
IIF
INSTITUTE OF
INTERNATIONAL
FINANCE
MAY 2016
GETTING SMART: CONTRACTS
ON THE BLOCKCHAIN

INTRODUCTION

Enabled by blockchain technology, smart contracts have the potential to transform commercial and financial agreements, facilitate faster securities settlement, new insurance products, better compliance solutions, and more transparency. For smart contracts to reach their full potential, however, key issues, both technical and legal, will need to be addressed. This paper will examine the promise of smart contract technology as well as the challenges and risks associated with its implementation.

A WORLD OF SMART CONTRACTS

A smart contract is a contract captured in code (Chart 1, pg.3) which automatically performs the obligations the parties have committed to in the agreement. The term was coined in the mid-1990s by Nick Szabo, a computer scientist who also studied law, though existed largely as a theoretical concept until the development of blockchain technology,[1] which has provided the necessary elements for smart contracts to function effectively, including cryptographic security and immutability.

Smart contracts self-execute the stipulations of an agreement when predetermined conditions are triggered. Once two or more parties consent to all of the terms within the contract, they cryptographically sign the smart contract and deploy it to a distributed ledger. When a condition specified in the code is met, the program automatically triggers a corresponding action. For instance, in theory a smart option contract could link to a market data service and automatically transfer shares from party A to party B in exchange for payment if the stock in question reaches a predetermined strike price. (Chart 2, pg.4) Or a smart insurance product could link to a weather data source and trigger a crop insurance payout if rainfall amounts drop below a particular level.

By removing the need for direct human involvement once a smart contract has been deployed onto a distributed ledger, the computer program could make contractual relationships more efficient and economical with potentially fewer opportunities for error, misunderstanding, delay or dispute.

According to Richard G. Brown, chief technology officer at R3, a consortium of banks, because a smart contract can operate on distributed asset ledgers, it can essentially act as an economic actor in its own right. A smart contract "responds to the receipt of information, it can receive and store value—and it can send out information and value (Chart 3, pg.5). It would be just like having a human who could be trusted to look after assets temporarily and who always did what they were told." This could have significant implications for the finance industry and beyond.

One of the most ambitious and well-known platforms being developed for advanced applications of the blockchain and smart contracts is Ethereum. Ethereum—an open-source development project that provides a decentralized platform for developers and entrepreneurs to create and publish next-generation distributed applications—uses blockchain technology to facilitate smart contracts that can act as a substitute to conventional business documents. The project's website emphasizes that the platform can be used to "codify, decentralize, secure and trade just about anything: voting, domain names, financial exchanges, crowdfunding, company governance, intellectual property, and smart property."

APPLICATIONS AND IMPLICATIONS

Combining law, computer science, and finance in unprecedented ways, smart contract technology has the potential to perform a wide variety of data-driven business functions and enhance transparency (Chart 4, pg.6).

1. For comprehensive background information on blockchain technology, please see our Banking on the Blockchain report.

Securities Trading

Due to legacy infrastructure, the time needed to transfer financial assets can be extensive. In the U.S., exchanges involving securities regularly take up to half a week, while loan settlements can extend to 20 days or more. This considerable time lag increases counterparty risk with serious regulatory consequences. Since the 2008 financial crisis, American and EU regulators have instructed banks to earmark larger amounts of capital to protect themselves from counterparty risk. Because smart contracts deployed on distributed ledgers could shorten settlement times from days or weeks to minutes for many financial products, they could mitigate risk and free up capital in the process, according to Blythe Masters, CEO of Digital Asset Holdings (DAH).

A number of firms are exploring and developing ways for smart contracts to be integrated with various securities, including bonds, futures, and options. New York City-based Symbiont, one of the leaders in the space, has created proprietary smart securities technology designed and built for capital markets. The technology allows financial instruments such as corporate bonds, syndicated loans, and bilateral swaps to be modeled in an "easy to understand programming language and fully digitized onto a distributed ledger." Mark Smith, the company's co-founder and CEO, told us that the use of a coding language reflecting native language was important to facilitate use by securities experts. The company, which issued its first private equity shares as smart securities using blockchain technology in 2015, is working with dozens of financial firms. According to a press release from early March, Symbiont is partnering with Ipreo—a data and software provider co-owned by Blackstone and Goldman Sachs—to create a new business that will seek to transform archaic procedures in the nearly five trillion dollar syndicated loans market. The press release states: "By integrating Ipreo's latest loan settlement platform and Symbiont's smart contract, the new business will deliver fully-automated settlement and maintenance, generating tens of millions of dollars in potential annual savings." Symbiont is also working with the State of Delaware, where over half of all publicly traded U.S. companies are incorporated, to allow smart contracts technology to register companies, track share movements, and manage shareholder communications in an automated digital environment. This is part of a blockchain initiative announced by Delaware Governor Markell on May 2 to create a "Delaware Blockchain" with Symbiont leading technology aspects and Pillsbury Winthrop Shaw Pittman leading legal and legislative elements. This early example previews some of the efficiencies smart contracts could deliver to corporations and government, as well as the potential impact of smart contracts on traditional market intermediaries.

