12-2019

# Smart contracts: A catalyst of the next global financial crisis?

Randall DURAN

Paul Robert GRIFFIN
*Singapore Management University*, paulgriffin@smu.edu.sg

# Smart contracts: A catalyst of the next global financial crisis?

DURAN, Randall; GRIFFIN Paul R.

Published in Journal of Financial Regulation and Compliance, 2019 December, Advance online. DOI: https://doi.org/10.1108/JFRC-09-2018-0122

**Abstract**

*Purpose* – This paper examines the risks associated with smart contracts, a disruptive FinTech innovation, and assesses how in the future they could threaten the integrity of the global financial system.

*Design/methodology/approach* – A qualitative approach is used to identify risk factors related to the use of new financial innovations, by examining how over-the-counter (OTC) derivatives contributed to the Global Financial Crisis (GFC) in 2007. Based on this analysis, the potential for similar concerns with smart contracts are evaluated, drawing on the failure of the DAO, which involved the loss of over $60 million of digital currency.

*Findings* – Extensive use of bilateral agreements, complexity and lack of standardization, lack of transparency, misuse, and speed of contagion were factors that contributed to the GFC that could also become material concerns for smart contract technology as its adoption grows. These concerns, combined with other contextual factors, such as the risk of defects in smart contracts and cyberattacks, could lead to potential destabilization of the broader financial system.

*Practical implications* – The paper's findings provide insights to help make the design, management, and monitoring of smart contract technology more robust. They also provide guidance for key stakeholders on proactive steps that can be taken with smart contract technology to avoid repeating oversights that contributed to the Global Financial Crisis.

*Originality/value* **–** This paper draws attention to the risks associated with the adoption of disruptive financial technology. It also suggests steps that regulators and other key stakeholders can take to help mitigate those risks.

## 1. Introduction

The rise of digital ledger technology (DLT) over the past decade has served as a disruptive force within financial services and has been driven by financial technology (FinTech) companies. While digital currencies, such as bitcoin (Nakamoto, 2008), were the first and are the furthest developed DLT implementations, many other applications, ranging from land registries to transactional systems for trade finance, are under development and undergoing testing. One of the more intriguing and promising DLT-related technologies are smart contracts (SCs). Smart contracts are, at best, software-based agreements that do not involve human mediators for execution (Szabo, 1997); they are now implemented as source code instructions that are typically stored and executed on distributed ledger technology. Smart contracts have the potential to automate and provide greater efficiency and assurance of the execution of contractual terms as compared with traditional contracts.

Like many FinTech innovations, due to their novelty, many of the risks related to smart contracts are not fully understood. Yet, given the high velocity of innovation and the rapid adoption of FinTech, it is important to consider the broader risks. More specifically, the evolution of smart contracts and how a broad expansion of their use could create systemic risks and threaten the integrity of the broader financial system. At the present time this risk may sound doubtful; however, it is worthwhile to consider the impact that another, relatively new financial technology, over-the-counter (OTC) derivatives, had in the early 2000s: OTC derivatives, which served as a catalyst for the Global Financial Crisis (GFC) in 2007.

There are a number of risks associated with DLTs and smart contracts that are currently understood (Luu et al., 2016; Weaver, 2018), but perhaps the greater risks are those that have not yet been uncovered. Because of the novelty of smart contracts, there has been limited exploratory analysis and research of their flaws and unexpected characteristics. Likewise, the complexity and rapid evolution of the information technology (IT) that underpins smart contracts makes it likely that structural and intrinsic risks may persist and continue to be found over an extended period of time. It is not unusual for critical security vulnerabilities to be found and exploited in decades-old core IT infrastructure components such as the 2017 WannaCry ransomware virus that affected old unpatched versions of Windows. Furthermore, smart contracts may be combined and interlinked so as to form dependencies and create a network of risks that can transcend the risks associated with individual contracts. That is to say, features or flaws in individual SCs may not be of major concern in themselves, but may lead to compounding risk when combined.

By reviewing how OTC derivatives contributed to the global financial crisis (GFC), similar dangers with smart contracts and other FinTech innovations can be identified. It is ironic that the use of OTC derivatives led to financial disaster for many financial institutions, when in fact those derivatives were designed as tools to help manage financial risk. This case demonstrates how new technologies that have a high pace of innovation, coupled with increasing usage across a large number of participants, can produce systemic instability (Helbing, 2013).

While there are fundamental differences between smart contracts (an information technology), and OTC derivatives (a financial innovation) there are also parallels with regards to the financial risks they can give rise to. For example, the 1994 bankruptcy of Orange County, which was a result of misuse of OTC derivatives (Noris, 1994), presaged the role these derivatives would play in the GFC more than a decade later. Similarly, the collapse of the Distributed Anonymous Organization (DAO) due to flaws in its use of smart contracts (Peck, 2016) could portend greater risks to come as the use of smart contracts become more widespread.

This paper analyzes parallels between risks associated with OTC derivatives and smart contracts in the context of their potential to destabilize the financial system. The aim is to provide insights to help make the design, management, and monitoring of smart contract technology more robust and less likely to lead to systemic-level risk. The structure of the rest of the paper is as follows. Section 2 reviews how OTC derivatives served as a catalyst for the global financial crisis. Section 3 examines the characteristics of smart contracts and how they are used, particular in the context of financial transactions. Section 4 covers the current issues and risks associated with smart contracts. Section 5 identifies similarities between

OTC derivatives at the time of their introduction as a new financial technology and smart contracts and discusses how the advancement of smart contracts could lead to concerns similar to those caused by OTC derivatives. Section 6 outlines risk mitigation strategies to help prevent, detect, and respond to threats that smart contracts may present to financial stability. Section 7 concludes with suggested steps that can be taken to provide safeguards against potential hazards related to smart contracts that are not currently evident and suggests areas for further research.

