REVERSE ENGINEERING SMART CONTRACTS: LET'S NOT KILL ALL THE LAWYERS (OR ANYONE ELSE) JUST YET

A business case for smart contracts argues that smart contracts will reduce transaction costs, performance risk, and transaction settlement times because they will simplify and automate tedious and repetitive processes currently performed by humans, and they will eliminate unnecessary intermediaries. Based on these assumptions, and without significant improvements in technology, smart contracts will be useful for transactions with straightforward performance mechanics that can be easily automated and that do not rely on observation or judgment.

Introduction

Financial institutions are among the leaders of smart contract innovation. Multiple parallel processes for the development of smart contracts and their infrastructure are being advanced. Experts predict that the first smart contracts will be active by the end of this year.

Much has been written about smart contracts, in particular during the last two years, during which developments on multiple fronts have occurred. The result is a publicly available, evolving, splintered body of work by consultants, law firms, and technology specialists, among others, that seeks to explain what smart contracts are and how they can be useful. This article distills and aggregates some of this literature to provide a framework for issues raised by smart contracts. It examines from a broader perspective how smart contracts are intended to function, what consequences might occur, and whether those consequences are desirable. This article:

1. overviews smart contracts;
2. describes the current technology financial institutions use to form, record, and perform their transactions, and briefly summarizes a business case for financial institutions to adopt smart contracts;
3. describes smart contract architecture and illustrates an efficiency;
4. highlights some business and legal issues to consider and proposes solutions to a few of them; and
5. concludes with sociopolitical implications raised by the technology on which smart contracts are built.

Simplified diagrams appear in this article to illustrate various concepts as a convenience only.

1. Overview of smart contracts

Smart contracts rely on blockchain technology, which was used initially to facilitate the sale and purchase of cryptocurrencies.

Smart contracts

Smart contracts (with the appropriate infrastructure) are intended to perform three functions that are supported by current technology: (1) they will be evidence of a contract; (2) they will act as a system of record; and (3) they will facilitate the automatic performance by contracting parties of those terms and conditions that can be translated into non-qualitative data. To accomplish these functions, smart contracts will translate a pre-existing contract into blockchain technology that interfaces with and can prompt those operations systems that are required to perform, or monitor the performance of, obligations under the smart contract. The more technologically ambitious predict that smart contracts will facilitate contract formation.

Blockchain technology

The internet, a decentralized network of computers serves as the foundation for blockchains. Like the internet, blockchains exist on decentralized networks of computers that leverage the connectivity provided by the internet. Often, blockchain is described as a network without a backbone. These descriptions, "decentralized" and "without a backbone" are negative; rather than describe what the internet and the blockchain are, these descriptions state what they are not. Visualizing what something is not is harder to do than visualizing what it is. Thus, a more adequate, if colloquial, description of the blockchain is that it looks like a fishnet. In fact, it is a fishnet that sits on top of a fishnet.[1]

Each computer that forms the blockchain network contains a ledger that records the same information and which builds on past recorded information. Once recorded, the information is supposed to be immutable.

There are two types of blockchains: (1) public, that users, who are anonymous to one another, access with keys; and (2) proprietary, that the parties to a smart contract also access with keys and where the parties may be disclosed to one another. One or more enterprise(s) own(s) all of the computers that comprise a proprietary blockchain.

Whether public or proprietary, the blockchains rely on media of exchange to complete the transactions that they record. These media, cryptocurrencies, tend to be either Bitcoin or Etherium, but some developers can create original technology for original proprietary blockchains.[2] Proprietary blockchains that use proprietary media would be attractive for regulated entities for a variety of reasons.

Sale and purchase of cryptocurrencies

The blockchain initially facilitated the settlement of contracts for the sale and purchase of cryptocurrencies. Contracts for the one-time payment of money in exchange for an asset can be simple. Performance of the contract occurs when: the buyer makes payment, the seller receives payment, the seller transfers title to the asset to the buyer, and the seller delivers the asset to the buyer.

---

[1] See, Ramo, Joshua Cooper, The Seventh Sense: Power, Fortune, and Survival in the Age of Networks, Little Brown and Company (2016), at 130 (Summarizing the concept developed by Paul Baran in 1961 of a non-centralized network over which data packets would travel as a solution to replace the vulnerable hub and spoke network the United States relied on during the Cold War – it would look like a "fishnet.")

[2] For simplicity, this article refers to that technology, along with Bitcoin and Etherium, as cryptocurrencies.

