# Understanding a Revolutionary and Flawed Grand Experiment in Blockchain: The DAO Attack

Muhammad Izhar Mehar[1] (mmehar18@schulich.yorku.ca)
Charles Shier[2] (cshier@jd20.law.harvard.edu)
Alana Giambattista[1] (agiambattista18@schulich.yorku.ca)
Elgar Gong[1] (egong18@schulich.yorku.ca)
Gabrielle Fletcher[1] (gfletcher18@schulich.yorku.ca)
Ryan Sanayhie[1] (rsanayhie18@schulich.yorku.ca)
Henry M. Kim[1] (hmkim@yorku.ca)
Marek Laskowski[1] (mlaskowski@schulich.yorku.ca)

[1]Harvard Law School
1563 Massachusetts Ave., Cambridge MA 02138

[2]Schulich School of Business, York University
4700 Keele St., Toronto, Ontario 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 executed autonomously. The DAO experiment failed shortly after inception as an anonymous hacker stole over $50M USD worth of Ethers out of $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 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

Electronic copy available at: https://ssrn.com/abstract=3014782

## 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.

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.

Electronic copy available at: https://ssrn.com/abstract=3014782

## 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).

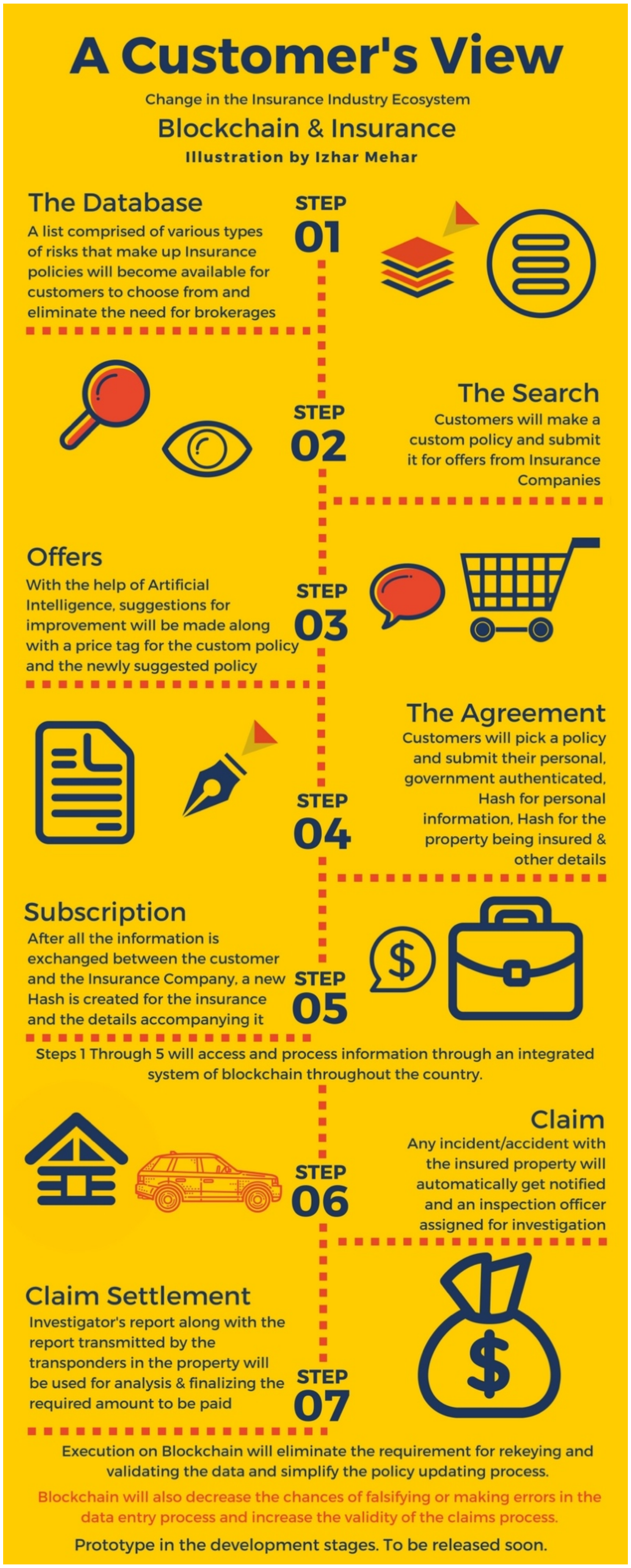
Though there are descriptions of The DAO Attack in practitioner literature [e.g. (Siegel, 2016)(Hertig, 2016)(del Castillo, 2016)], there are not many that seek to address it in an academic forum. The few extant academic works use the event as context for technical discussions about Blockchain (Atzei, Bartoletti, & Cimoli, 2017) or present it as an omnibus dissertation for Internet ethnographers (DuPont, 2018). Therefore, this paper addresses a literature gap insofar as we present a novel academic case study of The DAO Attack that can be used for management education pedagogy.

