



Taking Score on the Success of Blockchain, So Far

Rick Kuhn and Jeffrey Voas, NIST

Phillip Laplante, Penn State University

Five experts examine distributed ledger technology and blockchain, discussing their status in terms of adoption and success.

A recent article in *The Register* (United Kingdom) suggested that there has been little success in the application of blockchain (https://www.theregister.co.uk/AMP/2018/11/30/blockchain_study_finds_0_per_cent_success_rate). After reading it, we decided to inquire further, to dive deeper into this technology that often seems to be amorphous. People seem to confuse bitcoin and cryptocurrencies with blockchain.

There is also the question of distributed ledger technology (DLT) and how it relates to blockchain. Are these all of the same or different? A clearer understanding is needed. In a recent publication, we noted that DLT provides certain unique and valuable features for trust in

distributed systems, but changes may be needed to make it more practical for systems engineering.¹

In this virtual roundtable, we assembled five experts on DLT and blockchain. The members of this group have been involved in real deployments of these types and have authored articles on the theory of these technologies. The group included: Dylan Yaga, Angelos Stavrou, Jennifer Blair, Tom Costello,

and Ramesh Ramadoss. (See “Roundtable Panelists” for more information about the panelists.)

We hope that this virtual roundtable provides a better understanding of the current state of DLT and blockchain, both in terms of adoption and success. (Please note that the views presented here are those of the roundtable participants and authors and do not necessarily represent the views or policies of NIST.) It should provide a nice baseline to trace the developments of this topic beyond 2019.

COMPUTER: Most new technologies are promoted as being faster, better, and cheaper, but the usually unspoken phrase that accompanies this mantra is “choose any two.” Which of these three properties do you think blockchain and DLT best address? Which are most likely to be

sacrificed to gain the benefits of the other two? And to what degree does this vary with application domain?

DYLAN YAGA: It's difficult to do this as a blanket statement, since it's really on a per-implementation basis. For some, who have slow manual processes, these technologies could be faster and cheaper but not necessarily better since they ultimately achieve the same result. For some who do not have a lot of intermediaries to go through, they may be faster and better but not necessarily cheaper. The costs depend on the fees and agreements. For others, they could be better and cheaper, but if it uses a deliberately slow consensus mechanism, the technologies will be slower.

ANGELOS STAVROU: They are faster and better but not necessarily cheaper. In general, we have to accept a higher cost to gain the benefits of the other two. Blockchain is not about being cheaper but accomplishing things in a better way among entities that do not trust each other or are even competing.

JENNIFER BLAIR: While it's still early days, we're already seeing real business results delivered with blockchain in the better and faster categories. In the work we originated with Walmart (now called IBM Food Trust) with more than 80 companies involved, we're focusing on transparency in the supply chain—digitally tracing food products from an ecosystem of suppliers to consumers. Using the IBM blockchain platform, we improved traceability from seven days to 2.2 s. Frank Yannis (former vice president of food safety at Walmart and currently with the U.S. Food and Drug Administration) calls that speed “food traceability at the speed of thought.” That's blockchain changing everyday life by being faster.

A second example would be our own IBM Global Finance (IGF) dispute-

resolution work with blockchain. It helped free up more than US\$75 million of US\$100 million of cash flow stuck in a reconciliation cycle between ourselves and key partners. Within our IGF lending business, which does about US\$40 billion in business a year, we took our dispute-resolution times down from 44 days to under 10. That's faster, better, and represents a significant cost take out for our business.

Is blockchain/DLT the answer for everything? Of course not. We evaluate very specific criteria to identify a good blockchain use case and be sure

that we and our clients aren't starting blockchain projects that go nowhere after an initial proof of concept (PoC). We focus on mutually successful networks that have the right attributes and market momentum to accelerate to production/scale.

TOM COSTELLO: We haven't found any scenarios where DLT is faster or cheaper when mirroring existing business models. I would certainly say “better” and in some cases I would use the refined term(s) *unique/new*. Some solutions certainly disintermediate a

ROUNDTABLE PANELISTS

Jennifer Blair is North America Blockchain Innovation Services executive at IBM, where she is responsible for multimarket blockchain GTM strategy, enablement, and execution. She has cocreated and contributed assets to IBM's Blockchain Methodology and Delivery best practice and represents IBM in various industry partnerships and alliances. Contact her at jmblair@us.ibm.com.

Thomas Costello is the CEO of UpStreme, Inc., a business and technology management consultancy, specializing in project rescues and critical thinking relative to solutions and emerging technologies. He consults with both public and private sector organizations and is a noted author, speaker, and mentor. Contact him at tcostello@upstreme.com.

Ramesh Ramadoss is an entrepreneur, researcher, author, and international speaker and the founder and president of BitCasas Inc., a blockchain technology startup in Silicon Valley. He is a cochair of the IEEE Blockchain Initiative and the chair of the IEEE Blockchain Standards Working Group. Contact him at Ramesh@bitcasas.com.

Angelos Stavrou is a professor in the Department of Computer Science and director of the Center for Assurance Research and Engineering at George Mason University. Contact him at astavrou@gmu.edu.

