practice. In theory, if the blockchain's transactional computing capability is Turing complete, then it can implement any algorithm including a cellular automaton. Even though the notion of Turing completeness is usually associated with loops, this can be finessed with the method of unrolling the loop [9]. As a system, if transactions can be linked by validation rules in e.g., Script, to ensure that new transactions replicate the GA with some small chance of mutation, evolution is simulated [4]. Iteration within a GA is computationally heavy, and to do so on-chain within many transactions would require an economic or gamified incentive. More likely, iteration would be done off chain, with only the best optimized generation posted as a new epoch. In the future, genetic algorithm iteration could be programmed as a new proof-of-work process, re-using the energy currently spent on mining.

In practice, it is shown by Chepurnoy et al. that Turing-completeness of a Script-based blockchain system can be achieved through unwinding a set of recursive calls between multiple transactions and several blocks on a blockchain, instead of using a single block to do it [23]. Their method implemented a rule 110 cellular automaton (CA110), a control script to ensure that the CA110 transformation keeps the same rules during future iterations together with a validation script for the output representing the single bit, and the unbound grid (Figure 3).

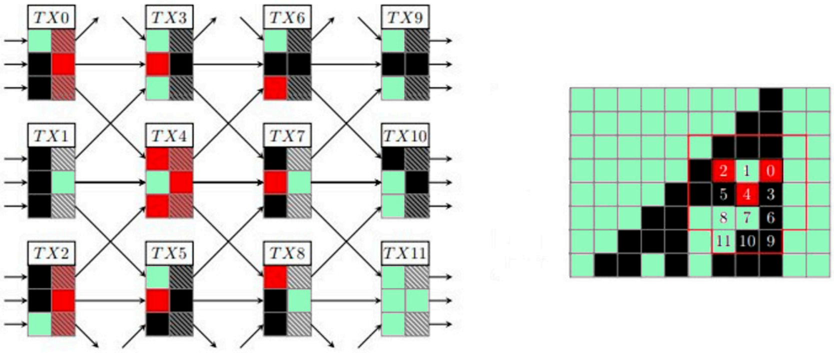


Figure 3. Evolution of a cellular automaton rule 110. Every non-boundary transaction spends three outputs, and generates three new ones with identical bit values. Hatching indicates "mid" flag being un-set. Numbers in the cells on the right pane correspond to the transaction numbers on the left [23].

Harris and Waggoner propose to reduce the current centralization of AI with a framework to post and train models on Ethereum blockchain [24]. Their experiment used a single layer perceptron model on reviews of movies. Ethereum's high gas costs limited their experiment to small inputs such as text.

3. Use Cases and Future Applications

A conspicuous question is, what would be our motivation for implementing genetic algorithms on a medium like blockchain, while more centralized approaches produce equally meaningful results without the cost of maintaining such a network? There are numerous reasons to store a neural network on the blockchain, many of which were explored in our previous work [4], but here we will narrow down the significant ones leading to our conclusion.

By investigating six use cases and future applications, we demonstrate how AI entities can utilize the capabilities of blockchain for important purposes including, but not limited to, deep learning, Internet of things (IoT) and Monte Carlo analysis. We also explore the possibility of storing externally trained AI agents on such a medium and utilize them via pay per use. Finally, we describe an already trained neural network employed to recover the relevant physical variables, both in quantum and classical systems.

3.1. The Integrity and Validity of Information

Blockchain as a data and framework store presents a number of advantages over the Internet or over internal stores. By way of two exemplary challenges to the AI world, we present how blockchain can address these in novel ways.

One of the biggest challenges in data science today is the collection of a proper dataset, which can be utilized for training a neural network. The pluralism of data over the Internet is enormous, but the quality is minimal due to the habit of people to post inaccurate things, mainly, because there is no control. A characteristic paradigm is the "fake news" explosion in recent years, which tends to propagate faster than well documented and verified news [25]. Internet giants like Facebook and Google have tried to tackle the problem via several computational methods, but even though there seems to be a sufficient theoretical basis for separating "signal" from "noise" [26], the problem still thrives as of today.

A second challenge is adversarial interference with the processing. Tesla's autopilot was shown to be vulnerable to remote root privilege attacks that could control the steering system and disturb the "autowipers" function [27]. By introducing false information in the physical world such as minor changes in the road, it was possible to mislead the car into the opposite lane. The consequential risks of such vulnerability include, but are not limited to, human injuries and death. Many other examples abound. Blockchains can address these issues in a comprehensive way through integrity, security, triple entry and provenance.

Data as fact integrity: The cryptographic inventions of digital signatures and hashes have led to a general technique for making data reliable within the context and limitations of the technical means, a characteristic called integrity. In practice this means that we can state with (cryptographic) certainty that a piece of data existed no later than a particular time, and that it remains untampered with. These cryptographic techniques need some software to deliver results. Timestamping [28] involves taking the hash of a document and placing it in a timed sequence of hashes that is kept alive essentially without limit on time. Each new document's hash is placed in a block, which is then hashed, along with a hash of the last block and the current time. As the cryptographic hash is essentially unforgeable without the actual block, this ensures both the inclusion of the new document(s) and the proof that the last block, and by induction all previous blocks and included documents, are securely timestamped. The reliability of the stamp of time is the reliability of the recording of the time in each block, and the space between the blocks.