The first step towards presenting a case study is to be able to understand the concept of Decentralized Autonomous Organization or "The DAO" and the attack, it is crucial for the readers to understand the underlying technology and innovations that enabled its inception. They include the following: Blockchain, Ethereum, Ether, Bitcoin, and Smart Contracts.

**Blockchain** has the potential to change the way data integrity is maintained in the world. It is a digital system, based on the Internet and a network of computers, to share and continually reconcile the shared version of truth (Tapscott, 2016). It represents a revolutionary system of tracking and maintaining the integrity of data safe from tampering by individuals or corporations (Mougayar, 2016). There is also no trusted third party or intermediary that approves or denies transactions. Rather, the millions of devices in the network running complex algorithms are responsible for validating transactions and uploading new blocks to the chain which implements a public ledger.

**Bitcoin** is an electronic currency that originally demonstrated the utility of Blockchain and its underlying concepts. The use of Blockchain allows organizations and individuals to keep a complete record of their own transactions on a public ledger without sacrificing anonymity (Swan, 2015). Users are able to track transactions anywhere in the world as Bitcoin keeps transactions within the ledger open to the public, although transactions are not directly tied to the identity of the transacting parties (Iansiti and Kakhani, 2017). Bitcoin maintains anonymity by only revealing the Bitcoin address or account of participants. The address allows anyone to trace transactions to individual addresses but does not reveal the details and personal information of the owner. Other features include lack of centralized authority, low transaction fees, and no involvement of banks or other middlemen. Instead, the digital ledger is maintained by a network of volunteers around the world who use computers to solve cryptographic (math) problems to record blocks of transactions (Ito, Narula, and Ali, 2017). These individuals are known as “miners” because they are rewarded with Bitcoins for their work on verifying (or mining) blocks. Mining is also the process by which new Bitcoins are issued. A predictable but declining issuance of new Bitcoins is ensured by the Bitcoin protocol, which also balances the difficulty of the problems as more miners join the network and computing power increases. A digital currency that uses cryptographic techniques to verify transactions and issue new units is called a *cryptocurrency*. Bitcoin is increasingly being adopted by many companies, organizations, and individuals around the world. It is becoming a common medium through which transfer of value can occur, and for which records are kept safe and untampered due to the properties of the Blockchain.

The **Ethereum** platform extends concepts from Bitcoin to make it easier for users to encode complex business logic into structured transactions referred to as *smart contracts*. Ethereum is a platform where virtual miners work to earn Ethers, the native cryptocurrency token of Ethereum by maintaining the integrity of the ledger (i.e. mining). This digital currency is used, in turn, for transactions on the platform. Smart contract is a term that describes computer program code that is capable of facilitating, executing, and enforcing the negotiation or performance of an agreement (i.e. contract) using Blockchain technology (Diedrich, 2016). Due to its use of Blockchain, the contracts are executed inexorably in accordance with their encoded logic, which cannot be tampered with.  In its simplest form, Ethereum is an open software platform based on Blockchain technology that enables developers to build and deploy decentralized applications (Gildstein, 2017). Bitcoin was used to fund the initial creation of Ethereum.



A Customer's View

Change in the Insurance Industry Ecosystem

Blockchain & Insurance

Illustration by Izhar Mehar

The Database

STEP 01

A list comprised of various types of risks that make up Insurance policies will become available for customers to choose from and eliminate the need for brokerages

The Search

STEP 02

Customers will make a custom policy and submit it for offers from Insurance Companies

Offers

STEP 03

With the help of Artificial Intelligence, suggestions for improvement will be made along with a price tag for the custom policy and the newly suggested policy

The Agreement

STEP 04

Customers will pick a policy and submit their personal, government authenticated, Hash for personal information, Hash for the property being insured & other details

Subscription

STEP 05

After all the information is exchanged between the customer and the Insurance Company, a new Hash is created for the insurance and the details accompanying it

Steps 1 Through 5 will access and process information through an integrated system of blockchain throughout the country.

Claim

STEP 06

Any incident/accident with the insured property will automatically get notified and an inspection officer assigned for investigation

Claim Settlement

STEP 07

Investigator's report along with the report transmitted by the transponders in the property will be used for analysis & finalizing the required amount to be paid

Execution on Blockchain will eliminate the requirement for rekeying and validating the data and simplify the policy updating process.

Blockchain will also decrease the chances of falsifying or making errors in the data entry process and increase the validity of the claims process.

Prototype in the development stages. To be released soon.

Fig. 1: An Illustration of the functionality of Smart Contracts through organizations such as The DAO in real life scenarios.

