AI and Blockchain: A Disruptive Integration

Thang N. Dinh, Virginia Commonwealth University

My T. Thai, University of Florida

AI and blockchain are among the most disruptive technologies and will fundamentally reshape how we live, work, and interact. The authors summarize existing efforts and discuss the promising future of their integration, seeking to answer the question: What can smart, decentralized, and secure systems do for our society?

AI and blockchain are among the key drivers behind innovation today. Both are introducing radical shifts in every aspect of our life and predicted to contribute trillions of US dollars to the global economy. The future is here, with autonomous cars and charming assistants who can make appointments on your behalf in natural conversations.[1] And the arrival of new content and economy sharing platforms will mean that users will no longer be forced to trust "unreliable middlemen" such as Facebook, Yahoo, and Equifax. So what would happen if we were to combine these two disruptive technologies? After introducing each technology, we share our vision of their combined future.

AI, as defined by Marvin Minsky and John McCarthy—the fathers of the field—is any task performed by a program or a machine that seems to require intelligence. AI systems often exhibit the following behaviors associated with human intelligence: planning, learning, reasoning, and problem solving, as well as social intelligence and creativity. The recent resurgence in AI is fueled by breakthroughs in machine learning, especially within the field of deep learning. It has also been driven by the explosion in available data, making the training of machine learning algorithms more effective. Besides bringing many exciting advancements, such as self-driving cars and delivery robots, AI also causes a series of concerns, from the creation of fake news—such
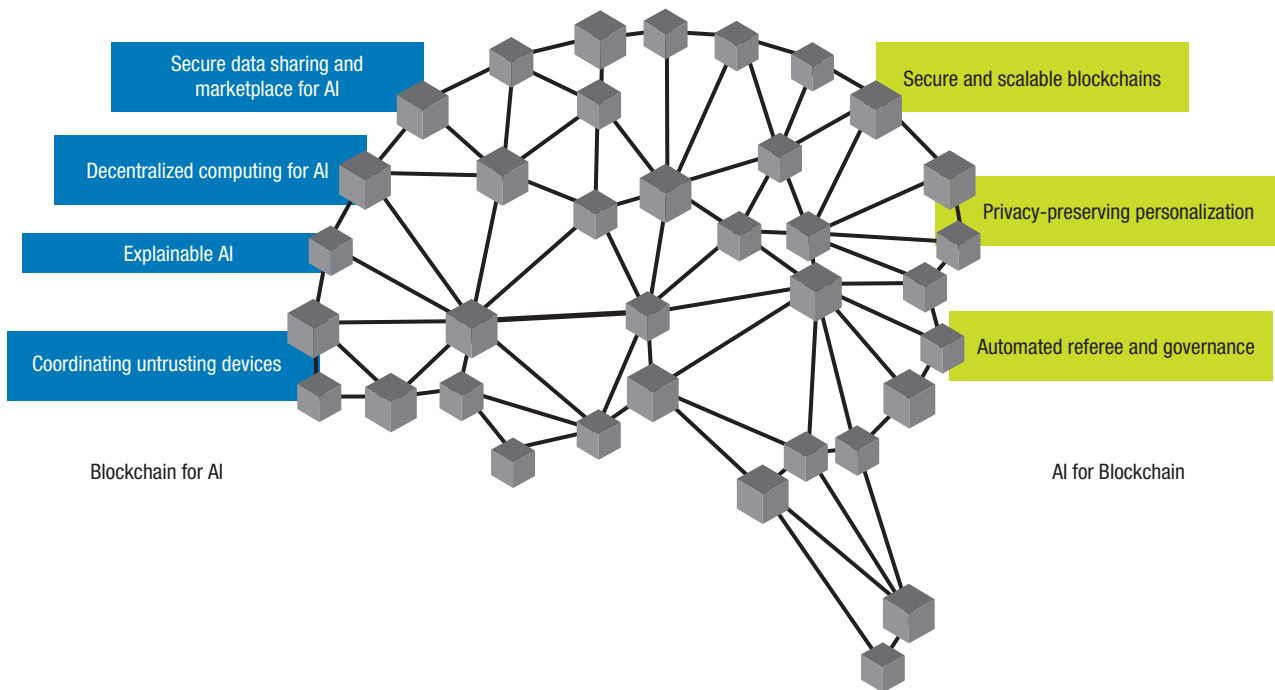
FIGURE 1. The integration of AI and blockchain: (a) blockchain for AI, and (b) AI for blockchain.

as fake and realistic photos, voice, and adult films[2]—to the invasion of privacy.[3] There are also concerns about the monopolization of AI power by a few big players, such as Google, Microsoft, and Amazon, because of high barriers to acquiring data, talent, and computing resources.