Facts by people, securely: Digital signing takes the evidence of a hash one step further by indicating who it was that made that stamp. Digital signatures are made by a private key, and verified by a public key, which latter also takes the form of an identifier for the private key called a pseudonym. This security model is essential for a blockchain as it ensures that only the proper pseudonymous agent, as holder of the private key, can make new transactions. Money is perhaps the most harshly attacked activity of humanity after wars, and therefore can only survive if protected by strong security. The cryptographic security model of pseudonymous digital signing used in blockchains is battle-hardened and is available for free for all other applications beyond transfers of value. This is no trivial benefit as the Internet has quite poor security models, and big Internet applications such as online banking and autonomous vehicles generally have trouble deploying robust security to users. Injection of information from unknown sources is rampant, and simply adding data stamping and signing as used in blockchain makes the attacker's job harder.

Facts as shared knowledge: A technique known as triple entry accounting [29] adds a further advantage captured by the aphorism "I know that what you see is what I see." Triple entry takes the above integrity techniques and makes records such as offers and acceptances, payments, receipts and invoices both shared and reliably the same to all relevant parties, which allows software to work with reliable raw data as facts produced by other parties; triple entry accounting does for trading groups what double entry accounting did for the firm. Independence from weak data, whether summarized, prepared, or sanitized, results in the elimination of diverging data sets and unreliable outcomes.

For example, clearing and settlement in financial trading is highly simplified if the data is already guaranteed to be the same for all.

Blockchains go further and incorporate a public database that ensures everyone has access to the same data, and some parties are financially motivated to keep that database alive. This ability to always find the data comes at the cost of privacy—whatever is posted to the blockchain as a document is readable by all. There is some promise of more exotic cryptography and software techniques to allow posting and recovery of private data into a public store, but these techniques remain experimental, and the bar of confidentiality or privacy is typically a high one.

Knowledge as truth: What remains is the provenance of the data at the time of posting. The blockchain supports two easy controls, and one hard control. Firstly, if the data is a financial transaction on a blockchain, in an asset mediated by that very blockchain, then the transaction record can support its own provenance, gained in part that someone went to the effort of moving money, and in other part that it cost a small fee. Secondly, the use of the pseudonymous digital signatures provides a minimal form of identity system: A document's utility and provenance can be analyzed within the context of all the documents posted by the same agent. If Alice generally posts good documents, then the next is likely to be good; if Bob posts fake news then people should expect more of the same. Pay on demand is discussed in the next section.

Consider two trivial statements, "this statement is true" and the equally light "this statement is false". Both can as easily be posted, but only one is reliable. Software can guarantee both statements were made at a time, but cannot guarantee the content is reliable or even meaningful.

Then, to encourage statements that may be relied upon by others requires more: Posters need to be incentivized to post useful and reliable statements, and to not post useless and unreliable ones. Due to the pseudonymous nature of blockchain, posting stake or gamification is suggested as a control however these methods limit participation through the cost of capital and time, and leave aside the question of how to punish [24]. A more serious feedback control on bad participation would be a due process to also incentivize agents to not post unreliable data. The process itself would also need to pass the same test of reliability as the statements delivered.

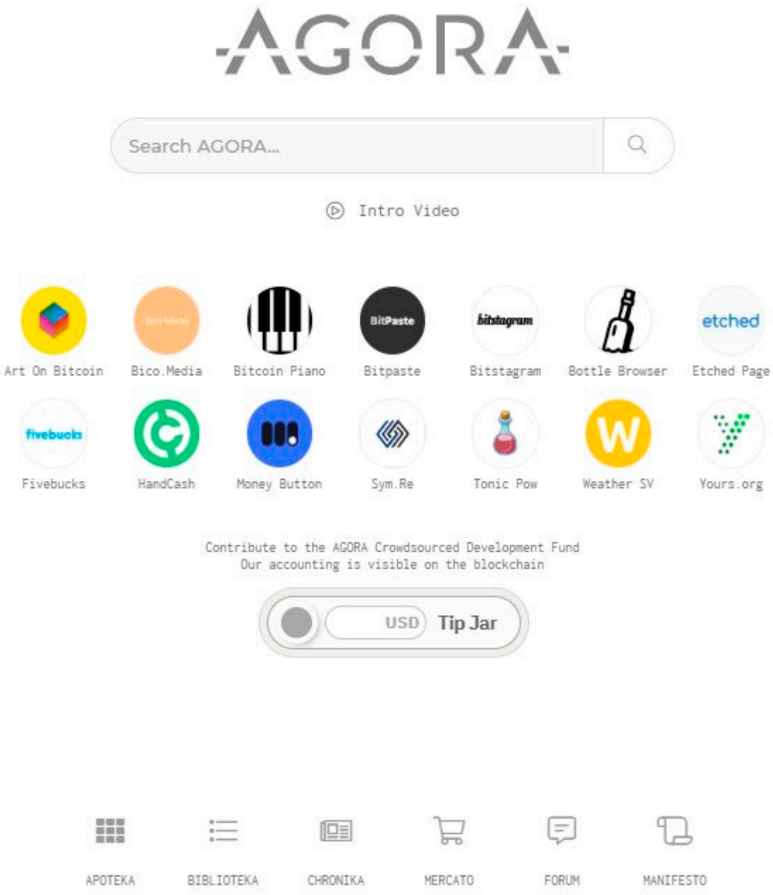
Such a due process is typically called Public Key Infrastructure (PKI). The more common Internet secure browsing form organizes a certification authority to make signed statements, called certificates. Its due process is described in documents such as a certificate practice statement, which are reviewed and approved by browsers and other relying parties. Reliance based on commercial authorities and their statements is typically only strong enough for relatively weak statements because it lacks an incentive model to properly handle the liability for bad data [30]. CAcert has extended the concept to cover a wide range of stronger statements through a cooperative form that includes arbitration to allocate liability in the case of bad data [31].