## 2. Issues and risks with OTC derivatives that led to financial instability

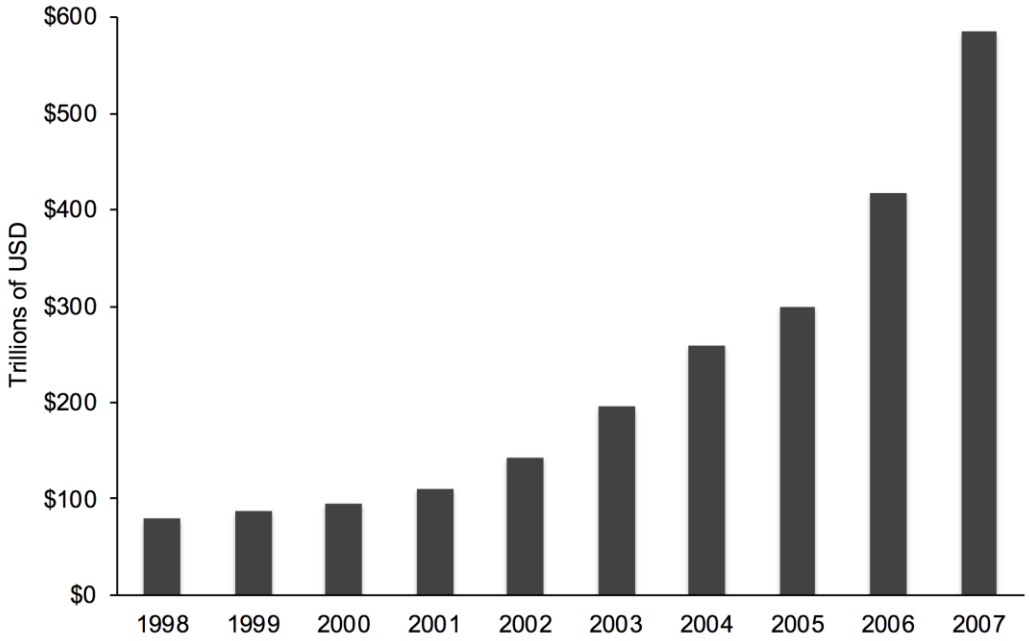
This section examines the background, concerns, and remedies to the issues and risks associated with OTC derivatives and their contribution to the Global Financial Crisis. Specifically, it looks at issues related to derivatives' complexity, the extensive use of bilateral agreements and lack of central counterparties, the use of OTC derivatives by the shadow banking system, lack of financial transparency, and speed at which risk-related problems unfolded. These factors will be discussed again in Section 5 in the context of similar concerns posed by smart contracts.

### Background

Many factors led to the Global Financial Crisis. The overall market environment was clearly one factor, where an extended period of low interest rates led to loose credit, use of extensive leverage, and an ongoing quest for higher yielding returns. In turn, risk taking increased and, in the U.S., a housing price bubble formed (Somanathan et al, 2015). Increased global interconnectedness was also clearly a factor that led to cascading risk and ultimately led to a crisis of confidence. OTC derivatives, at the time, a relatively young financial technology, also were a significant factor. They provide a means for creating new forms of leverage and enabled, and in some ways fueled, credit growth. OTC derivatives also provided sustenance for the shadow banking sector, which operated outside of regulators' purview.

Leading up to the GFC, the use of OTC derivatives grew substantially, as shown in Figure 1. While the OTC derivatives' ability to be customized to meet specific needs was a large part of their appeal, they were also popular because they were not as heavily regulated as listed derivatives. In particular, OTC derivatives in the form of credit default swaps (CDS) served as a relatively unregulated alternative to purchasing and selling insurance against defaults. Limited regulatory oversight of OTC derivatives made them attractive for use within the shadow banking system —'bank-like financial activities that are conducted outside the traditional commercial banking system, many of which are unregulated or lightly regulated' (FCIC, 2010). OTC derivatives were an integral part of the business strategies of off-balance-sheet entities, such as structured investment vehicles (SIV), as well as hedge funds and money market funds. Not coincidentally, the growth of the shadow banking sector grew in parallel with OTC derivatives to reach a point in 2007 where it was substantially larger than the size of the regular banking system in the U.S. (Pozsar et al., 2012).

Figure 1. Notional amounts outstanding for major OTC derivatives contracts




Because OTC derivative transactions were bilateral (not cleared through a central counterparty) and little or no regulatory reporting for their trading was required, the risk with their aggregate volumes was not readily apparent. Furthermore, the **complexity** and compound nature of derivative structures made it difficult to identify the ultimate risk bearer. For example, mortgage loans were bundled into securities, which were used to create derivatives in the form of credit default obligations (CDO). Subsequently, new CDOs were created as layers on top of pre-existing CDOs. In other words, older financial technology innovations, asset-backed and mortgage-backed securities, were combined with newer financial technology innovations in the form of CDOs and credit default swaps, to form structures where the risks were difficult to understand, let alone track. In particular, the models that credit rating agencies used to assess risk were not designed for the complexity and unique characteristics of these structures.

Ultimately, the size, complexity, interconnectedness, and leverage provided by the OTC derivative market, combined with opacity of risk exposures, led to a crisis of confidence. Lack of confidence in the solvency of counterparties and fears about the risks associated with derivatives caused parts of the credit and OTC derivatives markets to seize up. As a case in point, once the insolvency of large institutions became apparent as a material risk, repurchase agreement (repo) lenders withdrew from the market, in turn, causing the confidence crisis to become a liquidity crisis (Baklanova, 2015). In summary, novel use of OTC derivatives in conjunction with the financial environment exposed weaknesses in the financial market infrastructure. These, in turn, gave rise to financial contagion and ultimately led to widespread economic damage.