CHART 1
Sample Coding for a Smart Bond Contract

```
// Global parameters

uint bondNumberSold;
uint bondNumberAvailable;
mapping(uint => addressContainer)
bondDistribution;
uint numberOfAddress;
address currManAddress;
address KYCRegistryAddress;
uint onHold = 0;

// Bonnd Structure

struct BondData {
string isin;
uint[] paymentDates;
uint singleIssuePrice;
uint interestRate;
uint repayment;
string currency;
}

BondData bondData;

foundAddress = 1;
uint currentAmount =
bondDistribution[i].amountBond;
currentAmount = currentAmount + amount;
bondDistribution[i].amountBond = currentAmount;
bondNumberSold += amount;
bondNumberAvailable -= amount;
}
}

if(foundAddress == 0) {
bondDistribution[numberOfAddress].addr =
msg.sender;
bondDistribution[numberOfAddress].amountBond =
amount;
numberOfAddress++;
bondNumberSold += amount;
bondNumberAvailable -= amount;
}

ConfirmationBondSale(msg.sender, amount,
initAmount);

}
```

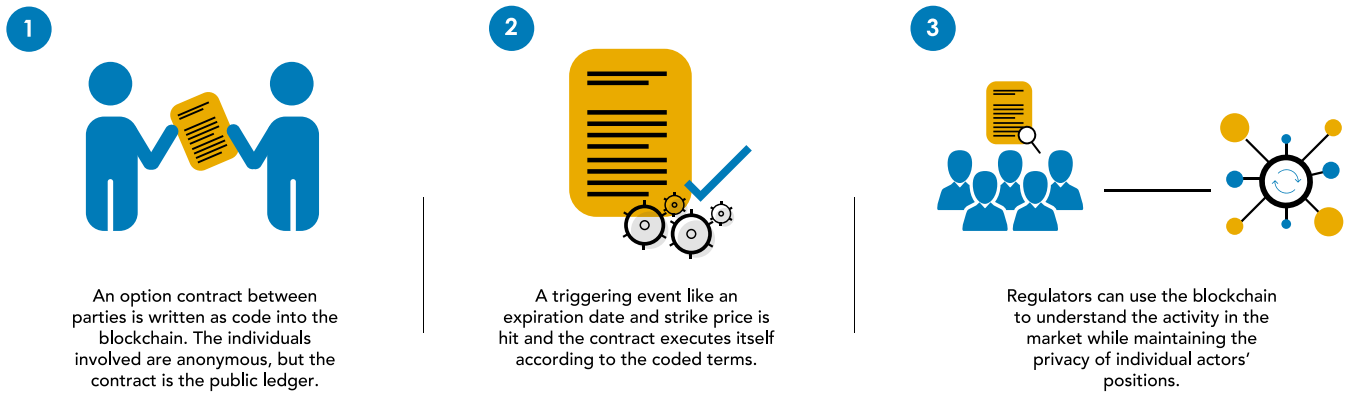
Source: UniCredit

In addition, it has been reported that UBS, in partnership with distributed ledger startup Clearmatics, is using Ethereum technology to build a smart bond platform that would execute commercial agreements automatically, for instance a note periodically paying interest to a holder.

Moreover, R3 announced in March that 40 of its bank consortium members—including Bank of America, BBVA, BNP Paribas, Citi, Credit Suisse, Goldman Sachs, HSBC, Mizuho Financial Group, and the Royal Bank of

Canada[2]—participated in an extensive trial of five distributed ledger technology vendors—Chain, Eris Industries, Ethereum, IBM, and Intel. According to the R3 press release, banks "evaluated the strengths and weaknesses of each technology by running smart contracts that were programmed to facilitate issuance, secondary trading and redemption of commercial paper, a short-term fixed income security typically issued by corporations to raise funding." Finally, Barclays successfully tested a way to trade derivatives using smart contracts on R3's very own distributed ledger system, Corda, which was released in April.

