The Convergence of IoT, AI and Blockchain Technologies

Mr. T.A. Balasubramanian
Managing Director, Maxigen Communications
tabbyindia@gmail.com

The traditional ways of data processing and storage based on data centers have been changing rapidly in the last decade. Isolated data centers maintained by elaborate IT departments in corporate offices have given way to a simple subscription model where companies access cloud computing services that are managed by cloud vendors such as Amazon, Microsoft, Google and IBM to serve hundreds of businesses. *Cloud computing* has evolved as a remote centralized solution to manage the surge of information. The cloud gives IT users of all kinds (corporations, small businesses and individuals) cost-effective access to processing, storage and networking facilities.

However, with the percolation of digital technology into every stream of human activity and the rapid growth of telecom infrastructure and smart mobile personal devices, IT services are grappling with new demands in accessibility and security. With the explosive acceleration of consumer-driven interactions, devices and data flows, cloud computing faces a new era of challenges in servicing the extended digital enterprise of today.

Edge computing: Clouds are, by design, remote processing and storage resources. To bring processing and storage closer to the devices generating data, the concept of *edge computing* has evolved in recent years. Edge computing (simply called 'the edge') is performed directly on (or very close) to the device, which is typically a programmable automation controller (PAC). It an IT architecture that minimizes or eliminates the need to use remote centralized cloud systems for processing. In many situations, on-device computing on the edge can dramatically improve the performance and processing speeds of the IoT simply by removing the distance and time handicaps associated with the cloud.

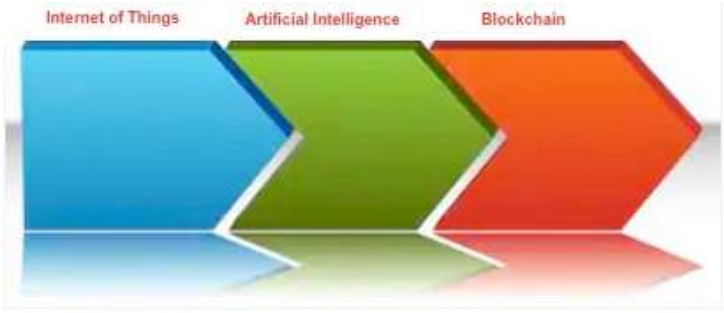
Fog computing: To maintain the integrity of edge computing, some standards have evolved in parallel. One such standard, proposed by Cisco (and available freely to users) is *fog computing*. Fog computing is typically more scalable than edge computing. It specifies standards for data flow, processing and storage on local area network nodes between the cloud and edge devices dispersed across distant locations.

IoT – the Internet of Things: Corporate boundaries and interactions between people and industries are no longer confined to a few secure business locations. Easy access to the Internet and mobile technology has driven computer networking devices into the domain of customers, distributors and virtually anyone who deals with a business. Computing devices are proliferating in millions of forms as nodes (or 'things' in general) on an extended Internet that embraces wireless stations and smartphones, as well as a variety of electronic products such as notepads and music systems. As the population of the *Internet of Things* (IoT, or small, embedded computing devices) widely distributed in remote places continues to grow exponentially, performance issues and processing delays are also multiplying.

Artificial Intelligence: *Artificial Intelligence* (AI) is the generic term that describes a class of independent software 'agents' or 'bots' built with the ability to learn and improve their skill to achieve a specific goal, without (or with partial) human intervention. AI programs are typically algorithms that are capable of learning from data, and modifying their own patterns of behavior.

Blockchain: As digital storage costs have come down, and networks have become more distributed, security and reliability concerns are increasingly being addressed by the concept of blockchains. These are open (but secure) distributed ledgers that provide a reliable way to protect IT assets of all kinds. With blockchain encryption, users can transfer or exchange all kinds of critical digital information securely, with no fear of attacks by hackers or inexplicable data losses.

In the past decade, we have seen how consumer and industrial products and services have been changing rapidly because of evolution in communication and networking technologies. Let's look at some paired possibilities of how convergence between IoT, AI, blockchain and the underlying infrastructural technologies of the cloud, big data and edge computing will most likely evolve to create a "whole" greater than the "sum of the parts."



Convergence of AI and IoT

Almost every sector of business has moved from the mere assembly of isolated products and services to the creation of a network of products and services that are collectively included in the IoT. With increasing focus on digital distribution of resources, the IoT itself is evolving, and there is a movement towards adding more intelligence to IoT, closer to the device. This is where parallel developments in artificial intelligence (AI) are providing a fertile ground for convergence.