**Concerns**

Having provided background on how OTC derivatives were involved in the GFC, we will next examine specific concerns in more detail, particularly as they relate to FinTech innovations. However, it is important to first note that OTC derivatives were not intended to be “financial weapons of mass destruction” as the prominent investor, Warren Buffet, referred to them. Rather, they were designed to reduce risk concentration by enabling risk to be spread across multiple and diverse parties (Merton, 2005). Herein lies the overarching consideration

to bear in mind: it is difficult to predict how and for what purpose new technologies will be used over the course of time.

A core concern related to OTC derivatives was the extensive use of ***bilateral agreements*** between financial counterparties. For the most part, these bilateral agreements were exclusive to the parties involved in the agreements and thus, at the time, the types and scale of the risk exposure was difficult to assess in aggregate terms. In particular, the CDOs market was fragmented, largely relationship-based, and did not have an integrated market (Lysandroua et al., 2014). Hence, the insolvency of one counterparty could trigger the insolvency of another, creating a chain reaction. In particular, regulators and broader market participants had poor visibility of the systemic risks that OTC derivatives presented. When the GFC unfolded, they found themselves trying to quickly gather information that was necessary to assess the situation and formulate a suitable reaction. Lack of information led to a trial and error approach to remediation, rather than being able to follow a response plan (Gregory, 2014).

The extensive use of OTC derivatives by the ***shadow banking system*** further complicated the understanding of the interconnections, scope, and scale of how OTC derivatives were used. In other words, there was insufficient financial transparency. By the nature of banks' off-balance-sheet vehicles being exempt from systematic regulation, they were able to amass large amounts of risk. The opaqueness of the shadow banking market and the complexity of the risk constituted by its OTC derivative holdings led to doubts and confusion in the broader financial system and contributed to the liquidity crisis (Lysandroua et al., 2014). The combination of the growth of the shadow banking system along with its increasing use of leverage, which was facilitated by the use of OTC derivatives, led to a point where the shadow banking system became a systemic risk.

The *speed* at which different reactions occurred was also a major challenge within the GFC. On one hand, the market was reacting almost instantaneously, revaluing risk premiums in real-time and creating liquidity draughts overnight. On the other hand, much of the information related to the financial instruments that underpinned the crisis, could not be quickly amassed and evaluated. Lack of digitalization and automation of many OTC derivative contracts created an information gap that limited the effectiveness of the crisis response. In turn, the **speed of contagion** and collapse by far outpaced the rate of which a well-informed response policy could be implemented.

**Post-crisis Remedies**

To address the concern related to the extensive counterparty risk created by excessive bilateral contractual exposures, global regulators required many OTC derivatives to be cleared through ***central counterparties***. This change eliminated counterparty risk directly between the users of OTC derivatives. This rule was applied to standardized contracts, which represented a large portion of the OTC derivative market. However, it was not practical for more tailored derivatives that had unique structures and parameters. The risk associated with those bespoke agreements could not be readily determined and managed by a central counterparty.

To address the problem of ***financial transparency***, the G20's Financial Stability Board (FSB) initiated a process of financial data reporting for OTC derivatives across multiple

jurisdictions (BIS, 2012; FSB, 2015). Derivative transactions were required to be reported within a short period, typically one day after the trade was completed, to a trade repository that was sanctioned by the relevant regulatory body. Types of transactions that were reportable and entities that were required to report varied by regulatory jurisdiction. Table 1 shows the coverage and implementation schedule of OTC derivatives trade reporting for G20 countries.

Table 1 Implementation schedule of OTC derivatives trade reporting

| Jurisdiction | Initial Compliance Date |
|---|---|
| United States | 12 Oct 2012 |
| European Union | 12 Feb 2014 |
| Japan | 1 Apr 2013 |
| Singapore | 1 Apr 2014 |
| Hong Kong | 9 Dec 2013 |
| Australia | 1 Oct 2013 |

Problems related to the use of OTC derivatives by the shadow banking system, were addressed largely by ratings agencies increasing their oversight of off-balance-sheet securitization vehicles, such as SIVs, which improved transparency (Bean, 2008). Additionally, the trade reporting in some regulatory jurisdictions required OTC derivatives transactions with nonbank entities, such as hedge funds, to also be captured.

Moreover, there was a shift towards automation in the back-office processing of OTC derivatives. While this was desirable from an efficiency standpoint, it was more of a necessity to ensure timely and accurate regulatory reporting of transactional and outstanding position information.

In summary, OTC derivatives contributed to the GFC as a result of their proliferation as bilateral agreements, complexity and lack of standardization, lack of transparency, misuse, and speed of contagion when problems occurred. Having examined how a new financial technology contributed to financial instability, the next two sections will provide background on and discuss issues and risk related to smart contracts, a new information technology.

## 3. The characteristics of smart contracts

This section examines the characteristics of smart contracts and their use, particular in the context of financial transactions. The term “smart contracts” was introduced by Nick Szabo in a paper in 1997 (Szabo, 1997) as automated legal agreements with automated penalties, but the term did not come into mainstream use until the Ethereum Foundation used the term to refer to pieces of code deployed on the Ethereum DLT in 2013 (Vitalik 2013). “Smart contracts” is now a generic term used in the DLT community to describe the building blocks of distributed applications (dApps) on Ethereum. On Corda, IBM Hyperledger Fabric and other DLTs there is the same concept of smart contracts but sometime referred to by other names such as “chaincode”.

The implementation of smart contracts differs from traditional software applications in that the programmatic source code used to construct smart contracts is deployed onto an immutable data store in a DLT. As the code cannot be changed a new version must be deployed and all pointers to the code must be updated to the code's new location on the blockchain.

There are many different implementation platforms for smart contracts, and the available functionality varies. For example, Bitcoin has limited functions such as time lock, whereas Ethereum's smart contracts are "Turing complete", which means that any programmatic function can be coded within them. Smart contracts can be written in many programming languages, which are often converted to common byte code that is stored and executed on its DLT. Solidity is a particular programming language designed for smart contracts and the most common language used to construct smart contracts that run on Ethereum.