BLOCKCHAIN'S ADVANCE

A blockchain is a public ledger, shared and agreed on by all users in a distributed network. Data records, for example, transactions, are stored in blocks together with hash values and timestamps. Every block is connected to the previous one, creating a chain (hence, the name). One key feature of blockchain is immutability; that is, it is almost impossible to modify any information without having network consensus.

Depending on the consensus protocol, that is, how the blocks are created, blockchain technologies are classified into two groups. In *proof-of-work* (POW) blockchains such as Bitcoin[4] and Ethereum, users—called miners—participate in a mining process to solve a computationally hard problem to create a new block. The miner who won the right to create a block earns a block reward and collects the transaction fee. POW protocols are, in general, energy-consuming. Also, they are subjected to majority hash rate attacks when the block reward reduces, as seen in recent events with Bitcoin-Gold, Verge, ZenCash, and other POW-based cryptocurrencies.[5] The new generation of protocols use *proof-of-stake* (POS) blockchains, in which there is no energy-consuming mining process. Instead, participants' chances

of creating a block increase with the amount of coins—the stake—that they have. The most notable among this group are Nxt, Peercoin, delegated EOS, bitcoin mimic Ouroboros,[6] iChing,[5] and a recent hybrid POS+BFT Algorand[7] from MIT.

Minus the current hype surrounding cryptocurrencies, which distracts from blockchain's true potential, blockchain technologies indeed are powering a new serverless Internet and decentralized web future in which "users are in control of their own data, identity, and destiny."[8] They will also revolutionize the healthcare system such that we will be able to track how our data records are used and have our own data copyrights. With the promising future, we will be given alternative, if not better, choices for every platform we know today, whether it is

Facebook, EBay, Uber, Airbnb, or even the energy market.

THE DISRUPTIVE INTEGRATION

On one hand, blockchain suffers from weaknesses such as security, scalability, and efficiency. On the other, AI has its fair share of issues with trustworthiness, explainability, and privacy. The marriage of these two technologies seems inevitable; they could complement each other to revolutionize the next digital generation. As shown in Figure 1, blockchain will bring trustlessness, privacy, and explainability to AI; in turn, AI can help build a machine learning system on blockchain for better security, scalability, and more effective personalization and governance.

BLOCKCHAIN FOR AI

Blockchain can power decentralized marketplaces and coordination platforms for various components of AI, including data, algorithms, and computing power. These will foster the innovation and adoption of AI to an unprecedented level. Blockchain will also help AI's decisions be more transparent, explainable, and trustworthy. As all data on blockchain is publicly available, AI is the key to providing users with confidentiality and privacy.

Secure data sharing

One of the driving factors behind the current AI revolution is the massive amount of data available for research, development, and commerce. Data is the new gold in today's data-driven economy. Yet, there are high barriers to getting access to this gold. First, it might be difficult to obtain sufficient data for your training models unless you are with one of the big players,

such as Facebook or Google. This ultimately deters the competition among AI researchers and companies that is needed to boost AI. Second, privacy is a critical and growing concern after a series of leaks and misuse of personal data. Notably, the recent Facebook scandal, in which 50 million users were profiled and targeted without consent by Cambridge Analytica, a political third-party firm. This targeting behavior is disturbing, and was compared to "a customized whisper campaign: Groups both ethical and malicious can divide Americans, whispering into the ear of each and every user, nudging them based on their fears and encouraging them to whisper to others who share those fears,"[9] by University of Maryland cybersecurity professor Timothy Summers.