CHART 2
Representaion of Smart Contracts on the Blockchain



Source: Deloitte University Press

Insurance

Smart contracts could also bring significant changes to the insurance industry.[3] Thanks to the self-executing characteristic of smart contracts, various processes could in theory become automated, saving time and money. For instance, upon verification of a policyholder's passing, a life insurance smart contract could immediately release funds to the chosen beneficiary. The coded contract would establish the moment of disbursement by scanning online death registries in real time. Many observers believe that this process, and others like it, would help eliminate the prolonged delays and multiple human interactions frequently necessary in claims processing today. Moreover, because a smart contract removes the need for costly human intervention once it has been deployed onto a distributed ledger, several experts claim that insurance companies could reduce operating costs, resulting in potential savings to their customers.

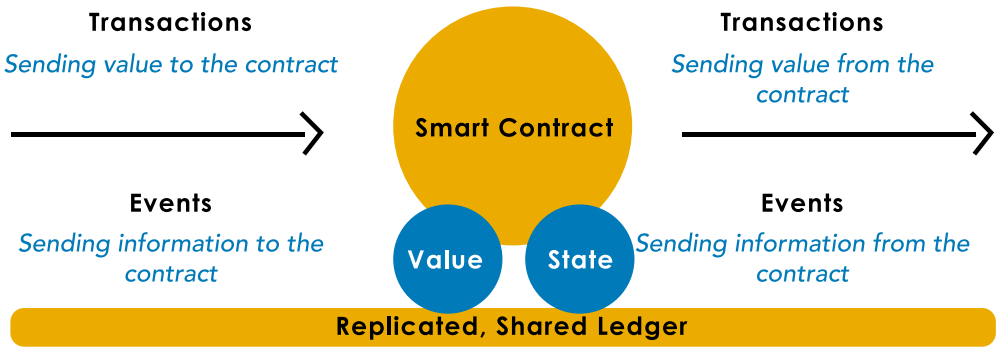
Another area where smart contracts could impact the industry is through peer-to-peer (P2P) solutions. Dynamis, a P2P insurance company, is developing a framework that uses smart contracts on the Ethereum blockchain to disintermediate traditional insurance firms by allowing policyholders to pool their funds and in the event of any claim, support one another financially. The company is focusing initially on unemployment insurance. According to the company's website, Dynamis "provides supplementary unemployment insurance by using the LinkedIn social network as a reputation system. Applicants for a new policy can use LinkedIn to verify their identity and

2. The full list of R3 member banks involved in this trial included Banco Santander, Bank of America, Barclays, BBVA, BMO Financial Group, BNP Paribas, BNY Mellon, CIBC, Commonwealth Bank of Australia, Citi, Commerzbank, Credit Suisse, Danske Bank, Deutsche Bank, Goldman Sachs, HSBC, ING Bank, Intesa Sanpaolo, J.P. Morgan, Macquarie Bank, Mitsubishi UFJ Financial Group, Mizuho Financial Group, Morgan Stanley, National Australia Bank, Natixis, Nordea, Northern Trust, OP Financial Group, Royal Bank of Canada, Royal Bank of Scotland, Scotiabank, SEB, Société Générale, State Street, TD Bank Group, UBS, UniCredit, U.S. Bank, Wells Fargo and Westpac Banking Corporation.
3. Innovation in the insurance industry will be the subject of our next fintech report.

employment status. Claimants can use their LinkedIn connections to validate that they are looking for work. The exercise of one's social capital within one's social network enables participants to obtain a new policy or open a new claim." The system, which is still in the development phase, could one day help reduce the costs of insurance.

Insurers might also customize their products by linking coded contracts with online devices. For example, travel insurance plans could collect premiums only when the smart contract is notified via the policyholder's smartphone that the person is indeed travelling. Similarly, a smart insurance contract could be embedded into vehicles and collect premiums based on the driving habits of the owner. Finally, the programmability of smart contracts may help minimize insurance fraud.

CHART 3
Smart Contract: A Visual



Source: Richard Gendal Brown

RegTech

Experts have also raised the prospect of smart contracts that enable more efficient regulatory and compliance functions, so-called "regtech." In theory, smart contracts could be coded to trigger automatic compliance with specific regulations or even internal compliance rules. Moreover, because contracts are documented on an immutable distributed ledger, a permanent financial audit trail would exist for interested parties, including regulators and supervisors.

