Blockchain Smart Contracts, Part 1

Introduction for Accounting and Auditing Professionals

Blockchain smart contract technology is having and will continue to have a significant impact on accounting and auditing. These systems have already been implemented in the Big Four accounting firms and other industry leaders. Given the nascent stage of blockchain smart contract technology, managers within this space are advised to follow the lead of early adopters of this technology. Therefore, it is important for accounting, auditing and IT management professionals to understand smart contract technology and applications and the exponential growth in this area, understand how and why blockchain smart contract technology is so revolutionary, and recommend common approaches developed by industry leaders to help other enterprises in the early stages of adopting blockchain smart contracts.

Definitions

The concept of smart contracts was proposed in 1996, 12 years before Bitcoin was invented by the pseudo-anonymous person (or persons) Satoshi Nakamoto. A smart contract was defined as "a set of promises, specified in digital form, including protocols within which the parties perform on these promises."[1] In the post-Bitcoin world, the term "smart contract" is a bit of a misnomer. It is simply a computer program that is almost exclusively stored on or interacts with a blockchain. Although there is no single agreed-on definition of blockchain, some define it as:

> *[A] distributed, append-only ledger of provably signed, sequentially linked, and cryptographically secured transactions that's replicated across a network of computer nodes, with ongoing updates determined by a software-driven consensus.*[2,3]

A modern blockchain smart contract is defined as a legally binding contract stored on a blockchain that automatically executes outcomes when certain predetermined criteria are met. Some examples of smart contracts that can enforce obligations include automated payment based on terms of agreement—based on sale of copyrighted material, sale of digital assets, and commitments made by executives to shareholders.[4,5] Smart contracts are generally enforceable so long as they follow the basic rules of a standard contractual agreement.[6,7,8] These smart contracts (computer programs) can then autonomously verify, enforce and execute terms

SAMUEL ZARUBA SMITH

Is a Ph.D. candidate at the University of Nevada, Reno (USA) and is associated with the university's center for cybersecurity. He has extensive IT experience as a full-time employee, management consultant and researcher for Bank of America, Microsoft, AT&T and the US National Science Foundation. His research interests include artificial intelligence, blockchain, security and distributed systems.

ANDY GARCIA | PH.D. CPA

Is a professor at Bowling Green State University (Ohio, USA). He has worked for a global accounting firm and a Fortune 500 company as an international auditor. Garcia has authored papers published in the *ISACA® Journal,* the *International Journal of Accounting and Information Management, Research on Professional Responsibility and Ethics in Accounting,* the *Journal of Accounting Education,* and *Internal Auditing.*

"Many see the growth in the adoption of blockchain smart contracts as a continuation of the so-called Fourth Industrial Revolution or Web 3.0."

within a stipulated legal contract.[9, 10, 11, 12, 13] Contract tasks, rules, conditions and stipulations are all agreed on by the various participating parties and then carried out by the smart contract computer program across the blockchain (or potentially any other network, such as a cloud network). **Figure 1** shows how a smart contract operates.

Smart contracts use smart controls, which are automated internal control functions within a blockchain-based network.[14] Examples of smart controls include automated application internal controls systems that may perform identification checks or check policy compliance to reduce liability. Smart controls, when combined with data analytics and continuous auditing and monitoring, can revoke a transaction that is not in compliance with enterprise policy or detect processes that are violating internal business rules. Smart controls can self-adjust to support intelligent, flexible and timely assurance[15]

Many see the growth in the adoption of blockchain smart contracts as a continuation of the so-called Fourth Industrial Revolution (4IR) or Web 3.0, encompassing artificial intelligence (AI), big data, the Internet of Things (IoT), blockchain and other technologies.[16] As increasing amounts of societal data must be analyzed in an iterative, private, secure and time-sensitive manner, blockchain-based technology such as smart contracts may be the best option for large and medium-size enterprises.[17] Leaders of modern enterprises, governments, and nongovernmental organizations should view blockchain smart contracts as an important part of any technology strategy.

