

Blockchain, Cybersecurity and Global Finance



Aligned with your business.



In today's increasingly digital environment, companies in and around financial services must innovate to remain competitive. This is so because in the near future, blockchain technology may become the new architecture of a reinvented global financial services infrastructure. The technology — a distributed, consensus-driven ledger that enables and records encrypted digital asset transfers without the need of a confirming third party — is revolutionary to global financial services, whose core functions include the trusted intermediary role (e.g., payment processor, trade finance partner, broker, dealer, custodian).

What Is Blockchain?

Blockchain technology is a decentralized ledger of digital asset ownership on which the asset owners, or users, can initiate transfer to other users whose interconnected computers run blockchain software ("nodes"). The transactions themselves are encrypted transfer data that, when confirmed (in batches, roughly every 10 minutes), comprise the "blocks" and when linked sequentially to the referenced prior block, comprise the "chain." Confirmation occurs when the first of these nodes, each of which maintains a current copy of the blockchain, verifies the transaction(s) by utilizing specialized computational software to solve a complicated encryption problem. Then, and only then, does this node add the new block sequentially into the chain, causing the other nodes to validate the solution and update their ledgers accordingly. This verification yields compensation (e.g., in bitcoins or other cryptocurrency) to the problem-solving node, a "miner," for the processing power expended in first successfully confirming the transaction.

Security Risks

Realizing this potential, global investment banks are beginning to develop public and private blockchain technology standards and protocols, with a goal of reimagining their daily operations within the global financial system. While the possibilities for financial innovation — shared ledgers and smart contracts to name a few — are dizzying, it is important to remember one thing: the speed and extent of acceptance of blockchain technology within the global financial services community will ultimately depend on the security of the network. Earlier this year, Interpol reported that blockchain can be repurposed by hackers to export malware to all computers within the network. Interpol proved this by introducing a proof-of-concept malware that showed the viability of such a cyberattack. In the event of an actual attack, blockchain's virtues, such as decentralization and immutability, would instantly become vices, as the malware would spread far and wide and the pollution would not be easily erased.

The intermediary functions described above are currently critical actions within global financial services, particularly in relation to financial asset trading; however, these activities are increasingly expensive, inefficient and, most dangerous of all, risky. They are expensive because the information technology investment and maintenance costs are significant. They are inefficient because although trading is swift for many financial assets, settlement is not, with too much reliance on back-office human agency and duplication of effort and systems. They are risky because settlement delay introduces counterparty risk, and data concentration on centralized servers introduces operational/systems risk. In short, they are increasingly capital-intensive activities in the post-credit



crisis milieu, where despite muted trading revenue, the demands of regulators grow louder for more transparent reporting and real-time risk exposure recordkeeping.

Other Considerations

Blockchain is both a secure means of digitized asset transfer and a virtually incorruptible record of such transfer, confirmed by processing power consensus and protected by ledger distribution, from the original “genesis” block all the way through the current transaction. A technology that can automate trust in the transfer for value of digitized assets poses an existential threat to the financial institutions that choose to ignore it. However, blockchain offers an opportunity for collaboration and codevelopment — creative construction rather than destruction — for financial institutions and other market participants that choose to embrace it, for the technology is an elegant response to each of the challenges mentioned above. Distributed ledgers reduce cost and risk and, through secure consensus verification, increase data integrity. Third-party disintermediation and the prospect for near real-time settlement increase efficiency.

How We Can Help

At this early stage, it is unclear whether development of a permissionless (public) or permissioned (private, for instance, accessible only to select trading partners

or transaction processors) ledger will be first to drive change in the global financial services industry. It is fair to say, however, that the more closed the ledger, the greater the concentration risk and, therefore, the greater the vulnerability to a cyberattack. Meanwhile, the more distributed the ledger, the greater the chance of irreparable damage in the event of such an attack. In other words, whichever course development follows, network security is paramount. Hunton & Williams’ global privacy and cybersecurity practice is a leader in its field. Although blockchain technology is nascent in application to the financial services industry, our lawyers have extensive experience assisting companies in preventing and managing cyber events. Combined with our regulatory, technology, finance and trading lawyers, we can help you address the potential cyber risks.

Blockchain’s potential for disruptive innovation within the financial services industry and beyond is great. It will be greater still if from the very beginning network security remains foremost in mind. If you have any questions regarding blockchain technology, please contact any of the lawyers listed below.

Key Contacts



Lisa J. Sotto

Partner

New York

lsotto@hunton.com | +1 212 309 1223



Laura Colombell Marshall

Partner

Richmond

lmarshall@hunton.com | +1 804 787 8013



Mike Kerrigan

Partner

Charlotte

mkerrigan@hunton.com | +1 704 378 4746



Scott H. Kimpel

Partner

Washington, DC

skimpel@hunton.com | +1 202 955 1524



Cecilia Y. Oh

Partner

Washington, DC

ceciliaoh@hunton.com | +1 202 955 1516

www.hunton.com | www.huntonprivacyblog.com



© 2017 Hunton & Williams LLP. Attorney advertising materials. These materials have been prepared for informational purposes only and are not legal advice. This information is not intended to create an attorney-client or similar relationship. Please do not send us confidential information. Past successes cannot be an assurance of future success. Whether you need legal services and which lawyer you select are important decisions that should not be based solely upon these materials. Photographs are for dramatization purposes only and may include models. Likenesses do not necessarily imply current client, partnership or employee status. Contact: Walfrido J. Martinez, Managing Partner, Hunton & Williams LLP, 2200 Pennsylvania Avenue, NW, Washington, DC 20037, 202.955.1500