Dylan Yaga is a computer scientist and researcher at NIST/ITL/CSD. He has been investigating blockchain technologies and systems as the NIST/ITL/CSD blockchain program leader. He was the lead author on the NISTIR 8202—Blockchain Technology Overview, which outlined the technological components and mechanics of how many blockchain technologies work. Contact him at dylan.yaga@nist.gov.

process by reducing the number of players or steps. That can be faster.

RAMESH RAMADOSS: In 2008, Bitcoin was introduced by Satoshi Nakamoto as peer-to-peer electronic cash. He used blockchain to solve the double-spending problem. The transactions are approved and recorded in an immutable ledger by peers through a consensus protocol, or proof of work, as shown in Figure 1. Initially, the distributed ledger underlying Bitcoin was referred to as blockchain. In 2013, Vitalik Buterin extended this concept and proposed Ethereum as a global distributed computing platform programmable through smart contracts. In 2015, the Linux foundation launched the Hyperledger project, which develops industry-grade blockchain tools and technologies. In a broader sense, both blockchain and DLT can be defined as a software architecture that runs on a distributed peer-to-peer computer network. It combines several existing concepts, for example, cryptography, consensus, and economic incentives.

Over the last decade, several architectural variations have been introduced that can be broadly categorized as public, permissioned, or private blockchains. These blockchain architectures have evolved over time to address tradeoffs among three factors: better (trust in the transaction),

faster (transaction speed), and cheaper (transaction cost).

It is quite challenging to make any general statement about blockchain/ DLT. The first public blockchain, Bitcoin, was primarily designed to provide decentralized trust to transactions at the expense of high cost and slow transaction speed due to the proof of work consensus protocol. The private blockchain Hyperledger fabric is designed to provide faster transaction speed by limiting the number of transaction validators, which can be viewed as a tradeoff on trust.

COMPUTER: Can you identify projects where there have been measurable benefits that result specifically from DLT? That is, the benefits should be beyond what might be achieved by automating a previously manual process. It has been argued that many supply chain DLT projects would have the same improvements with a conventional distributed database.

YAGA: No. Most people discuss with me their project proposals or projects they are planning to work on. The only time I have been included on success stories, or anything that mentioned metrics, has been by companies that have a blockchain platform that they are promoting.

In most talks I have with people who are seeking to replace systems with blockchain technologies, I urge them to take metrics on everything, on

the existing system and the proposed blockchain system and compare.

STAVROU: DLTs are designed to offer a trusted and verifiable datastore where parties that do not trust each other can verify and attest to transactions. This cannot be achieved by a conventional distributed database due to the way peer interactions are verified and recorded. Moreover, the way that transactions are stored in DLTs makes them chained to each other, so even if there is limited collusion, it cannot change the recorded information.

BLAIR: In 2019, everyone seems to be in the blockchain business, and there are some exciting new ideas as a result of this market enthusiasm, which is awesome. There are significantly fewer teams, though, that are proven in moving networks from ideation through to production and operating at scale.

As a result, the direct costs and other investments you see from some participants and stakeholders in the marketplace to build and join these new business ecosystems vary wildly. I don't think it's accurate to say at this time that you'll consistently sacrifice one for the others. To get better, faster now doesn't mean that your costs will be through the roof. In fact, there are specific governance planning and design actions that will reduce the risk of your marginal dollar investment in new blockchain initiatives.

RAMADOSS: As of today, the top decentralized applications (DApps) on the popular Ethereum blockchain fall in the category of gaming, gambling, and exchange. Blockchain enthusiasts believe that we are at the early stages of technological development and adoption when it comes to public blockchains. Using Hyperledger-based private blockchain, IBM has demonstrated that tracking time can be reduced from days to minutes on the food supply chain. Hyperledger enables multiparty transactions to be carried out on a single shared ledger using private state channels.

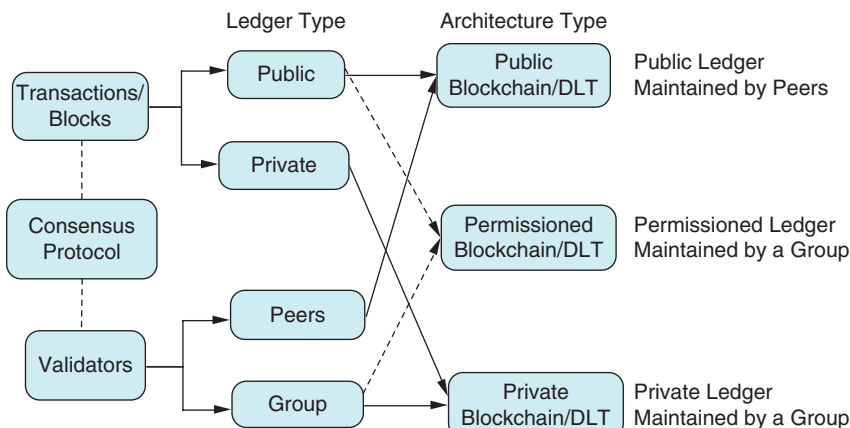


FIGURE 1. The types of ledgers. (Image courtesy of Ramesh Ramadoss.)

This is a significant improvement over a conventional database. Carrefour, Dole Food, Kroger, Nestlé, Tyson Foods, Unilever, and Walmart are partnering with the IBM Food Trust. Walmart plans to sell bags of lettuce that are tracked using blockchain technology by the end of this year. The United Nations World Food Program plans to test blockchain for the tracking of food delivery in East Africa.

