Blockchain Applications in Distributed Simulation

Roger Smith, Danielle Julian
Florida Hospital Nicholson Center
Celebration, FL
Roger.Smith@flhosp.org, Danielle.Julian@flhosp.org

ABSTRACT

We investigated the operational capabilities of blockchain and several other distributed ledger techniques that are being used in cryptocurrencies. Our objective was to characterize the capabilities of the techniques and their limitations as they apply to distributed healthcare and simulation applications. This paper reports on the capabilities that appear to be applicable to distributed training simulation. It also discusses the limitations of these techniques which may impact practical applications.

Blockchains or distributed ledgers lend themselves most readily to services like the distributed network loggers and After Action Review systems that are used in networked simulation events. The logger applications record the stream of messages that have been exchanged between simulators, while AAR applications analyze and replay the data to provide feedback to the participants. In addition to logging messages, a blockchain adds features that are important in currency exchanges, such as partial anonymity, security against forgery, distributed validation, immutability of recorded transactions, and public access to the log. These features require computer resources for hash functions, encryption, and network communication, which can result in slow transactions and limitations on the size of the chain that maintains the ledger.

After investigating multiple distributed ledger techniques, our conclusion is that the core features of blockchain are not useful for replacing existing services in distributed simulation. This conclusion is derived from the fact that blockchain was created to enable the processing of valuable data between participants who do not trust each other, and within a system that was previously highly inefficient and costly because of the convoluted mechanisms needed to prevent fraud. Distributed military simulation systems are composed of nodes that are trusted and which have been configured for performance in the absence of internal network threats. Therefore, the core advantages of blockchain are not applicable in this environment. However, the components of blockchain may provide secure, verifiable identifiers for network participants and indices across multiple legacy data storage services, which may be useful new services for simulation operators and sponsors.

ABOUT THE AUTHORS

Roger Smith, Ph.D., is an expert in the development of simulation devices and training programs. He has spent 25 years creating leading-edge simulators for the Department of Defense and Intelligence agencies, as well as accredited methods for training with these devices. He is currently the Chief Technology Officer for the Florida Hospital Nicholson Center where he is responsible for establishing technology strategy and leading research experiments. He has served as the CTO for the U.S. Army PEO for Simulation, Training and Instrumentation (PEO-STRI); VP and CTO for training systems at Titan Corp; and Vice President of Technology at BTG Inc. He holds a Ph.D. in Computer Science, a Doctorate in Management, an M.S. in Statistics, and a B.S. in Applied Mathematics. He has published 3 professional textbooks on simulation, 12 book chapters, and over 100 journal and conference papers. His most recent book is *A CTO Thinks About Innovation*. He has served on the editorial boards of the *Transactions on Modeling and Computer Simulation* and the *Research Technology Management*.

Danielle Julian, M.S., is a Research Scientist at Florida Hospital's Nicholson Center. Her current research focuses on robotic surgery simulation and effective surgeon training. Her current projects include intelligent tutoring system, rapid prototyping of surgical education devices, and the evaluation of robotic simulation systems. She is a certified instructor for surgical robotics courses delivered to surgeons and OR staff members. Her background includes research in Human Factors and learning and training to enhance the higher-order cognitive skills of military personnel. She is currently a Ph.D. student in Modeling and Simulation at the University of Central Florida where she previously earned an M.S. in Modeling and Simulation, Graduate Simulation Certificate in Instructional Design, and a B.S. in Psychology.

Blockchain Applications in Distributed Simulation

Roger Smith, Danielle Julian
Florida Hospital Nicholson Center
Celebration, FL
Roger.Smith@flhosp.org, Danielle.Julian@flhosp.org

BACKGROUND

The recent explosion in media attention to Bitcoin and its underlying ledger technique, the blockchain, has led every industry to proclaim plans to investigate or implement blockchain technology in a wide variety of applications. The proponents of these plans describe the advantages of systems that use the public, encrypted, pseudonymous, immutable, distributed ledger for their customers or for society as a whole. But these descriptions often contain little depth of understanding of the capabilities and limitations of blockchain techniques, requiring interested parties to conduct their own research and analysis. This paper describes these investigations as they apply to distributed simulation.

In 2008, Satoshi Nakamoto (pseudonym of the anonymous author) published a white paper on the internet describing a method for creating a digital currency called Bitcoin which was impervious to fraud and could be used by globally distributed parties who did not trust one another (Nakamoto, 2008). The computer algorithms within Bitcoin were constructed so that each party could trust the digital system even though they may not necessarily trust each other. This cryptocurrency concept made use of many established and well researched techniques to support its functionality, which included a timestamp server, blockchain storage, proof-of-work method, distributed ledger storage, incentive system for participation, archiving of old transactions, fractional coinage, and privacy protection. Together these created a digital currency that, as of this writing, has proven to be unbreakable and impervious to theft or deception. However, there have been several third-party data storage systems that have been looted of funds stored outside of the core Bitcoin blockchain.