AI's impact on IoT

By nature, artificial intelligence systems are ideally deployed to make sense of big data (the vast streams of data being produced in the physical world by human-to-machine and machine-to-machine interactions). They are essentially software modules built to take human-independent decisions in machine-to-machine or man-machine environments. AI programs are increasingly being invoked to work in tandem with IoT data flows to make sense of it all. Specifically, here are some ways this convergence might work.

Economies of operation: While collecting data in vast streams, an IoT device must make an intelligent decision as to when and where a collection of data is sufficient for the prediction of a result. This is where an AI algorithm might kick in smartly to prevent any excess or wasteful spillover in the store of data. This intelligence will produce economies of operation by reducing loads on storage, servers and computational cycles. Consequently, there is a saving in energy and costs. Another possible point of convergence is in predictive maintenance. In a network which includes hundreds of equipment, AI algorithms embedded alongside IoT devices can produce early warning signals to pinpoint likely points of failure, and in some cases, take corrective steps automatically.

Computing on the device: In business critical applications, users need to cache data in central storage and for performing high intensity computations. In such applications, the cloud is still needed to provide the extra layer of security and to prevent a possible network collapse. Edge or fog computing enables on-device (or close-to-the-device) computation. This proximity reduces problems of latency due to slow response time on a cloud and curtails exposure of data on a network. AI can place edge computing algorithms directly on a device to perform most of the routine operations with no latency.

Security: AI algorithms might be used to add preventive as well as predictive intelligence to identify possible security threats to an IoT system and prevent breaches. For example, the startup AnChain (www.anchain.ai) offers transaction protection using AI as well as blockchain concepts.

IoT's impact on AI

While AI will boost the efficiency of IoT networks, the reverse effect is also possible – the multiplying number and spread of IoT devices will be a bonanza for AI innovation – where more intelligence can be added in specific situations. Let's look at some ways in which the convergence of IoT and AI is evolving.

Sense-making: In terms of numbers, it is estimated that, by the year 2020, there will be over 30 billion connected IoT devices, and users will spend around $250 billion on IoT networks. Presently, IoT nets are picking up over 2.5 quintillion bytes of data every single day. All this data needs to be processed and analyzed by intelligent sense-making programs and fed to systems that can do something useful in real life applications – which is one point of convergence where AI algorithms come in.

Higher efficiency levels: In both products, as well as services, IoT data streams can be processed with higher efficiency (than presently possible) with the use of AI interventions. For example, applications in healthcare presently use remote monitoring to send signals or critical data about patients to doctors. IoT devices can provide speedier and more intelligent levels of healthcare – for example, an AI-enabled 'smart' bed can detect when a patient's position needs to be adjusted and perform the task without the need for human intervention.

Design modifications: Miniature IoT devices are easy to embed or integrate into products and services in a limitless number of ways. The design of any product – such as a motor vehicle – can be improved in various ways by adding AI capabilities to IoT devices. For example, an autonomous vehicle might be equipped with motion sensors to decide whether an obstacle is in its travel path. By adding an AI algorithm to the design, the sensors can be given the 'smart' ability to analyze whether the object is a person or another vehicle.

Convergence of Blockchain and IoT

Blockchains are increasingly being used in automated cloud and edge transactions. With the proliferation of IoT and AI, there are numerous innovative products and services evolving with blockchain features to provide a layer of security. Blockchain technologies are typically built in an IoT network design where each participant computer or device is a node,

to provide a means of authentication in the stages of data capture and validation. Here are some points of convergence between blockchain and IoT networks.

Distributed networks: The blockchain concept has become feasible because computer networks on the Internet are deployed as linked nodes across vast distances to enable a distribution of workloads. In new approaches to high-performance computing applications, a dedicated IoT system would include common computer nodes linked dynamically for parallel processing. In such a decentralized high-performance system, blockchain schemes can be built in readily to validate and authenticate data exchanges between the nodes. Several companies are working on projects to make the power of such decentralized heterogeneous networks accessible to customers anywhere.

Secure data storage: While the blockchain protocol itself is based on ledger designs that do not rely on voluminous data, blockchain nodes can act as reliable guardians to protect large databases (databanks and data lakes) that form an essential component of IoT networks in big data applications. They can be deployed at strategic control points to validate and authenticate access points.

Facilitating data sharing: While the technology for connectivity of IoT devices between all kinds of industries is easily available, there is reluctance to share IoT generated data across different industries (for example, between retail and banking businesses) because of reliability, security and integrity concerns. The use of traceable blockchain protocols can facilitate cross-functional and cross-business data sharing because it can be based on a common trust-worthy system of token validation and authentication.