COMPUTER: Looking at an often-proposed use case for DLT, real estate transactions, what measurable improvements could be provided? In many places, it is already possible to conduct the entire transaction electronically and have the resulting records filed with the government electronically as well. Given that government is inherently involved with property records anyway, what benefits could blockchain provide that are not already possible with a low-cost real estate firm as a trusted third party?

YAGA: Blockchain systems work best when they are 100% digital, since assets can be tracked and rules enforced completely within the system. Once you start to use blockchains to record real-world assets, you are once again dealing with humans who need to be trusted.

The examples given for real estate transactions often include some oppressive government that ignores or alters your claims to the land based on a traditional registry system. This scenario often argues that a blockchain could stop this, since the records could not be altered or removed. While it could prevent alteration or transfer of the land claims, what would stop the oppressive government from simply ignoring the blockchain registry all together? The real feat would be to convince an oppressive government that it should use a system that it could not easily control.

STAVROU: One of the improvements could be globally verifiable transactions and bids for real estate values that are immutable and can be audited. That will force sellers, buyers, and real estate

agents to be honest with their offerings and transactions. The government will be able to audit the transaction records automatically. That would prevent any parties from altering information at any level and reduce the risk that is currently handled by title agencies. The entire transaction model will also benefit from this technology because buyers can potentially place bids for the real estate and the DLTs can faithfully keep the order of transactions. Currently, we rely on real estate agents to perform that duty, which cannot guarantee fairness. The real estate firm can also include ancillary information about the transaction including bid information that can easily be accessed by a government auditor and the government (and state) title offices.

BLAIR: Yes. Blockchain is a team sport. Among other things, it can be used to optimize large flows of capital and data across the enterprise ecosystem. Additionally, it allows you the opportunity to design and create a democratized data market place where previously undiscoverable insights or patterns could lead to new and exciting opportunities for the mutual benefit of the group.

Our TradeLens solution, underpinned by blockchain, has more than 90 network participants today, including five of the six largest shipping carriers. We're working together to reimagine global trade and improve the movement across strategic trade lanes. It compresses the data for a single shipment, 200 docs and 30 actors/entities, into a single trusted process.

Another example. IBM buys billions of dollars in labor annually. We were finding pockets within the company where between 9 and 11% of the invoices we received had a reconciliation issue. We had to expend significant time and resources to identify the problems and correct them. We worked with five of our major U.S. contractors to go after this problem in a small way to start and leveraged blockchain to collectively address it.

This process was able to verify that the right resource was matched with the right credentials, that contracted work was done in the agreed upon time frame and at the agreed rate. Together, in fewer than six months, we expect to go from an average reconciliation cost of US\$250 per invoice to zero cost by using our blockchain implementation. Our partner will get paid faster by IBM, incur significantly fewer payment disputes, pass our audits more easily, and have an immutable performance record with our team.

COSTELLO: Watching the ransomware attack currently in progress in Baltimore, Maryland (where the city has been unable to close any real estate transactions and where all data may potentially be permanently lost), a distributed model with numerous copies would absolutely provide benefit to all parties concerned.

RAMADOSS: In the United States, there are over 600 Multiple Listing Service (MLS) agencies that list real estate properties for sale. Currently, the property transaction information is maintained in several databases by these agencies. Private blockchain platforms, such as Hyperledger, enable multiple parties to transact among themselves on a shared ledger. It is possible that all transactions could be recorded in a private consortium blockchain shared by all MLS agencies. Practically speaking, it might be a daunting task to convince all agencies to adopt such a solution.

In the United States, property ownership records are maintained by 3,007 counties in various databases. The recording fees vary from county to county. Also, some counties charge fees for obtaining copies of existing records. Given such a fragmented system from record keeping to fee structure, it is difficult to envision all counties agreeing to use a single shared ledger. It is possible that a statewide regulation could enable

implementation of a blockchain solution. For example, the state of Ohio is taking the lead in this area.

COMPUTER: Continuing in the same vein as the previous question, one advantage cited for blockchain is the removal of the need for trusted third parties. Is this really possible? For many or most areas of commerce, governments must be involved, and this is certainly true of high-value areas such as real estate. The value provided by third parties in these cases is typically not the data management so much as checking the complex legal agreements involved.

YAGA: Trust will always be involved in these systems; trust is just being displaced, from humans arguing about paper deals within the context of a legal system to programmers and governance working within the execution environment. It is likely that existing trusted third parties would need to be involved, but in different capacities. Rather than the arbiter of deals, they could check and approve smart contracts for correct behavior. They could perform audits to ensure that the smart contracts continue to be executed correctly. They could play a role in the governance of the system, to ensure that changes do not run afoul of regulations.