At the same time, cryptocurrencies have limits. This diagram illustrates that cryptocurrencies appear to be a mere medium of exchange whose value is expressed in the terms of real world currencies that are backed by the full faith and credit of their respective governments. Cryptocurrencies, whether proprietary or backed by no one, depend on the blockchain for their existence; they have no "inherent value".[3]

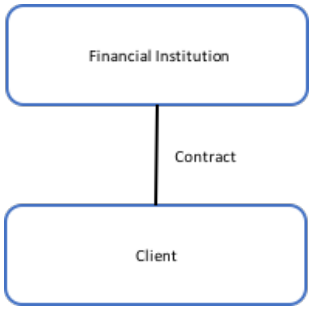
Yet, as a medium of exchange, cryptocurrencies could radically simplify existing payment mechanisms among financial institutions. That could explain why cryptocurrencies are fueling the development of the blockchain for more complicated payments and other applications.

2. Current technology; business case for smart contract technology

This section: describes the current technology financial institutions use to form, record, and perform their contracts now; then summarizes a business case for smart contracts. Together, they serve as a basis for understanding how smart contract technology could represent an improvement over current technology.

Contracts

A contract is a relationship between the parties to it that the law will recognize and enforce, if certain elements are present. Evidence of a contract may be oral or written, whether on physical or electronic media.



If written, the writing may be as informal as a few numbers or words sketched on a cocktail napkin, or it can be as formal as the parties and their lawyers desire.

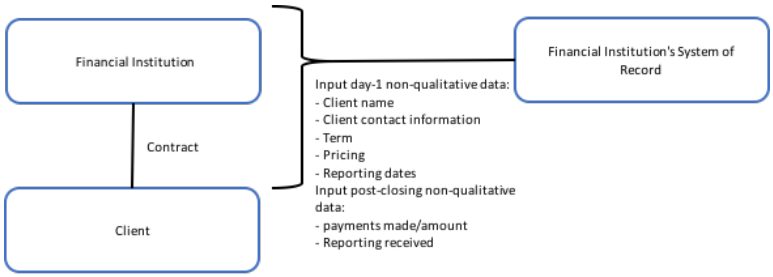
Systems of record; automation

Systems of record already exist. They can take many forms: spreadsheets, calendars, or sophisticated computer programs.[4] Irrespective of their form, systems of record are master sources of

[3] This muted view of cryptocurrencies, shared by many large banks and, recently, by Tidjane Thiam, the chief executive of Credit Suisse, may not be shared by all. In early November, the press reported that hedge funds are investing increasing amounts of money in Bitcoin, whose value has increased by 600% since the beginning of 2017, and that Bitcoin derivatives are being developed to allow institutions to trade it without the risk of acquiring it. Popper, Nathaniel, *Hedge Funds Push the Price of Bitcoin to New Highs*, The New York Times, November 6, 2017 (Viewed November 16, 2017). Perhaps Bitcoin has intrinsic value; perhaps this is opportunistic behavior.

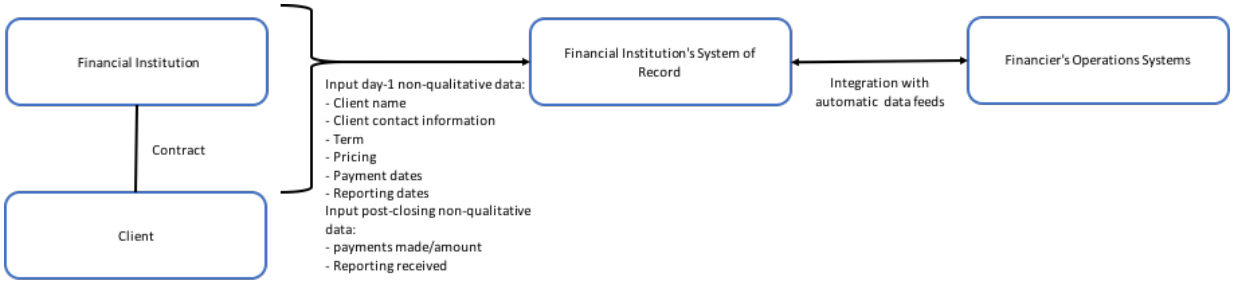
[4] This brief list is not exhaustive nor are the solutions mutually exclusive.

data that financial institutions rely on to track and facilitate the performance their transactions. For example, they may crystallize non-qualitative data set out in contracts, such as: party identity, contact information, currency, pricing, term, due dates, and reporting dates.



Where a financial institution has a sophisticated system of record, an employee typically uploads the contract data into the system of record using a graphical user interface. Post-funding, systems of record may also include contract performance history, such as when payments are made and in what amount and whether reporting has been received.

The ideal system of record would be integrated into a company's operational systems with automatic data feeds and automatic event triggers. A company's operational systems might include, for example: pricing, accounting, tax, regulatory reporting, a document library (electronic or physical), bank accounts, and invoicing:



In the real world, the extent of that automation varies. For example, while the vast majority of invoicing may occur automatically, there may be a small percentage of invoices that must be issued manually, and all of the invoices issued will be double checked by employees. Some may even post or fax the invoices to their clients, instead of emailing them. The business concerns include: the management of transactions that have unique features that render automation impractical; and/or compliance with confidentiality obligations and/or policies.

