Volume 6, No. 1 | January–February 2023

RAIL

The Journal of Robotics, Artificial Intelligence & Law

fastcase FULL COURT PRESS

RAIL
The Journal of Robotics, Artificial Intelligence & Law
Volume 6, No. 1 | January–February 2023

THE JOURNAL OF ROBOTICS, ARTIFICIAL INTELLIGENCE & LAW (ISSN 2575-5633 (print) /ISSN 2575-5617 (online) at $495.00 annually is published six times per year by Full Court Press, a Fastcase, Inc., imprint. For customer support, please contact Fastcase, Inc., 711 D St. NW, Suite 200, Washington, D.C. 20004, 202.999.4777 (phone), 202.521.3462 (fax), or email customer service at support@fastcase.com.

Publishing Staff
Publisher: Morgan Morrissette Wright
Production Editor: Sharon D. Ray
Cover Art Design: Juan Bustamante

Cite this publication as:

The Journal of Robotics, Artificial Intelligence & Law (Fastcase)

A Full Court Press, Fastcase, Inc., Publication

Editorial Office

711 D St. NW, Suite 200, Washington, D.C. 20004
https://www.fastcase.com/

POSTMASTER: Send address changes to THE JOURNAL OF ROBOTICS, ARTIFICIAL INTELLIGENCE & LAW, 711 D St. NW, Suite 200, Washington, D.C. 20004.

Articles and Submissions

Direct editorial inquiries and send material for publication to:

Steven A. Meyerowitz, Editor-in-Chief, Meyerowitz Communications Inc., 26910 Grand Central Parkway, #18R, Floral Park, NY 11005, smeyerowitz@meyerowitzcommunications.com, 631.291.5541.

Material for publication is welcomed—articles, decisions, or other items of interest to attorneys and law firms, in-house counsel, corporate compliance officers, government agencies and their counsel, senior business executives, scientists, engineers, and anyone interested in the law governing artificial intelligence and robotics. This publication is designed to be accurate and authoritative, but neither the publisher nor the authors are rendering legal, accounting, or other professional services in this publication. If legal or other expert advice is desired, retain the services of an appropriate professional. The articles and columns reflect only the present considerations and views of the authors and do not necessarily reflect those of the firms or organizations with which they are affiliated, any of the former or present clients of the authors or their firms or organizations, or the editors or publisher.

QUESTIONS ABOUT THIS PUBLICATION?

For questions about the Editorial Content appearing in these volumes or reprint permission, please contact:

Morgan Morrissette Wright, Publisher, Full Court Press at mwright@fastcase.com or at 202.999.4878

For questions or Sales and Customer Service:

Customer Service
Available 8 a.m.–8 p.m. Eastern Time
866.773.2782 (phone)
support@fastcase.com (email)

Sales
202.999.4777 (phone)
sales@fastcase.com (email)
ISSN 2575-5633 (print)
ISSN 2575-5617 (online)

Smart Contracts: A Few Tips to Avoid Being Outsmarted

William L. Carr and Henry M. Grabbe*

In this article, the authors lay out a basic understanding of the relationship between smart contracts and Internet of Things devices and identify a few tips to help avoid some of the potential risks of integrating smart contracts into a business.

Proponents of digital innovations such as blockchain, the Internet of Things ("IoT") and smart devices have hailed the introduction of such technology as the Fourth Industrial Revolution. When used together, they may create self-executing "smart contracts" for a variety of transactions. Smart contracts do not need to rely on IoT devices, but when they do, these devices are critical to the system, most importantly because they collect and transfer the transaction-related data that triggers the execution of the contracts. But how is that data verified, and what happens if the IoT devices are wrong?

This article lays out a basic understanding of the relationship between smart contracts and IoT devices and identifies a few tips to help avoid some of the potential risks of integrating smart contracts into a business.

What Is a Blockchain?

A blockchain acts as a distributed and immutable ledger for recording transactions including those involving smart contracts. Businesses most often use permissioned blockchains, which allow only authorized users to access the blockchain on a shared network and add data blocks, such as transactions, to it. There is no single "master copy" of the blockchain, but everyone can be confident that their copy of the blockchain is accurate because when one participant adds a transaction to the ledger, it is visible to all others on the network. These participants independently verify the new transaction and come to a consensus in real-time about whether it should be permanently added to the blockchain. The chain cannot

Robotics, Artificial Intelligence & Law / January–February 2023, Vol. 6, No. 1, pp. 41–44.