STAVROU: Yes, one of the advancements of using DLTs is the removal of trusted third parties. Parties are no longer considered trusted; they are considered participants. If more than 50% of the participants are honest, the entire system is guaranteed to operate honestly under some assumptions about participation independence and Byzantine fault tolerance of the system. One aspect of having a truly trusted third party is that this party can become the keeper of audit data, forcing others, the nontrusting entities, to become honest. In other words, in the single trusted-entity scenario, the trust is centralized, and the burden

of safekeeping of the data is with that trusted party. In blockchain, more parties are forced to be trusted. Having a default trusted entity participating reduces the risks that one of the parties will misbehave. At the same time, the trusted parties do not become the sole keeper of the data, and they can still audit the information, providing a level of fault tolerance and distributed access of information that was not available before.

BLAIR: It is possible to remove the need for a trusted third party, yes. However, cutting a third party out of the process is not always a necessity for a strong blockchain. Some people believe that blockchain is exclusively leveraged to disintermediate someone else in an industry or capital value chain. While many blockchain projects have started with that idea, it's simply not the only case for work and disruption in the space.

We've made recent announcements about work we're leading around responsible sourcing of minerals. With companies like RCS Global, Ford, LG Chem, and Volkswagen, starting with cobalt and leveraging blockchain to work with key certification bodies, mining companies and brand owners across the supply chain deliver better insight into what's happening onsite at the level the work is being done to ensure materials are responsibly sourced.

COSTELLO: While there are limited and interesting examples where removing a governing authority would be useful, the vast majority of cases seen thus far are closed environments that still have some form of trusted authentication by named parties, not random miners. That may be more of a transitional user-adoption aspect, a feature that comforts potential users in some cases. But there are models where a finite group of validators provides an enhanced security to the model.

RAMADOSS: Crypto enthusiasts envision a world where cryptocurrencies will be adopted everywhere in the

future. Today, only a handful of merchants accept bitcoin and other cryptocurrencies. As a result, a third party, for example, a cryptoexchange, is needed to convert these cryptocurrencies to fiat for real-world transactions (food, transportation, housing, and so on). When blockchain-based cryptographic tokens are used to represent fractional ownership of a real-world asset, there is a need for a trusted third party that serves as a custodian for the asset. In the case of a stablecoin, fiat currency is held under a trust, and an administrator (a trusted third party) is needed to oversee the trust. For tokenized crowdfunding of a real estate asset, a manager (a trusted third party) is needed. In many business use cases, we are seeing reintermediation (with new intermediaries) instead of disintermediation.

COMPUTER: Could a blockchain solution result in higher costs in some cases? For example, blockchain cannot prevent human error, so if a shipment is incorrectly labeled (either inadvertently or maliciously), might it be more expensive to correct this after discovery in a DLT application?

YAGA: Could it be possible? Sure. As with most real-world automated systems, they need frequent monitoring and quality checks. A blockchain can only enforce the rules encoded within it. If someone maliciously labels an empty box and ships it, there's nothing a blockchain can do.

Multiple independent and automated sensors recording data in addition to human-based data may be able to help detect errors. But, again, malicious attempts to fool sensors into giving good data to the blockchain may be a problem.

STAVROU: Yes, there are many cases in which misuse of DLTs can incur high maintenance costs without a return on investment. The case of a label or data element that needs to be modified can be burdensome, especially when the entire system is within a trusted

boundary. However, being able to track information among untrusted parties, including shipment between different companies using a DLT, has benefits that can counterbalance the difficulty of modifying records that will require an additional DLT transaction. Ultimately, during system design that includes consideration of day-to-day operations, one needs to consider if DLT brings value or increases the costs disproportionately and can be easily replaced with a trusted distributed database.

BLAIR: Yes, which is why spending time on the front end with an experienced partner and your potential network or ecosystem peers before you've invested to build something, to make sure you've selected the right technology platform to deliver your desired business results, is critical. It's not about just having a business case, that's the most basic of criteria. It's leveling up into a strategy around operational governance and network orchestration. Do you understand the value levers for yourselves and others in your potential network? Can you think through what incentives look like, not just for current competitors in your ecosystem but for future competitors entering the space?

RAMADOSS: Blockchain/DLT is an append-only immutable ledger that provides trust to transactions recorded. However, this trust cannot be extended to the physical world. For example, blockchain and Internet of Things (IoT) technologies can be used for tracking of shipments from the manufacturer to the distributor. IoT devices equipped with radio-frequency identification, near-field communication, or Bluetooth can be used to collect sensor data for monitoring a range of critical parameters from temperature to container weight. However, blockchain cannot prevent human errors, for example, the incorrect labeling of products or malicious counterfeit. We still need to have a certain level of trust in the manufacturers.

COMPUTER: Related to the above, might blockchain applications result in inflated confidence in the security of a process, making it easier for someone to commit fraud in the unavoidable human parts of the process?

YAGA: Yes. Security is often front and center with most blockchain discussions and presentations, discussing how it is more secure than nonblockchain systems. However, it's still software, and all software contains bugs and errors.

A lot of blockchain software is open source. We often cite open source software as being less buggy than proprietary software, for example, the more eyes on it, the better. But longstanding bugs in widely used open source Internet technologies are quite the norm. (Heartbleed comes to mind.)

An example of the inflated confidence would be when the Ethereum blockchain suffered from what some would label an attack; others would say clever programming. When the Decentralized Autonomous Organization smart contract lost 3.6 million ether, the attacker realized it could exploit the smart contract in accordance to its own rules and what was allowed by the system. The often-touted phrase that "code is law" would make one think that if you can execute it, it's within the rules. However, Ethereum rolled back the effects of the attack. Exploiting human error will be just as prevalent as with nonblockchain systems.