Types of Smart Contracts

There are two types of smart contracts: deterministic and nondeterministic. Deterministic smart contracts do not require information from an external party (outside the blockchain), whereas nondeterministic smart contracts do require external information (oracles or data feeds). Deterministic smart contracts may include the transfer of records of property ownership (on the blockchain system) or various on-chain payment transactions.[18] An example of a nondeterministic smart contract is one that requires externally provided data such as geospatial (global positioning system [GPS]) data for the contract to be executed and does not have that information available on the blockchain.

Blockchain Smart Contract Architecture

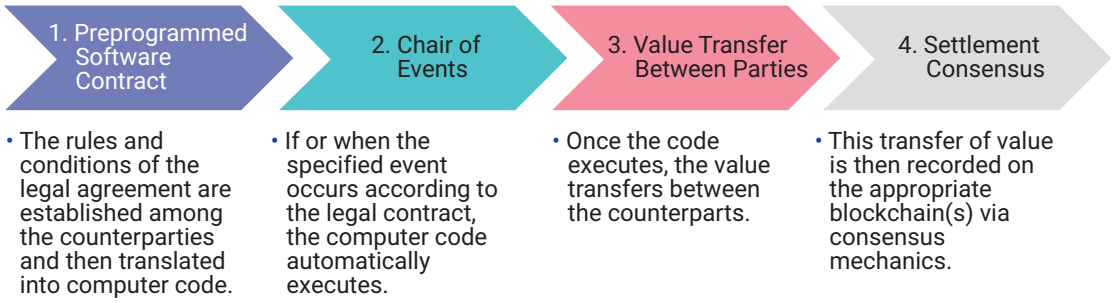
A blockchain entity can be private or public and permissioned or permissionless (**figure 2**).[19] Other blockchain attributes that are important to auditors include trustlessness, immutability (unchangeability), distributed consensus and transparency.[20]

Permissionless Blockchains

A permissionless blockchain has the attribute of trustlessness, meaning that no single blockchain participant can rely on other participants' honesty. On a permissionless blockchain, there are no central authorities or intermediaries, and transaction records are immutable once they are added to the blockchain.[21, 22] On permissionless blockchains, individual members of the network maintain their own identical copies of the blockchain, and all the members constantly synchronize their copies of the blockchain with one another to achieve (distributed) consensus. This guarantees that the

FIGURE 1

Sequence of Smart Contract Execution



data on the blockchain are correct, complete and up to date by means of a transparent process. Even though individual users do not exchange their personally identifiable information (PII) during this synchronizing process, all transactions on the blockchain are transparent (visible) and traceable to the entire network.[23] The typical example of a public permissionless blockchain is Bitcoin or Ethereum.

Blockchain smart contract technology is evolving rapidly, and there are multiple areas in which the permissioned-permissionless distinction may affect smart contract adoption. For example, zero knowledge proofs allow public permissionless blockchains to store data securely and privately, which may increase the adoption of public permissionless smart contract systems. Enterprises that previously rejected smart contracts or other forms of data storage on public permissionless blockchains due to security or privacy issues may be encouraged to reevaluate their understanding of the technology. Zero knowledge proofs—a cryptography technology that allows one party to prove to another party that a given statement is true without revealing any other information about that true statement—and similar techniques are still in the nascent phases of research, and many new open-source projects are addressing this topic in a variety of blockchain ecosystems (e.g., Bitcoin, Ethereum, Filecoin).[24]

"Enterprises that previously rejected smart contracts or other forms of data storage on public permissionless blockchains due to security or privacy issues may be encouraged to reevaluate their understanding of the technology. "