IoT's effect on Blockchain

As decentralized systems with millions of IoT nodes proliferate, a major challenge is to build systems that are economical as well as easy to manage. Let's consider some ways in which IoT design can have an impact on blockchains.

Reducing data load and bandwidth: Research and experiments are under way to produce reliable convergent models of IoT-blockchain architectures that might also be supported by AI protocols for intelligent management of data streams. Data loads in IoT network systems can be extreme. The intelligence of handling data for the blockchain is determined by the structure of the IoT-blockchain interfaces. Mediation by built-for-the-task AI algorithms will ensure that only the relevant data is used. The appropriate design of intelligent IoT nodes will help reduce data loads and the bandwidth requirements.

Upgrading nodes: In distributed IoT systems used in blockchains, the simpler (or lightweight) node devices are often passive links on a chain, passing on data to the full power nodes where the actual storage and validation functions to create new blocks are performed. With improved architecture and support from AI, the next generation of IoT devices will be able to upgrade lightweight nodes into full power nodes.

Lower energy requirements: High energy usage is presently a major concern with IoT-blockchain networks. With improvements in IoT architecture, the energy consumption patterns of blockchain devices will change to produce a 'greener' network.

Convergence of Blockchain and AI

AI algorithms are becoming common in a wide range of industries, ranging from healthcare and manufacturing to consumer goods and aerospace. In many cases, there is a need to bring in layers of authentication to ensure the fidelity of operations or even the value of the product of the service. This is the niche where blockchain can converge with AI to create new levels of security or transparency.

Traceability: Blockchains are models of transparency. They carry a complete and perfect record of historic data blocks in an immutable form, and they cannot be altered by stray hackers. AI algorithms, however, are typically black boxes. They don't make the process of decision-making visible because of numerous levels of complexity embedded in the design. So it's possible to envisage a convergence of the two technologies in the area of transparency and accountability. For example, in applications such as machine-to-machine communications, where no human intervention is possible, the inclusion of a blockchain audit trail will provide a layer of traceability that might help in tuning up performance or to create a rigorous system of preventive maintenance.

Boosting AI efficiency: AI algorithms are typically 'trained' on an enormous variety of simulated data sets before they can become 'intelligent' enough to be moved into real world situations. Blockchain protocols can ensure that the training data sets are 'cleanly validated' or otherwise purposed intelligently for the task. In a network, blockchains can draw upon hundreds of IoT nodes to simulate the necessary training data feed for an AI algorithm to sharpen its functional efficiency.

Democratic data access: Many companies are working on the creation of blockchain-enabled secure access to tap big data marketplaces. These access services will enable even small companies to create and refine economical AI products and services by opening up and democratizing data that only large corporations are currently able to tap. For example, companies such as Ocean Protocol (www.oceanprotocol.com) offer what they call 'tokenized' service layers that act as an intelligent blockchain agent between 'data providers' and 'data consumers' in an open market. In a typical use case, a small market research company may be a data consumer, whereas many large telecom service corporations may be data providers. In this scenario, a secondary benefit to the providers is that their big data assets can be easily monetized with blockchain tracking.

De-risking operations: a blockchain layer will act as a security lock on AI programs that run on data access objects (DAOs) that act as interfaces in client networks. A DAO is a mechanism that acts as an abstract layer that protects a database from direct interactions with clients (which may affect the integrity of data sets).

AI's effect on blockchain

While blockchain protocols are virtually tamper-proof, there are limitations and some areas of concern in the usability of the technology universally. AI is being applied to solve some of these issues.

Energy management: Blockchain operations consume vast amounts of energy as the processing and verification steps in transactions increase in complexity and blocks are maintained indefinitely. AI algorithms are already in use for optimizing energy usage in many networks. It is natural, therefore to expect that future developers will continue to refine and use AI-based protocols to solve blockchain's energy management issues. These initiatives may be directly focused on energy savings, or they may be indirect results produced though performance improvements or design innovation.

Computing: Typically, blockchain uses a brute force approach to identify every possible solution and checking if each of them meets a problem specification before any transaction is validated. AI algorithms could be trained on suitable problem solving sets to learn and evolve intelligent ways to handle this bottleneck.

Speed and performance: Blockchains are notoriously slow. For example, a typical cryptocurrency blockchain works at a speed between 3 to 15 transactions per second (as compared to normal legacy computers which process thousands of transactions per second). This is because blockchains use rigorous and extensive consensus mechanisms to achieve total authentication. AI developers are working on new consensus protocols that could help boost blockchain's sluggish speeds and thereby improve performance. For example, one method, called 'sharding' uses parallel processing across blockchain nodes to speed up consensus.