The concept behind a **Distributed Autonomous Organization (DAO)** is to program the required rules and decision making apparatus of an organization into code, eliminating the need for governing roles. The DAO leverages the incorruptible digital ledger of Blockchain, and the digital currency and smart contracts of Ethereum to build an organization without the oversight of managers. Corporations at their very core are a set of complex agreements that are executed by managers and employees of the corporation, and The DAO mimics the entire system but replaces humans with its respective technology and code. The following is a guide of how a DAO works (del Castillo, 2016)(Siegel, 2016):

- A group of programmers writes smart contracts (programs) that will guide and run the organization
- There is an initial funding period, in which people add funds to The DAO by purchasing tokens that represent ownership – this is called crowdsale, or an ICO – to give it resources it needs
- After the funding and the funding period of The DAO is over, The DAO starts to operate
- People then can make proposals to The DAO on how to spend the money, and the members who have bought in can vote to approve these proposals
- Once the proposals are accepted, the smart contracts guide the terms of the project and execute it accordingly.

The use of Blockchain and Ethereum allows the investors to make sure that the contracts are executed according to the terms without any tempering and misconduct. All the transactions are recorded on Blockchain and only when they fulfill the requirements of the smart contract are the parties paid the prescribed amount.

## 3. The Organization: “The DAO”

In order to understand “The DAO”, it is important to know what led to its creation, what benefits it offers, who created it, and what the creators’ backgrounds are.

**Creation of The DAO.** The incentive to eliminate agency costs that are created through agency relationships motivated the creation of The DAO (Kaal, 2016). The objective was to remove the presence of agents or managers in a traditional corporate hierarchy. An agent has the management control to act in the best interest of the principal, the shareholder or party with ownership. This forms the basis of an agency relationship. Corporate entities rely on the connectivity between principals and agents and the effectiveness of these agency relationships to function efficiently. However, the disconnection between the decision-making authority and the party with ownership can cause a conflict as a result of differing interests between their roles. Thus, corporations face additional costs to effectively govern any divergences arising from the structure of agency relationships.

The costs associated with agency relationships are borne by both parties. The principal faces the charges to monitor or control the agent including the costs of audits, while the agent experiences the bonding costs to establish the structure of the relationship. Corporate governance mechanisms are used to minimize the costs of the relationship, and any information asymmetries that exist between the two parties, as well as any risks resulting from the agent abusing its power and not acting in the best interest of the principal. Contracts and agreements are created to protect the principal and ensure that the agents are governed by rules and operate with proper conduct. However, a lack of trust is still evident between the agent and the principal as agents may not agree with the rules put in place or may simply choose to not abide with the regulations. The outcome results in an agency problem—for example, the agent may steal investment money from the principal. The agency problem is present within many corporations that have governance mechanisms put into place. These agency problems cannot be resolved through legal infrastructure, as small agents are vulnerable to the risk of mismanagement from the principal. These risks are amplified in situation of crowdfunding, as agents may not have the ability to identify the agency problem.

The consequences and increasing presence of the agency problem motivated the creation of The DAO, making use of smart contracts that are written and embedded on the Ethereum Blockchain. The use of Blockchain proposes a solution to the agency problem by engendering transparency and trust. The Blockchain makes use of smart contracts to verify and monitor transactions, reducing the costs that principals incur to monitor the agent. Cryptographic hashes provide transaction guarantees by providing a mathematically proven system. Governance rules are encoded using smart contracts and these control mechanisms. The Blockchain is immutable as no user is able to alter the rules embedded within the Blockchain code, in theory, preventing any fraudulent transactions. The decentralization inherent in Blockchain design also makes it difficult to reverse or alter information existent on the Blockchain.  Thus, corporate governance or intermediaries are no longer required, forming the Decentralized Autonomous Organization (DAO) structure.