Other tasks that do not lend themselves to automation include complex tasks, such as covenant compliance. There, the client must do the work necessary to prepare and submit a covenant compliance certificate to the financial institution. The employees of the financial institution then verify the information on the certificate by comparing the certificate to the client's data. Assuming the client data includes its financial statements, the financial institution's employee will review the notes to the financial statements. Depending on whether the covenant compliance certificate is acceptable, the employees confirm within the system that the client has satisfied its obligations or that follow up action is required.

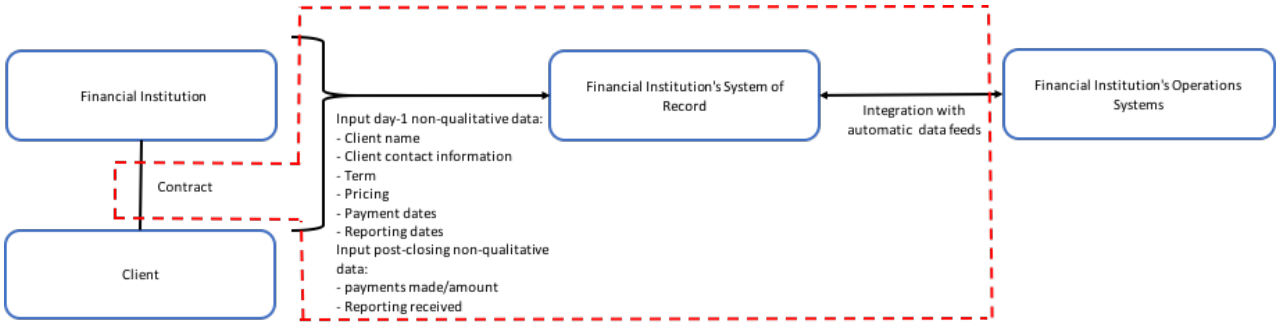
Automatic payments already exist. For example, some financial institutions in the United States may require their clients to set up an automated clearing house authorization for direct debits, whereas some financial institutions in the United Kingdom may require their clients to provide them with its analogue. In either case, the result is the same: the client authorizes an automatic payment made from

its account to the account of the financial institution of amounts owing to the financial institution as and when they are due.

A business case for financial institutions to adopt smart contracts

In 2016, Capgemini Consulting and Capgemini Consulting Technology Outsourcing published an article titled, Smart Contracts in Financial Services: Getting from Hype to Reality, which describes a business case supporting the adoption of smart contracts in the consumer lending, the syndicated lending, and the insurance markets, among other things.[5] Essentially, financial institutions, which have costly redundant or overlapping legacy systems, need a solution that streamlines their processes. Replacing these legacy systems with simpler, standardized solutions is predicted to result in savings, quantified by Capgemini, that will benefit both financial institutions and their clients.

The proposed smart contract solution merges evidence of the contract with the system of record and ties both into operations systems. The red dotted line represents the perimeter of smart contract functionality.