Initially, Bitcoin existed as an alternative online currency that was embraced by anti-government enthusiasts and certain forms of illegal trade (Walport, 2015; Antonopolous, 2017). But as these users and enthusiasts created a demand for the cryptocurrency by accepting it for payment and accumulating it as an investment, it gained many of the features of traditional fiat currencies issued by governments. By 2014, Bitcoin had attracted enough users and investors that the price of each coin increased from 1/10 of a penny in 2009, to $2,000 in 2014, and reaching a peak of more than $19,000 in 2017 - attracting the attention of investors, speculators, and entrepreneurs who sought to capitalize on this new concept (Popper, 2016).

Early entrepreneurs sought to duplicate Bitcoin's success by creating alternative cryptocurrencies (referred to as "alt-coins") that possess many of the features of Bitcoin combined with variations that appealed to the unique needs of other users and industries. Two of the most successful have been Litecoin which has a lower value, faster transaction times, lower transaction fees, and is positioned as a form of "digital silver" to match Bitcoin's status as "digital gold" (Popper, 2016). It sought to create a currency that was more practical for real world product and service purchases. Another was Ethereum which sought to extend the capabilities of digital currency by adding a programming platform that would connect "smart contracts" to the exchange of digital currency (Buterin, 2017). With Ethereum, a user can specify conditions (the contract) under which a transaction will take place. Initially, Ethereum and its programming language were used to create yet more custom alt-coins without having to program an entire currency system from scratch. It has now become the most popular platform for businesses seeking to create digital contracts that can specify programmed conditions for issuing digital credentials (e.g. auto registration, college diplomas, property deeds) or paying for services. The currencies or contracts for many of these coins are referred to as "tokens" when they are claims on some piece of data or product, rather than representing direct digital currencies.

At the time of writing of this paper, there were over 1,600 digital currencies tracked by the CoinMarketCap web site and over 1,500 more that are too obscure to be considered a global market participant (CoinMarketCap.com, May 1, 2018). Each of these is tied to unique software algorithms and rules, and many are a form of business service or data exchange.

Traditional businesses, such as financial clearing houses and healthcare systems, recognized that cryptocurrencies and digital tokens were being created to provide a competitive, and sometimes more efficient, alternative to their

core business services (Yaga, 2018). Along with the speculative appreciation in the values of Bitcoin, Ethereum, Litecoin, and others, this competition contributed to the explosion of interest by business leaders in using the underlying technologies of these coins to transact international business, especially when trust between the trading partners cannot be guaranteed. This led to the rapid growth of the number of coins and tokens, but also to an expansion in the types of functions that are provided by these digital currencies. Currently, these projects offer services that can be grouped into four categories: (1) digital currency (Bitcoin, Litecoin, Monero), (2) finance (Tether, Binance coin, Kucoin), (3) programming platform (Ethereum, Cardano), and (4) business service exchange (OmiseGO, Enjin, Medicalcoin). This paper explores unique features that appear in several projects that may be applicable to distributed simulation services.

CHARACTERISTICS OF A BLOCKCHAIN

Blockchain is the core technology within the Bitcoin system that has attracted the attention of traditional businesses. The blockchain is a network distributed algorithm that stores a complete list of all spending transactions on a large number of computers, estimated to be in the tens of thousands for Bitcoin (https://bitnodes.earn.com/dashboard/; Iansiti, 2017). The blockchain is structured such that it is nearly impossible to falsify transactions anywhere on the chain or network. It can be understood as a combination of the following unique components or services.

Transactions. At the core of the system are the transactions that are stored on the chain. For Bitcoin, these are records of the transfer of assets (purchases, sales, and splits of digital currency). A transaction record contains a unique transaction identifier; the amount of the asset to be transferred; the input which is the source of the funds; and the outputs, usually at least two, one for the amount to transfer and a second for the remainder that is returned to the original owner (i.e. the change). Transactions are roughly equivalent to DIS PDUs (Distributed Interactive Simulation Protocol Data Unit) and other simulator state update messages.

Blocks. A blockchain does not link together a sequence of transactions. Rather, transactions are grouped together, hashed together, processed together, and linked into the blockchain as a single item - a block. This is why the system is called a "blockchain" instead of a "transactionchain". In the Bitcoin system, the distributed computers that are processing the transactions can group multiple transactions that have been requested at the same time into a single block to reduce the computation and messaging required to process or clear all of them. This approach fits well with distributed simulation data logging and with some AAR functions, which are discussed later. Each block contains a block number, hash value for the block's header, hash value for the previous block's header (which forms the chain), Merkle tree root hash, timestamp, size of the block, "nonce" value, and all of the transactions included in the block. This paper does not explore the purpose of the Merkle tree. But the "nonce" value is essential for understanding Bitcoin and will be explained.

Chaining Blocks. Diagrams of the block data structure (Figure 1) illustrate how these are linked together into a longer chain. The actual mechanism is similar to the linked lists that are common in most programming languages. This chain is the record of all transactions that have occurred for the system it manages (e.g. cryptocoins, health records, network simulation packets). Once recorded into this linked structure the records cannot be removed or changed without invalidating the sequence of hash values stored in each block. Data written into a blockchain is permanent. In a consistent distributed simulation data logger, identical copies of these chains of data would exist on each computer node that is storing blockchain records.