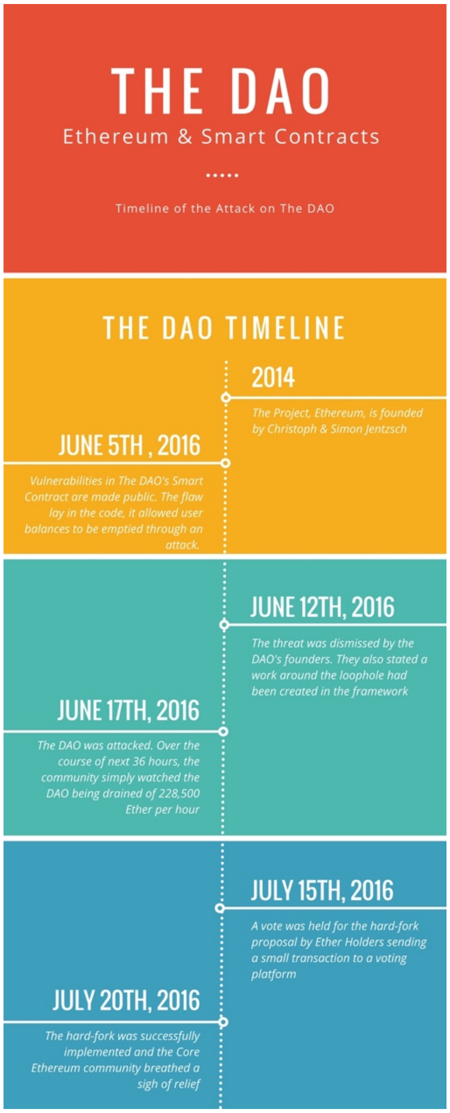
**Benefits of The DAO**. The DAO operates on a distributed consensus model. The DAO enables the users, DAO token holders, to control their contributions. By returning power from the hands of agents to the owners of DAO tokens, users are prevented from mismanaging investor funds thus resolving the agency problem. To prevent a majority user with <51% of tokens from transferring the funds to themselves, The DAO can split such that minority users who disagree with a proposal are able to receive their portion of Ether on that investment prior to the formation of a new DAO where the users who agree with the proposal can spend their Ether (Blockchannel, 2016).

The first existing DAOs were software controlled community organization experiments that sought to re-visit certain characteristics of traditional corporate governance, substituting voluntary compliance to a corporation’s charter with actual compliance with a pre-agreed computer code. The DAO is the most well-known example of a DAO, gaining a substantial amount of media attention throughout its initial creation phase, raising a total of $168 million USD from individual investors, earning the title of the largest crowdfunding project to date, though this title has since been eclipsed by more recent ICO’s.

The DAO is beneficial as it addresses the lack of authority and control influenced by minority owners. Provisions in corporate governance and statute law have attempted to address this problem, however many of these solutions are unsuccessful because minority owners lack the voting rights and influence to retrieve their capital. The DAO addresses this issue by distributing the authority equally to token holders.

**Founders of The DAO**. With the intention of providing a new decentralized business model for corporations, cofounders Christoph and Simon Jentzsch of Slock.it, a company incorporated in Germany, created The DAO. With a thorough background in theoretical physics, Christoph Jentzsch formulated the code behind The DAO. His extensive knowledge of physics has allowed him to develop sophisticated software solutions for high performance computing on specialized hardware. As a lead tester, Christoph has been involved in the Ethereum project since 2014. Simon Jentzsch, was also intensively involved in the venture of The DAO. As project manager, developer and software architect, he led the growth and expansion of Slock.it.

Slock.it was founded in 2015 with a vision to connect a variety of smart locks (as in actual physical ones like deadbolt locks) to the Blockchain, enabling them to directly receive payments which could then be used to rent, sell or share real-world assets such as real estate properties and vehicles. This ability was coined the Universal Sharing Network. At the center of The DAO lies the Ethereum network mediating interactions between physical locks and virtual, online, Blockchains. With the development of prototypes, Slock.it cofounders recognized the full potential of The DAO and were determined to expand the business to establish a foundation for a decentralized sharing economy. Before The DAO, Jentzsch brothers created Slock.it as a simplified smart contract that provided token holders with voting power about what actions token holders should take. This premature crowdfunding contract soon transpired into The DAO, where token holders were given more power (Jentzsch, 2016). Token holders had full command of the funds that were released subsequently after a successful vote on a detailed proposal. The DAO relied on a participatory crowd for its investment decision-making, requiring positive votes from 20% of tokens issued for a proposal to be deemed acceptable.



2014

The Project, Ethereum, is founded by Christoph & Simon Jentzsch

JUNE 5TH , 2016

Vulnerabilities in The DAO's Smart Contract are made public. The flaw lay in the code, it allowed user balances to be emptied through an attack.

JUNE 12TH, 2016

The threat was dismissed by the DAO's founders. They also stated a work around the loophole had been created in the framework

JUNE 17TH, 2016

The DAO was attacked. Over the course of next 36 hours, the community simply watched the DAO being drained of 228,500 Ether per hour

JULY 15TH, 2016

A vote was held for the hard-fork proposal by Ether Holders sending a small transaction to a voting platform

JULY 20TH, 2016

The hard-fork was successfully implemented and the Core Ethereum community breathed a sigh of relief

Fig. 2: Timeline for the DAO Attack

## 4. Attack on The DAO

To fully understand how The DAO was attacked, it is important to know how the hack was performed, the impact it had on the broader Blockchain community, the difference between Ethereum Classic and Ethereum, and what the future may entail for the community.