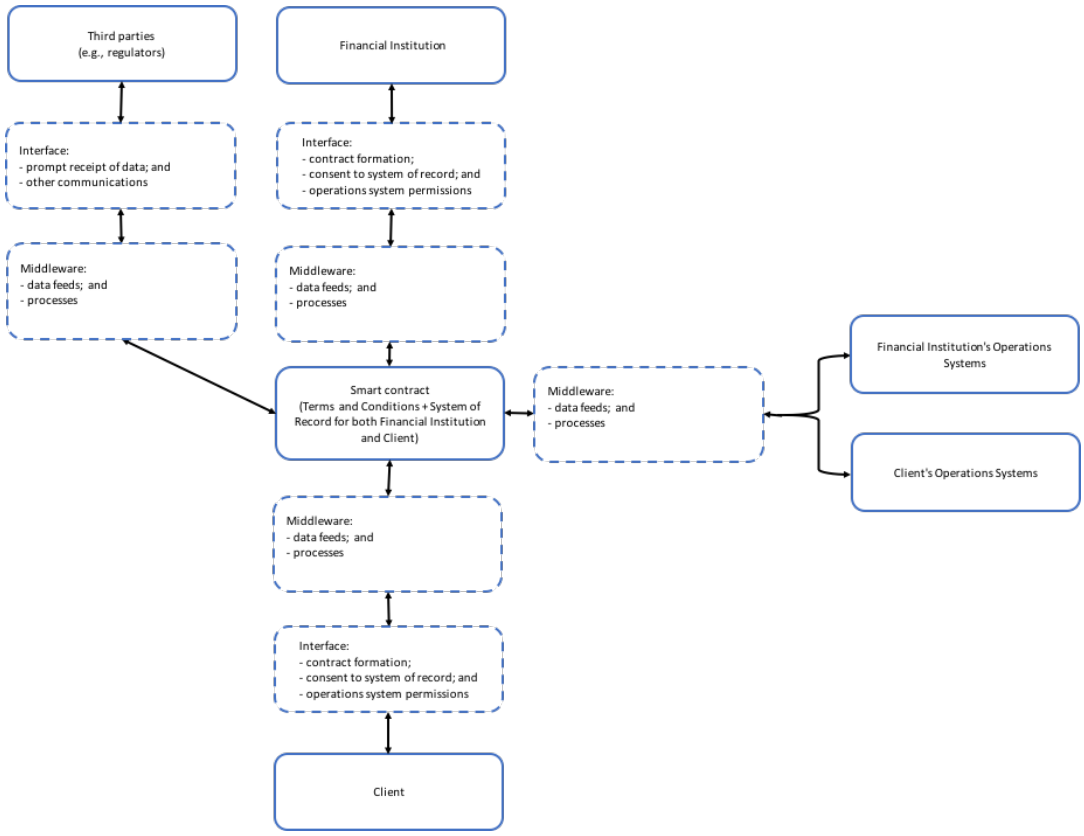


3. Smart contract architecture; proposed efficiency

The broader smart contract solution advocated by Cap Gemini includes data feeds among a variety of operations systems, contract parties, and third-parties, such as regulators. One must also consider crucial operational aspects of a functioning system, such as how the blockchain that hosts the smart contract will interact with the client, the financial institution, and the other parties as well as off-chain data. Two solutions are graphical user interfaces and middleware.

At present, the blockchain user experience tends to be poor because it relies on text-based user interfaces that require specialized coding skills. Developers are working on graphical user interfaces that overcome this hurdle, because improved user experiences are predicted to lead to widespread acceptance of blockchain. Middleware describes a solution that will connect both the operations systems of the client and the financial institution to the smart contract as well as other data that is external to the blockchain, to the extent that is required or desirable for the smart contract to function.[6] If these solutions can be adopted by financial institutions, a simplified diagram of the relationships among the parties might look like this:

[5] Capgemini Consulting and Capgemini Consulting Technology Outsourcing, Smart Contracts in Financial Services: Getting from Hype to Reality, https://www.capgemini.com/consulting-de/wp-content/uploads/sites/32/2017/08/smart_contracts_paper_long_0.pdf (Viewed on October 22, 2017).
[6] SmartContract has developed ChainLink, one such middleware. Their website (www.smartcontract.com) clearly defines middleware and illustrates its applications.



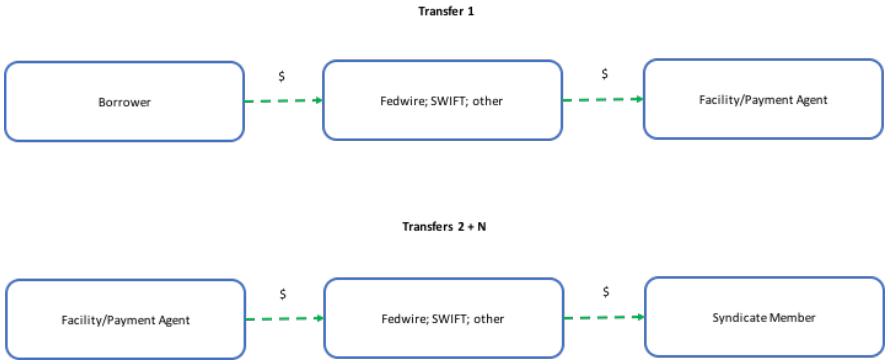
Though complex and costly to develop, this architecture is predicted to render processes, like payment mechanics, more efficient.

Payments

Currently, a payment between financial institutions will transit Fedwire, SWIFT, or another payment system.

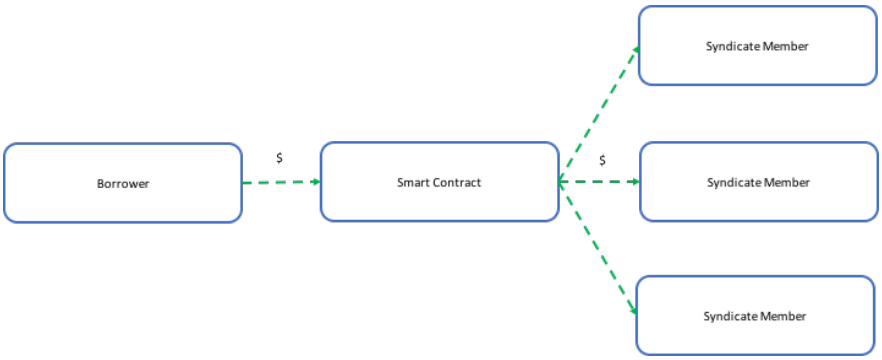
Of course, this is just a simplified diagram of a simple payment structure. It omits details such as correspondent banks and borders, and it omits the work that the Federal Reserve Bank and SWIFT conduct in order to vet payments for sanctions issues. This diagram also shows that blockchain is an incremental improvement over Fedwire and SWIFT. This is because both Fedwire and SWIFT transactions usually settle during the same day, subject to timing issues.