STAVROU: It really depends on the specific application and implementation of the blockchain technology and what the goals are. It is certainly possible that DLTs can introduce failure scenarios that were previously not feasible.

BLAIR: I don't agree with the idea that blockchain results in an inflated sense of confidence in the security of a process. I do believe, and have seen first-hand, projects I've led and been a part of that permissioned blockchains create confidence in the

enterprise for teams operating and transacting in this tamper-evident digital platform.

RAMADOSS: Yes, it is possible to use blockchain as marketing jargon to inflate confidence in the minds of consumers. We still need to rely on the producer's trustworthiness during the preparation and packaging of the products. As an example, it is possible to track a bottle of olive oil from the manufacturer to the store using blockchain and IoT. However, we would still need to rely on the manufacturer's certification regarding the purity and percentage of mixing of olive oil from different sources.

COMPUTER: What about the privacy implications of DLT? If transactions are impossible to remove, how do you meet the requirements of General Data Protection Regulation (GDPR) and other rules allowing consumers to have their private data deleted?

YAGA: I am not completely sure since it may be difficult to determine what constitutes people's private data when within a system they cannot control.

What if their private data means anything personally identifiable? Then by not storing personally identifiable information on a blockchain. Even encrypted data have a life span and will eventually become decryptable, either by flaws found in the algorithm or advances in computing power or even theft/loss of decryption keys.

If their private data means the above and then any interaction the person has made within your system? Complying with GDPR may be impossible depending on how one defines private data. It might be easier to exclude all entities (businesses, citizens, residents, and so on) under the protection of GDPR from using your system than trying to accommodate GDPR.

STAVROU: While most of the current DLT designs keep data unprotected and public in the DLT, there

are ways of shielding data within a blockchain, either by creating smart contracts around them or storing them on side chains or other side permission-based databases that can safeguard the information. In other words, the DLT becomes the pointer to the external data instead of the actual storage of the data. Without those new designs, the original DLTs are not GDPR compliant, and they offer very little protection for privacy and data safeguards.

BLAIR: We recently published a white paper on blockchain and GDPR where we talk about the synergies and challenges and reality that these two initiatives are aligned in a number of areas including the principles of secured and self-sovereign data (individuals in charge of their data). My colleague Bertrand Portier, who coauthored this article, points out that, in general, it is recommended to not store personal data on chain. The data that goes on chain is the record that a valid and successful transaction occurred. The entities involved in the transaction or any information that could lead to their identification doesn't have to be stored on chain. Instead, personal data that needs to be accessed can be stored in a side database that is private to only the interested entities and is not immutable (for example, Hyperledger Fabric Private Data Collection). This way, the personal data are still provided access to using blockchain protocols (for example, gossip dissemination) and a record of the data access transaction exists on the blockchain, but no personal data are on chain and personal data can be forgotten (erased).

COSTELLO: Fascinating question. The GDPR right to be forgotten is absolutely not possible in these models unless the creators/validators are abstracted. But does the DLT live within the authority of these governmental/regulatory bodies, or are they outside and therefore indifferent to these laws/statutes?

RAMADOSS: The privacy implications of blockchain/DLT depends on whether the data are stored in a public blockchain or a private blockchain. Yes, it is not possible to remove data stored in a blockchain as it is fundamentally designed as an append-only ledger. The current public blockchains will not meet the GDPR requirements. Currently, the European Commission is conducting research on this topic.

COMPUTER: Smart contracts are touted as a way to execute transactions automatically, but they are really just software. Does it make sense to entrust millions of dollars to self-executing processes, when it may be difficult or intractable to correct the results?

YAGA: We trust the majority of our lives to digital and increasingly automated processes. Nearly everything that is manufactured has some level of automation during its creation, from food, life-saving drugs, automobiles, and electronics.

The difference may be that those real-life objects have quality assurance, humans checking that the products meet specifications and can prevent the products from getting to consumers. Often, manufacturing has the same issues as a blockchain, since things cannot be unmade (you cannot deconstruct a chicken nugget once it's made), and if defects are found they must be discarded.

Perhaps, for certain transactions (for example, transfers in the millions of dollars) there is a human in the system. The smart contract will send money to escrow and will be released (or returned) after a human review. It would need to be a cost/benefit analysis: how much are you willing to trust to automation?

STAVROU: The principle behind smart contracts is both theoretically and practically sound. However, some of the implementations fall short of the expectations for fault tolerance and bug-free operation similar to many

software systems that we have in place now. While the current practices are deficient, there is certainly a lot of history behind software fault tolerance that, if put in place, can allow the secure and safe operation of software systems including smart contracts. The other aspect that is causing the issues is the automated nature of the processes that needs to be replaced by human-assisted approvals putting humans in the loop when transactions are critical in value or volume and need to be supervised. Being able to put the human back on the loop in DLT systems is crucial if we want these systems to have wide deployment and acceptance.

BLAIR: We already trust software today to execute work in financial and other systems, so in that sense we're not crossing the chasm in the Enterprise with blockchain. Also, correcting transactions can be made on the blockchain; it doesn't delete the previous, which is seen as a positive for many as you can begin to analyze and understand patterns. Also worth mentioning is that a database of today may not keep a record of all of transactions whereas blockchain automatically does.