**The Discovery of a Flaw in the Code.** On June 5th 2016 it was revealed to the public that The DAO's smart contracts had significant vulnerabilities. The flaw lay in the code for a smart contract, which allowed user balances to be emptied through an attack. This was first casually discovered by a user of GitHub, a web-based software development platform. The user, Chriseth, notified key developers working with Ethereum and the Blockchain foundation founder, Peter Vessenes. Peter then went on to publish an article detailing the vulnerability with The DAO (Vessenes, 2016). The flaw in the code allowed an attacker to withdraw their balance stored in The DAO repeatedly before the balance was adjusted. This threat was dismissed by The DAO's founders, Slock.it on June 12th 2016. In a web article, Slock.it founder, acknowledged that there was a vulnerability that was accidentally introduced in Ethereum smart contracts due to inherent design flaws in the Solidity smart contract programming language which was used in the creation of The DAO (Tual, 2016). He also stated that a work around to the vulnerability was created in The DAO's framework and that no DAO funds were at risk of the bug any longer. Five days later, on June 17th 2016, The DAO was attacked.

**How the Attack Was Performed.** There is debate as to whether the attack constitutes being classified as a "hack" (DuPont, 2018). There is a belief among some in the Ethereum community that "code is law." If this tautology is true, then The DAO's attacker simply used its code as written for an unintended purpose. The loophole allowed the attacker to drain The DAO using the aforementioned splitting function. Normally, the splitting function allows contributors who have Ether in The DAO to withdraw their contributions if there is disagreement with how the funds are being used. The very nature of The DAO gives contributors this freedom to cash out, both their initial contributions and reward tokens for participating. However, at the time of the attack, there were no Ether present in The DAO's rewards account, therefore all of the funds stolen were user contributions. The attacker was able to take advantage of the fact that the smart contract only verifies the user balance once, at the beginning of the split request. By repeatedly requesting splits before the attacker's balance was adjusted, the attacker was able to fool The DAO into giving out more funds than the attacker's original balance. Code was used where one request immediately triggered another before balances were adjusted and the process was repeated up to 20 times. The Ethers then were put into a duplicate of The DAO, essentially a Child DAO. The caveat regarding this newly created child DAO was that the Ether could not be accessed until the initial funding period of 28 days had elapsed.

The attacker might never be able to access the stolen Ethers because any attempts to cash out would raise alarms at exchanges or other facilities where Know your Customer (KYC) rules apply. Over the course of 36 hours, the community simply watched as The DAO was drained of 228,500 Ethers per hour. The decentralized nature of The DAO and Ethereum required voting and majority consensus to be reached before the attack could be put to a halt. Until voting and consensus could be reached, as numerous copies of the entire Ethereum blockchain were synchronized throughout the world, the Ethereum community could only watch as these copies reflected depleting debits to The DAO balances. Similarly, since it was permissible within the rules of the The DAO for a Child DAO used to store syphoned funds to be created and split off from The DAO, the Ethereum community could only just watch.

As there was no fast solution to updating the smart contract, the community responded in the meantime by trying to mitigate the theft of Ethers. Another group of individuals, so-called "white-hat" hackers, began their own draining of The DAO in order to move the remaining Ethers into an ostensibly safe place; another child DAO. The idea was to drain Ether faster than the attacker and by June 22nd, all of the accessible Ether in The DAO had been emptied by the original attacker or other actors.

**Impact of the Attack.** Despite the restrictions on the attacker accessing the funds, the attack still had a significant impact. While the attack completely shut down The DAO, it also had broader effects on the Ethereum and Blockchain communities. At the time of the attack, The DAO contained 15% of all the Ethers in the world. The theft significantly devalued the digital currency, dropping the price of Ether from $20 USD to below $13 USD. Although the attacker may not have been able to access the Ether, it has been theorized that his incentive came from short trading against the currency. Aside from the price change, the attack also brought up some ethical decisions for the affected communities. The debate created three possible alternatives for how to deal with the aftermath of the attack on The DAO.

The first alternative was to do nothing and let the attacker keep the roughly $50 million dollars USD in stolen Ethers. This approach was consistent with the doctrine that "code is law" and that the attacker now has the rights to the Ethers since they merely used The DAO's code as written. The second alternative was to blacklist the child DAO that the attacker funneled the Ether into, to make it unusable. This is known as a soft fork (a fork is a one-time fix by creating an offshoot Blockchain) and would have resulted in the Ethers contributed by investors being lost. However, it would have prevented the attacker from gaining further from the exploit. The third option was to rewind the smart contracts through special consensus of the miners and return all of the stolen Ethers to a modified original DAO, which would only allow for withdrawal of the original funds. From there, the Ethers would be restored to investors and The DAO would be shut down. This solution had the support of The DAO and Ethereum's founders, but it would violate the immutability of the Blockchain, and therefore, the integrity of Ethereum. The decentralized nature of the Blockchain was meant to take decision making powers out of the hands of human beings. However, a reversal of the attack would signal that the system is still controlled by people and not immutable, unbiased code (Hertig, 2016).

