Journal of Cases on Information Technology
Volume 21 • Issue 1 • January-March 2019

Understanding a Revolutionary and Flawed Grand Experiment in Blockchain:

The DAO Attack

Muhammad Izhar Mehar, York University, Toronto, Canada

Charles Louis Shier, Harvard Law School, Cambridge, USA

Alana Giambattista, York University, Toronto, Canada

Elgar Gong, York University, Toronto, Canada

Gabrielle Fletcher, York University, Toronto, Canada

Ryan Sanayhie, York University, Toronto, Canada

Henry M. Kim, York University, Toronto, Canada

Marek Laskowski, York University, Toronto, Canada

ABSTRACT

In spring 2016, the Distributed Autonomous Organization (The DAO) was created on Ethereum. As with Bitcoin, Ethereum uses a P2P network, where distributed ledgers are implemented as daisy-chained blocks of data. Ethereum's native cryptocurrency, Ethers are spent to execute pieces of code called smart contracts. Investors paid their Ethers for the DAO to operate and received the opportunity to vote on and become investors in venture projects proposed by Ethereum-based startups. Transactions and settlements between investors and startups are executed autonomously. The DAO experiment failed shortly after inception as an anonymous hacker stole over $50M USD worth of Ethers out of the $168M invested. The Ethereum community voted to return (or fork) the state of the network to one prior to the hack, returning Ethers back to investors and shuttering the DAO. However, this action arguably represented as a bailout—ironically, Bitcoin was conceived as a reaction against the 2008 bailout of US banks—and violated the ledger immutability and "code is law" ethos of the blockchain community.

KEYWORDS

Blockchain, Digital Currency, Bitcoin, Ethereum, Decentralized Autonomous Organization

1. SYNOPSIS OF "THE DAO"

On April 30th, 2016, leveraging the Ethereum Blockchain platform, a group of programmers launched a crowd-funding effort for a project known as the "The DAO (Decentralized Autonomous Organization). Unbeknownst to the organizing group, the software on which The DAO was created contained a bug introduced by a programming error, making the project vulnerable to exploit.

DOI: 10.4018/JCIT.2019010102

The mission of The DAO was to act as a self-directed venture capital fund, with contributors voting directly on proposed projects, and votes being allocated proportionately based on contributed capital (DuPont, 2018). In other words, investors would exchange Ethers, the native cryptocurrency associated with the Ethereum platform, for tokens during an Initial Coin Offering (ICO), and then projects would receive approval or rejection in a democratic fashion as directed by the votes of token holders. By the end of May 2016, $168 million USD worth of Ether had been raised by The DAO through the most successful crowdfunding campaign up to that point in history. By June 13th, 2016, an attacker had used a mechanism intended to splinter off "child" DAOs to syphon over one third of the invested Ether into a child DAO under control of the attacker. Since the child DAO was based on the same code as the original, the funds were inaccessible for 28 days (the length of the original funding window).

As the DAO represented the largest project in Ethereum's ten-month existence, any actions taken by the Ethereum Foundation or miners and mining pools would have large repercussions on the platform's future. Thus, there was major contention over the three leading alternatives being proposed: do nothing and allow the hacker to appropriate the stolen funds after the 28-day holding period; build a blacklist into the Ethereum code, effectively freezing the syphoned Ethers in the child DAO (the soft fork proposal); or unwind the hack entirely, returning all syphoned Ethers to The DAO and reimbursing investors (the hard fork proposal). The potential legal implications of each of option were numerous, as was the potential impact of trust in the network. For example, if the community decided to do nothing, they opened themselves to liability from investors of The DAO who lost over $50 million USD of Ethers. On the other hand, if the hard fork proposal received approval by the Ethereum community, confidence in the network's system of transactions and smart contracts having ultimate transactional authority—i.e. the immutability of the ledger—would be destroyed. This would be analogous to taxpayers bailing out failing financial institutions.

In the end, the Ethereum Foundation moved forward with the hard fork, and the funds were returned to The DAO investors. The minority who disagreed with this action however continued maintaining the original Blockchain under the moniker of Ethereum Classic (Reyes, Packin, and Edwards, 2017). With Ethereum Classic, miners continue to use the old Blockchain from before the funds were returned to The DAO investors, regarding the bailout as a corruption of the immutable ledger. Today, Ethereum Classic operates as a parallel version of the Blockchain where the precedent of "code is law" and the immutability of the Blockchain continue to be paramount.

2. CONCEPTUAL UNDERSTANDING AND LITERATURE REVIEW: BLOCKCHAIN, DIGITAL CURRENCIES AND THE SMART CONTRACT

The genesis of these innovations that spawned The DAO is a famous white paper from one or a collection of pseudonymous authors who penned the name Satoshi Nakamoto. The paper laid out the framework for Bitcoin, and introduced notions of Blockchain (Nakamoto, 2008). It drew on research in automatic verification systems (Haber & Stornetta, 1991; Massias, Avila, and Quisquater, 1999), cryptography (Merkle, 1980 Menezes, Van Oorschot, and Vanstone, 2009; Schneier, 2007), and distributed databases (Özsu & Valduriez 2011; Bernstein & Goodman 1981). Moreover, Bitcoin to some extent, but especially The DAO is inspired by theories from Economics and Organizational Studies. They include contract agency cost (Ross, 1973; Eisenhardt, 1989), contract theory (Gale & Hedwig, 1995; Bolton and Dewatripont, 2005), auction mechanisms (Edelman, Ostravsky, and Schwartz, 2007; Roth, 2002), theories of innovation (Greenstein, 2015; Moeen & Aggarwal, 2017), and virtual organizations (Handy, 1995; Markus & Agres, 2000).

Though there are descriptions of The DAO Attack in practitioner literature (e.g. (Siegel, 2016; Hertig, 2016; del Castillo, 2016)), there are not many that seek to address it in an academic forum. The few extant academic works use the event as context for technical discussions about Blockchain (Atzei, Bartoletti, & Cimoli, 2017) or present it as an omnibus dissertation for Internet ethnographers