COSTELLO: The inability to refine the rules model without terminating the model is a significant problem for any long-term scenarios. However, short-term, discrete, and definable end-state models (few actors, few rules, and so on) do work well and allow for refinement of the next wave.

RAMADOSS: Public blockchains are designed to transact with anonymous parties. Each account is associated with a public key and a private key. The private key must be kept as a secret just like the bank PIN. Significant crypto-holders/investors transact with blockchain through a cryptoexchange, which holds the private key information. The security breach of cryptoexchanges and stealing of users' cryptocurrencies is an ongoing issue. Private

blockchains are designed to transact with known parties. It is possible to transact and run self-executing processes that involve millions of dollars. Large banks are looking at blockchains for interbank transactions.

COMPUTER: Where are we on the Gartner hype curve for cryptocurrency and for other applications of DLT? Have we passed the peak of inflated expectations?

YAGA: Last I saw it, they replaced cryptocurrency with blockchain on their curve. I would say that it's likely in the trough of disillusionment. During this past year, I have seen more negative articles questioning blockchain's usefulness. This is fine and should not be used everywhere, but in the beginning and expansion phases of any technology this is what tends to happen. Blockchain will find great applications, ones that fit the technology perfectly and make sense.

STAVROU: I believe we have passed the peak of inflated expectations, and we are at the trough of disillusionment territory.

BLAIR: I think we're getting there, yes. What I've seen is that 2016 was the year of the blockchain PoC. In 2017 and 2018, we saw a shift in focus to broaden the network, ecosystem, and partner play, and in 2019 we've seen a blockchain focus set in for our top clients in one or two key areas of value versus 10 pipe projects with unproven and unvalidated life span. We're seeing energy and investment aligned mainly to the projects with the best chances for success at scale and with thoughtfulness around governance, membership, market incentives, and network orchestration metrics for success.

COSTELLO: I believe we're just passing the peak of inflated expectations. It is hard to tell how much air will be let out of the wide array of dreamy visions and what the bottom will look like.

RAMADOSS: Between 2014 and 2015, Gartner marked cryptocurrencies in the peak of the inflated expectations segment of the hype cycle. In 2016, Gartner started to use the term *blockchain* in its hype cycle, which is an acknowledgment that blockchain is more than cryptocurrencies, with the introduction of smart contracts. Between 2016 and 2018, Gartner moved blockchain from peak of inflated expectations over to trough of disillusionment. However, Gartner added blockchain for data on the innovation trigger segment of the 2018 hype cycle. We can say that blockchain is still at the hype phase and has not passed the peak of inflated expectations.

COMPUTER: Blockchain was originally developed for cryptocurrency, and a few firms have tried accepting bitcoin. But bitcoin and other cryptocurrencies have lost 80% to 90% of their peak value as of this writing, and they continue to be highly volatile but with an overall downward trend. Many financial experts argue that they will eventually be worth little or nothing since they have no intrinsic value and are not guaranteed by any government. Do you think bitcoin and other cryptocurrencies will eventually fade away?

YAGA: Many cryptocurrencies were founded specifically to have a currency that was not controlled or guaranteed by any government and will likely always have some value. They may fade away from the public perception, but, due to their decentralized nature, I do not think they will ever disappear since the most passionate users can keep the systems alive.

STAVROU: It is not clear because many applications use them to piggy-back their transactions so their value is not necessarily defined directly by their own transactions but from transactions of other instruments that use bitcoin (primarily) and others as a means to distribute and validate their transactions.

DISCLAIMER

Certain commercial entities, equipment, or materials may be identified in this document to describe an experimental procedure or concept adequately. Such identification is not intended to imply recommendation or endorsement by NIST, nor is it intended to imply that the entities, materials, or equipment are necessarily the best available for the purpose.

For instance, Elastos is one of these systems that use bitcoin and others to maintain the validity of their DLT.

BLAIR: The token economy is still in its infancy overall, but we're seeing and well down the path of @ IBM are some incredible opportunities in this space. As an example, we've launched a blockchain-based payment solution called IBM Blockchain World Wire, which uses Stellar's protocol to clear and settle cross-border payments in near real time. Stellar can handle exchanges between fiat-based currencies and digital assets. Using this protocol, IBM and our partners are creating the potential to change the way money is moved around the world, helping to drastically improve international transactions and advancing financial inclusion in developing nations.

To use the new payment system, two financial institutions have to agree on the currency, a stablecoin or any digital asset, to be used as a bridge asset between any two fiat currencies. The companies will use their existing payment system, connected to World Wire's application programming interface, to convert the first fiat into a digital asset. World Wire will then convert the digital asset into the second fiat currency simultaneously, completing the transaction. The details of the transactions will be recorded onto an immutable blockchain for clearing. Net is that we will continue to explore use cases with business networks that we have developed, as a user of the token. We see this

as a way of bringing financial settlement into the transactional business networks that we have been building.

COSTELLO: I believe cryptocurrencies will only be interesting to gamblers, tax evaders, and people getting out of crashing currencies with no access to other tangible government-backed currencies. I don't think they'll disappear, but I don't see them replacing government-backed currencies for primary life/existence.