There are numerous obstacles to regtech use cases, including the willingness of regulators to sanction them, but if realized these applications could have profound implications for an industry facing skyrocketing regulatory and compliance costs. In a 2014 letter to shareholders, JPMorgan Chase said that it added 13,000 employees from 2012-14 to support regulatory, compliance and control efforts, at a cost of $2 billion. In the same years, it spent a combined $600 million on technology for regulatory and compliance functions. Deutsche Bank spent an additional €1.3 billion on new regulatory requirements in 2014, and UBS spent $946 million on regulatory demands the same year. Deloitte estimates that the European insurance industry spent between $5.7 and $6.6 billion in 2012 to comply with new regulations.

The Internet of Things and Smart Property

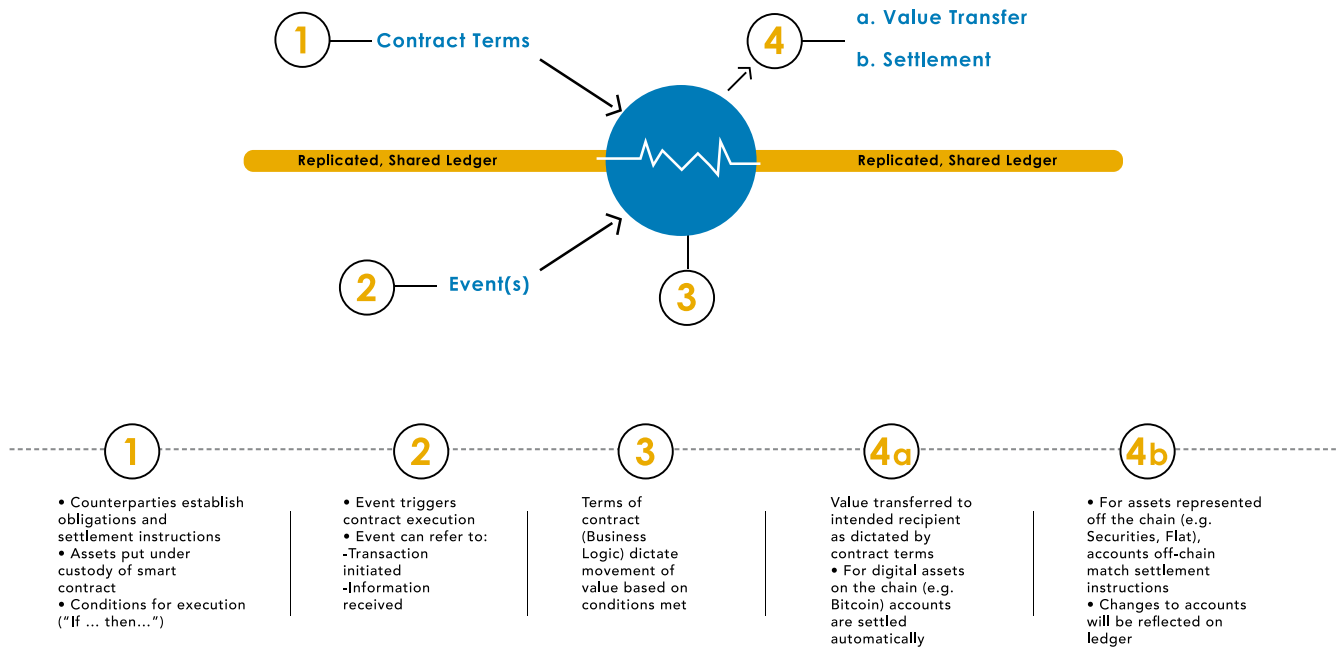
A far-reaching potential use case for smart contracts is to connect them with the Internet of Things (IoT). This could, according to some advocates, allow the transfer, access, and ownership of property that can communicate with the online world—what is often referred to as "smart property,"[4]—to be controlled via blockchain and smart contract technology. This would have a significant impact on the global economy according to various

4. Smart property could include houses, cars, boats, and appliances.

experts as the technology could permit property ownership to be transferred in a safe, quick and transparent manner without an intermediary as per the agreed to conditions set out in the smart contract.