In syndicated loan transactions that are in repayment, for example, multiple wires are sent: once for the payment made by the borrower to the facility and/or payment agent; and again, one time for each payment made by the agent to each member of the syndicate:



All of the work performed by the agent to verify the receipt of funds from the borrower and then to transfer the correct amount of funds to each syndicate member adds execution risk and takes an enormous amount of time.

Instead, smart contracts promise a single transfer made by a borrower to the smart contract that then automatically divides the payment among the syndicate members:



Even if conceptually blockchain appears to be an incremental improvement in structure, achieving a simplified payments process that reduces settlement times among many parties, such as those among a single borrower and a syndicate of lenders, could add tremendous value to parts of the economy. That the foundations for payment transfers using blockchain technology already exist perhaps explains why financial institutions have focused on payments as a foundational step to developing blockchain technology for broader applications.

Indeed, on October 16, 2017, IBM announced it had developed a blockchain solution that facilitated cross-border payments. "The solution is already processing live transactions in 12 currency corridors across the Pacific Islands and Australia, New Zealand and the United Kingdom. Using a blockchain distributed ledger, all appropriate parties have access and insight into the clearing and settlement of financial transactions. It is designed to augment financial flows worldwide, for all payment types and values, and allows financial institutions to choose the settlement network of their choice for the exchange of central bank-issued digital assets."[7]

[7] Source: http://www-03.ibm.com/press/us/en/pressrelease/53290.wss (Viewed on November 9, 2017).

4. Some issues to consider

Hacking; fraud; other illegal activity

Although the blockchain itself is impervious to hacking and fraud due to its multiple ledger functionality, its access points represent its weakness. For example, hackers have been able to compromise private keys to steal cryptocurrencies from the wallets attached to them.

The blockchain could also be used to perpetuate fraud or other illegal activity. For example, until technology permits assets in international transport to be linked to sensors at each link in the chain of custody, asset management applications will remain dependent on truthful, accurate input by humans. This risk, though, is mitigated by the use of proprietary blockchains. Each participant is known, and each participant should have controls in place to ensure information entered into the blockchains is accurate.

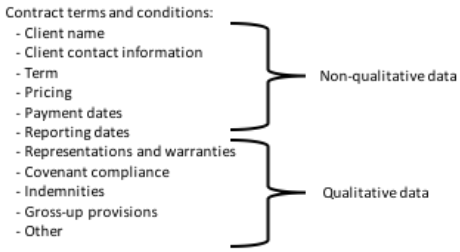
Privacy rights

A related concern, particularly as to the placement of sensors, is privacy rights. One might take the view that the development and adoption of sensors could result in a digital Panopticon. Yet, many people already willingly live in similar circumstances: they may use electronic passes to access public transport; they may live in cities where CCTV is omni-present; they may use smartphones and have set them to track and record various personal data. The appropriate outcome will result from a dialogue among privacy advocates, business interests, and politicians.

Smart contracts are limited by their logic and inability to perceive the world

A smart contract, without human intervention, is merely a tool that records data and triggers pre-defined automatic processes. Smart contract programming relies conditional logic that is built on a foundation of assumptions. By itself, the logic is incapable of observing the world, understanding the world, revisiting its assumptions, or reviewing or modifying the direction of its programming, and it is incapable of anticipating or examining changed circumstances that may reveal the limitations of the conditional logic. If anything, without human intervention, smart contract learning will be limited to reinforcing the assumptions that underlie the programming. This is why, outside of relatively straightforward transactions or a significant leap in programming technology, smart contracts will not supplant human intervention in transaction formation and performance.

Consider this list of sample terms and conditions that appear in many finance documents; it divides those terms and conditions into ones comprising non-qualitative and qualitative data:



As a system of record, smart contracts will be able to record non-qualitative data. Systems of record may also be set up to record the presence of qualitative data, such as representations and warranties, which itself is non-qualitative data. Smart contracts may even record the exact language of those representations and warranties, but they would be unable to take automatic action in accordance with them. That is because whether a party has complied with a representation and warranty is a question of

fact that requires data of the then-existing facts and circumstances that the system of record would not have access to, absent highly sophisticated middleware with a corresponding network of sensors that can feed data to that smart contract. Also, it may be that whether a representation and warranty has been complied with turns on a question of judgment, such as "reasonableness." The question, "What is reasonable?," requires: observing and understanding the current state of affairs at any given time, including what other market participants are doing and/or how case law elucidates (or not) what is reasonable; and understanding the relationship between that state of affairs, the contract language, and a counterparty's behavior.