After a software developer writes a smart contract, it is deployed onto the DLT, validated for correctness (by miners on the Ethereum DLT) and then it is available to be called by any authorized party. This is ideal for business processes that span multiple organisations. For example, in the context of trade finance, a letter of credit is requested from an issuing bank by an importer of goods, the document is sent to the importer's advising bank, and then authorised by the exporter. Many steps in this process are currently performed manually which is slow and error prone. Using a smart contract application to manage letters of credit, all parties involved in the process can be authorised to see the document and processing status in real-time and take action accordingly.

Smart contracts can also call other smart contracts and there is no limit to the complexity of the applications that can be built. Furthermore, processing can take place between independent DLTs, such as Corda and Quorum further increasing the potential capabilities and the interconnectedness of data and processes.

Cryptocurrencies are one category of application that have been built using DLTs and, whilst being the initiator of the first DLT, bitcoin, their use is to transfer value between parties in a DLT. Cryptocurrencies can also be used as a way to support a DLT platform such as using Ether (the native cryptocurrency of Ethereum) to reward the miners for validating data and smart contracts in the DLT. Cryptocurrencies may also represent a physical asset such as real estate or diamonds or it may represent national currencies (Dale B. 2018).

Some of the key reasons DLTs and smart contracts are gaining in popularity include:

- Convenient - DLT technology offers fast, secure and convenient transaction processing.
- Low cost - smart contracts can remove intermediaries, such as banks, from processes, thus reducing transaction costs.
- Decentralization - no central organisation is required to execute smart contracts since the accounting activities are distributed across many different entities on the network.
- Transparency - DLT technology allows the details of every single transaction in the network to be stored in an immutable form. These records form audit trails that are available for inspection by authorised parties.
- Pseudonymity - DLT and smart contract users' identities are stored by unique identifiers that typically cannot be used alone to determine the identity of the user.

The current use of DLTs in finance is still very much in its infancy. There are a number of companies running proof-of-concept exercises, and some in a pilot phase, for example HSBC trade finance deal in May 2018 (HSBC 2018). There is a long way to go before the technology, operations and governance for DLT and smart contracts are ready to support large volumes and sensitive customer data but DLT applications offer great potential for business process that involves multiple parties. As the technology, security, governance of DLT and other issues and risks are being addressed over time and there is little doubt that decentralised solutions will become prevalent, integrating with centralised systems where necessary. The next section will highlight some of the key issues and risks that are currently concerns for the development and use applications based on smart contracts

## 4. Current issues and risks with smart contracts

Besides having the inherent risks of new technologies, DLTs have their own unique drawbacks as well. In the context of financial stability this section looks at a number of attacks on DLTs that can exploit vulnerabilities in the consensus protocol, data storage, applications connecting to DLTs, and bugs in smart contract code. Systemic problems could also arise from the complexity, interconnectedness, unexpected behaviour, and change management of smart contracts. For this paper the “DAO attack” on the Ethereum DLT is most interesting and will be covered in more depth.

### Consensus

The most critical element of DLTs is the consensus mechanism that ensures all data in the DLT is validated and that all the nodes in the network have a consistent copy of the entire ledger. The most well-used method is the “Proof of Work” (PoW) consensus protocol that is used to validate bitcoin transactions. However, PoW requires a significant amount of electrical power and only performs at a low processing rate of 16 transactions per second. Other consensus protocols are in use and more are being developed that are faster and less power hungry such as Raft, Proof-of-Stake and Hashgraph to name a few.

Any flaws in the consensus protocol, such as allowing a collusion of participants to change valid data, runs the risk of organisations legally misusing or even exploiting the flaw for illegal gains (Table 2). Once a flaw is discovered it could potentially be exploited quickly and widely.

### Data Privacy

Data stored on a DLT is visible to all nodes and to make transactional data private, it has to be stored in an encrypted form on the DLT or stored outside of the DLT, i.e. “off-chain”. Storing data in an encrypted form is risky if new technology, such as quantum computing, is developed that can break the encryption method used and hence, make the data readable. Alternatively, a vulnerability could be discovered with the encryption protocol used that renders it insecure. Storing data off-chain but keeping a reference to data on the DLT keeps the data safe, allows for validation if required and also allows the data to be destroyed if necessary, according to data management policies. The drawback of storing data off-chain is that the transactional process becomes dependent on the availability of a trusted party that provides the storage facility.

The balance here is to allow data to be as accessible as needed for the parties involved but as secure as possible to avoid data leakage. Regulators may also need access to the data to ensure transparency of risks (Table 2).

**Platform Component Security**

The most common cybersecurity problems that DLTs have encountered so far have been vulnerabilities in various peripheral components that work with and support DLTs, such as digital wallets and cryptocurrency exchanges. These have been hacked often (Neuron, 2018) and for example Mt Gox, which was the largest bitcoin intermediary and the world's leading bitcoin exchange, had a security breach on 19 June 2011 when it was announced that approximately 850,000 bitcoins belonging to customers and the company were missing and likely stolen, an amount valued at more than $450 million at the time. Also notable is a Hong Kong-based cryptocurrency exchange platform, Bitfinex which had 120,000 bitcoin, worth $72 million, stolen on 2 August 2016 due to a failure in their multi-signature wallets. More recently, in June 2018, hackers stole US$40 million in various cryptocurrency tokens from the Korean exchange Coinrail. It is important to acknowledge these problems with the current cryptocurrency organizations but at the same time it is crucial to recognize that these were all centralized entities that got hacked due to security issues that are not directly related to the cryptographic protocols. In other words, so far, no blockchain has been hacked directly (Risber J. 2018).

Standardisation and certification of platform components would help create a more robust DLT eco-system by component reuse, reducing complexity and increasing the ability to assess risks (Table 2). However, it should be noted that standardization also increases the speed and impact of problems discovered in the components.

**Smart Contract Breaches**

Beyond the cybersecurity threats to DLTs and cryptocurrencies, smart contracts have their own unique security concerns. These have led to problems such as the The DAO losing US$55 million in 2016, ShadowFork freezing US$1 million in 2018, and Parity losing US$50 million and freezing another $150 million in 2017. (Morisander, 2018).