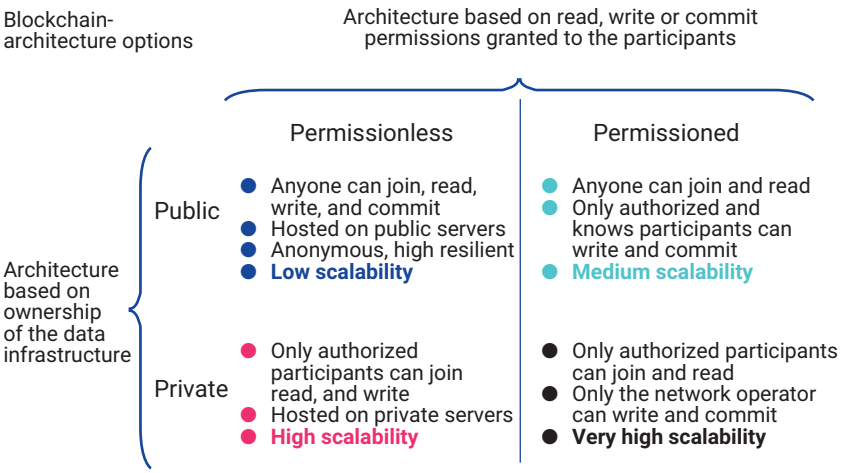
Permissioned Blockchains

Permissioned blockchains are not trustless. Individual transactions are subject to approval by a predesignated authority, and individual transaction records may be changed or reversed if the majority of blockchain members choose to do so. In a permissioned blockchain, trust in the blockchain is based on the credibility of the predesignated authority and the consensus protocol of that specific blockchain's architecture. Permissioned blockchains lack the transparency of permissionless blockchains, as blockchain participants may have only part of the master blockchain record, and some blockchain members are subject to access and control restrictions. Permissioned blockchains may have the characteristics of both public and private blockchains, whereby anyone may join the permissioned network, but only after validation of their identity.[25]

FIGURE 2

Two-by-Two Blockchain Matrix

Most commercial blockchain will use private, permissioned architecture to optimize network openness and scalability.



Source: Carson, B.; G. Romanelli; P. Walsh; A. Zhumaev; "Blockchain Beyond the Hype: What Is the Strategic Business Value?" McKinsey & Company, 19 June 2018, *www.mckinsey.com*. © 2022 McKinsey & Company. All rights reserved. Reprinted with permission.

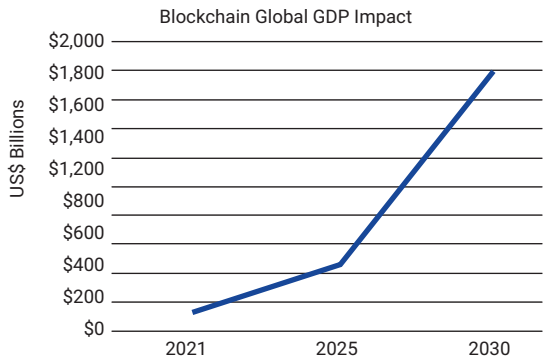
Commonly, permissioned blockchains are more suitable for business and government environments.[26, 27] JP Morgan's banking blockchain is an example of a private permissioned blockchain that enables smart contracts.[28] It represents one of the standard industry implementations of blockchain and smart contract technology. Similarly, the Hyperledger Fabric blockchain—a joint project by Linux Foundation, IBM, Intel, Microsoft and many other enterprises—is a permissioned blockchain that maintains public attributes commonly employed in the open-source software ecosystem.

Expected Growth in Blockchain Technology

Economists expect blockchain and associated smart contract technology to contribute US$422 billion to the worldwide gross domestic product (GDP) by 2025 and US$1.76 trillion by 2030 (**figure 3**).[29]

FIGURE 3

Anticipated Growth in Blockchain Contributions to GDP



The adoption of blockchain smart contract technology has been increasing and is projected to grow at nearly exponential rates. Economists also predict that by 2030, 10 to 15 percent of the world's infrastructure and business projects will incorporate blockchain in some way. Globally, more than 40 million jobs are predicted to be significantly impacted by blockchain technology adoption by 2030.[30] Based on 2018 market cap data, economists predict that by 2030, the top-five uses for blockchain technology (including associated smart contract technology) will be data provenance, payments, identity, contracts and customer engagement.[31] Data provenance is predicted to be the largest area affected by blockchain smart contracts because it includes the entire life cycle of data generation, commonly referred to as data lineage.