Hashes. Hashing is a function which turns any string of input data into a unique digital number of a uniform length. This number is a unique "signature" representing the original data. Bitcoin and many cryptocurrencies use Secure Hash Algorithm 256 (SHA-256). This algorithm turns every input stream into a string of exactly 256 bits of data that are represented as 32 characters (32 characters x 8 bits/char = 256 bits) (Yaga, 2016). This 256-bit hash value can be used to verify that the original input data has not been corrupted in any way. If even a single bit of the original data is changed, then the hash algorithm will return a completely different value. Hashing is performed both before sending data and after receiving it to ensure that the data has not been corrupted during transmission or storage. For the Bitcoin blockchain, SHA-256 is used to create both a unique ID for transactions and as the linking reference in the next block to be added to the chain of transactions, creating a chain of blocks.

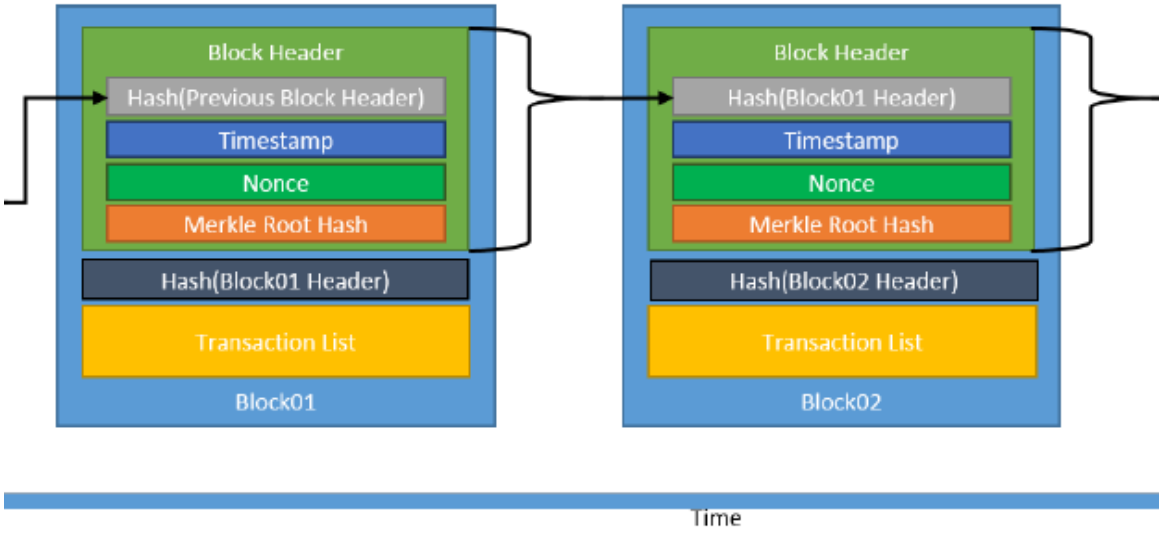

Figure 1. Bitcoin blockchain structure

Asymmetric-Key Cryptography. Transactions and Bitcoins are owned by unique digital addresses that are derived through asymmetric-key cryptography, a.k.a. public key cryptography or PKI. This system generates two digital keys that work together, referred to as the private and public keys. These are generated such that the data that is encrypted with one of them can only be decrypted with the other. The public key is shared with the world at large and parties wishing to send assets use the public key of the intended recipient to encrypt (or sign) the transaction. This encrypted data can then only be decrypted with the private member of the pair. The private key must be kept completely private from the world to preserve secure ownership of assets on the chain. If a private key is leaked to other parties, then those parties have access to and ownership of all assets that are signed with its matching public key. This type of security is essential in a network of untrusted participants, but is less valuable in a private, trusted, networked simulation in which all participants have been vetted and the data does not have intrinsic financial value.

Addresses & Private Key Storage. Each transaction on the blockchain is actually owned by a digital address that may not be traceable to the person or organization that controls it. Each address is formed by hashing the public key of its owner with another unique value. The person who controls the key has control or ownership of the asset listed on the blockchain. It is possible for each transaction to be owned by a unique address or for all transactions to be owned by a single address which is reused. Since private keys are "the key" to the entire security of the blockchain system, protecting them is essential. Private keys may be stored at a digital brokerage firm (e.g. Coinbase.com accounts use this method), in a local personal computer file, on an encrypted USB stick, or even written to paper. If this key is stolen, then the money it protects can also be stolen. If this key is lost then the money it protects is also lost. There is no "key recovery" service as with most internet account passwords, lost keys result in lost funds or lost data.

Distributed Ledgers. Blockchains are also known as distributed ledgers because each chain has identical copies spread across multiple computer servers. These distributed copies contribute to the availability of data by resisting computer crashes and denial of service attacks on individual computers that store the blockchain. They also contribute to the security of the system, insuring that any accepted copy of the chain must match other copies of the chain. Crashing or corrupting one instance of the blockchain does not destroy the entire system. The Bitcoin blockchain is currently duplicated across thousands of computer nodes. This number is driven by the open, permissionless nature of the system which allows anyone to become a node on the network. Such wide, ad hoc duplication would not be useful or efficient for distributed simulation.