The most analysed case is a The DAO which was a smart contract distributed application running on the Ethereum platform as a decentralised autonomous organisation (DAO). It was set up by a group of people to run a crowdfunding organisation that was operated entirely using smart contracts. The idea of DAOs have been around for some time (Dilger, 1997) and is ideally a legally incorporated entity that runs as a business but is fully automated. In June 2016, hackers exploited a vulnerability in The DAO code that enabled them to siphon off one third of The DAO's funds to a subsidiary account. In this case, there were two problems, the flaw that enabled the hacking and the reaction to the problem.

The hack was initiated due to a coding bug in one of the functions in the smart contracts running The DAO that allows users to spin off a separate company, take their money from the original company and transfer it to the new one. The code was re-entrant --i.e. it could be interrupted during its execution and then be initiated again before its earlier invocation had completed-- and subsequent invocations did not check if the funds had already been withdrawn. The hacker called the function multiple time removing their same funds multiple

times. By chance there was other, unrelated, code that stopped the attacker from immediately moving the funds from their account out of the Ethereum network.

What is also relevant for this paper is that after the attack had been discovered, two groups formed within the Ethereum community with different opinions on what to do. One group believed that the cryptocurrency that had been stolen should be deactivated so the hacker would not gain from their actions. This approach required changing some Ethereum code and a second group formed that opposed this approach because it went against the underlying philosophy that The DAO's behaviour should be determined only by its original code and without external interference. The code change was made, but the second group of "purists" continued to use the old DLT prior to the change. This created a fork in the DLT and resulted in two cryptocurrencies Ethereum, which used the new DLT, and Ethereum Classic, which uses the original DLT (Leising, 2017).

Given the newness of smart contracts, other attacks and programming errors will likely be found and additional risks that smart contracts present include the lack of precedence for resolving conflicts that arise with smart contracts. It is unclear how corporate law and regulatory agencies might treat automated organisations, such as The DAO, and contracts made with and within it when issues arise. With The DAO, there was also a risk that a "corporate veil" would not apply to protect investors from individual legal and financial liability for actions taken by The DAO and by contractors in which The DAO invested. Furthermore, from a legal and regulatory perspective it is unclear in many jurisdictions whether The DAO (and recent cryptocurrency token providers) were selling securities, and if they are, what type of securities those might be.

Similar to component risks mentioned above, standardisation of smart contracts would help create a more robust DLT eco-system by reuse by reducing complexity and increasing the ability to assess risks (Table 2). However, standardization can also increase the speed and impact of problems discovered in a smart contract.

**Interconnectedness**

The final risk to be addressed is that smart contracts can, and do, call other smart contracts within DLTs and across DLTs to facilitate end-to-end business processes, for example, cross-border settlement (MAS 2017). The interconnectedness of smart contracts could lead to a ripple effect and a rapid propagation of problems from one DLT to another. Likewise, it will increase the complexity of the DLT eco-system, thus increasing the risk of changes to the system, making it more difficult to identify potential issues, and making the resolution of problems more difficult and complicated (Table 2).

Having reviewed some of the known issues and risks with smart contracts, the next section will examine these and consider how they compare with problems encountered previously with OTC derivatives.

## 5. Parallels between OTC derivatives and smart contracts in relation to financial integrity

At first glance, there may seem to be little commonality between OTC derivatives and smart contracts. The former is a financial technology that is based on written legal agreements,

whereas the latter is an information technology based on digital ledger technology. Nevertheless, there are several similarities worth examining, as outlined in Table 2. These, in conjunction with other risks that are specific to smart contracts, could potentially threaten the integrity of the financial system under certain circumstances.

Table 2 Similarity of risks between OTC derivatives and smart contracts

| **Risk** | **Affect with OTC Derivatives** | **Potential concern with smart contracts** |
|---|---|---|
| Proliferation of bilateral agreements | Critical levels of counterparty risk that was difficult to assess the systemic impact | Flaws or problems with smart contracts could undermine the integrity of vast numbers of corporate agreements leading to a crisis of confidence |
| Complexity and lack of standardization | Unique and complex financial structures made it difficult to assess risks | Unique and complex technical implementations make it difficult to assess risks |
| Lack of transparency | Led to lack of trust between market participants and a crisis of confidence; hindered regulatory monitoring of aggregate risk | Anonymity could lead to difficulty in assessing risk exposure and remediating crisis situations |
| Misuse | Enabled the shadow banking system to avoided regulatory oversight, hiding potential financial risk | Use by legitimate and unlawful businesses to circumvent legal and regulatory restrictions, hiding potential financial risk |
| Speed of contagion | Regulators and governments could not respond as fast as the markets reacted | The technology would act so fast that regulators and governments would not be able to intervene, only respond after the fact |

The proliferation of bilateral OTC derivative agreements, which led to critical financial dependencies between counterparties could easily occur with smart contracts when the use and sophistication of smart contracts grows to the point where they are facilitate businesses transactions on a regular basis. Without a specific need or mandate to centrally clear or settle smart contract agreements, there is little reason why agreements should not be bilateral and thus, known only to the counterparties involved. Likewise, because of the relative ease of implementing smart contracts, the ultimate scale of the number of smart contract agreements could easily dwarf traditional contracts. Systemic risk could arise from failure or flaws with of the contractual mechanics, i.e. smart contract technology, rather than the agreements themselves. It is unclear how millions of bilateral agreements between thousands of counterparties could be dealt with, say in the case of the discovery of a cybersecurity vulnerability that was common to a large number of agreements, which could corrupt those transactions. The fact that the collapse of The DAO was a non-event systemically was largely due to its recent invention. Had it been established longer, with more investors, larger in financial size, or had it been used as the base source code for other smart contracts, the impact could have been much more severe. While, overall, the scale of smart contract use does not present an immediate concern, their impact would be significant if and when major business areas, such as trade finance, adopt and employ smart contracts on a wide-scale basis.

