Article

The Top Blockchain Patents of 2018

01.07.19
Law360

This year promises to be a significant year for blockchain and cryptocurrency due to advances in the underlying technology and increasing levels of adoption by corporations and large financial institutions. This article highlights 10 U.S. blockchain patents issued in 2018 that are particularly interesting or noteworthy in order to provide insight into the future direction of the technology.

What is a blockchain patent, anyway?

A search of the U.S. Patent and Trademark Office patent database for terms like "blockchain," "bitcoin," "cryptocurrency" and "distributed ledger" results in a total of 361 patents issued in 2018. But while these relevant search terms might exist in the patent specifications, not all of the patents actually relate to blockchain technology. For example, one patent describes a new parking meter system that can be configured to accept payment in bitcoin (US 10,134,201). Because patents like these are only tangentially related to blockchain technology, they were not counted in the following analysis of blockchain patents issued in 2018.

Exactly 200 blockchain patents were issued in the United States in 2018. Of these, the top five patent assignees were:

1. Bank of America Corp. (19 patents)
2. IBM Corp. (16 patents)
3. Accenture Global Solutions Limited (nine patents)
4. Winklevoss IP LLC (eight patents)
5. ALTR Solutions Inc. (seven patents)

The following blockchain patents issued in the United States in 2018 stand out as being particularly interesting or noteworthy. It should be stated that this list and the associated analysis is provided for educational purposes only, as no attempt has been made to evaluate the patents against any piece of prior art or otherwise determine their validity.

1. Digitally Encoded Seal for Document Verification

U.S. Patent No. 9,855,785 (Nagelberg)
Assignee: UIPCO LLC

Recall for a moment the wax seals used in the medieval ages to verify the authenticity of a physical document. This invention describes a similar system of placing a digital seal (like a bar code) on a document that contains a hash value that can be used to authenticate various features of the document. In some embodiments, the seal may be employed in conjunction with a blockchain network to enable the transfer of digital currency or perform other actions when the seal is scanned.

2. Digital Currency Mining Circuitry With Adaptable Difficulty Compare Capabilities

U.S. Patent No. 9,942,046 (Drego, et al.)
Assignee: 21 Inc.

The process of verifying and recording new transactions in a distributed ledger is referred to as mining because the completion of the operation typically rewards the miner with a new unit of cryptocurrency. This patent describes an improved system and method for mining that involves using cryptographic hashing circuitry to generate a hash output, and using bit comparison circuitry to check a subset of bits in the hash output to identify a possible partial solution. Various features of this solution are then tested in a way that can improve speed and performance of the mining operation.

3. Hybrid Blockchain

U.S. Patent 9,959,065 (Ateniese, et al.)
Assignees: Accenture Global Solutions Limited, GSC Secrypt LLC

One of the greatest positive attributes of blockchain is that its data is essentially "immutable," meaning that it is virtually impossible to edit or delete a record on the blockchain. This feature can also be a drawback, for example, if confidential or other sensitive information needs to be removed from the chain. This patent addresses this issue with the creation of a hybrid blockchain consisting of a core part of a block that is effectively immutable and a tertiary part of the block that can be modified under certain conditions.

4. System, Method and Computer Program Product for Privacy-Preserving Transaction Validation Mechanisms for Smart Contracts That Are Included in a Ledger

U.S. Patent No. 9,992,028 (Androulaki, et al.)
Assignee: IBM

Privacy is a major concern of blockchain developers and an issue that has been gaining an increasing amount of attention from government regulators around the world. This patent describes a way for users to control the confidentiality of their transactions on a blockchain. For example, for a payment transaction, an entity may hide information about the transaction to all but a restricted number of validating entities. While hidden by public validators, the transaction result may still be verifiable by public validators so that it may be added to the blockchain. In addition, confidential smart contracts are not "inferable" by entities that have no access to them.

5. Method and System for Linkage of Blockchain-Based Assets to Fiat Currency Accounts

U.S. Patent No. 10,026,082 (Davis)
Assignee: Mastercard International Inc.

This invention attempts to address issues with long processing times and a lack of risk and fraud detection systems present in existing (i.e., nondistributed) payment transaction systems. The patent describes the use of traditional payment networks in combination with blockchain currencies to provide consumers and merchants the benefits of the decentralized blockchain while still maintaining security of account information and a strong defense against fraud and theft. This is done in part by having a user hold two linked accounts with a central authority, one account in fiat currency and another in cryptocurrency, in a way that allows a payment processor to process payments faster and with less risk.

6. Cryptocurrency Payment Network

U.S. Patent No. 10,055,715 (Grassadonia, et al.)
Assignee: Square Inc.

This patent describes a financial transaction between a customer and merchant wherein the customer can pay in any currency and the merchant can be paid in any currency. Such a system would make it easier and less risky for retailers to accept cryptocurrency at the point of sale, therefore leading to greater adoption of

cryptocurrencies by retailers. It is no surprise that Square, a leader in cutting edge payment systems, would be interested in implementing this technology.

7. Immutable Logging of Access Requests to Distributed File Systems

U.S. Patent No. 10,114,970 (Goldfarb, et al.)
Assignee: ALTR Solutions Inc.

Unauthorized users of a distributed database may attempt to change data records and mask their activity by deleting access logs. This invention describes a tamper-evident access log built on the blockchain architecture in combination with Merkle Tree cryptography in a way that is expected to reduce the number of read/write operations necessary to transact with the chain, reducing potential latency.

8. Integrity Verification of an Audio-Visual Data Stream

U.S. Patent 10,136,098 (Altenburger, et al.)
Assignee: IBM

How can you trust a picture or video when they are now so easy to manipulate with basic software tools? This patent applies the concept behind blockchain technology to help solve this problem. Think of each frame of a video as a "block" that can be hashed and connected to the next frame in a "chain" of records. A water mark stored on each frame indicates the hash value of the preceding frame. If one or more of the frames are altered, the hash values will no longer add up and the viewer will be able to determine that the video or audio file has been edited.

9. Systems, Devices and Methods for Detecting Double Signing in a One-Time-Use Signature Scheme

U.S. Patent No. 10,148,441 (Kaliski, Jr.)
Assignee: Verisign Inc.

This invention addresses a vulnerability in public/private key transactions in which the sender attempts to clone a one-time-use private key and engage in a second transaction with it. Because of network delays, for example, the receiver might not be aware of both transactions before verifying the respective transactions or the available funds of the sender may not be up to date. This is done by comparing the one-time-use public/private key pair to values in a transaction database and generating an alert if the public/private key pair was used more than once.

10. Resource Allocation and Transfer Utilizing Holds and a Distributed Network

U.S. Patent No. 10,158,703 (Kurian)
Assignee: Bank of America

Utilizing a distributed network of systems for allocating and transferring resources between entities (e.g., users, institutions or the like) by providing holds on the resources, allocating the resources, and transferring the resources by utilizing allocation identifiers and/or holding pools, if needed. The use of allocation identifiers and/or holds on the resources improves upon the processing speeds and power of systems used for the resource transfers between entities.

The full article can also be viewed here.

William Zac Duffy is a senior attorney at Munsch Hardt Kopf & Harr PC.

The opinions expressed are those of the author(s) and do not necessarily reflect the views of the firm, its clients, or Portfolio Media Inc., or any of its or their respective affiliates. This article is for general information purposes and is not intended to be and should not be taken as legal advice.

Primary Contacts

William Zac Duffy
Dallas
214.855.7591
zduffy@munsch.com

Related Practices

Litigation
Intellectual Property Litigation

Related Industries

Technology & Telecommunications