Blockchain can encourage data sharing because it provides transparency and accountability regarding which users' data is accessed, when, and by whom. As blockchain puts the control of data back into users' hands, they will have more confidence in sharing data and knowing that their data will be used properly to provide better personalization or for other good causes. The potential impact of this is tremendous. For instance, doctors and researchers could access (anonymized and huge) medical records and cases, substantially expediting the discovery of cures for diseases and the development of better treatment paradigms and medical procedures. Patients with rare diseases, especially, would find new hope, as doctors could access similar cases from all around the world. Some part of that vision has become reality with development efforts from the Centers for Disease Control and Prevention and many other blockchain-based health companies.[10]

Your data, your price

Beyond sharing and controlling your own data, blockchain technologies could let you sell your data via smart contracts. This enables data marketplaces without middlemen, making them more secure and private. Such marketplaces will lower the barrier for smaller players, leveling the playing fields and thus fostering innovations. Through technology such as zero-knowledge proofs, businesses and researchers might search for relevant information without knowing the details of the data, or the identity of the data owners. We cannot stress enough the huge impact of being able to filter out and locate the data you want while keeping users' privacy intact. It will possibly even ignite another round of AI evolution. For example, Nebula Genomics, a start-up cofounded by Harvard University's George Church, provides a marketplace that connects people who want their genomes sequenced with companies who want this data.[11] In a similar effort, Longenesis provides a platform to share and monetize life data such as medical record and health data.[12]

Selling your spare computing power

Blockchain can leverage more distributed computing power for AI through a decentralized market for computing power, that is, blockchain-based cloud computing. AI developers can now make use of millions of GPUs from gamers to prepare, model, train, and deploy their machine learning algorithms. Gamers, whose GPUs are often utilized for a small fraction of time, can list their computing time for bids in the form of AI smart contracts, and get paid.

If you are thinking that this idea of selling spare computing power is not new, you are right. Grid computing—a once very popular idea—found limited application and was not meant for adoption by the masses. In contrast, today's market for AI-supported cloud computing enjoys numerous applications, as many as AI can power. Further, incentivization via cryptography token payment attracts more users to sell their computing resources.

Coordination of untrusting devices

There is also a bright future for AI on devices, in which untrusting devices, for example, swarm robotics, Internet of Thing devices, or cell phones, will coordinate and make joint decisions.[13] In those scenarios, blockchain will serve as a coordination platform in which adversaries can compromise the security only if they hold the majority. Applications of this paradigm can range from updating software for your refrigerators to coordinating swarm robotics in tactical missions. The dark side of this, however, is that it can be used to maintain commands and controls for botnets and malware programs. Currently, security experts can shut down those harmful programs at once by locating their centralized control center. If they replaced that single point of failure with blockchain, there would be no easy resolution but to kill them one by one.

Explainable AI

Despite the wide success of machine learning in building autonomous systems that are capable of perceiving, learning, and acting on their own, there is reluctance to adopt these systems in practice. One reason is that with machine learning techniques,

for example, deep learning, it is difficult to understand what exactly goes inside the black boxes. Thus, decisions made by those systems are unexplainable to human users and thus cannot be verified or trusted. Hesitation is even higher in the fields of medical research and financial planning, where explainability becomes crucial as wrong decisions could imply loss of life or economic disaster. It is essential that we have an immutable trail to track the development of the data flow and complex behaviors of AI-based systems.

Blockchain can do exactly that, tracking every turn in the data-processing and decision-making chain. Through tracking behaviors of AI-based systems across different data input and

application scenarios, we gain more understanding of and confidence in the decisions made by those systems. Even better, human users will have a clear trail to trace back the machine decision process, making justification of those decisions much easier. Furthermore, it provides insights into tuning those black boxes to balance performance and prediction accuracy with the explainability of the system. In case of unfortunate incidents, these blockchain-based trails will be essential to determine whether humans (and who specifically) or machines are at fault.

AI FOR BLOCKCHAIN

The design and operation of a blockchain involves thousands of parameters and tradeoffs between security, performance, decentralization, and many others. AI can ease those decisions, and automate and optimize blockchain for higher performance and better governance. Moreover, as all data on blockchain is publicly available, AI plays a key role in providing users confidentiality and privacy.