Contract negotiation and formation

The blockchain, by itself, is ill-suited to facilitate contract negotiation and formation, because the blockchain records the final terms of a contract. A possible solution would leverage current techniques used to enter into some kinds of contracts, such as those that rely on master agreements with supplements or confirmations that activate and/or deactivate standard provisions. For example, a graphical user interface might allow parties to check and uncheck provisions. This solution would only really be appropriate for simple, standardized contracts like consumer loans and car rental agreements. Any solution raises ethical issues, should non-lawyers draft and/or interpret the terms and conditions of these contracts.

Unauthorized practice of law

In some jurisdictions, only lawyers may practice law. The practice of law usually includes the drafting and interpretation of contracts and other legal instruments. Sanctions for the unauthorized practice of law can include criminal liability, such as fines and/or incarceration, and be either misdemeanors or felonies. Therefore, smart contract developers would be well advised to ensure that they act in compliance with unauthorized practice of law statutes.

So long as the smart contract is limited to acting merely as a system of record, that party will likely not run afoul of statutes governing the unauthorized practice of law. For example, financial institutions often include a term in their finance documents according to which clients agree that the books and records of the financial institution are evidence of the debt owed to the financial institution, and that evidence is conclusive and binding on the client, absent manifest error. If, however, the smart contract suggests an interpretation of the qualitative obligations in a contract, whether to encourage or discourage future action, or to determine whether a party performed or failed to perform its obligations and imposes consequences, then the smart contract and, by extension, the developer and/or the owner of the smart contract, if it is proprietary, may be crossing the line into the unlicensed practice of law.

If technology evolves to the point where smart contracts can do more than merely record non-qualitative data, smart contract developers must involve lawyers who also have coding expertise to ensure that the terms and conditions of the contracts are coded correctly.

Evidence issues

Some progressive jurisdictions have passed legislation that encourage the adoption of blockchain technology. In some instances, the legislation ties the blockchain to the state's code of evidence to make it clear that the data in a blockchain is self-authenticating, just like records maintained by the government. As a practical matter, this means that courts may forego authentication to assume the data recorded in the blockchain is what it purports to be. However, it would be quite a logical jump if the legislation also assumed that smart contracts are true, valid, or legal contracts. If the legislation went so far as to assume that smart contracts are true, valid, or legal contracts, then it would be difficult reverse transactions based on a defectively formed contract, including due to fraud.

Attorney-client privilege; discretion

Some jurisdictions may give greater deference to attorney-client privilege than others. In those more protective jurisdictions, regulated institutions may determine that they prefer not to provide automatic data feeds to their regulators. For example, they may wish to determine whether the data is covered by privilege and, if so, whether to exercise it. Or, institutions that are present in multiple jurisdictions will have to consider how to balance waiver of privilege issues, such as where a less deferential jurisdiction requires disclosure of documents that could be privileged in a more deferential jurisdiction. Waiver of privilege issues are not new, but it is not clear that algorithms can analyze both documents and the broader circumstances of an investigation and a regulated business in order to determine whether documents should be withheld from a regulator on the grounds of privilege.

A related consideration is the exercise of discretion. Regulators and regulated financial institutions should ask themselves to what extent they are willing to subject themselves to the automatic transfer of the information contained in a smart contract. A regulated financial institution may wish to review any and all information that it transmits to its regulator. Conversely, the regulator may not wish to receive all of the information contained in the smart contract, but it may wish to receive more information than the financial institution wants to provide to it (at least initially). Indeed, finding the appropriate balance is part of the challenge of evaluating the extent of smart contract connectivity and its desirability.

Amendments, waivers, and other in-life documents

Even though smart contracts, once published in a blockchain, are immutable, amendments, waivers and other documents can still be given effect. As with paper documents, a new document would be created that refers to the initial document and that describes the effect the new document would have on the initial document. The flexibility of blockchain technology will govern whether the new document can be drafted surgically or must be more comprehensive such as a restatement of the initial document that includes whatever changes the parties require.

Record retention

At present, individuals and institutions are subject to record retention rules that require them generally to hold on to records (electronic or physical) for a finite time. If the blockchain permits records to be retained indefinitely from the birth of a particular blockchain, should document retention obligations remain the same or be extended? If they are extended, for how long should they survive?