RAMADOSS: Bitcoin and cryptocurrencies are speculative investments and thus are highly volatile. However, stablecoins backed by fiat currency and tokenized assets are expected to address the volatility issue. In 2018, the number of stablecoins increased from four to 20. In 2019, many projects issued asset-backed tokens (for example, gold, real estate). Many banks and governments are working on issuing stablecoins so I strongly believe that cryptocurrencies will continue to thrive as large corporations and central banks are swiftly entering this space.

COMPUTER: Given that blockchain is being explored for use across virtually every industry, what kinds of regulatory oversight is going to happen in those industries that are heavily regulated, such as health care, finance, drug discovery and production, food production, and so forth?

YAGA: Likely the same amount of oversight that happens now, but it could be done more frequently or in real time. Oversight committees could view blockchain data as a data stream to analyze and look at things as they happen, rather than on an ad hoc or annual basis.

STAVROU: The DLTs that are currently developed are far from being able to directly support the regulated environments that many industries require, both in terms of integration and support of existing regulatory systems.

New regulations and new technologies will fill those gaps. Thus, while DLTs have properties favorable to regulation, they do not necessarily meet those regulations when it comes to their own operation and day-to-day transactions.

BLAIR: What we're seeing in the industrial market today, for example in the heavily regulated chemicals and petroleum space, is that new regulatory processes will likely be led (and likely funded) by business ecosystems to drive more efficient protocols and interactions with business through this enhanced visibility. That being said, we have seen many regulators who are curious and energized observers at this juncture and many who are keen to participate in the design discussions that may impact the future of work and key functions in their space.

COSTELLO: I originally expected (irrationally) that governments would get ahead of the industries and jump in where they could logically contribute or benefit by building citizen-oriented DLT systems (voting, public interaction, and so on). The reality is that most governments (municipal, state, and federal) are too broke or slow to be able to build any substantial applications in the DLT space (they can barely fund the antiquated systems they currently run). So how will they handle performing forensics or auditing of DLT systems (in response to critical issues and/or opportunities)? Probably like they always do; legislate it to a crawl until they can find a way to monetize it for taxes.

RAMADOSS: Finance and banking industries were the early adopters of blockchain. The R3 consortium, with more than 200 financial institutions, developed the Corda blockchain platform that is being used in finance and commerce. Other industries, such as energy, health care, food production, and so on, will face a lot of regulation challenges from their respective regulatory bodies.

COMPUTER: Blockchain has been suggested to find applications in virtually every application domain. But what is the most surprising, realistic application that you see, and what are the benefits there?

YAGA: The most realistic application that I have seen is using a blockchain to track where donated money is spent. Regardless of the application (charity or political), lots of people donate money, and that is the end of their knowledge of what happens. By tracking it on a blockchain, it could be possible to see where their money is spent. Once a system is in place to trace where money is spent, it could be enhanced to allow people to decide where their donations are spent by providing categories of spending and giving donors a choice. The benefits would be to give both transparency and choice to the donors, which would in turn bolster donations. There is an added benefit that it could help to reduce fraud, since the trail of transfers would be recorded and can be audited at any time.

STAVROU: There are clearly applications in the financial industry, health care, and supply chain. I can pick the clinical trials application that seems to be gaining steam and being part of the IEEE standards process. See

- ▶ https://www.healthit.gov/sites/default/files/1-78-blockchainandhealthitalgorithmsprivacydata_whitepaper.pdf,
- ▶ <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5676196/>,
- ▶ <http://www.clinicalinformaticsnews.com/2018/09/19/blockchain-in-clinical-trials-a-new-era-for-our-data.aspx>,
- ▶ <https://clinicaltrials.gov/ct2/show/NCT03479034>.

BLAIR: That's an easy one actually. Today, IBM has a large number of resources responsible for keeping our supplier information current across not only

our enterprise resource planning but across a number of other supporting applications (and have ~15,000 suppliers globally). This supplier information is only as current as our last inspection, so it can be behind the curve in terms of the real-time insight required to make decisions. We feel this particularly with our Tier 2 and 3. What we've done to solve this challenge is create a LinkedIn-like experience with blockchain for buyers, such as ourselves and our suppliers, such that a supplier can surface its digital identity and other info one time to the blockchain network, and IBM and whomever else they do business with that they give permission to can access that information real time. Everything from key leadership, financials, certifications, and other specifics we require of our suppliers to share. We call this our trust your supplier blockchain network, and we've just made this commercially available in the second quarter of this year. The pilot we ran with 40 of IBM's key suppliers was so successful, in fact, that our chief procurement officer is now implementing this for U.S. suppliers in 2019 and for our global suppliers starting in 2020. We will achieve immediate real-time access to supplier data at a fraction of the cost, a 70–90% reduction in cycle time to onboard new suppliers and a 50% cost reduction for supplier onboards. For our suppliers, this is their feedback: a 50% reduction in administrative cost for maintaining status and collateral for buyers, accelerated onboards, and improved discovery for buyers on the network.

COSTELLO: We're not in the gambling space, but it appears to have quite a lot of potential compared to all other endeavors we've seen. The bettors can remain anonymous, the transaction could be tax free (invisible but probably not legal), and all funds would be certain on both sides of the event.