Mining & Nonces. The creation, storage, and maintenance of the blockchain occurs on an ad hoc, distributed network of voluntarily contributed computers. This distribution contributes to its availability, security, persistence, and scalability. Therefore, Bitcoin must contain some method for motivating and rewarding participants for contributing their computer resources. This is accomplished through a competitive reward for processing transactions. Computers that serve as full hosts on the network can compete with each other for the right to process the next block (group of transactions) and add it to the chain. To win the competition a computer must use a hash function to find a "nonce" ("nonce" is a concatenation of "number used once" and is an integer between 0 and 4,294,967,296). In most blockchain systems the target answer has a specified number of leading zeros. This

requirement is the basis of the computational competition and requires significant computer power to discover. Therefore, when one is discovered it represents a "proof of work" (POW) that has been performed. Because of the mathematic nature of hashing, it is not possible to predict which input to a hash will result in the desired output. Therefore, this competition is a race through a random set of input values until an acceptable nonce is found. The average number of hashes required to discover an appropriate nonce is 10,000 terahashes (10^{16}) (Evans 2016). Once found, these nonces are easy to verify. So, the winner presents the nonce to the network for verification and is awarded the right to process the next block. Along with this award comes a newly minted set of Bitcoins or alt-coins. These coins are created by the software, have the value of any existing coin, and expand the currency within the system. The Bitcoin reward is currently 12.5 Bitcoins, which on May 1, 2018 were worth approximately $8,950 each, placing the value of the award at $111,875. The size of these rewards indicates why so many computers are participating in the competition and supporting the Bitcoin currency.

BLOCKCHAINS BEYOND BITCOIN

Such an uncrackable ledger of exchange has the potential to be trusted with a much larger set of valuable digital assets than just cryptocurrencies. Researchers and entrepreneurs have suggested that a blockchain would be ideal for storing digital records of asset ownership (deeds to land or vehicles), licenses (driver's and other professional credentials), health records (personal health information, lists of clinical providers), and supply chain transactions (movement of products from source-to-shelf). Unique projects have been created to demonstrate blockchain implementations to support each of these applications.

Figure 2 illustrates how a blockchain might contain the records of vehicle registrations, modifications, and sales. Since a vehicle (e.g. automobile, boat, RV) is a persistent object like a Bitcoin, it has a life through which it is transferred between owners and its characteristics are updated, such as accident and maintenance records. A publicly accessible blockchain could be used to make universally visible and validated records of the ownership of these vehicles. Since the address of ownership does not directly identify the owner, it would not reveal who the owner of a vehicle was unless the owner shared the necessary public address with a potential buyer of the vehicle.

Distributed simulation PDU processing is similar to tracking vehicles. A chain would link together the movement and state changes of each object in the simulation. Each simulation object could be stored on its own unique chain, or multiple objects could be processed together so the histories of groups of objects operating in the same region or cooperating with each other would be stored together in the same set of blocks. Multiple grouping and separating rules could be created to optimize performance.

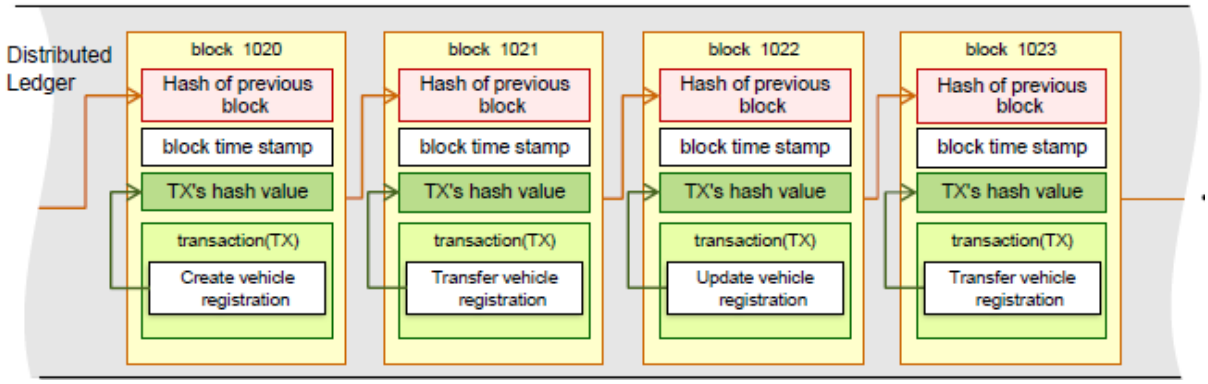

Figure 2. Blockchain example for non-financial records, e.g. vehicle registrations.

As multiple business projects have emerged it has become clear that some of the features required to support cryptocurrencies are not necessary, and are even hinderous, for these businesses. This has led to many alternative implementations of the original blockchain, which are generically referred to as distributed ledgers. Two of the largest supported ledger projects are the Hyperledger Fabric by the Linux Foundation and Corda by the R3 financial consortium (Valenta, 2017; Yaga, 2018). These and many other custom implementations have created alternative designs that retain the functionality and security of the original blockchain but avoid much of the processing overhead and storage limitations. Table 1 provides some of the key feature differences between each of the major blockchain implementations.

As an example, the R3 CORDA project is a distributed ledger specifically created for use in global financial transactions. Davison (2017) provides a clear example of why blockchain is valuable in this industry. A purchase using a Visa credit card is processed within seconds at the point of sale. But that transaction goes through a series

of 17 unique steps before it is confirmed, funds are transferred to the merchant, and funds are debited on the buyer's account. These steps can take between three and seven days to occur. If this same system were processed through a CORDA blockchain service, the transaction could complete verification and the funds would be delivered to the merchant in a matter of minutes. This would speed the movement of money and eliminate the expenses from multiple intermediate parties that participate today. These types of cases have stimulated the broad interest in the technology for other businesses and for events like distributed simulation.