Blockchains are therefore not only ideal storage for the data of deep learning, they include much data worth analyzing, and they are ideal storage for the trained frameworks themselves. In time we expect the discrimination between good and bad data to become easier based on pseudonyms and incentive models.

3.2. Programs Stored on Chain and Composed Within Transactions—Pay Per Use

As above, a blockchain forms a novel method to store information on a public space, via a payment procedure [32]. As well as static information such as literature or news, we could also store the code for programs in much the same was as Github [33], and indeed, the underlying git system is very like a blockchain in many respects. These programs can be read freely as they are part of the immutable data of the chain. Each transaction that posts data on the blockchain costs money and thus it is uneconomical and non-incentivized to continue posting programs unless there is at least a minimum revenue possibility.

A collection of on-chain applications can be made browsable via a portal such as Agora [34], forming a new channel for distribution of software (Figure 4). This lays the foundation for a long held ideal of programmers, being an independent marketplace where the developers can be paid for their work without any intermediates [35]. The space is fairly new at the moment of writing but it does not lack for novelty and innovation, including applications in art, music, money and weather. Other applications that could fit include IoT sensors over power grids, security systems or transport networks.



Contribute to the AGORA Crowdsourced Development Fund
Our accounting is visible on the blockchain

Figure 4. Agora, the homepage for Metanet [33].

By employing the OP_RETURN op_code instruction of Bitcoin Script [7], a new world of application utilization emerges. Transactions can refer to and run other programs on a "pay per use" basis, allowing for programmers to 'compose' larger programs out of many smaller ones. An example of pay per use is found in Moneybutton [36]. With such tools it is possible to construct a 'Metanet' being an immutable version of Internet as we now experience it.

3.3. Trained AI Frameworks that can be Parsed Via Pay on Demand

As well as storing code and programs on the blockchains, we could also post trained neural networks. Then, users could post new transactions that cited and used the trained CNN frameworks to check the submitted information [24]. For example, consider a deep learning algorithm like Sci-kit in Python [37], that classifies documents, in a very different approach to that we might expect: Words can be represented as embedding vectors with the idea that two words that are semantically similar to each other have similar vectors (Figure 5) [38].

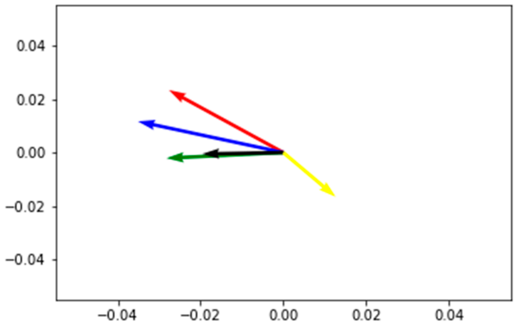


Figure 5. Representation of a 2D embedding space with five embedding vectors each representing a different word [38]: Red—queen, blue—king, green—man, black—woman and yellow—oil.

Under such a model, concepts that are similar to each other are close together (e.g., man and woman) in this embedding space and concepts not related are further apart (e.g., oil). Therefore, assuming that the embedding vectors for dogs and puppies are close together, the similarity of two documents talking about dogs and puppies will be recognized by a machine learning algorithm or a deep neural network trained on that topic [38]. Such tools, well composed, could assist programmers in their use of the aforementioned code repository.

3.4. Artificial Intelligence Agents Trained Via Submitted Blockchain Data and Operated on Chain.

An artificial intelligence agent (AIA) goes one step further than a trained framework by utilizing the new data in the user's request to advance the neural network forward by a new epoch; in other words, it learns as it works. Fitness is determined when minimal or no other changes are required with any future submitted data. Let us consider an example extended from above. In the recent years, a plethora of authored code in various programming languages has been stored in repositories such as GitHub [33]. Complex algorithmic programming is a time consuming and costly task; a programmer requires a high intellect and years of education, and complex tasks often require many months of collaborating work between several parties.