After several days of voting, the Ethereum community agreed to implement the hard fork solution. This created a new Ethereum Blockchain where the transactions deemed offensive were rewound to their state before the attack. A minority dissented and continued to mine the old Ethereum chain, where the blocks remained untampered with. This unforked version was dubbed Ethereum Classic (ETC). The hypocrisy of the hard fork has become evident more recently, as errors resulting in losses of Ethers of similar scale have not been similarly reversed by the core Ethereum community.

**Ethereum Classic vs. Ethereum.** It is important to identify the similarities and differences between Ethereum Classic (ETC) and Ethereum (ETH) in order to understand why the main Ethereum platform divided into two smaller competing Blockchain platforms. Basic similarities include: both networks run on a Blockchain, and are peer-to-peer systems. A peer to peer system exists when one computer or laptop can connect to another computer or laptop anywhere in the world without a central server or authority. Because they cannot be shut down by central authority, both networks are censorship free. Another similarity is that unlike Bitcoin neither network has a mining cap. Without a mining cap, both Ethereum platforms have an unlimited supply.

**A Divided Ethereum Community**. So why are there now two Ethereum platforms opposed to only one? The Ethereum Foundation and core Ethereum community focused on implementing a soft fork launched on June 24th, intended to censor the incoming transactions from the hacker. However, due to a flaw in the code of the soft fork, miners decided that they were not going to implement it. Still, within the 28-day initial funding period, the community debated the implementation of a hard fork. On July 15th, a vote was held for the hard fork proposal by Ether holders sending a small transaction to a voting platform. By June 20th, the hard fork was successfully implemented and the core Ethereum community breathed a sigh of relief. Some dissented, and hours later, miners resumed mining the original chain, and Ethereum Classic (ETC) was born and it currently maintains all of the same structural components and mechanisms of the original Ethereum Blockchain (Dannen, 2017). The forked Blockchain continues to be considered the main Ethereum network.

The debate on whether or not the hard fork proposal should be implemented lasted a span of 18 days, between June 28th and July 15th (Cryptocompare, 2017). Both supporters and detractors of the proposal had valid reasons to justify their position. The table below compares the arguments of both sides of the Ethereum community regarding the hard fork proposal.

Table 1: Ethereum Fork Pros and Cons

| Supporters | Detractors |
|---|---|
| ● Given these circumstances, the code of law is too drastic, so “humans should have the final say through a social consensus” (Blockgeeks, 2017);<br>● It is ethically wrong for the hacker to profit, so community intervention is needed;<br>● The slippery slope argument is invalid because people can make decisions rationally in each situation;<br>● Leaving Ether in the hacker’s hands can lead to a decrease in its value in the future;<br>● The proposal is not a bailout because the funds are simply being returned to the original investors;<br>● The war between white-hat hackers and the hacker would stop;<br>● Unethical people will think twice about using Ethereum;<br>● The proposal eliminates the need for regulators and the legal system to intervene (Blockgeeks, 2017) | ● Code is law - original consensus rules of Ethereum and The DAO should stand regardless of the situation;<br>● Blockchain events are immutable and shouldn’t change regardless of the outcome;<br>● Slippery slope argument: once you make one change in one place, it is likely for more changes to occur elsewhere;<br>● Returning the lost funds is short sighted, which could reduce the value of Ether;<br>● The hard fork proposal is a bailout (Blockgeeks, 2017). |

The sole purpose of the hard fork was to return all stolen Ether from The DAO to a refund smart contract, which is exactly what happened. The democratic nature of this vote has been called into question, as Ethereum community members were given one vote per Ether that they held, making the outcome “one dollar, one vote” rather than “one person, one vote.”

**The Future of Ethereum**. Having two Blockchains comes with advantages for Ether holders. First, original Ether holders saw their account balances double, as duplicate tokens were created on the ETC chain. In other words, those holders who had tokens on the original Blockchain at the time of the fork now have the same amount of tokens on the new version. Another advantage of having two Blockchains is that Ether holders can now trade ETH tokens for ETC tokens since ETC now trades on exchanges such as Poloniex, Kraken, Shapeshift, and Bitfinex. However, there are problems that Ether holders can experience such as sending tokens to an ETC address instead of an ETH address or vice-versa, resulting in lost tokens.