Security and scalability

Unless the adversary owns the majority mining power, blockchain is almost impossible to hack. The applications and functionalities built on top of the blockchain platform are, unfortu-

nately, not as secure. For example, the decentralized autonomous organization (DAO), one of the largest crowd-funding groups with $150 million of a cryptocurrency called Ether, was the victim of a $50 million theft.[14] The hacker exploited several mistakes made in the writing of the smart contracts that allowed repeated transactions to be run that withdrew more money than the fund put in. With the incredible progress made by machine learning, a blockchain governed by an intelligent machine learning algorithm might be able to detect the presence of attacks and automatically

[**UNLESS THE ADVERSARY OWNS THE MAJORITY MINING POWER, BLOCKCHAIN IS ALMOST IMPOSSIBLE TO HACK.**]

invoke the appropriate defense mechanisms. When the damage is unavoidable, the AI might at least isolate the attacked component from the blockchain platform, keeping the rest safe from the attack. A similar AI can be used to govern the blockchain, making it more scalable and robust. For example, when there is a spike in the number of transactions, the AI might be smart enough to increase the block creation rate, which would increase the throughput at the cost of longer confirmation times.

Privacy and personalization

If you worry about whether the next election will be compromised or whether your data is safe on social networks, blockchain is for you. Blockchain can give you back control over your personal data. But it comes with a cost. In traditional centralized settings, such as Facebook, Netflix, or YouTube, collected user information is analyzed to personalize the content for users. That's how you can go to Facebook to find posts from the friends you interact most with, or logon to Netflix and be presented with movies that reflect your taste. Getting back your privacy means no one knows what you like—so you will probably have to scroll through many pages to find relevant content, without the help of automatic customization. But is there a way to achieve both privacy and a personalized experience?

AI comes to the rescue with a new content selection model. A decentralized content provider, for example, a social network on blockchain, can leverage AI on the users' side to personalize content. A machine learning program will run on users' devices to analyze their browsing behaviors and hobbies. Relevant content to the users

will be pulled, rather than pushed, and displayed to users.[15] Note that the whole computation is performed locally—no personal data ever leaves the users' devices. Further, sanitization of users' content preferences may be performed to prevent content providers from profiling users. Thus, this new pulling-based model provides both privacy and personalization at once.

The rise of the machine

Many movies have predicted a future in which machines will rise and govern every aspect of human life. That future, or at least a part of it, is already here. Smart contracts, a type of language, have been deployed on blockchain to resolve contracts among users, deciding who will get paid. For now, however, smart contracts are not so "smart" and limited to only simple forms of contracts.

With the rapid advancement of machine learning, AI will be capable of refereeing more complex situations. Users will eventually be able to resolve on-chain (even off-chain) disputes without going to a court room.[16] After evidence and documents are provided, AI could perform automated arbitration in an unbiased and tamper-resistant manner. All decisions would be data-driven, and, thus, more consistent and justified.

Despite rapid development, both AI and blockchain still have a long road ahead of them. For AI, the most recent development is the announcement of Google Duplex, which can make automatic phone calls on your behalf. It is great, until you read that the scope of the project limits the possible tasks to exactly three: restaurant reservations, hair salon

appointments, and holiday hours. And despite AI's recent, huge advancements in algorithms and the enormous amount of computing power and data, it just cannot keep up with the infinite complexity of the human world. For blockchain, the recent security incidents with Etherum, ZCash, Bitcoin-Gold, and many other cryptocurrencies suggest that it will be some time until we can enjoy both secure and scalable blockchains for real-world applications.

On the road to the future, the companionship between blockchain and AI will provide unlimited innovations and revolutions to our society—perhaps 'til death do them part. ◼

REFERENCES

1. Y. Leviathan, "Google Duplex: An AI System for Accomplishing Real-World Tasks Over the Phone," 8 May 2018, Google AI Blog; https://ai .googleblog.com/2018/05/duplex -ai-system-for-natural-conversation .html.
2. A. Hern, "AI Used to Face-swap Hollywood Starts into Pornography Films," 25. Jan 2018, *The Guardian*; www.theguardian.com/technology /2018/jan/25/ai-face-swap -pornography-emma-watson-scarlett -johansson-taylor-swift-daisy-ridley -sophie-turner-maisie-williams.
3. J. McGrath, "A.I. Will Make Smart Homes Autonomous, But Don't Expect Perfection or Privacy," 8 June 2018, Digital Trends; www .digitaltrends.com/home/ai-will -make-the-smart-home-autonomous -but-dont-expect-perfection-or -privacy.
4. S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," 2008; https://bitcoin.org /bitcoin.pdf.