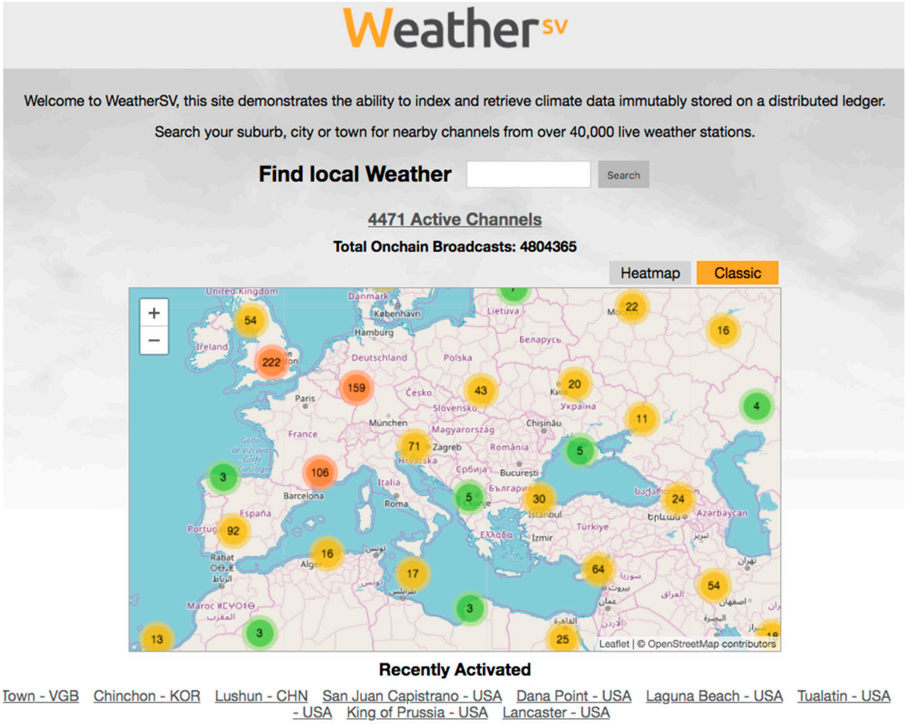
Blockchains can assist in two ways. Firstly, as above, a blockchain can store the code. Secondly, an AIA, encoded on the blockchain, can assist the programmer in many ways: Conversion of code from one language to another, searching for algorithms that match patterns, conformance of requirements or documentation to code and eventually in authoring new algorithms. Using deep learning techniques and big data mining from existing code repositories, this AIA would present a reliable, secure and disruptive technology.

AIAs are described in computer science as abstract entities that are able to monitor and evaluate certain parameters through various input sources (i.e., IoT sensors, I/O raw data, databases, ontologies, etc.) towards achieving a rational goal [39,40]. Their basic role is usually described as that of an actuator, with the simplest implementation of an AIA to be derived from a reflex machine, such as a thermostat, but they can vary from very simple to extremely complex. There are four architectures of AIA to be considered [39]: (a) Logic-based agents (decision of action is derived via logical inference), (b) reactive agents (decision is based in some form of direct mapping from situation to action), (c) belief–desire–intention agents (decision depends upon the manipulation of data structures) and (d) layered architectures (decision is realized via various software layers, each depended on its environment at different levels of abstraction). There are also five classes of AIA to be considered [40]: (a) Simple reflex agents, (b) model-based reflex agents, (c) goal-based agents, (d) utility-based agents and (e) learning agents.

All the above AIAs learn from the submission of fresh data, e.g., code from programmers from anywhere in the world, who will be incentivized to post their work on the blockchain, either for gaining revenue, or under a specific license (i.e., Opensource, MIT, etc.). Moreover, a new opportunity emerges through the concept of AIA paying another AIA for services or paying a sensor for data. An example is WeatherSV (Figure 6), which offers weather prediction to users in their selected territory by utilizing the data collected by a set of global IoT sensors. The service can be activated for a cost of $5 AUD and delivers hourly reports for about 123 days, based on current fees of Bitcoin SV [41].

The notion of live data feed and immutable storage can form a basis for implementing several other applications such as decentralized logistics, as shown in the work by Christodoulou et al. [42], also as a supply chain for manufacturing, the agricultural sector or even a modern city. A Smart City [43] that uses different types of electronic IoT sensors to collect data and then uses the data to manage assets and resources efficiently can use the blockchain as an immutable record ledger both for integrity, for deep learning and also for historical purposes. For example, Zweispace in Japan now stores the national earthquake sensor data on the blockchain [44].

By utilizing the proper AIA or CNN with the data provided on chain, we can have productive outcomes towards the implementation of a far more economic and robust Smart City economy. A similar opportunity applies wherever there are vast amounts of both data and users learning from that data: Traffic control and other problems in transportation and supply chain, education and health. Additional applications of AIAs on chain can facilitate analysis of financial markets, DNA for rare genetic disease detection, high definition imaging of stellar bodies for possible collision detection, auditing and protection of network against attacks and more.



Welcome to WeatherSV, this site demonstrates the ability to index and retrieve climate data immutably stored on a distributed ledger.

Search your suburb, city or town for nearby channels from over 40,000 live weather stations.

Find local Weather

4471 Active Channels

Total Onchain Broadcasts: 4804365

Recently Activated

Town - VGB Chinchon - KOR Lushun - CHN San Juan Capistrano - USA Dana Point - USA Laguna Beach - USA Tualatin - USA - USA King of Prussia - USA Lancaster - USA

Figure 6. WeatherSV demonstrates the ability to index and retrieve climate data immutably stored on a distributed ledger [41].

A collaboration of AIAs as a swarm is also applicable via payments in the form "Machine paying Machine" in order to achieve solutions to more complex tasks.

3.5. Proof of Work Via dSHA256 as a Source of Randomness and Monte Carlo Method Via ASICs

The concept of proof of work (PoW) as introduced in Bitcoin is a reward mechanism to the solvers of a random puzzle. A hash puzzle is a set of mathematical problems, which are solved by creating a hash that conforms to a specific requirement, being firstly a hash over a new proposed block. Secondly, in the block's header, an extra value called a 'nonce' or 'number-once-used' is cycled repetitively to produce a trial hash value with a large number of leading zeros.

Solving the puzzle is competitive and thus computationally difficult. Unless the cryptographic hash function used for calculating the block hashes is broken, the only fruitful strategy is to try different nonces until a solution is found [45]. Bitcoin uses the SHA-256 hash function [46], which is a leading standard for hashes.