Another example of growth is in central bank digital currencies (CBDCs), which have been widely adopted in the financial world, with prototypes currently in place in China, Nigeria and the European Union, and in research and development in several countries including India, the United Kingdom and the United States.[32] CBDCs are expected to be enabled via private permissioned blockchains so that the central bank of a country can maintain control over its monetary policy.[33, 34] More than 60 percent of world governments are conducting studies related to the adoption of CBDCs, including all members of the G20.[35]

A survey of Fortune 500 companies indicates that corporations will spend roughly US$20 billion per year on blockchain and smart contract technical services.[36, 37] The fastest growth in the adoption of blockchain technology is expected to occur in the manufacturing and resources sector, with an estimated 60.5 percent increase in blockchain spending by 2024. The second-fastest growth rate is predicted to be in the distribution and services sector, with an estimated 58.7 percent increase in blockchain spending by 2024.[38, 39, 40] In addition, given that five to 10 percent of all insurance claims are fraudulent, blockchain will greatly reduce the number of undetected fraud cases in a variety of sectors, including those in the public sector.[41] Blockchain smart contracts will revolutionize fraud prevention, and there is a large body of research surrounding that application.[42, 43, 44] Smaller rates of blockchain spending are expected in the professional services, healthcare and retail sectors.

Challenges to Auditors

Permissionless and permissioned blockchains present different sets of challenges to auditors. Due to the lack of a centralized authority to verify the existence, ownership or measurement of transactions recorded on the blockchain, permissionless blockchains may present the most difficult challenges. In addition, there is no centralized authority to report cyberattacks, fraud or other security threats; instead, the community of blockchain participants and the blockchain auditors must rely on one another. Another significant challenge of permissionless blockchains is the need for auditors to be proficient in a variety of blockchain smart contract technologies and their associated consensus mechanisms.[45]

> "Data provenance is predicted to be the largest area affected by blockchain smart contracts because it includes the entire life cycle of data generation."

Auditors and their clients will most likely prefer private permissioned blockchains and associated smart contracts because of their similarity to traditional centralized data storage and legacy IT systems. Existing business networks can be utilized via private permissioned blockchains to meet the demands of privacy and business-to-business coordination. In

LOOKING FOR MORE?

- Read *Blockchain Fundamentals Study Guide. www.isaca.org/emerging-tech-blockchain*
- Learn more about, discuss and collaborate on emerging technology in ISACA's Online Forums. *https://engage.isaca.org/onlineforums*

addition, private permissioned blockchains allow auditors to offer rating services. Finally, auditors themselves may act as the designated authority over a permissioned blockchain so that auditing can be outsourced.[46] The hierarchical structural similarities between traditional, centralized, top-down managerial structures and private permissioned blockchains make the latter the clear choice for traditional industries adopting smart contract technology.

Conclusion

Blockchain smart contracts are evolving rapidly, and while it may be tempting to defer learning about them, this technology is here to stay, and it presents opportunities to those accountants, auditors and financial services organizations that take the time to enhance their knowledge. The exponential growth in an increasing number of open-source projects related to blockchain smart contracts indicate that professionals in the financial services domain need to familiarize themselves with and master this technology.

This information on the smart contracts' origins, definitions, conceptual frameworks, market segments and impact on the auditing profession should help professionals make more informed choices about their future adoption of blockchain smart contracts. Blockchain smart contracts are part of the growing decentralized finance (DeFi) or Web 3.0 ecosystem, and there is an increasing amount of literature on this topic.[47, 48] Understanding the auditing, security and maintenance of blockchain smart contracts is the next step and is discussed the second part of this two-part series, "Blockchain Smart Contracts Part 2, Applications and Recommendations."[49]

Endnotes

1 Szabo, N.; "Smart Contracts: Building Blocks for Digital Market," 1996, *https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart_contracts_2.html*

2 Casey, M. J.; P. Vigna; "In Blockchain We Trust," *MIT Technology Review*, vol. 121, iss. 3, 2018, p. 10–16

3 Sheldon, M. D.; "A Primer for Information Technology: General Control Considerations on a Private and Permissioned Blockchain Audit," *Current Issues in Auditing*, vol. 13, iss. 1, 2019, p. A15–A29, *https://doi.org/10.2308/ciia-52356*