ISSN 2575-5633 (print) /ISSN 2575-5617 (online)

be altered once the new transaction is verified, time-stamped, and linked sequentially to the chain.

What Is a Smart Contract?

A smart contract, in turn, is a data block that is added to a blockchain ledger for verification. This data block is made up of a line of code that sets the contract provisions between the parties. In the simplest sense, smart contracts are a series of if-then conditions that provide data transmission in accordance with the parties' agreement.

Once added to the ledger, individual computers in the blockchain network—also known as "nodes"—collect and verify data demonstrating a party's performance of the "if" condition, make a cryptographic signature in the smart contract code, and then automatically transfer something of value, such as money or cryptocurrency, to the counterparty's account. This allows contracts to be performed and signed simultaneously, thereby dispensing with future obligations or renegotiations.

What Is the Role of IoT Devices?

While smart contracts constitute blocks on the chain, IoT devices are the nodes integrated into a blockchain's network. This integration allows smart contracts to reflect real-world conditions by relying on IoT devices to verify data inputs instantaneously that then trigger smart contract conditions. Generally speaking, an IoT device is an electronic product that connects to a wireless network to collect, store, and transfer data among other IoTs. These devices are all around us: smart watches, home security systems, pet and baby monitors, smart appliances, pacemakers, and home assistants. And the demand for IoT devices is growing exponentially. This year, the IoT market is expected to grow 18%[1] to more than 14 billion connections. As the market expands, so too will the ways in which businesses use IoT devices to optimize operations.

Here is one example of how a smart contract could work together in the health and life sciences industry: a manufacturer wins a contract to supply a national pharmacy with insulin. With every delivery, the manufacturer must provide the pharmacy with proof of origin, chain of custody, and certification that the product

was maintained at a temperature between 36 and 46 degrees Fahrenheit between the time of shipping all the way through its final delivery. The manufacturer enters a smart contract with a shipping company, which is written into a code on a permissioned blockchain, and IoT devices with access to the blockchain network (such as GPS tracking devices and temperature gauges) collect relevant data that also is recorded on the blockchain.

Once the devices verify the insulin has been delivered to a location specified in the smart contract and that it was always maintained within the appropriate temperature range, the contract is fulfilled, and payment is automatically transferred from the national pharmacy to the insulin manufacturer and from the manufacturer to the shipping company.

Tips for Use of Smart Contracts

The use of smart contracts may create efficiencies when IoT devices successfully capture relevant data points, such as reducing costs of resources otherwise required to ensure performance, automating recordation of essential characteristics to remove the risk of human error, and minimizing the need to litigate contract breaches. The prospect of guaranteed performance and mitigating transaction costs is a tempting benefit, but it does not come without risk. Thus, at a minimum, anyone contemplating a smart contract should take the steps described below.

Know the Identity of Your Counterparty

Although businesses almost certainly will use permissioned blockchains, which make the identity of your counterparty more easily detectible, permissionless blockchains allow the user to act with complete anonymity. There are many reasons this is important. For example, it is important to know your counterparty to evaluate risk of nonperformance or malperformance.

Know the Location of Your Counterparty

While location of performance may be easily discernible from the smart contract, the physical location of your counterparty may trigger additional obligations, such as data privacy laws.

Know Your Coder

The information on the blockchain cannot be changed once it is entered. It is important that the information being added to the blockchain is written correctly to avoid unintended (and irreversible) consequences.

Know Who Is Responsible if a Smart Device Makes a Mistake

IoT device integration is designed to minimize human inefficiencies related to contract performance, but these devices may create new inefficiencies because they do not allow for intervention in unforeseen circumstances during contract performance. IoT devices are not infallible. Using the example above, it is possible that a smart device in the insulin contract reports the wrong temperature, exchange rate, interest rate, or location of delivery. Any one of these incorrectly reported variables could detrimentally affect a party to the smart contract.

Notes

* William L. Carr, a partner in the Philadelphia office of Faegre Drinker Biddle & Reath LLP, prosecutes and defends complex litigation on behalf of businesses and individuals. Henry M. Grabbe, an associate in the firm's Philadelphia office, assists clients with litigation and dispute resolution. The authors may be contacted at william.carr@faegredrinker.com and henry.grabbe@faegredrinker.com, respectively.

1. https://iot-analytics.com/number-connected-iot-devices/.