Table 1. Feature Comparisons of the Leading Distributed Ledger Implementations

Feature	**Bitcoin**	**Ethereum**	**Hyperledger Fabric**	**R3 CORDA**
Description	Dedicated Blockchain System	Generic Blockchain Platform	Modular Blockchain Platform	Specialized Blockchain for Financial Industry
Block Payload Limit	1 Mb	~780Kb	100Mb	Unknown
Block Creation Rate	10 min/block	17 sec/block	Variable	Variable
Transaction Processing Rate	5 trans/sec	25 trans/sec	Variable	Variable
Interoperability	No	No	Potential Plugin	No
Mode of Operation	Permissionless, Public	Permissionless, Public & Private	Permissioned, Private	Permissioned, Private
Consensus	PoW Mining, Ledger Level	PoW Mining, Ledger Level	Flexible, Transaction Level	Notary Nodes, Transaction Level
Smart Contracts	None	Programmable (Solidity)	Programmable (Go, Java)	Programmable (Kotlin, Java), Attach Legal Prose
Currency	Bitcoin	Ether, Optional Tokens in Contracts	None Native, Optional Tokens in Contracts	None

Sources: Valenta, 2017; Evans, 2016

APPLICATION TO DISTRIBUTED SIMULATION

With an understanding of the purpose and structure of Bitcoin and blockchain, this section explores the application of these ideas to distributed simulation problems.

Examining the architecture and functionality of a large distributed simulation system (Figure 3), there are two immediately obvious applications for the technology. Since a blockchain stores a sequence of transactions, it would appear to be similar to the function of a distributed data logger or collector. These loggers capture the stream of simulation data packets on the network (e.g. DIS PDUs, HLA RTI updates, TENA messages) (Powell, 2012), which may be used later to replay specific portions of the distributed simulation. After Action Review (AAR) systems also create archives of relevant transactions on the network, or receive a feed from a data logger, to analyze the events that occurred and to provide instruction to the training audience. Can a blockchain improve on the process through which either of these functions are accomplished? We examine each of the blockchain components and activities to identify which may and which may not contribute to these services in a distributed simulation.

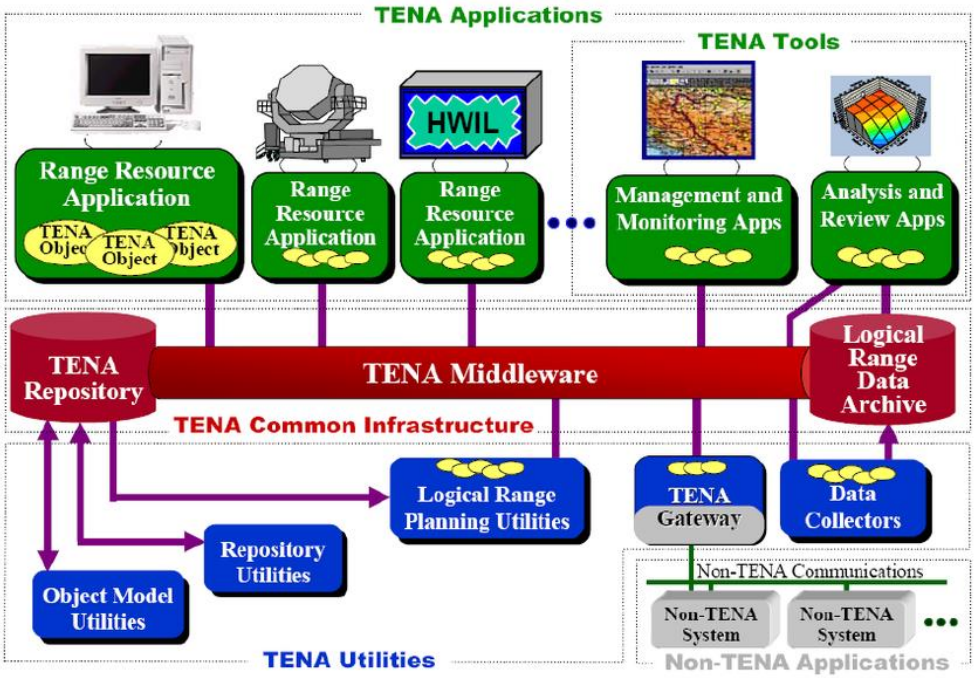

Figure 3. TENA Distributed Simulation Architecture (Powell, 2012)

Open Public Network. Bitcoin and most cryptocurrencies operate on an open public network on which all transactions are visible, though the participant's identity is masked. For these networks any computer can offer itself up as a hub for any of the services that are performed. When the financial industry examined Bitcoin and blockchain for its operations, this was one of the first features that they identified as being undesirable for their business (Brown, 2016). Like financial operations, the transactions that are occurring within a military distributed simulation are not for open public consumption since the data may be classified or sensitive. In both industries, it is necessary for the data to remain within a controlled network. Therefore, a distributed simulation blockchain would operate within a closed private network. Only designated and approved nodes would be allowed to perform services or view data on the blockchain. Distributed simulation occurs on a closed, private, controlled network, so physical connectivity does not exist for the data to be open to the public. This security is helpful in eliminating the need for some of the other blockchain features described below.