4 Diedrich, H.; *Ethereum: Blockchains, Digital Assets, Smart Contracts, Decentralized Autonomous Organizations*, Wildfire Publishing, Australia, 2016

5 Tapscott, D.; A. Tapscott; "How Blockchain Will Change Organizations," *MIT Sloan Management Review*, vol. 58, iss. 2, 2016, p. 10

6 Drescher, D.; *Blockchain Basics: A Non-Technical Introduction in 25 Steps*, Apress, USA, 2017

7 *Op cit* Sheldon

8 Appelbaum, D.; R. A. Nehmer; "Auditing Cloud-Based Blockchain Accounting Systems," *Journal of Information Systems*, vol. 34, iss. 2, 2020, p. 5–21, *https://doi.org/10.2308/isys-52660*

9 Kiviat, T. I.; "Beyond Bitcoin: Issues in Regulating Blockchain Transactions," *Duke Law Journal*, vol. 65, 2015, p. 569

10 Peters, G. W.; E. Panayi; "Understanding Modern Banking Ledgers Through Blockchain Technologies: Future of Transaction Processing and Smart Contracts on the Internet of Money," SSRN, 18 November 2015, *https://papers.ssrn.com/sol3/papers/cfm?abstract_id=2692487*

11 Tasca, P.; T. Aste; L. Pelizzon; N. Perony; *Banking Beyond Banks and Money*, Springer, Switzerland, 2016

12 Zhang, F.; E. Cecchetti; K. Croman; A. Juels; E. Shi; "Town Crier: An Authenticated Data Feed for Smart Contracts," Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, Vienna, Austria, October 2016

13 Dai, J.; M. A. Vasarhelyi; "Toward Blockchain-Based Accounting and Assurance," *Journal of Information Systems*, vol. 31, iss. 3, 2017, p. 5–21, *https://doi.org/10.2308/isys-51804*

14 *Op cit* Sheldon

15 *Op cit* Dai and Vasarhelyi

16 Schwab, K.; *The Fourth Industrial Revolution*, Portfolio Penguin, UK, 2017

17 Vaghela, A.; A. Suthar; "A Review of Big Data Analysis Using Smart Contract," *Juni Khyat*, vol. 10, iss. 12, 2020, *https://www.researchgate.net/publication/350048650_A_REVIEW_OF_BIGDATA_ANALYSIS_USING_SMART_CONTRACT*

18 Alharby, M.; A. Van Moorsel; "Blockchain-Based Smart Contracts: A Systematic Mapping Study," 26 August 2017, *https://arxiv.org/pdf/1710.06372.pdf*

19 *Op cit* Sheldon

20 Liu, M.; K. Wu; J. J. Xu; "How Will Blockchain Technology Impact Auditing and Accounting: Permissionless Versus Permissioned Blockchain,"