Boosting efficiency: Blockchain sizes are growing at a phenomenal rate. For example, it is estimated that every 10 minutes, 1MB of data is being added to the existing stack of the Bitcoin blockchain, which has reached about 197 GB in January 2019. AI designers are exploring ways to use sharding or new types of decentralized learning models to improve the efficiency of blockchain handling.

Summing Up

As the digital economy evolves, legacy data processing is being transformed into an open source model that includes data processing and storage in clouds, and extends to edge computing and a distributed intelligence in billions of IoT devices and embedded interfaces. Computing power is now available at the level of miniature and mobile devices, and it is economical enough to reach even the lowest strata of society. Computer processing power has become the most accessible democratic asset for people, available to anyone, anywhere, at any time.

In tandem with these developments, we are witnessing greater intelligence and autonomy being added to computing infrastructures everywhere. The convergence of IoT, AI and blockchain technologies is creating a wave of new business opportunities and innovations. It is also opening up unlimited possibilities for penetrating the culture and lifestyles of individual consumers in myriad ways. With digital services becoming more predominant than traditional products and markets, we will continue to see the evolution of new business models that combine IoT, AI and blockchain functions to deliver value to consumers, supply and distribution chains, corporations, and even entire 'smart cities'.

References

Hypernet Protocol - Distributed High-Performance Computing Powered by Blockchain Technology
https://hypernetwork.io/HypernetWhitePaper_v1.1.pdf

Reyna, A., Martin, C., Chen, J., Soler, E., Diaz, M. (2018). "On blockchain and its integration with IoT. Challenges and opportunities".
https://www.sciencedirect.com/science/article/pii/S0167739X17329205

Size of the Bitcoin blockchain from 2010 to 2019, by quarter (in megabytes)
https://www.statista.com/statistics/647523/worldwide-bitcoin-blockchain-size/

Outlier Ventures (2017). “Blockchain-Enabled Convergence”. White Paper.
https://outlierventures.io/convergence-wp

Outlier Ventures (2018). “The Convergence Ecosystem”. White Paper.
https://outlierventures.io/research/introducing-the-convergence-ecosystem/

Mr. T. A. Balasubramanian is a chemical engineering graduate from IIT, Madras, and an alumnus of IIM, Calcutta, with a post graduate degree in management. He worked for over 15 years in the corporate sector with Hindustan Petroleum Corporation Limited (HPCL), as a Systems Manager. In this position, he was responsible for software design and development for various commercial applications.

In 1993, he launched a startup, Maxigen Communications, a marketing communications consultancy service. In the past two decades, he has been engaged in the strategic and creative management aspects of communication across a range of business domains including infotech, business processing, hospitality, engineering consultancy and manufacturing. Since 2007, he has conducted 'Creativity and Innovation' training programs for leading global companies as well as interest groups. He is currently working on innovative content design for the global online digital education market.

As a writer and editor, he has held positions with publications such as Computer Age (Contributing Editor) and Business Computer (Technical Editor), and written columns for IT and business publications such as Business World (on Infotech Trends), Computers Today (on Computer Industry and Technology topics), Express Computer (on Technology Insights) and Dataquest (Humor for CIOs). He has also contributed articles for the Economic Times and Business Standard.

10 Blockchain Implementation Risks in International Development

One of the most discussed technologies today is distributed ledger technology, a decentralized system for recording transactions with mechanisms for processing, validating and authorizing transactions that are then recorded on an immutable ledger.

Distributed ledger technology exploits a set of well-established principles, including public key cryptography, peer-to-peer (P2P) networking, and consensus algorithms (e.g., proof-of-work (PoW), proof-of-stake (PoS), Federated Byzantine Agreement).

Blockchain is one implementation of distributed ledger technology (DLT), and other new technologies such as Directed Acyclic Graph (DAG) are emerging. IOTA and Hashgraph are examples of DAG-based DLTs.

Distributed ledger technology hasn’t yet reached maturity therefore it brings in certain implementation risks that are important to comprehend and wherever possible to mitigate before deployment.

A good understanding of the risks would assist in deciding whether DLT or a centralized database would be more appropriate, and further choosing the appropriate DLT for a given scenario as the risks vary with the type of deployment, i.e. permissioned (private) or permissionless (public).

- Is software code mature enough to replace the law?
- Standards are underdeveloped and not mature yet
- Energy requirement can be high
- Trusting the blockchain developers and managers
- Increased responsibility on the user
- Implementing data privacy legislation
- Policy and regulatory risks
- Speed of transactions
- Malicious users
- Identity and security

Read the full post at www.ictworks.org/blockchain-implementation-risks/