Today, the Internet of Things includes billions of nodes sharing data through the Internet. These range from cars and appliances to energy and transport infrastructure. According to Gartner, a global IT research and advisory firm based in the U.S., 2016 will see 5.5 million new "things" become connected to the Internet daily, and by year's end the world will have 6.4 billion connected devices—up 30% from the previous year. By 2020, that number is forecast to reach 20.8 billion (Chart 5, pg.7). Going forward we will see exponential growth in the volume of data (Chart 6, pg.7), thanks in large part to the vast and valuable information that Internet-connected properties and devices will transmit.

CHART 4
Smart Contracts Applied in a Business Setting

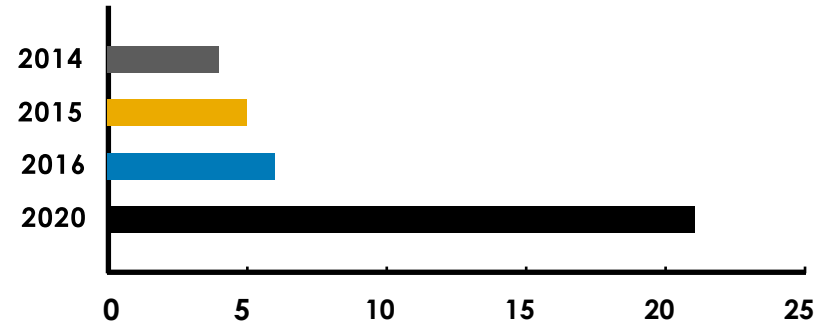


Source: BBVA Research

The confluence of these various technologies and trends could lead to many intriguing opportunities with widespread implications. For instance, German startup, Slock.it, is using smart contracts on the Ethereum platform to allow people to "rent, sell or share anything—without middlemen." IoT-enabled physical devices or properties such as apartments, cars, parking spots, bicycles, and washing machines could all be controlled using the technology. According to co-founder Christoph Jentzsch, "When someone purchases a Slock,[5] it will be connected to the Slock smart contract in the Ethereum blockchain and controlled by it…The owner of a Slock can set a deposit amount and a price for renting his property, and the user will pay that deposit through a transaction to the Ethereum blockchain, thereby getting permission to open and close that smart lock through their smartphone. The deposit will be locked in the Ethereum blockchain until the user decides to return the virtual key by sending another transaction to the Ethereum blockchain. Then the contract will be automatically enforced. The deposit will be sent back to the user minus the price for the rental which will be automatically sent to the owner of the Slock."

5. According to the company's website, a "slock" is a smart, safe, and secure lock.

CHART 5
Internet-Connected Devices
installed units, billion



Source: Gartner

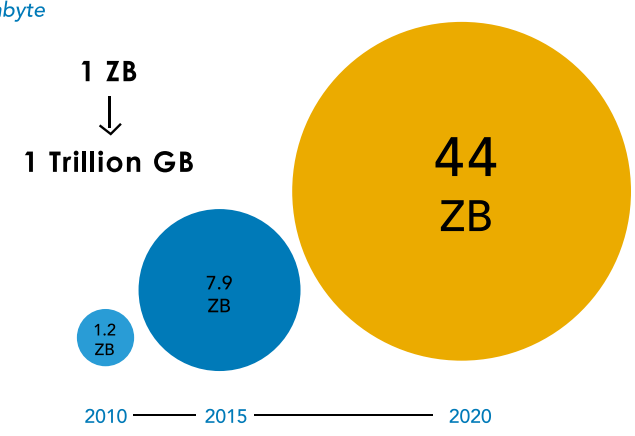
Another company looking into connecting the Internet of Things with smart contracts is IBM. Through the use of its Watson IoT Platform, the company envisions barcode scanners, radio-frequency identification (RFID) chips and other technologies to transmit data to distributed ledgers to validate or update smart contracts. In a company press release from February, IBM provided an example of how the process could work, "As an IoT-connected package moves along multiple distribution points, the package location and temperature information could be updated on a blockchain. This allows all parties to share information and status of the package as it moves among multiple parties to ensure the terms of a contract are met."

Combining these technologies could help facilitate the decentralization of the sharing economy and disrupt disruptors such as Airbnb and Uber. Visionaries see many intriguing opportunities, including providing car-leasing companies the option to program into a smart contract the automatic deactivation of the digital key needed to operate a leased vehicle if a loan payment is missed by the counterparty and semi-autonomous appliances that are capable of independently ordering and paying for supplies. It does not take a lot of creativity to imagine all of the far-reaching applications—as well as the implications for traditional intermediaries—resulting from smart contract, distributed ledger and IoT technologies operating collectively.