The fastest participant to find and propagate a winning solution is rewarded. Bitcoin also includes two feedback loops that vary over time. Firstly, the difficulty, or the minimum threshold of number of zeros, is varied every two weeks to keep the expected time to solve around 10 min. Secondly, the reward paid for solving the puzzle halves every four years.

At the time of writing, the reward stands at 12.5 Bitcoins [47] and the Bitcoin Hashrate is estimated on average at 53.85 Eh/s (SHA-256) [48]. That gives us 53.85×10^{18} random numbers per second, in effect, making the miners pseudo-random number generators (PRNGs). The result of this is the generation of an impressively large number of random numbers, for every block. A well-known computational method that is capable of providing solutions in Non-deterministic Polynomial-time – Hard (NP-hard) and Non-deterministic Polynomial-time – Complete (NP-complete) problems via utilizing the random numbers that a SHA256 miner can produce is the Monte Carlo method. Monte Carlo is a category of computational algorithms, which is based on continuous and repetitive random sampling in order to solve complex problems. The underlying concept is to use random solutions to solve problems that can be deterministic in nature. The method is often used in physical and mathematical cases and is very useful when it is difficult or impossible to use other approaches. The Monte Carlo method is used in three categories of problems: Optimization, numerical integration and guessing results from a probability distribution [49].

As a side-effect of PoW, blockchains can extend their activity to solving massive Monte Carlo problems. Blockchains are in effect the biggest PRNG in the world right now and probably the fastest PRNG swarm that could solve literally any computationally hard problem via utilizing the Monte Carlo method.

3.6. Solving Physical Problems via CNNs and Simulation of Quantum Computing

There are numerous studies demonstrating the abilities of a neural network. For instance, a deep neural network is able to learn through training and produce fairly accurate predictive results correlated to the dataset they trained on, while recurrent neural networks are being used towards the deterministic analysis of speech recognition, down to video prediction [50]. Neural networks can be trained offline and then can be stored on the blockchain and parsed via pay per use. On another note, because of the fact that users will be using the medium to submit data the entity can evolve to a higher scale and store a more advanced version of itself for later use.

One of the most difficult tasks in neural network mechanics is to understand how they function and how they are able to extract results. They are often used as "black boxes" and consequently our perception of the mechanics of them are limited. Several studies have tried to analyze the inner-works of CNNs but we believe the most prominent way to answer this question is the simulation of physical concepts and the solution analysis.

What we propose is not new; several studies have tried to employ a CNN towards simulation of a "human-like problem analysis" and the results were quite impressive. We now know that a Region-based Convolutional Neural Network (R-CNN) can be trained recursively to analyze problems via data pretty much like a human brain can. Moreover, the outcome is extremely accurate to the expected results. The materialization graph of SciNet, a CNN that represents the aforementioned process is displayed below (Figure 7) [51].

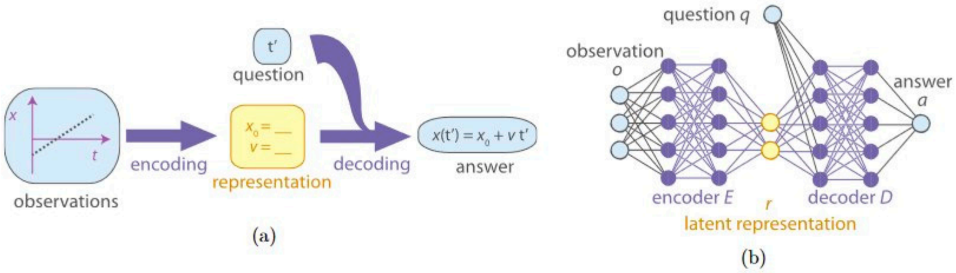
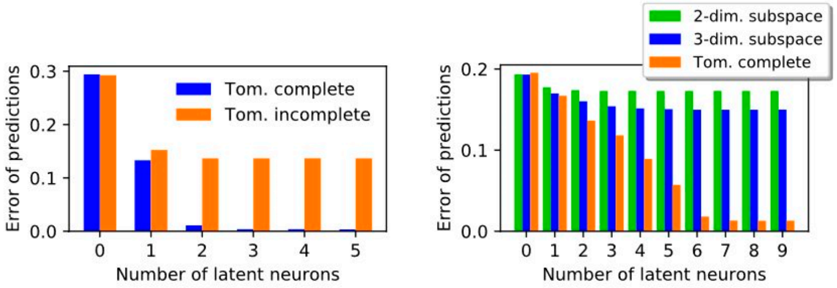


Figure 7. Learning physical representations. (**a**) Human problem analysis. Experimental observations are compressed into a simple representation (encoding). If any question is asked about the physical setting, the human should be able to produce a correct answer using only the representation and not the original data. The process of producing the answer (by applying a physical model to the representation) is called decoding; (**b**) Neural network structure for SciNet. Observations are encoded as real parameters fed to an encoder (a feed-forward neural network), which compresses the data into a representation (latent representation). The question is also encoded in a number of real parameters, which, together with the representation, are fed to the decoder network to produce an answer [51].

In the aforementioned work and by utilizing the same concept it is shown that, based only on (simulated) experimental data and without being given any assumptions about quantum theory, SciNet recovers a faithful representation of the state of small quantum systems and can make accurate predictions (Figure 8) [51].



(a) One qubit.

(b) Two qubits.