5. J.I. Wong, "Every Cryptocurrency's Nightmare Scenario is Happening to Bitcoin Gold," 24 May 2018, Quartz; https://qz.com/1287701/bitcoin-golds-51-attack-is-every-cryptocurrecnys-nightmare-scenario.

6. A. Kiayias et al., "Ouroboros: A Provably Secure Proof-of-Stake Blockchain Protocol," *Proc. 37th Ann. Int'l Cryptology Conf.* (CRYPTO 17), 2017, pp. 357–388.

7. J. Chen and S. Micali, "Algorand: Scaling Byzantine Agreements for Cryptocurrencies," arXiv preprint, 2016, arXiv:1607.01341.

8. G. Wood, "Web3 Foundation," 2017; https://web3.foundation.

9. T. Summers, "Facebook is Killing Democracy with Its Personality Profiling Data," 21 Mar. 2018, The Conversation, htttps://theconversation.com/facebook-is-killing-democracy-with-its-personality-profiling-data-93611.

10. M. Mettler, "Blockchain Technology in Healthcare: The Revolution Starts Here," *Proc. IEEE 18th Int'l Conf. e-Health Networking, Applications and Services* (Healthcom 16), 2016, doi:10.1109/HealthCom.2016.7749510.

11. A. Maxmen, "AI Researchers Embrace Bitcoin Technology to Share Medical Data," 9 Mar. 2018 *Nature*; www.nature.com/articles/d41586-018-02641-7.

12. K. Gammon, "Experimenting with Blockchain: Can One Technology Boost Both Data Integrity and Patients' Pocketbooks?," *Nature Medicine*, vol. 24, 2018, pp. 378–381.

13. A. Pentland and E. Castello Ferrer, "Blockchain: A New Framework for Robotic Swarm Systems," Media Lab Research MIT; www.media.mit.edu/projects/blockchain-a-new-framework-for-swarm-robotic-systems/overview.

14. N. De, "Hacks, Scams, and Attacks: Blockchain's 2017 Disasters," 29 Dec. 2017, coindesk; www.coindesk.com/hacks-scams-attacks-blockchains-biggest-2017-disasters.

15. *Basic Attention Token (BAT): Blockchain Based Digital Advertising*, white paper, Brave Software, 13 Mar. 2018; www.basicattentiontoken.org/BasicAttentionTokenWhitePaper-4.pdf.

16. N. Lomas, "What Do AI and Blockchain Mean for the Rule of Law?," 12 May 2018, Techcrunch, https://techcrunch.com/2018/05/12/what-do-ai-and-blockchain-mean-for-the-rule-of-law.

17. L. Fan and H.-S. Zhou, "A Scalable Proof-of-Stake Blockchain in the Open Setting (or, How to Mimic Nakamoto's Design via Proof-of-Stake," 2018; https://eprint.iacr.org/2017/656.pdf.

ABOUT THE AUTHORS

THANG N. DINH is an assistant professor in the computer science department at Virginia Commonwealth University; co-director of Lab-B, an interdisciplinary research lab on blockchain; and co-founder of Fractal Platform, an ecosystem for decentralized applications. His research interests include blockchain optimization, network science, and security. Dinh received a PhD in computer engineering from the University of Florida. Contact him at tndinh@vcu.edu.

MY T. THAI is a UF Research Foundation Professor in the Computer and Information Science and Engineering department, University of Florida. Her research interests include scalable algorithms, big data analysis, cybersecurity, and optimization in network science and engineering, including communication networks, smart grids, social networks, and their interdependency. The results of her work have led to six books and more than 140 articles published in leading journals and conferences, including IEEE MSN 2014 Best Paper Award and 2017 IEEE ICDM Best Papers Award. Thai has been a TPC-chair for many IEEE conferences; served as associate editor for the *Journal of Combinatorial Optimization (JOCO)*, *IEEE Transactions on Parallel and Distributed Systems*, and *IEEE Transactions on Network Science and Engineering*; and a series editor for *Springer Briefs in Optimization*. She was the founding editor in chief of the *Computational Social Networks* journal, and has received many research awards including a UF Provost's Excellence Award for Assistant Professors, UFRF Professorship Award, Department of Defense (DoD) Young Investigator Award, and NSF CAREER Award. Thai received a PhD in computer science from the University of Minnesota. Contact her at mythai@cise.ufl.edu.