Other Use Cases

There are many other areas where smart contracts may be leveraged. For instance, the technology could simplify the loan and collateralization process. By using smart property as collateral, people could borrow money more easily, according to some industry observers. Moreover, should a borrower fail to make payments to a lender, the computer program could automatically rescind the digital keys that grant the defaulter access to the collateral. Some observers believe that this may lead to increased lending because in the event of a default, repossessing collateral would be cheaper and less time-consuming for lenders. In addition, smart contracts could help partially automate escrow accounts and inheritance procedures, leading to cost-savings and overall efficiency gains, according to several experts. Finally, smart contract technology could be used for real estate applications, making home ownership more affordable by helping eliminate mortgage processing fees, as well as improving and modernizing land registry systems with increased verifiability and transparency of land offices' activities, thereby reducing the likelihood of fraud and corruption, especially in countries where the rule of law is fragile. Eris Industries, a small but growing technology company with offices in London, Berlin, and New York City, highlights its technology as a vehicle for such purposes. Its platform, Eris, which has been forked from Ethereum, is a free and open-source software that

CHART 6
Active Growth of Global Data
zettabyte



Source: CSC, IDC

"allows anyone to build their own secure, low-cost, run-anywhere data infrastructure using blockchain and smart contract technology," according to the company's website. Nina Kilbride, a developer at the company, told the IIF that for real estate applications, users may use Eris for "deed and lien registries, mortgage originations, collateral agreements and derivative assets." Eris offers other use cases as well and the firm has formed a strategic partnership with PricewaterhouseCoopers for smart contracts and works with leaders in the finance industry, including R3 and Suncorp—a financial services company based in Australia.

OUTSTANDING ISSUES

As with other cutting-edge innovations, concerns and questions abound, including issues surrounding technical viability, legal validity, the potential to facilitate criminal activity, and implications for financial stability—all of which will need to be addressed moving forward.

Technical

There are several technical concerns surrounding the innovation that could hinder its implementation in the real world. The first is irrevocability. One of the essential benefits of smart contracts is the automatic performance of its obligations. However, in the existing world of "dumb" contracts, contracts can be discharged by impossibility (the death of one of the parties or destruction of the subject matter of the contract), by illegality (including illegality that arises after the contract is finalized) and so on. Flexibility is built into contract law to avoid the need for lawyers to anticipate and negotiate every possible outcome. A smart contract, however, becomes irrevocable once the coded agreement is deployed on a distributed ledger. Several observers believe this rigidity could hinder the technology's potential and recommend mechanisms that provide ways to amend smart contracts when mutually desired, or when deemed necessary from a legal or regulatory point of view. For example, a smart contract could be set to trigger a payment to a party who then appears on a financial sanctions list. At an IIF Blockchain Roundtable in Washington, D.C. on April 14, Ari Juels, co-director of the Initiative for Cryptocurrencies & Contracts (IC3) at Cornell Tech, noted that this perceived lack of flexibility in smart contracts could be addressed by inserting an "escape hatch" into the code of the contract thereby providing someone with the right cryptographic key to interject and modify the agreement if necessary.

The second technical concern centers on the ability to integrate external data sources. Because blockchain is a consensus-based system, each node on the blockchain has to agree on any external data triggering a smart contract condition. In order to avoid the need for each separate node to download and verify external data, some systems rely on "oracles" to verify the data and embed it in the chain. That is technically feasible, but means that the oracle now acts as an intermediary, undermining some of the benefits of a distributed system.

The third technical challenge facing smart contract adoption is the limited use of distributed ledger technology today. Given that shared, replicated ledgers are required for the functioning of smart contracts, the standardization and widespread adoption of blockchain technology is paramount to the success of algorithmic agreements. Consequently, the challenges facing the adoption of distributed ledger systems—including interoperability issues, scalability, and the cost of overhauling legacy infrastructure—are indirect obstacles to smart contract deployment.[6]

6. Please see our earlier report for an explanation of the obstacles to distributed ledger technology adoption.

Finally, in view of the complex skills required to develop and deploy smart contract systems, only a select few people could make use of it today. More user-friendly platforms based on everyday language will need to emerge for commercial adoption and network effects to take place.