Antitrust

Antitrust issues arise out of collaboration among market participants who provide goods and services. Collaboration by itself should not give rise to liability for antitrust violations so long as prices for consumers do not increase as a result of the collaboration. In fact, Cap Gemini determined that both financial institutions and consumers would save money with smart contracts. A danger is that once smart contracts become common and operations costs decrease due to economies of scale and improvements in technology, prices for consumers remain the same or increase because proprietary blockchains are owned and/or operated by a select few.

Sanctions

If blockchains are proprietary where the parties are not anonymous, at first glance, financial institutions would manage sanctions issues, such as conducting anti-money laundering due diligence and ensuring that payments are made in compliance with sanctions, in the future as they have in the past with minor adaptations for technology. For example, the blockchain adds no value to an anti-money

laundering due diligence exercise, even if it can appear to be a mere "check-the-box" exercise. The diligence exercise is an iterative process that requires a human to review the documentation received (often in various non-standard forms; sometimes from more than one jurisdiction) and ask further questions, if necessary, to ensure that the proposed client can be cleared.

Considering payments, this might include a confirmation by the sender of funds that the payment remains in compliance with applicable sanctions, and the blockchain that transmits the funds may have programming that mimics the analysis completed by Fedwire or SWIFT. Or, perhaps the funds transfer process includes an intermediate step where Fedwire or SWIFT conducts its analysis to sign off on the funds transfer. More complex issues arise with public blockchains where payments can be made anonymously.[8]

Withholding taxes

Withholding taxes due on cross-border payments raise a few issues. Does the payee remain a withholding agent with an obligation to collect and remit withholding tax to the government, or does the blockchain (and its owner, if it is proprietary) take over that role? If so, how?

Stamp taxes

Stamp taxes may attach to certain kinds of contracts with parties located in jurisdictions with stamp tax legislation. Would the smart contract, as evidence of the contract, attract stamp duty in lieu of, or in addition to, stamp duty which would otherwise attach to an underlying written contract, if one exists?

Liability for blockchains

If no one owns or controls a blockchain that forms the basis of a smart contract, then who is responsible when the blockchain causes an injury that results in damages? Most institutions and other users of blockchain based technology will almost certainly demand accountability, and they will want to avoid the reputational tarnish that may come with using public, anonymous blockchain networks. In that respect, the owner of a blockchain network supporting smart contracts may demand payment for access to its network. The components of the pricing might include amounts for the rights to access and use the network, and compensation for the operation and maintenance of the network.

5. Conclusion

The term "smart contract" is a misnomer, but it suggests ambition for continuing innovation. Innovation is occurring on multiple fronts, with a result being increasing interconnectedness globally, and one cannot predict how today's technology will evolve.

---

[8] Of the banks identified by IBM in its announcement that, itself, has a dateline of Toronto, only one – TD Bank, a subsidiary of The Toronto-Dominion Bank of Toronto, Canada – appears to be a financial institution based in the US or the US branch of a non-US financial institution, and it is not clear what involvement TD Bank had in the development of the payment systems. The announcement refers to other, unidentified banks, so it is possible that other US or European financial institutions were involved in the development of IBM's cross-border blockchain payment system. Further, it appears that no cross-border payments supported by IBM's blockchain solution transited the United States. The banks identified by IBM are: Banco Bilbao Vizcaya Argentaria, Bank Danamon Indonesia, Bank Mandiri, Bank Negara Indonesia, Bank Permata, Bank Rakyat Indonesia, Kasikornbank Thailand, Mizuho Financial Group, National Australia Bank, Rizal Commercial Banking Corp. (RCBC) Philippines, Sumitomo Mitsui Financial Group, TD Bank, and Wizdraw (HK) of WorldCom Finance. (Source: http://www-03.ibm.com/press/us/en/pressrelease/53290.wss (Viewed on November 9, 2017)).

Currently and into the near future, smart contracts promise to simplify the performance of some contracts. As innovative as smart contracts are, they have inherent limitations that will require continued human intervention in contract negotiation, formation, and performance. Although a goal may be to translate qualitative data into non-qualitative data to the greatest extent possible, the performance of smart contracts will still require human judgment to analyze qualitative data. And, they will remain dependent on the input of real-world observations that only humans can provide. Instead, efficiencies will be achieved at a process level, and labor will almost certainly shift in accordance with redefined business parameters.

From a broader perspective, one should be skeptical of what smart contract developers hope to achieve and what smart contracts can do. That skepticism, however, must be tempered by perspective on the proper goals for technology and what technology can achieve. Finding the right balance among these competing concerns will require a continuing dialogue among stakeholders.