Mining Competition. To attract the computing resources necessary to operate a cryptocurrency, the blockchain process usually contains a competitive mining process in which participants expend huge amounts of computer power to solve difficult computational puzzles as fast as possible (called "proof-of-work"). This process has been criticized as wasteful of international energy resources and potentially detrimental to other social needs. A few cryptocurrencies have created a "proof-of-stake" model which eliminates most of the energy consumption but favors big owners of the currency over new entrants (Yaga, 2018). Proponents for closed professional services like finance (and distributed simulation) argue that even this method is not necessary when operating within an existing trusted business environment. If the blockchain truly offers business advantages, then it is a service that customers will pay for. The sponsors of a simulation event already pay for the computing and human resources to conduct the event. If blockchain is a superior solution then it would either reduce costs for this system or provide additional valuable services. So, mining competitions are not necessary. The processing of blocks containing simulation transactions can be awarded in a round-robin fashion to the distributed computers providing the service, and no additional financial reward is necessary to incentivize participation.

Addresses & Cryptography. Transactions and blocks require an assignment of unique addresses for all participants. Both financial and simulation applications have this same need. Simulation federations assign a unique ID to each of the participating entities, whether they are simulation executables that are modeling the world, user interface devices, data loggers, or AAR tools. To be a fully functional node, these have an assigned identity that is logged into the transactions that are published. In a closed private network these are usually assigned by the central authority. There is no need for ad hoc universal ID generation. Public key cryptography (PKI) and hashing of keys are the method used by cryptocurrencies to arrive at unique IDs. Within a private distributed simulation, PKI may still offer a valuable service by generating and using an irrefutable participant address, insuring that all data origination is accurate and cannot be spoofed either accidentally or intentionally.

Distributed Ledger. Blockchains maintain exact copies of the chain, blocks, and transactions on multiple computer servers. These servers communicate with each other to ensure that the copies they possess are all identical. This process is part of defending the network from attack. In a simulation event, maintaining multiple copies of the chain incurs computer processing and network traffic costs, but having multiple copies of the list at different geographic locations is advantageous. When it is necessary to read the data from the chain, an AAR system could read it from the closest local server. A distributed ledger is also crash resilient. When one of the servers goes down all the others continue to provide service.

Blocks & Chaining. Packaging transactions into blocks with the hashing, PKI, and redundancy of the Bitcoin system is essential to maintain security and trust. Distributed ledgers and blockchains are often compared to centralized databases when illustrating their advantages for trust, security, and availability. Since data is secured with encryption and protected from fraud or spoofing by the chain structure, the blockchain can be published publicly and remain secure from tampering or unauthorized decryption. In the absence of this open-network threat environment, blocks and chains lose some of their attractiveness over more efficient means of storage.

Payload Size. A single block in the a blockchain can contain from one to hundreds of transactions. The Bitcoin system is programmed to add one block to its chain approximately every ten minutes. Therefore, there is an advantage for a single block to carry more than one transaction off the queue waiting to be processed. For distributed simulation a different balance of payload size to block creation rate is probably appropriate, for the same reasons that these have been adjusted for other cryptocurrencies like Litecoin and Ethereum. Simulation transaction blocks would need to be added much more rapidly because of the large volume of network messages generated during these events. Additional work needs to be done to identify the optimal balance between payload size and block creation rate for a distributed simulation.

Interoperability. The blockchain systems underlying each of the cryptocurrencies are unique implementations that are not compatible with each other. The major distributed ledger projects – Ethereum, Hyperledger Fabric, and R3 CORDA - are not interoperable with each other. Similarly, Bitcoin, Ripple, Monero, Stellar, and Zcash are all non-interoperable currency systems. The means for posting blocks and synchronizing the distributed ledger are not based on standard on-the-wire protocols or services in the manner that DIS and HLA have used to achieve interoperability. Currently, a distributed ledger system created by one vendor must be used by all participants in the system of transactions, there are no cross-vendor interoperability solutions.

Blockchains of Metadata. The collection and storage of Patient Health Information (PHI) is a medical problem with similarities to distributed simulation. PHI is currently fractured across multiple providers and universally accessible to none of them. The data is voluminous and stored in multiple legacy database systems (Cyran, 2018; Ekblaw, 2016). Each individual patient is similar to a battlespace object (e.g. aircraft, tank, aggregate unit) in that both represent a persistent object that undergoes state changes and event processing over time. Distributed simulation systems collect and store data across multiple existing and heterogeneous legacy applications. Therefore, one potential use of distributed ledgers, which has been proposed for medical PHI, may be useful in distributed simulation. The individual records would remain in the current legacy or siloed databases, and a public blockchain could be used as an index to all the silo locations. Existing storage methods would not change, but another layer of object and event tracking could be added to improve the ability to link, locate, and retrieve all the data that is in storage.

ALTERNATIVE DISTRIBUTED LEDGERS

There are dozens of alternative cryptocurrencies and distributed ledger applications that use a method other than blockchain to store and manage transactions, some of which may be of interest for distributed simulation.