The problems related to complexity and lack of standardization, which were encountered with OTC derivatives, are also potential risks for smart contracts. The customization of smart contracts increases the risk of design and implementation errors, as was the case with The DAO, as well as makes it more difficult to assess their potential risk under various conditions. The time required to analyze and fully understand the structure of each unique agreement increases the challenge of quantifying aggregate risk. The availability of different technology platforms for implementing smart contracts, as well as different versions of the same platform, adds further to the challenge of assessing and managing their risk.

Concerns related to lack of transparency, which occurred with OTC derivatives, could be an issue for smart contracts. Without understanding who the counterparties are in different types of smart contract agreements, how many of those agreements are in place, what the aggregate financial risk that is represented by these agreements, it will be difficult to assess the systemic risk. Having a handle on such information would be critical in a situation in the future where there is a fault in the smart contract infrastructure. As seen in the case of The DAO, the investors were anonymous, and the individuals and corporate bodies affected could not be easily determined. Assessing the broader impact and entities affected would be paramount for avoiding a crisis of confidence, as occurred in the GFC. While the use of DLTs could provide a source of open and immutable records that could be used in such emergency situations, the value of this information would be dependent on how easily it could be accessed and interpreted.

Like OTC derivatives, smart contracts could potentially be used to circumvent regulatory oversight. Digital currencies provide an example of how DLT technology has been adopted by entities outside of the mainstream financial system. To avoid financial transaction monitoring and anti-money laundering (AML) checks instituted by banks, cybercriminals have leveraged digital currencies, such as bitcoin. Likewise, banks' reluctance to facilitate digital currency transactions, has further led to the emergence and growth of digital currency exchanges. These exchanges, in some cases, have avoided regulatory oversight and thus have become part of the shadow banking system. In the case of smart contracts, they may inadvertently, or by design, taken on characteristics of other financial instruments but avoided treatment as such. This in turn could lead to significant off-balance-sheet exposures that are not readily apparent to auditors or regulators.

The fully automated nature of smart contracts, could greatly accelerate the speed at which a financial crisis related to them would unfold. If there was a large-scale failure related to smart contracts, it is unlikely that regulators would be able to manage the situation as it occurred; they may only be able to take remedial action after its course was run. As a case in point, the high degree of automation and interconnectedness of electronic trading in the financial markets have led to several "flash crashes" that occurred with such speed: it has not been possible to determine the underlying cause and remedies until long after the problem occurred (CFTC, 2010). Where regulators had hours and days to take actions to try to limit the damage in the GFC, a chain reaction that involved many interconnected smart contracts could be over in a matter of minutes or seconds. Likewise, while historically, regulators have had the ability to nullify paper-based legal agreements by fiat, they will likely find it more difficult to intervene and stop or alter the automated execution of smart contracts.

## 6. Risk mitigation strategies for smart contracts

With these common risk areas in mind, this section considers what can be done to mitigate and reduce the likelihood of the use of smart contracts leading to systemic financial instability. Generally, the goals of risk mitigation are prevention, detection and effective response which can be largely achieved by means of standardisation, surveillance, data collection and analysis. The specific risk areas that are considered and the corresponding mitigations are shown in Table 3. All of these risks can be amplified by the growth of the DLT and smart contract ecosystem; however, by pressing for technical improvements, better monitoring, and robust standards in DLT and smart contract technology, regulatory bodies could reduce the risks that have been outlined. The next subsection identifies the areas where DLT and smart contracts could be enhanced. The subsection that follows it will show how those improvements help to reduce risk.

Table 3. Summary of risks and mitigations for smart contracts

| Risk | Mitigation |
|---|---|
| Proliferation of bilateral agreements | Monitoring |
| Complexity and lack of standardization | Standardized data and code, regulatory sandbox |
| Lack of transparency | Monitoring |
| Misuse | Monitoring, proactive regulation |
| Speed of contagion | Throttles and kill switches |

**Enhancements**

Standardisation of data and code in smart contracts is a major factor that would improve their robustness, and enable an automated environment to be created that supports robust testing and certification. Standardised data structures can provide references that make it easier to identify anomalies and detect defects and standardised code brings about consistent processing, with less room for unexpected behaviours. These can ensure that basic “hygiene” functions such as limit checking and reporting are included. Standards could also include mandatory failsafe mechanisms, such as throttle-backs and kill-switches, that could provide a means for regulators or other government bodies to intervene during a crisis.

Another area of improvement could be the use of more restrictive programming languages for constructing smart contracts. Most smart contracts are written in languages that are “Turing complete” meaning that they can perform any operation. This enables the applications to perform any function, but also allows many types of bugs to be introduced into the code. By limiting the flexibility of the coding language, the range of potential defects would also be reduced (Egelund-Muller, 2017). Ideally, a ‘sweet spot’ would be found whereby a language would provide sufficient capabilities for most smart contract processing, but no more. Use of more restrictive programming languages could also make it easier to automatically analyze smart contract code to reduce risk and improve efficiency. Leveraging development and deployment environments that facilitate code reuse, instead of code copying, would also decrease the number of defects in smart contract code when corrections are made to the code.

Data collection and monitoring is another area of enhancement. The data stored in a DLT is robust in that it can be validated by multiple parties before being finally stored and made immutable, and it can also be publicly inspected. However, the data is siloed within each DLT network and can be buried in blocks of thousands of transactions. Given that it is likely that many different DLTs will proliferate, real-time data collection, aggregation and analysis will be critical for monitoring purposes. Current DLT platforms provide functions for data to be communicated to off-chain storage facilities. Additionally, they could provide functions to allow distribution of transaction details or status information to be communicated on channels dedicated for transactional monitoring and data collection. Super-node validation is common in many private DLTs and is a structure to consider for constant monitoring of the networks and for implementing crisis management. Super-nodes could also communicate warnings and have agreed protocols for crisis response.