The future of the Blockchain community is uncertain only because there are endless possibilities for Blockchain to be implemented in almost every industry. Given the nature of Blockchain, the financial services industry is most likely going to act on implementing this platform as their new facet for transactions. "With banks urgently seeking to reduce costs, the potential security, convenience and efficiency of Blockchain networks is a major driving force in the face to adoption" (Weisfeld, 2017). Since Blockchain is in its early phase of expansion, in order to reach mainstream adoption in approximately 5 to 10 years, it needs to overcome both commercial and technology barriers. Selecting the optimum business model for Blockchain is very critical in order to determine if the benefits outweigh the drawbacks of each business model, and if a certain model will result in more or less barriers than others. Below is a list of the possible business models that Blockchain can implement in order to achieve a wide-scale adoption (Weisfeld, 2017):

- Open sourced
- Licensed product (FinTech driven solutions)
- Platform-as-a-Service (PaaS)
- Distributed peer-to-peer funded model
- Consortium based
- Centralised utility;
- Led by regulator or central bank

## 5. Conclusion

This paper aims to introduce the key concepts behind The DAO, outline its creation and discuss the issues that it faced. Blockchain and smart contracts are two of the underlying concepts that change the way transaction and data integrity are maintained. They open the door to a new type of organization where all of the governing responsibilities are processed through code. This structure offers many advantages. It removes the need for governing directors who must be compensated, as well agency costs of these directors. It ensures that no individual can tamper with decisions that have been made because they are made permanent in code. In practice, these characteristics can be detrimental if such a structure is implemented too quickly. A ready, fire, aim approach can lead to flaws in code, which causes problems down the road due to their permanence. This was evident when The DAO, the first such implementation, had its investor funding stolen through a programming bug. This attack opened the discussion for legal and ethical issues. An exception was made to the idea that "code is law", which satisfied stakeholders by reversing transactions and returning funds to investors. Although the core Ethereum community favoured this approach, there were a group of dissenters who split off to create a second Ethereum network. While there is uncertainty over what the right course of action was, it is unequivocal that the next implementation of a DAO should take a more precautionary approach.

## References

Atzei, N., Bartoletti, M., & Cimoli, T. (2017). A Survey of Attacks on Ethereum Smart Contracts (SoK). *Proceedings of the International Conference on Principles of Security and Trust* (April, 164-186). Springer, Berlin, Heidelberg.

BlockChannel (2016). What Is A “DAO”? How Do They Benefit Consumers? *Medium*, March 21. Retrieved March 3, 2017, from https://medium.com/blockchannel/what-is-a-dao-how-do-they-benefit-consumers-f7a0a862f3dc#.pqlc5v1tb.

Blockgeeks (2017). What is Ethereum Classic? Ethereum vs. Ethereum Classic: An In-Depth Guide by Blockgeeks. *Blockgeeks*. Retrieved August 4, 2017, from https://blockgeeks.com/guides/what-is-ethereum-classic/.

Bolton, P., and Dewatripont, M. (2005). *Contract Theory*. MIT Press: Cambridge, MA USA.

Bernstein, P. A., & Goodman, N. (1981). Concurrency control in distributed database systems. *ACM Computing Surveys (CSUR)*, 13(2), 185-221.

Cryptocompare (2017). The DAO, The Hack, The Soft Fork and The Hard Fork. *cryptoCompare*.com, July 5, 2017. Retrieved August 4, 2017, from https://www.cryptocompare.com/coins/guides/the-dao-the-hack-the-soft fork-and-the-hard fork/.

Dannen, C. (2017). *Introducing Ethereum and Solidity*. Berkeley CA: Apress.

del Castillo, M. (2016). The DAO Attacked: Code Issue Leads to $60 Million Ether Theft. *CoinDesk*, June 17. Retrieved November 25, 2017, from https://www.coindesk.com/dao-attacked-code-issue-leads-60-million-ether-theft/.

Diedrich, H. (2016). *Ethereum: Blockchains, Digital Assets, Smart Contracts, Decentralized Autonomous Organizations*. CreateSpace Independent Publishing Platform.

DuPont, Q. (2018). Experiments in Algorithmic Governance: A history and ethnography of “The DAO,” a failed Decentralized Autonomous Organization. In M. Campbell-Verduyn (Ed.) *Bitcoin and Beyond: Cryptocurrencies, Blockchains and Global Governance*. Routledge Publishing.

Eisenhardt, K. M. (1989). Agency theory: An assessment and review. *Academy of Management Review* 14(1), 57-74.

Edelman, B., Ostrovsky, M., and Schwarz, M. (2007). Internet advertising and the generalized second-price auction: Selling billions of dollars worth of keywords. *The American Economic Review*, 97(1), 242-259.

Gale, D., and Hellwig, M. (1985). Incentive-Compatible Debt Contracts I: The One-Period Problem, *Review of Economic Studies* 52, pp. 647-64.