RaiBlocks Latticework. The RaiBlocks (recently rebranded as Nano) cryptocurrency has modified the basic blockchain to create a “latticework” or “personal chain” (Figure 4a). In this system, each user ID has its own dedicated blockchain, rather than all transactions sharing a single chain as with Bitcoin (LeMahieu, 2017). This means that when a coin is transferred from one owner to the next, the transaction is between two separate chains and does not impact the processing of other transactions across other chains within the currency. This allows transactions to be split into many independent parallel processes, rather than focusing the entire network on a single block at a time. This latticework may be more efficient for processing state changes for distributed simulation objects and adding those changes to the chain. The structure is well aligned with the object and patient metadata case described earlier.

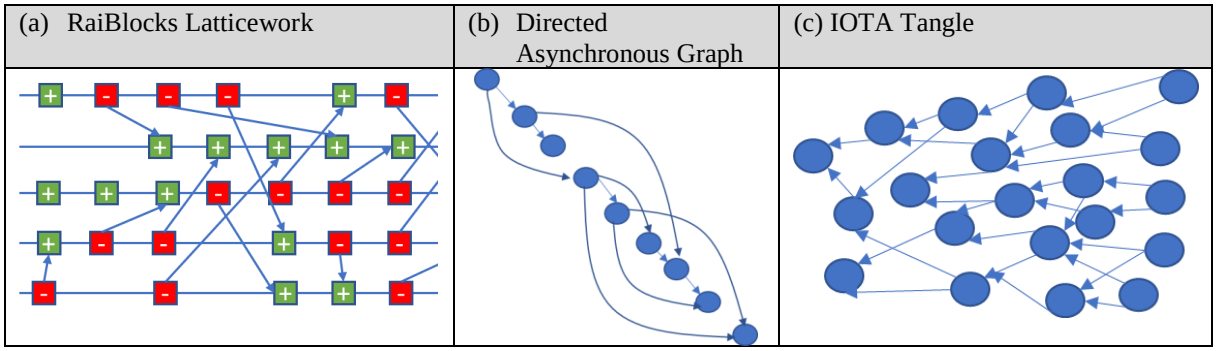

Figure 4. Alternative Blockchain Structures

IOTA Tangle. The IOTA cryptocurrency has created a custom directed asynchronous graph (DAG) that they call the "tangle" for storing their transactions (Popov, 2017). "Directed" refers to a network of nodes that are all connected in the same direction, often referred to as forward (Figure 4b). "Asynchronous" means that a node is not connected to itself. A tangle is not a linear chain as in Bitcoin and Ethereum, but a custom DAG network in which each new block is linked to exactly two previous blocks (Figure 4c). This tangle has a tree-like structure that can be searched from current through past transactions. But the relationship of the transactions is descending time, with no other associating variables. Therefore, searching it to extract data is in reverse time order (newest to oldest), which is not conducive to simulation data analysis and replay.

NITRO & ENJIN Tokens. Searches for blockchain implementations that address distributed simulation systems revealed no existing projects specifically for this community. However, there are cryptocurrencies and blockchains designed to be used in multiplayer, networked gaming applications. Since, gaming programs have provided useful technologies and insights to military training problems in the past - e.g. Virtual Battle Space 1-2-3, America's Army, Full Spectrum Warrior, MS Flight Simulator, X-Plane – their blockchain projects may be similarly useful.

ENJIN uses the Ethereum network to create a custom coin called the "ENJ" (ENJIN, 2017). This is proposed as a universal currency across videogames to purchase and store in-game objects. Game developers would implement the ENJIN coin in their software such that in-game gold, weapons, etc. can be converted into ENJ if the player wishes. The player's ENJIN wallet contains both ENJIN coins and lists of in-game objects with value. Using ENJIN, these objects could be bought and sold between players within a native market, rather than through eBay, Steam, and other external markets. Wealth earned in one game could also be transferred to another game using the ENJ as a common currency in the two economic systems.

The NITRO project offers a means for avid gamers to fund the development of new games, like a Kickstarter campaign (NITRO, 2017). Gamers would contribute real fiat currencies or Ether to support the development of a new game. They then become part of a community discussion and reward system using the NITRO currency "NOX". The funded games would use NOX as the in-game currency for purchasing virtual items, thus increasing to the value of a NOX. Gamers who supported development of a game with their donations would receive NOX rewards for participating in discussions, as incentives from sponsors promoting a game, and by performing valuable in-game activities. NOX would be sold and traded on an external exchange or within the games they support. The developers offer no mechanism to convert NOX back into national fiat currency. So, all wealth accumulated would remain within the game world.

These two projects are typical of the concepts being created and promoted for multiplayer computer games. But they do not offer services that would be valuable and useful to military distributed simulation systems.

CONCLUSION

Evans (2016) summarizes the findings of a Boston Consulting Group study on blockchain with a few principles defining its usefulness. The first of these is that, "It makes sense to expend resources on digital tokens and blockchains only when multiple entities are transacting at high cost and with imperfect trust" (p. 49). Military distributed simulation events are not characterized by either of these. Its systems have been architected to optimize both computing and network resources and do not include manual human intermediaries in transactions. Participants in the network are also trusted members of a selected community. There are no rogue actors seeking to thwart the successful operations of the nodes or the network itself. In other industries at least one or both situations exist – e.g. finance, healthcare, supply chain – making blockchain a potential replacement for the methods now in use.