Current Issues in Auditing, vol. 13, iss. 2, 2019, p. A19–A29, *https://doi.org/10.2308/ciia-52540*
21 Crosby, M.; P. Nachiappan Pattanayak; S. Verma; V. Kalyanaraman; "Blockchain Technology: Beyond Bitcoin," *Applied Innovation Review*, iss. 2, June 2016
22 *Op cit* Liu *et al.*
23 *Ibid*.
24 Boneh, D.; "Blockchain Primitives: Cryptography and Consensus," a16z Crypto Startup School, Stanford University, California, USA, May 2020, *https://a16z.com/wp-content/uploads/2020/05/Dan_Boneh-Blockchain_Primitives-1.pdf*
25 *Op cit* Peters and Panayi 2015
26 American Institute of Certified Public Accountants (AICPA) and Chartered Professional Accountants of Canada (CPA Canada), *Blockchain Technology and Its Potential Impact on the Audit and Assurance Profession*, Deloitte Development LLC, Canada, 2017, *https://www.aicpa.org/content/dam/aicpa/interestareas/frc/assuranceadvisoryservices/downloadabledocuments/blockchain-technology-and-its-potential-impact-on-the-audit-and-assurance-profession.pdf*
27 *Op cit* Liu *et al.*
28 *Op cit* Dai and Vasarhelyi
29 PricewaterhouseCoopers, *Time for Trust: The Trillion-Dollar Reasons to Rethink Blockchain*, October 2020, *https://image.uk.info.pwc.com/lib/fe3111707564047570 1c74/m/2/434c46d2-a889-4fed-a030-c52964c71a64.pdf*
30 *Ibid*.
31 *Ibid*.
32 Atlantic Council, "Central Bank Digital Currency Tracker," *https://www.atlanticcouncil.org/cbdctracker/*
33 Sharma, T. K.; "Advantages and Disadvantages of Permissionless Blockchain," Blockchain Council, 2021, *https://www.blockchain-council.org/blockchain/advantages-and-disadvantages-of-permissionless-blockchain/*
34 Sharma, T. K.; "Public vs. Private Blockchain: A Comprehensive Comparison," Blockchain Council, 2021, *https://www.blockchain-council.org/blockchain/public-vs-private-blockchain-a-comprehensive-comparison/*
35 Bank of International Settlements (BIS), "Central Bank Digital Currencies: Foundational Principles and Core Features," 2020, *https://www.bis.org/publ/othp33.pdf*
36 Mitic, I.; "45 Blockchain Statistics and Facts That Will Make You Think: The Dawn of Hypercapitalism," Fortunly, 21 March 2022, *https://fortunly.com/statistics/blockchain-statistics/*
37 Carson, B.; G. Romanelli; P. Walsh; A. Zhumaev; *Blockchain Beyond the Hype: What Is the Strategic Business Value?* McKinsey and Company, USA, June 2018, *https://www.mckinsey.com.br/~/media/McKinsey/Business%20Functions/McKinsey%20Digital/Our%20Insights/Blockchain%20beyond%20the%20hype%20What%20is%20the%20strategic%20business%20value/Blockchain-beyond-the-hype-What-is-the-strategic-business-value.pdf*
38 Carter, R.; "The Ultimate List of Blockchain Statistics (2022)," Findstack, 21 March 2022, *https://findstack.com/blockchain-statistics/*
39 ReportLinker, "Global Blockchain Technology Industry," Globe Newswire, 5 March 2021, *https://www.globenewswire.com/news-release/2021/03/05/2187809/0/en/Global-Blockchain-Technology-Industry.html*
40 Cision PR Newswire, "Global Blockchain Technology Market Report 2021-2027: Market to Reach US$ 30.7 Billion—Blockchain to Improve Transparency, Security, Immutability and Accessibility of Financial Systems and Processes," 12 April 2021, *https://www.prnewswire.com/news-releases/global-blockchain-technology-market-report-2021-2027-market-to-reach-us-30-7-billion---blockchain-to-improve-transparency-security-immutability--accessibility-of-financial-systems--processes-301266654.html*
41 Higginson, M.; J.-T. Lorenz; B. Münstermann; P. Braad Olesen; *The Promise of Blockchain*, McKinsey and Company, USA, March 2017, *https://www.mckinsey.com/~/media/McKinsey/Industries/Financial%20Services/Our%20Insights/The%20promise%20of%20blockchain/The-promise-of-blockchain.ashx*
42 *Op cit* Peters and Panayi 2015
43 *Ibid*.
44 *Op cit* Liu
45 *Ibid*.
46 *Ibid*.
47 Sander, P.; "Decentralized Finance Will Change Your Understanding of Financial Systems," *Forbes*, 22 February 2021, *https://www.forbes.com/sites/philippsandner/2021/02/22/decentralized-finance-will-change-your-understanding-of-financial-systems/?sh=7e950e4f5b52*
48 Economist, "Adventures in DeFi-Land," 18 September 2021, *https://www.economist.com/briefing/2021/09/18/adventures-in-defi-land*
49 Smith, S.Z.; A. Garcia; *ISACA® Journal,* vol. 4, 2022, *https://www.isaca.org/archives*