Crisil
Coalition
Greenwich

# Distributed Ledger Technology: What We Can Learn from Recent Blockchain Attacks

August 22, 2016

Blockchain technology, now often referred to as Distributed Ledger Technology (DLT), is taking financial services by storm. Recent work by Greenwich Associates shows that financial services companies are investing heavily in bringing the technology to market and are optimistic that it will have a meaningful impact within two years.

However, there remain significant obstacles that need to be overcome to make that a reality: most notably, security. In a new report released today, *Securing the Blockchain*, we discuss some of the key topics around blockchain security including consensus, transaction confidentiality and securing private keys. Many of these topics are now front and center in light of recent events.

**Securing Private Keys**

The security around private keys is a particularly relevant topic now given the recent hacking of the Bitfinex exchange in which bitcoins worth about $70 million were stolen. Although the exact details of the attack are not yet available, it is clear that the hackers were somehow able to access the private keys that secured customers' accounts and steal the bitcoin.

Private keys can be thought of as secret codes or passwords that prove ownership of digital assets. Technology companies developing permissioned blockchains for financial services will need to completely rethink the multi-sig/cold storage approach currently employed by digital currency exchanges. Although these solutions can be highly secure, this security comes at the cost of lower efficiency and higher administrative overhead. Indeed, it was shortcuts taken by the Bitfinex exchange that led to the theft and not the technology itself.

**Immutability**

The other issue that arises is what can be done after an attack takes place. As these are digital assets that were stolen, they exist only in computer code. It is therefore possible to 'roll-back' the blockchain to a previous version of the code that existed before the hack.

From the blockchain's point of view, it's as if the hack never took place. While this isn't being considered with respect to the Bitfinex hack, it is exactly what happened with the Ethereum blockchain when an attacker tried to steal about $50mm of the digital currency, Ether. This was, and still is, a hugely controversial move that required the cooperation of most of the participating nodes on the network. Until now, one of the fundamental attributes of blockchains was their immutability – i.e., that they represented a record of every transaction that

could not be tampered with or undone.

Throughout financial services today there is functionality to undo transactions: stock exchanges reserve the right to cancel clearly erroneous trades, credit card companies can reverse fraudulent transactions, and all trade processing software has the ability to cancel and correct mistakes.

As the industry develops DLT solutions for financial services, it will need to address the issue of immutability – is this in fact a bug and not a feature? Or should the industry build functionality to record or impose counteracting transactions that have the same effect as reversal but preserve the benefit of a complete historical transaction record?

**Smart Contracts**

The attempt to steal $50 million of Ether, exposed security vulnerability around smart contracts – a computer program that can execute the terms of a contract and transfer value between parties. In this case an investment fund (called the DAO) was built on top of the Ethereum blockchain using smart contracts.

However, poor design of the smart contract code enabled the hacker to gain access to the funds. Smart contracts are seen as an important part of DLT solutions, with applications in collateral management, OTC derivatives and other use cases. If a smart contract has the ability, for example, to trigger payment flows between banks and other entities, the potential impact could be much larger than $50 million.

Aside from the potential for the smart contract to be hacked, there is also the possibility that a bug in the code could cause it to malfunction and trigger significant erroneous payment flows - we have seen similar such events happen in financial markets before at great cost.

For these reasons it is important that the industry work together to develop best practices, safeguards and controls to prevent these types of events from occurring. In this regard, the recent formation of the Smart Contracts Alliance by the Chamber of Digital Commerce is a strong step in the right direction.

The implementation of distributed ledgers in financial services has significant potential to reduce settlement times, eliminate frictions, decrease costs, and streamline workflows. While striving to attain these benefits, the industry must also focus on security. Digital assets and DLT represent an entirely new way of transacting - as such we will need a new approach to securing the blockchain.

---

www.greenwich.com | ContactUs@greenwich.com

Our suite of analytics and insights encompass all key performance metrics and drivers: market share, revenue performance, client relationship share and quality, operational excellence, return on equity, behavioral drivers, and industry evolution.

## About CRISIL

CRISIL is a leading, agile and innovative global analytics company driven by its mission of making markets function better. It is majority owned by S&P Global Inc., a leading provider of transparent and independent ratings, benchmarks, analytics, and data to the capital and commodity markets worldwide.

CRISIL is India's foremost provider of ratings, data, research, analytics, and solutions with a strong record of growth, culture of innovation, and global footprint.

It has delivered independent opinions, actionable insights and efficient solutions to over 100,000 customers through businesses that operate from India, the U.S., the U.K., Argentina, Poland, China, Hong Kong, and Singapore.

For more information, visit www.crisil.com

## Disclaimer and Copyright

 This Document may contain analysis of commercial data relating to revenues, productivity and headcount of financial services organisations (together with any other commercial information set out in the Document). The Document may also include statements, estimates and projections with respect to the anticipated future performance of certain companies and as to the market for those companies' products and services.

The Document does not constitute (or purport to constitute) an accurate or complete representation of past or future activities of the businesses or companies considered in it but rather is designed to only highlight the trends. This Document is not (and does not purport to be) a comprehensive Document on the financial state of any business or company. The Document represents the views of Coalition Greenwich as on the date of the Document and Coalition Greenwich has no obligation to update or change it in the light of new or additional information or changed circumstances after submission of the Document.

This Document is not (and does not purport to be) a credit assessment or investment advice and should not form basis of any lending, investment or credit decision. This Document does not constitute nor form part of an offer or invitation to subscribe for, underwrite or purchase securities in any company. Nor should this Document, or any part of it, form the basis to be relied upon in any way in connection with any contract relating to any securities. The Document is not an investment analysis or research and is not subject to regulatory or legal obligations on the production of, or content of, investment analysis or research.

The data in this Document may reflect the views reported to Coalition Greenwich by the research participants. Interviewees may be asked about their use of and demand for financial products and services and about investment practices in relevant financial markets. Coalition Greenwich compiles the data received, conducts statistical analysis and reviews for presentation purposes to produce the final results.

THE DOCUMENT IS COMPILED FROM SOURCES COALITION GREENWICH BELIEVES TO BE RELIABLE. COALITION