RAMADOSS: A wider adoption of blockchain in various application domains requires solutions or improvements in

the areas of scalability, interoperability, and governance. Currently, there are several interesting projects underway, for example, banking for unbanked, personal identity, data privacy, land registry, and so on. These projects are developing DApps on public blockchains to solve socioeconomic problems and still have a long way to go for adoption. In the private blockchain space, leading cloud service providers, such as Alibaba, Amazon, Baidu, IBM, Microsoft, Oracle, and Tencent, are offering blockchain-as-a-service platforms. It is interesting to see large tech corporations that are moving into this space and developing blockchain-based solutions to improve efficiency in the financial market, supply chain, trade, and so on.

COMPUTER: Forecasting 10 years into the future, discuss the status of blockchain in the global economy at that time.

YAGA: I hope by then we will have found the perfect application for blockchain technologies. People will not discuss blockchain technology as a major selling point of their application, in the same way that people do not discuss the fact that their application is TCP/IP enabled.


STAVROU: DTLs will be part of (some) industrial applications that demand transparency, auditability, and immutability and involve parties with mutual distrust (or lack of trust).

BLAIR: Blockchain will go from an emerging technology to an existing technology. It will be one of the overwhelming infrastructures for collaborative platforms. Where time and quality and performance constraints intersect, blockchain offers an exciting and open alternative to create and learn about and deliver real business results.

COSTELLO: There will be some form of small cryptocurrencies in use around the world (far fewer than today). There will be limited applications across a few industries or governmental agencies

and perhaps a very few that will be heavily engaged. The deeper understanding and use will be hidden from the typical consumer or business executive, like Linux is hidden within the devices those people use every day. They'll know it is out there, they won't know how it works, and they won't really care.

RAMADOSS: In the next five to 10 years, tokenized assets, equity, and stocks and bonds issued on blockchain will revolutionize the capital market and enable cross-border participation. In the enterprise space, blockchain will see a strong adoption in many industries that involve multiparty transactions and become an invisible technology in many cases.

 Our experts are in general agreement on most aspects of DLT. It seems clear that blockchain is like many other new technology areas. There was a great deal of hype and overconfidence at first, but this is now moderating to some extent, and there are some hints at success. Especially for digital assets, blockchain systems can improve the speed and auditability of transactions, and successes include asset tracking and account reconciliation. But there is still a great deal of confusion as to where a blockchain solution makes sense and where a conventional distributed database would work as well or better.

Tradeoffs are always part of engineering, and blockchain is no different. Some of our experts suggested that not only is it impossible to achieve all three of the properties faster, better, and cheaper, in some cases, blockchain solutions may provide only one. While blockchain is often promoted as a way to avoid any dependence on third parties, there was consensus that this is not always possible and that users should be careful about trying to extend blockchain trust to the physical world. In real estate and many other areas of commerce, the law makes third-party involvement

unavoidable, but this third-party reliance may take different forms with DLT. The role of government in this area is evolving and may require some time before answers are clear.

Another concern regarding law and regulation is consumer privacy. Recent legal developments, such as GDPR, have privacy rules that are incompatible with most DLT. While DLT could assist privacy in some ways, putting users more in charge of their data, our expert comments suggest that privacy may be one of the most difficult problems in applying DLT. Most blockchain solutions to privacy are based on not using blockchain for any private data. Yet, under GDPR, even partially anonymized data must be considered privacy sensitive. This constraint raises questions regarding the value of DLT if most data must be kept off blockchains.

Another very difficult problem is the use of smart contracts, which are simply computer programs that may, of course, contain errors and security vulnerabilities. With existing data-management methods, fraudulent transactions can usually be reversed, unless the stolen funds have been converted into assets that are easy to hide and transport. With DLT, anonymous transactions on blockchains can magnify the risk that funds will be irretrievable. Determining how to include humans in smart contract-based processes is another problem where research was suggested.

Blockchains and DLT have been surrounded by hype and often wild claims for several years. Separating facts from nonsense can be a challenge in this environment. We hope that this article will contribute to

understanding this often confusing and misunderstood new technology. **□**

REFERENCE

1. R. Kuhn, D. Yaga, and J. Voas, "Rethinking distributed ledger technology," *Computer*, vol. 52, no. 2, pp. 68–72, 2019.

RICK KUHN is with NIST. Contact him at kuhn@nist.gov

JEFFREY VOAS is with NIST. Contact him at jeffrey.m.voas@gmail.com.

PHILLIP LAPLANTE is with Penn State University. Contact him at plaplante@psu.edu.



Call for Articles

IEEE Pervasive Computing

seeks accessible, useful papers on the latest peer-reviewed developments in pervasive, mobile, and ubiquitous computing. Topics include hardware technology, software infrastructure, real-world sensing and interaction, human-computer interaction, and systems considerations, including deployment, scalability, security, and privacy.

Author guidelines:
www.computer.org/mc/pervasive/author.htm

Further details:
pervasive@computer.org
www.computer.org/pervasive

IEEE pervasive COMPUTING
 MOBILE AND UBIQUITOUS SYSTEMS

Digital Object Identifier 10.1109/MC.2019.2932253