Figure 8. Quantum tomography. SciNet is given tomographic data for one or two qubits and an operational description of a measurement as a question input and has to predict the probability of outcomes for this measurement. It was trained with both tomographically complete and incomplete sets of measurements, and found that, given tomographically complete data, SciNet could be used to find the minimal number of parameters needed to describe a quantum state (two parameters for one qubit and six parameters for two qubits) [51].

The implementation of neural networks based on similar technologies when implemented on the blockchain can dramatically amplify their computation abilities via the utilization of a PRNG engine provided by the PoW procedure as per solving complex problems. Furthermore, such a computational entity can provide solutions to many problems that are now impossible to approach (e.g., deterministic computing and chaotic system analysis).

4. Discussion

The implications of such a hypothesis are enormous. Ray Kurzweil predicted that by the end of 2029 the world would possibly have one AI that matches human intelligence [52]. What we show in this paper endorses this prediction, and suggests the possibility this could happen much earlier. Preliminary forms of such entities are already in existence [53], so it is not a matter of if, rather when this happens. The evolutionary process, from a certain point forth, follows an exponential curve.

Hence, when the critical point of reaching human intelligence is met, then it might be a matter of months or even days before it expands to much higher levels. The materialization of such an entity on a blockchain provides many pros and cons that we have presented in this paper. The cost of PoW, the cryptographic security procedure and the mandatory usage of tokens for fees, ensures that such an entity will not be able to interact without a fee. This is both good and bad.

Several times in the past, the scientific world has witnessed an inherent limitation of every formal axiomatic system. Each system could contain problems that were impossible to be solved from the theory itself. The incompleteness theorem of Kurt Gödel [54] describes this barrier and predicts that a new theory needs to be invented, in effect to expand the old theory, so that science will once again be able to produce solutions to problems. Gödel expansions are the path to innovation, the "secret" ingredient for new science. They happened with Riemannian geometry and relativity theory, with the parabolic and Euclidean geometry, with the information technology and physics, biology, mathematics and now with an artificial intelligence of a generic form (AGI).

If such a computational entity were to be materialized and controlled by only one company or one country, it would likely be the biggest tragedy for all the rest of us that do not possess a similar entity. Blockchain forms the most adequate medium for such a computational scheme, since it is decentralized, secure, non-controllable and it will be accessible by everyone [24]. Numerous scientific problems will find their solutions by only utilizing a portion of the computational power that this entity will have. Personalized medicine will also benefit, since by using newer encryption mechanisms in blockchain it will be technically possible to store medical information such as a person's DNA on it and get medical results privately. As a concept, AGI on the blockchain even suggests a step towards direct democracy as it was presented by the ancient Greeks; a cornerstone for building up the next evolutionary step for humanity.

5. Conclusions

Bitcoin's creation in 2009 was a revolutionary idea in the financial world. It is considered as the digital cash of the new age. It is secure, non-centralized and can provide the world with "honest", non-inflatable money. Game theory is utilized in maintaining consensus, without the need of any central corruptible authority, while competition with national monies can present a check on inflation, sorely lacking in the international financial system since the demise of gold as a real force.

Implementing a swarm of AIAs on the blockchain can form what is described as the Church–Turing–Deutsch principle machine, which could in turn, open a brave new world of applications for a better humanity from computer assisted governance to extinction level events predictions. With emergent technologies such as the human–machine interface and intelligence augmentation devices, able to decode human brainwave patterns, such an entity could directly interact with the human brain, use it as a dataset to acquire information on how it functions and ultimately, provide extensive knowledge in many fields of science, which was previously impossible to acquire. Using deep machine learning techniques, the evolutionary level of the algorithmic entity could reach unprecedented levels exponentially, by utilizing the big data acquired by smart contracts, everyday transactions, weather conditions, IoT or stored literature on a blockchain.

The interaction with such an entity could be achieved via interpreted commands using the transaction system. For this, blockchain tokens (e.g., coins) will be used as a means of transaction and fees are important. At the first stages of evolution the system would provide low-level programming support, but could be educated through machine learning to accept natural language interaction.

Finally, a point of discussion could be about "what happens next"? At this point, a reference to the great text of Isaac Asimov, "The Last Question" [55] is needed:

Can this chaos not be reversed into the Universe once more? Can that not be done?

Author Contributions: K.S. conceived the ideas and authored the paper except for Section 3.1. I.G. authored Section 3.1, helped in reforming some ideas and both contributed in minor corrections.

Funding: This research received no external funding.