In distributed simulation blockchain appears to offer an opportunity to add services to improve tracking and awareness of the location of data that is already being stored within existing applications for data logging and AAR. But it appears to offer few advantages in directly replacing the storage mechanisms that are already used by those systems.

Blockchain is such a new technology that potential users are still discovering and creating viable and valuable applications for it. Though we find few practical uses in this first investigation, future work may create tools that are more amenable to the challenged faced in distributed simulation.

REFERENCES

Antonopoulos, A. (2017). *Mastering Bitcoin: Programming the open blockchain*. Sebastopol, CA: O'Reilly Media.

Clauson, K., Breeden, E., Davidson, C. Mackey, T. (March 2018). Leveraging blockchain technology to enhance supply chain management in healthcare: An exploration of challenges and opportunities in the health supply chain. *Blockchain in Healthcare Today Journal*, 1(1).

Cyran, M. (March 2018). Blockchain as a foundation for sharing healthcare data. *Blockchain in Healthcare Today*, 1(1).

Davison, R. (Nov 2017). The blockchain evolution. Presentation at HPE Connect Conference. Available at: https://youtu.be/q-iJW_qSD8k

Ekblaw, A., Azaria, A., Halamka, J. and Lippman, A. (Aug 2016). A case study for blockchain in healthcare: "Medrec" prototype for electronic health records and medical research data. *2016 IEEE International Conference on Open and Big Data*.

Evans-Greenwood, P., Hillard, R., Harper, I., Williams, P. (2017). *Bitcoin, blockchain and distributed ledgers: Caught between promise and reality*. Deloitte Consulting – Australia.

Evans, P. (2016). *Thinking outside the blocks: A Strategic perspective on blockchain and digital tokens*. The Boston Consulting Group.

Halamka, J. (March 2018). Real blockchain use cases for healthcare. *Blockchain in Healthcare Today Journal*, 1(1).

Halamka, J. Lippman, A., Ekblaw, A. (March 2017). The potential for blockchain to transform electronic health records. *Harvard Business Review*.

Iansiti, M., Lakhani, K. (Jan 2017). The truth about blockchain. *Harvard Business Review*.

Kuo, T., Kim, H., Ohno-Machado, L. (2017). Blockchain distributed ledger technologies for biomedical and health care applications. *Journal of the American Medical Informatics Association*, 24(6), 1211-1229.

Popper, N. (2016). *Digital Gold: Bitcoin and the inside story of the misfits and millionaires trying to reinvent money*. New York: Harper Paperbacks.

Powell, E. & Noseworthy, J. (2012). The Test and Training Enabling Architecture, in *Engineering Principles of Combat Modeling and Distributed Simulation*, ed. A. Tolk. Hoboken, NJ: John Wiley & Sons.

Valenta, M., Sandner, P. (June 2017). Comparison of Ethereum, Hyperledger Fabric, and Corda. Working paper from Frankfurt School of Finance & Management, Frankfurt, Germany, available at: http://explore-ip.com/2017_Comparison-of-Ethereum-Hyperledger-Corda.pdf

Walport, M. (2015). *Distributed ledger technology: Beyond blockchain – A report by the UK government Chief Scientific Adviser*. UK Government Office for Science.

Yaga, D., Mell, P., Roby, N., Scarfone, K. (Jan 2018). *Blockchain technology overview: Draft NISTIR 8202*. National Institute of Standards and Technology, US Department of Commerce.

Cryptocurrency White Papers: (These papers are listed separately because they are published directly by the cryptocurrency development teams without peer review or external editor verification. However, in this rapidly developing area these are often the only sources for information about the details of the cryptocurrency projects.)

Brown, R., Carlyle, J., Grigg, I., Hearn. M. (Aug 2016). Corda: An Introduction. Corda Project. Available at: https://docs.corda.net/head/_static/corda-introductory-whitepaper.pdf

Buterin, V. (2017). Ethereum white paper. Available at: https://www.ethereum.org/pdfs/EthereumWhitePaper.pdf

ENJIN Development Team. (Sept 2017). ENJIN Coin: Smart cryptocurrency for gaming. Available at: https://enjincoin.io/

LeMahieu, C. (2017). RaiBlocks: A feeless distributed cryptocurrency network. Available at: https://raiblocks.net/media/RaiBlocks_Whitepaper__English.pdf

Mazieres, D. (Feb 2016). The Stellar consensus protocol: A federated model for internet-level consensus. Available at: https://www.stellar.org/papers/stellar-consensus-protocol.pdf

Nakamoto, S. (Oct 2008). Bitcoin: A peer-to-peer electronic cash system. Bitcoin.org. Available at: https://Bitcoin.org/Bitcoin.pdf.

NITRO Development Team. (Dec 2017). NITRO: Blockchain to democratise the utility of video-games economy. Available at: https://www.nitro.live/

Poon, J. (Jue 2017). OmiseGO. Available at: https://cdn.omise.co/omg/whitepaper.pdf

Popov, S. (Oct 2017). The Tangle. Available at: www.iota.org/IOTA_Whitepaper.pdf