Enhanced regulatory involvement is another area that would help reduce risks if implemented in a way that does not impede innovation or create regulatory arbitrage situations. A regulatory “sandbox” --a special set of rules that enables businesses to perform limited tests of innovations in a live environment without having to comply with the full set of regulatory guidance that would be required for a regular implementation-- has been implemented in several countries and has room for further enhancement (Ng, 2018). The sandbox could be further extended to support automated testing, registration and certification for smart contracts and DLTs. In this case, the owner of the smart contract could provide the code in a specific format so that the automation would automatically analyse and document the code, test the behavior, and analyze the complexity and viability of the smart contract. This also provides tracking and an overview of the levels of sophistication being deployed.

**Risk Reduction**

Problems related to the proliferation of bilateral agreements can be addressed by monitoring smart contract agreements. If all agreements are executed by smart contracts and the DLT platforms they run on are open to inspection and can be easily interpreted by auditors and regulators, then monitoring oversight would be fairly straightforward. However, it is more likely that obtaining smart contract data from multiple DLTs in many different formats would make this approach impractical. Alternatively, built-in reporting capabilities within smart contracts could provide automated reporting of contractual details and lifecycle events to regulatory bodies, enabling them to monitor smart contract usage on a continual basis. This approach could also address risks related to lack of transparency. While it would be impractical to require monitoring for all smart contracts, it may be possible to prescribe monitoring requirements for classes of smart contracts that present significant risk.

The complexity of smart contracts is likely to increase as more assets become digitized on DLT platforms and more DTL platforms are developed. Code and data standardization will enable automated analysis of potential defects and behavior abnormalities *in vitro*. Likewise, regulatory sandbox enhancements, as described above, would help monitor how the complexities of smart contracts may interact and create problems *in vivo*. Lack of standardization could be tackled by the establishment of best practice guidelines for constructing smart contracts and, potentially, verified and enforced by testing in regulatory sandbox environments.

The risks of the misuse of smart contracts is likely to always be present as long as there are incentives and means to avoid oversight. Monitoring and reporting of smart contract activity would enable illicit or questionable smart contract transactions to be identified. Likewise, proactive regulatory steps, could be taken to reduce the risk of misuse. For example, to address issues related to the potential anonymity of the parties involved in transactions, use of standardized legal entity identifiers could be required so that the participants could be accurately identified. Likewise, if smart contracts were used in high volumes to hold funds in escrow and facilitate transfers, counterparty risk could balloon without having netting facilities in place. In this case, it may be prudent to require certain types of smart contracts to be settled via a central counterparty or consortium rather than through bilateral agreements. Note however, that the approach of relying on a centralized service provider is inherently at odds with the decentralized model that DLT platforms espouse.

The speed of contagion between smart contracts in a DLT environment is perhaps the most likely risk that could lead to a financial crisis. However, the use of standardized designs for smart contracts that include embedded failsafe mechanisms will help prevent chain reactions from getting out of control. Likewise, robust monitoring and reporting capabilities will enable rapid detection. Moreover, testing in a sandbox environment can support the development and testing of crisis response plans.

## 7. Conclusion

This paper has identified a number of potential risks related to smart contracts that could trigger financial instability and has reviewed past problems with OTC derivatives as a context for understanding these risks. Mitigations have also been suggested to help manage these risks, with the aim of helping to ensure that the financial ecosystem built upon smart contracts is stable and secure. As a conclusion, this section briefly discusses the relevance of exogenous risks for smart contracts, identifies areas for future research, and considers the trade-offs between various levels of regulatory intervention in rapidly developing FinTech, such as smart contracts.

Unlike OTC derivatives, where the risks were primarily endogenous and related to their usage by market participants, smart contracts also face substantial exogenous risks. Cyberattacks that target smart contract code directly or the DLT infrastructure that it relies upon could also lead to business disruptions and potential financial instability. Physical disasters, both natural or man-made, could also disrupt the processing of some or all smart contracts, causing major turmoil. The disruption to interbank payments following the terrorist attacks on September 11, 2001 provides an example of how external events can cripple what appear to be resilient systems (Lacker, 2003). While in this case, regulators were able to intervene to help avoid a banking crisis, they may not have the same latitude if a similar type of problem were to occur with smart contracts.

Based on this analysis, there are several areas of future research that would be valuable. One area of interest is research on the mechanisms that can be incorporated into smart contracts to facilitate regulatory reporting. Another area is how smart contract programming languages can be constructed and used to reduce the risk of programming defects. It would also be helpful to better understand and model how the interconnectedness of smart contracts could cause potentially destabilizing chain reactions. Likewise, there are a number of interesting questions related to the legal consequences of flaws or defects that might arise

with smart contracts, e.g. who is liable in cases where problems result from the interactions of multiple smart contracts. Finally, research into the characteristics of a regulatory environment or environments that can help ensure robust and transparent regulated transactions including further work on the open source development of legal repositories of clauses (Selman 2018).

As always, there is a trade-off between the cost and value of adding controls and monitoring to rapidly evolving FinTech, such as smart contracts, with the aim of avoiding potential catastrophes. On one hand, excessive intervention slows growth and stifles innovation. On the other hand, taking a *laissez faire* approach is imprudent given the likelihood of the eventual problems that may arise. It is important for guidelines to be put in place at an early stage of the development process to help set expectations as to what best practices are necessary. Doing so too late in the process may result in the persistence of vulnerabilities and risks that have been already embedded in infrastructure components. Likewise, requiring changes to established practices could lead to disaffection within the ecosystem. Nonetheless, it is important to keep in mind that innovation in financial and information technology are forces that help boost economies, and in turn, help to stave off financial crises. Thus, it is disadvantageous to place too heavy of demands on them without cause. In many cases, it may be judicious to closely monitor the progression of the technology, plan responses for potential disruptions, and be able to quickly respond with preventative measures when specific risks become clearly apparent.