Gildstein, A. (2017). *Ethereum: The Blueprint on How to Buy, Sell and Make Money with Ethereum in 1 Day*. Gildstein Publishing.

Greenstein, S. (2015). *How the Internet Became Commercial: Innovation, Privatization, and the Birth of a New Network*. Princeton University Press: Princeton, NJ USA,

Haber, S., & Stornetta, W. S. (1997). Secure names for bit-strings, *Proceedings of the 4th ACM Conference on Computer and Communications Security* (April, 28-35). ACM Press.

Handy, C. (1995). Trust and the virtual organization. *Harvard Business Review*, 73(3), 40-51.

Hertig, A. (2016). Ethereum's Two Ethereums Explained. *Coindesk*, July 28. Retrieved March 1, 2017, from https://www.coindesk.com/Ethereum-classic-explained-Blockchain/.

Ito, J., Narula, N., & Ali, R. (2017). The Blockchain Will Do to the Financial System What the Internet Did to Media. *Harvard Business Review*, March 9. Retrieved November 25, 2017, from https://hbr.org/2017/03/the-blockchain-will-do-to-banks-and-law-firms-what-the-internet-did-to-media

Jentzsch, C. (2016). The History of the DAO and Lessons Learned. *Slock.it Blog*. August 24. Retrieved March 3, 2017, from https://blog.slock.it/the-history-of-the-dao-and-lessons-learned-d06740f8cfa5#.wc6625gge.

Kaal, W. (2017). Blockchain Solutions for Agency Problems in Corporate Governance. *Medium*, February 4. Retrieved March 4, 2017, from https://medium.com/@wulfkaal/Blockchain-solutions-for-agency-problems-in-corporate-governance-a83aae03b846#.f2665rysu.

Iansiti, M., & Lakhani, K. R. (2017). The Truth about Blockchain. *Harvard Business Review*, 95(1), 118-127.

Markus, M. L., & Agres, B. M. C. E. (2000). What makes a virtual organization work?. *MIT Sloan Management Review*, 42(1), 13.

Massias, H., Avila, X., & Quisquater J. (1999). Design of a secure timestamping service with minimal trust requirements. *Proceedings of the 20th Symposium on Information Theory in Benelux* (May). IEEE Computer Society.

Menezes, A. J., Van Oorschot, P. C., & Vanstone, S. A. (1996). *Handbook of applied cryptography*. CRC press.

Merkle, R.C. (1980). Protocols for public key cryptosystems. *Proceedings of the Symposium on Security and Privacy* (April, 122-133). IEEE Computer Society.

Moeen, M., & Agarwal, R. (2017). Incubation of an industry: heterogeneous knowledge bases and modes of value capture. *Strategic Management Journal*, 38(3), 566-587.

Mougayar, W. (2016). *The Business Blockchain: Promise, Practice, and Application of the Next Internet Technology*. Wiley Publishing.

Nakamoto, S. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System*. Bitcoin.org.

Özsu, M. T., & Valduriez, P. (2011). *Principles of distributed database systems*. Springer Science & Business Media.

Ross, S. A. (1973). The economic theory of agency: The principal's problem. *The American Economic Review*, 63(2), 134-139.

Roth, A. E. (2002). The economist as engineer: Game theory, experimentation, and computation as tools for design economics. *Econometrica* 70(4), pp. 1341-1378.

Reyes C., Packin N, & Edwards B. (2017). Distributed Governance. *William & Mary Law Review*, 59(1).

Schneier, B. (2007). *Applied cryptography: protocols, algorithms, and source code in C*. John Wiley & Sons.

Siegel, D. (2016). Understanding the DAO Attack. *Coindesk*, June 25. Retrieved November 25, 2017, from https://www.coindesk.com/understanding-dao-hack-journalists/.

Swan, M. (2015). *Blockchain: Blueprint for a New Economy*. O'Reilly Media.

Tapscott, D. (2016). *Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World.* Portfolio Penguin Publishing: Toronto, ON Canada.

Tual, S. (2016). No DAO funds at risk following the Ethereum smart contract 'recursive call' bug discovery. *Slock.it Blog*, June 12. Retrieved March 7, 2017, from https://blog.slock.it/no-dao-funds-at-risk-following-the-Ethereum-smart-contract-recursive-call-bug-discovery-29f482d348b#.nt0cwh8sl.

Vessenes, P. (2016). More Ethereum Attacks: Race-To-Empty is the Real Deal. *vessenes.com*, June 9. Retrieved March 5, 2017, from https://vessenes.com/more-Ethereum-attacks-race-to-empty-is-the-real-deal/.

Weisfeld, N. (2017). Blockchain Technology. *Finextra*, February 22. Retrieved March 6, 2017, from https://www.finextra.com/blogposting/13729/Blockchain-technology.