Acknowledgments: The authors would like to thank Bernhard Frank Müller Hug, Georgios N. Papageorgiou and Emmanouil Benis for their helpful discussions and proofreading on early drafts of this work.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. *The Archimedes Palimpsest*; University of Pennsylvania Libraries: Philadelphia, PA, USA; Available online: http://archimedespalimpsest.net/ (accessed on 1 June 2016).
2. Cultural Tragedy: Massive Inferno Engulfs 200-Year-Old Museum in Brazil. Available online: https://www.cbsnews.com/news/fire-national-museum-brazil-rio-de-janeiro-today-2018-09-02/ (accessed on 6 March 2019).
3. Wright, C. *(Pseudonym: Nakamoto, S). Bitcoin: A Peer-to-Peer Electronic Cash System*; Whitepaper: Sydney, Australia, October 2008.
4. Sgantzos, K. Implementing a Church-Turing-Deutsch Principle Machine on a Blockchain. In Proceedings of the 12th Hellenic Society for Computational Biology and Bioinformatics Conference, Athens, Greece, 11–13 October 2017; Available online: https://sites.google.com/site/hscbb17/program/HSCBB17-Booklet.pdf (accessed on 26 May 2019).
5. Meiklejohn, S.; Pomarole, M.; Jordan, G.; Levchenko, K.; McCoy, D.; Voelker, G.M.; Savage, S. A fistful of bitcoins: Characterizing payments among men with no names. In Proceedings of the 2013 Conference on Internet Measurement Conference, Barcelona, Spain, 23–25 October 2013.
6. Merkle, R.C. A Digital Signature based on a Conventional Encryption Function. In *Advances in Cryptology—CRYPTO '87, Santa Barbara, California, August 21-25, 1988, Lecture Notes in Computer Science*; Springer: Berlin, Germany, 1988; Volume 293, pp. 369–378.
7. Khalilov, M.C.K.; Levi, A. A Survey on Anonymity and Privacy in Bitcoin-like Digital Cash Systems. *IEEE Commun. Surv. Tutor.* **2017**, *20*, 2543–2585. [CrossRef]
8. Opcode List in BitcoinSV (v. 0.2). ©2009 S. Nakamoto, ©2009–2016 The Bitcoin Core developers, ©2018-19 Bitcoin Association. Distributed under the Open BSV Software License. Available online: https://github.com/bitcoin-sv/bitcoin-sv/blob/master/src/script/script.h (accessed on 12 June 2019).
9. Aisopos, K.; Kakarountas, A.P.; Michail, H.; Goutis, C.E. High throughput implementation of the new Secure Hash Algorithm through partial unrolling. In Proceedings of the IEEE 2005 International Workshop on Signal Processing Systems (SiPS'05), Athens, Greece, 2–4 November 2005; pp. 99–103.
10. Wang, H. A Variant to Turing's Theory of Computing Machines. *JACM* **1957**, *4*, 63–92. [CrossRef]
11. Alberts, B.; Johnson, A.; Lewis, J.; Raff, M.; Roberts, K.; Walter, P. *Molecular Biology of the Cell*, 5th ed.; Garland Science: New York, NY, USA, 2007; pp. 264–328.
12. What is DNA Replication? Available online: https://www.yourgenome.org/facts/what-is-dna-replication (accessed on 24 February 2017).
13. Genetic Algorithms, Mathworks. 2017. Available online: https://www.mathworks.com/matlabcentral/fileexchange/11565-genetic-algorithms-application (accessed on 25 May 2019).
14. von Neumann, J. The General and Logical Theory of Automata. In *Cerebral Mechanisms in Behavior—The Hixon Symposium*; Jeffress, L.A., Ed.; John Wiley & Sons: New York, NY, USA, 1951; pp. 1–31.
15. Gardner, M. Mathematical Games: The fantastic combinations of John Conway's new solitaire game of life. *Sci. Am.* **1970**, *223*, 120–123. [CrossRef]
16. Wolfram, S. Statistical Mechanics of Cellular Automata. *Rev. Mod. Phys.* **1983**, *55*, 601–644. [CrossRef]
17. Wolfram, S. *A New Kind of Science*; Wolfram Media Inc.: Champaign, IL, USA, 2002.
18. William, G. Cellular automata as convolutional neural networks. Department of Applied Physics, Stanford University. *arXiv* **2018**, arXiv:1809.02942.
19. Michael, O.R. Turing, Church, Gödel, Computability, Complexity and Randomization: A Personal View. Available online: http://www.bu.edu/cphs/files/2013/08/Rabin.pdf (accessed on 26 May 2019).
20. Nielsen, M. Interesting Problems: The Church–Turing–Deutsch Principle. Available online: http://michaelnielsen.org/blog/interesting-problems-the-church-turing-deutsch-principle/ (accessed on 31 May 2019).
21. Deutsch, D. Quantum theory, the Church—Turing principle and the universal quantum computer. In Proceedings of the Royal Society, London, UK, July 1984.