Legal

Not surprisingly, there is substantial work to do sorting through the legal issues regarding smart contracts. For example, smart contracts present challenging issues of jurisdiction: which courts would litigate any dispute and whose laws would apply to determine the legality of the contract or to resolve any interpretive questions? In the course of considering a contractual dispute, could a litigant submit the blockchain as a business record or is it hearsay? How would parties demonstrate acceptance of contractual terms in a way that satisfies courts?

Because few lawyers have the coding skills to draft their own smart contracts, computer programmers would play a larger role, creating new liability questions for faulty algorithms and even ethical issues regarding the practice of law by non-lawyers.

Conceivably, smart contracts could reduce some legal cost around contract execution and dispute resolution by making execution automatic. However, legal cost could shift from execution to the drafting phase. As Houman Shadab, a professor at New York Law School, has pointed out, "By requiring parties to strictly commit, at the outset, to decisions of a smart contract, the need for transactional attorneys and others to structure smart contractual relationships may increase. Parties would most likely want to specify a more detailed range of contingencies and outcomes ahead of time before committing themselves to abide by the decisions of a software-driven contract."

Any smart contract on a public or permissionless system could run up against consumer privacy laws and could involve complicated anti-money laundering (AML) and know your customer (KYC) procedures. Smart contracts in some areas would implicate specific commercial law provisions. For example, would the Uniform Commercial Code (UCC) need to be amended to accommodate securities transactions on a smart contract?

Criminal Activity, Financial Stability, and Consumer Protection

According to a pre-publication paper released by the Initiative for Cryptocurrencies & Contracts (IC3) at the Jacobs Technion-Cornell Institute at Cornell Tech in New York City, several potential risks could arise with smart contract technology on certain types of decentralized distributed ledgers such as Ethereum. Examples cited by the report's authors—Ari Juels and Elaine Shi, two professors from Cornell University, and Ahmed Kosba, a researcher at the University of Maryland—include "leakage of confidential information, theft of cryptographic keys, and various real-world crimes such as murder, arson, and terrorism." Because the technology allows mutually distrustful parties to confidently and anonymously engage with one another, and the automatic execution of agreed terms, it could create new underground markets whereby malicious agents could hire hackers, assassins, or terrorists, to carry out criminal and even sinister acts depending on their objectives. Once the contract receives confirmation that a job has been completed—for instance, by automatically scanning media outlets for reports of a terrorist attack—it would release funds to the perpetrators.

In addition, financial stability and consumer protection are key areas of concern according to a report recently released by the IMF. "Widespread use of smart contracts could increase risks to financial stability by automatically propagating adverse events through the financial system, with self-reinforcing feedback loops (similar to the risks posed by automated high-speed trading)." The report goes on to state, "The complexity of smart contracts may also make it hard for consumers to understand what they are agreeing to. Regulators and the court system may find it difficult to keep pace with these developments." Axel Weber, chairman of UBS, also listed this as a potential consumer protection concern at the IIF Blockchain Roundtable in April when he asked, "Are smart contracts maybe too smart for the ultimate users?"

While the aforementioned list of concerns is extensive, advocates of the technology maintain that technological advances, industry collaboration, legal framework developments, advances in effective laws, and appropriate and reasonable oversight should not only be able to minimize them but also ensure that the benefits of smart contracts would far outweigh the risks. While this may prove to be true, the legal and technical questions and challenges surrounding smart contracts, combined with the various risks, will likely contort lawyers, policymakers and computer scientists for years to come.

CONCLUSION

Enabled by blockchain technology, the possibilities surrounding smart contracts are far-reaching and could significantly impact the finance industry and the economy as a whole moving forward. Thanks to the technological characteristics of smart contracts—namely the ability to securely receive, store and send both information and value based on predetermined rules and conditions mutually agreed to by contract counterparties—they could help decentralize the model of trust, speed up settlement times, reduce the need for costly intermediaries, enhance transparency, automate processes, reduce legal disputes, mitigate risk, and become the norm for countless types of transactions. However, for smart contracts to achieve this potential and become widely adopted by the mainstream economy, issues regarding legal legitimacy, regulation, technical viability, and the standardization and broad-based implementation of distributed ledger technology will need to be addressed.

Questions or comments regarding this publication may be addressed to:

Kristen Silverberg
Managing Director
ksilverberg@iif.com

Conan French
Senior Technology Advisor
cfrench@iif.com

Dennis Ferenzy
Associate Economist
dferenzy@iif.com

Stephanie Van Den Berg
Program Associate
svandenberg@iif.com