**References**

Baklanova, V. (2015), “Repo and Securities Lending: Improving Transparency with Better Data,” *OFR Brief Series 15-03*, April 23, 2015, Office of Financial Research

Bank for International Settlements (2012), “Report on OTC derivatives data reporting and aggregation requirements,” available at: www.bis.org/cpmi/publ/d96.pdf

Bean, B (2008), “Enhancing Transparency in the Structured Finance Market,” *FDIC Supervisory Insights*, Summer 2008.

Egelund-Muller, B., Elsman, M., Henglein F., Ross O. (2017), “Automated Execution of Financial Contracts on Blockchains,” *Bus Inf Syst Eng,* 59(6):457–467

Commodity Futures Trading Commission and Securities & Exchange Commission, “Findings Regarding the Markets Events of May 6, 2010, Report of the Staffs of the CFTC and SEC toThe Joint Advisory Committee on Emerging Regulatory Issues,” September 30, 2010, http://www.sec.gov/news/studies/2010/marketevents-report.pdf.

Dale, B. (2018), “The Right Way to Think About Crypto Tokens”, https://www.coindesk.com/right-way-think-crypto-tokens/ . Retrieved 29 Aug 2018.

Dilger, W. (1997), “Decentralized autonomous organization of the intelligent home according to the principle of the immune system”, 1997 IEEE International Conference on (Vol. 1, pp. 351-356). IEEE.

Duran, R. (2017) *Financial Services Technology*, Cengage Learning Asia, Chapter 7.

Financial Crisis Inquiry Commission (2010) “Shadow Banking and the Financial Crisis”, Preliminary Staff Report, May 4, 2010.

Financial Stability Board (2015) “Reporting financial transactions to trade repositories in the Americas,” www.fsb.org/wp-content/uploads/Reporting-Financial-Transactions-to-Trade-Repositories-in-the-Americas.pdf

Gregory, J. (2014) *Central Counterparties: Mandatory Central Clearing and Initial Margin Requirements for OTC Derivatives*, Wiley, July 21, 2014, Chapter 4

Helbing, D. (2013) “Globally networked risks and how to respond,” *Nature*, 2 May 2013, Vol. 49, pp. 51-59

HSBC (2018) “HSBC and ING execute groundbreaking live trade finance transaction on R3’s Corda Blockchain platform”, 14 May 2018, https://www.hsbc.com/news-and-insight/media-resources/media-releases/2018/hsbc-trade-blockchain-transaction-press-release. Retrieved 29 Aug 2018.

Lacker, J.M. (2003) “Payment System Disruptions and the Federal Reserve Following September 11, 2001,” Federal Reserve Bank of Richmond Working Paper 03-16

Leising, M. (2017), “The Ether Thief”, *Bloomberg*, https://www.bloomberg.com/features/2017-the-ether-thief/. Retrieved 29 Aug 2018.

Luu, L., Chu, D., Olickel, H., Saxena, P., Hobor, A. (2016), “Making Smart Contracts Smarter”, *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, pp. 254-269

Lysandroua, P. and Nesvetailova, A. (2014) “The role of shadow banking entities in the financial crisis: a disaggregated view,” Review of International Political Economy, 2014

Monetary Authority of Singapore (2017) “Project Ubin: Central Bank Digital Money using Distributed Ledger Technology”, http://www.mas.gov.sg/Singapore-Financial-Centre/Smart-Financial-Centre/Project-Ubin.aspx. Retrieved 29 Aug 2018.

Merton, R.C. (2005), “You Have More Capital Than You Think,” *Harvard Business Review*, November 2005, pp. 85-94

Morisander (2018) “The biggest smart contract hacks in history or how to endanger up to US $2.2 billion,” Retrieved 28 August 2018. https://medium.com/solidified/the-biggest-smart-contract-hacks-in-history-or-how-to-endanger-up-to-us-2-2-billion-d5a72961d15d

Nakamoto, S. (2008) “Bitcoin: A Peer-to-Peer Electronic Cash System,” https://bitcoin.org/bitcoin.pdf. Retrieved 27 August 2018

Neuron (2018), “List of cryptocurrency exchange hacks,” https://rados.io/list-of-documented-exchange-hacks/. Retrieved 28 August 2018.

Ng D. and Griffin P. (2018) “The Wider Impact of a National Cryptocurrency,” https://www.globalpolicyjournal.com/articles/world-economy-trade-and-finance/wider-impact-national-cryptocurrency

Norris, F. (1994), “Orange County Crisis Jolts Bond Market,” *New York Times*, 8 Dec 1994, pp. 1

Peck, M.E., “DAO May Be Dead After $60 Million Theft,” IEEE Spectrum,17 June 2016, http://spectrum.ieee.org/tech-talk/computing/networks/dao-may-be-dead-after-40million-theft

Pozsar, Z., Adrian, T., Ashcraft, A. and Boesky, H. (2010) *The Shadow Banking System*, The Federal Reserve Bank of New York.

Risberg, J. (2018), “Yes, the Blockchain Can Be Hacked”, https://coincentral.com/blockchain-hacks/. Retrieved 29 Aug 2018.

Selman, D. (2018), “REALLY Smart (and Legal!) Contracts”. https://medium.com/@Clause/really-smart-and-legal-contracts-a77fcd1d0d10. Retrieved 28 Aug 2018.

Somanathan, T. V. and Nageswaran, V. A. (2015), *The Economics of Derivatives*, Cambridge University Press; 1st edition (March 2, 2015), Chapter 9

Szabo, N. (1997) “Formalizing and Securing Relationships on Public Networks,” First Monday. Retrieved 27 August 2018.

Vitalik, B (2013) "Ethereum Whitepaper," github. Retrieved 1 June 2017.

Weaver, N., “Risks of Cryptocurrencies,” *Communications of the ACM*, June 2018, VOL. 61, No. 6