22. LeCun, Y.; Bengio, Y.; Hinton, G. Quantum Deep Learning Triuniverse. *Nature* **2015**, *521*, 436. Available online: https://www.scirp.org/reference/ReferencesPapers.aspx?ReferenceID=1899138 (accessed on 3 June 2019). [CrossRef] [PubMed]
23. Chepurnoy, A.; Kharin, V.; Meshkov, D. Self-Reproducing Coins as Universal Turing Machine. 2018. Available online: https://arxiv.org/pdf/1806.10116.pdf (accessed on 6 June 2019).
24. Justin, D.; Harris, B.W. Decentralized & Collaborative AI on Blockchain. In Proceedings of the 2019 IEEE International Conference on Blockchain (Blockchain), Atlanta, GA, USA, 14–17 July 2019.
25. Donath, J. Why Fake News Stories Thrive Online. 2016. Available online: https://edition.cnn.com/2016/11/20/opinions/fake-news-stories-thrive-donath/ (accessed on 10 June 2019).
26. Gerck, E. The Einstein Phenomenon and Fake News. 2019. Available online: https://www.researchgate.net/publication/331561385_The_Einstein_Phenomenon_and_fake_news (accessed on 10 June 2019).
27. Tencent Keen Security Lab. Experimental Security Research of Tesla Autopilot. 2019. Available online: https://keenlab.tencent.com/en/whitepapers/Experimental_Security_Research_of_Tesla_Autopilot.pdf (accessed on 09 June 2019).
28. Haber, S.; Stornetta, W.S. How to time-stamp a digital document. *J. Cryptol.* **1991**, *3*. [CrossRef]
29. Grigg, I. Triple Entry Accounting. 2004. Available online: https://iang.org/papers/triple_entry.html (accessed on 26 June 2019).
30. Grigg, I. PKI Considered Harmful. 2008. Available online: https://iang.org/ssl/pki_considered_harmful.html (accessed on 26 June 2019).
31. Grigg, I. An Open Audit of an Open Certification Authority. Large Installation Systems Administration (LISA). 2008. Available online: https://iang.org/papers/open_audit_lisa.html (accessed on 26 June 2019).
32. Media, B. Add any File to the BSV Blockchain. 2019. Available online: https://add.bico.media/ (accessed on 10 June 2019).
33. Github.inc. The World's Leading Software Development Platform. 2019. Available online: https://github.com/ (accessed on 10 June 2019).
34. Agora Startup Page for Bitcoin SV Applications & Services. Available online: https://www.agora.icu/ (accessed on 12 June 2019).
35. Grigg, I.; Petro, C.C. Using Electronic Markets to Achieve Efficient Task Distribution. In Proceedings of the Financial Cryptography First International Conference FC'97, Anguilla, British West Indies, 24–28 February 1997; Springer-Verlag: Germany 1997 LNCS1318. Available online: https://iang.org/papers/task_market.html (accessed on 10 June 2019).
36. Money Button Is an API and a UI/UX Layer for the Bitcoin SV Blockchain. Available online: https://docs.moneybutton.com/ (accessed on 7 June 2019).
37. Brownlee, J. A Gentle Introduction to Scikit-Learn: A Python Machine Learning Library. 2014. Available online: https://machinelearningmastery.com/a-gentle-introduction-to-scikit-learn-a-python-machine-learning-library/ (accessed on 26 June 2019).
38. Hamel, L. Deep Learning Finds Fake News with 97% Accuracy. 2019. Available online: https://opendatascience.com/deep-learning-finds-fake-news-with-97-accuracy/ (accessed on 10 June 2019).
39. Weiss, G. *Multiagent Systems*, 2nd ed.; The MIT Press: Cambridge, MA, USA, 2013.
40. Stuart, J.R.; Norvig, P. *Artificial Intelligence: A Modern Approach*, 2nd ed.; Prentice Hall: Upper Saddle River, NJ, USA, 2003; Chapter 2; ISBN 0-13-790395-2.
41. WeatherSV, Index and Retrieve Climate Data Immutably Stored on a Distributed Ledger. 2019. Available online: https://weathersv.app/find (accessed on 11 June 2019).
42. Christodoulou, P.; Christodoulou, K.; Andreou, A. A decentralized application for logistics: Using blockchain in real-world applications. *Cyprus Rev.* **2018**, *30*, 171–183.
43. McLaren, D.; Agyeman, J. *Sharing Cities: A Case for Truly Smart and Sustainable Cities*; MIT Press: Cambridge, MA, USA, 2015.
44. Zweispace Starts to Record Tokyo Earthquake Detector Data into the Bitcoin SV (BSV) Blockchain. Available online: https://coingeek.com/zweispace-starts-to-record-tokyo-earthquake-detector-data-into-the-bitcoin-sv-bsv-blockchain/ (accessed on 14 June 2019).
45. Eastlake, D., III; Hansen, T. US Secure Hash Algorithms (SHA and SHA-Based HMAC and HKDF), RFC 6234 (Informational), Internet Engineering Task Force. 2011. Available online: http://www.ietf.org/rfc/rfc6234.txt (accessed on 12 June 2019).

46. Tschorsch, F.; Scheuermann, B. Bitcoin and Beyond: A Technical Survey on Decentralized Digital Currencies. *IEEE Commun. Surv. Tutor.* **2016**, *18*, 2084–2123. [CrossRef]
47. George, P. Bitness: Bitcoin Usage in an Enterprise Environment, Opportunities and Challenges. Master's Thesis, University of Greenwich, London, UK, 2013.
48. Hashrate Comparing data. Available online: https://blockchair.com/compare (accessed on 14 June 2019).
49. Kroese, D.P.; Brereton, T.; Taimre, T.; Botev, Z.I. Why the Monte Carlo method is so important today. *WIREs Comput. Stat.* **2014**, *6*, 386–392. [CrossRef]
50. Mathieu, M.; Couprie, C.; LeCun, Y. Deep multi-scale video prediction beyond mean square error. *arXiv* **2016**, preprint. arXiv:1511.05440.
51. Iten, R.; Metger, T.; Wilming, H.; del Rio, L.; Renner, R. *Discovering Physical Concepts with Neural Networks*; Institute for Theoretical Physics: ETH Zurich, Zurich, Switzerland, 2018.
52. Kurzweil, R. Don't Fear Artificial Intelligence. 2014. Available online: http://time.com/3641921/dont-fear-artificial-intelligence/ (accessed on 14 June 2019).
53. Watson, AI for Business, 2016–2019, ©IBM. Available online: https://www.ibm.com/watson/ (accessed on 14 June 2019).
54. Gödel, K. Über formal unentscheidbare Sätze der Principia Mathematica und verwandter Systeme I. *Monatshefte Math. Phys.* **1931**, *38*, 173–198. [CrossRef]
55. Asimov Isaac. The Last Question", Science Fiction Quarterly. 1956. Available online: https://www.multivax.com/last_question.html (accessed on 14 June 2019).

© 2019 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (http://creativecommons.org/licenses/by/4.0/).