Skepticism

Both the automatic performance of a contract and automatic reporting imply a loss of discretion; time and judgment are at risk. Importantly, contract parties may lose the freedom to fail to perform (for example, efficient breach of contract) or to change the manner in which they perform. And the assumptions that undergird the programming logic will be self-reinforcing. For example, a basic credit analysis relies on this assumption: metrics of past behavior (usually, financial statements from the last three years) are predictive of future credit strength and consequent performance under a financing. Imagine a cash flow solvent borrower with an otherwise difficult credit profile who would rather incur debt than issue equity to grow. There, past behavior will not necessarily predict future success; trust and a desire to help is the bridge between the past and the future. Eliminate these attributes, and a potential negative effect of the logic and its assumptions is that they will create economic castes and discourage the risk-taking that might otherwise lead to innovation and economic prosperity.

Technologically, analogous issues arise in connection with sentencing software used in Wisconsin to evaluate recidivism risk as a component of sentencing.[9] In October, Ellora Thadeny Israni, a former software engineer at Facebook who is now a J.D. candidate at Harvard Law School, published an article in the New York Times titled, When an Algorithm Helps Send You to Prison. Her article states that the sentencing software used in Wisconsin is built on assumptions that may reflect and exacerbate bias. A third-party study found that the recidivism software used in Wisconsin and elsewhere "predicts black defendants will have higher risks of recidivism than they actually do, while white defendants are predicted to have lower rates than they actually do. ([T]he company that produces the algorithm, disputes this analysis.) The computer is worse than the human. It is not simply parroting back to us our own biases, it is exacerbating them."[10] Because the logic, like that used in smart contracts, is conditional and built on assumptions, these biases can create a self-reinforcing feedback loop that results in

[9] The scope of the analogy is restricted to solely technology because the logic underlying both smart contracts and the recidivism software is conditional. This is also because the relationship between civil rights and private enterprise varies among countries. In the United States, for example, civil rights can end at the door of private enterprise. Individuals and private enterprise may agree to, among other things, binding arbitration (waiver of constitutional and statutory rights to trial in front of a judge or jury), random drug testing (the Fourth Amendment limits the ability of the government to conduct searches to where probable cause exists, unless an exception applies), and constraints on – with consequences, such as termination for – exercising freedom of speech (the First Amendment). Of course, the freedom a private enterprise has to constrain its workforce and counterparties is limited by other laws, such as US Federal and State laws prohibiting certain kinds of discrimination as well as harassment.

[10] https://www.nytimes.com/2017/10/26/opinion/algorithm-compas-sentencing-bias.html (Viewed on October 26, 2017).

sentences that are harsher than those a judge might have issued, had she considered all of the facts and circumstances to exercise discretion and judgment on an individual basis (as permitted by law).[11]

Where a sentence issued on the basis of the recidivism software was challenged for violation of due process and disclosure of the source code was demanded, the software developers refused to disclose the code. Israni is troubled that the Wisconsin Supreme Court rejected the appeal and that the Supreme Court of the United States declined to hear appeal.[12] This is because, unlike judges, the programmers have accountability to no one, other than their employers. In contrast to Wisconsin, Israni highlights reports published detailing the operation of an algorithm that New Jersey and Ohio used to reform bail proceedings. These reports allowed experts to determine that constitutionally impermissible factors were absent from the algorithm. Unlike the opaque recidivism risk software, the bail algorithm led to reductions in the pre-trial jail population and pre-trial crime.

To build on Israni's point: governmental tyranny can arise out of opacity and the government's abdication of its responsibilities.[13] Which leads to a concern expressed by Joshua Cooper Ramo, the co-chief executive officer and vice-chairman of Kissinger Associates: networks and their software are generally opaque to their users. Only a select few understand how they function, and they stand to gain corresponding power and wealth accordingly.[14] Users of these networks may be relinquishing freedom for the convenience of expedited analysis and decision-making, trusting that the programmers and architects of the network have done the right thing and have been able to program a logic that everyone can agree with. Ramo argues that no one should either rely on the technicians or on the politicians to resolve these issues; the electorate should rely on itself. The electorate has a responsibility to itself to exercise due skepticism to ensure it understands what these solutions are and what their impact will be.[15]

---

[11] *Id*.

[12] The Supreme Court of the United States does not have to give a reason why it declines to hear a case. One possibility, however, is that the technology is too new, and the Court was deferring to the democratic process to resolve these issues.

[13] Santo, Alysia, *How Conservatives Learned to Love Free Lawyers for the Poor*, September 24, 2017, https://www.politico.com/magazine/story/2017/09/24/how-conservatives-learned-to-love-free-lawyers-for-the-poor-215635 (Viewed on November 10, 2017) (Describing how conservatives supported providing a free defense for the indigent – where government had failed to do so and, instead, had extracted plea bargains – as a check on government tyranny.).

[14] "If connection changes the nature of an object, it also elevates those who control that connection to a level of rare power and influence." […] "How should we weigh their courage in innovation against their wisdom and power? Think of the computer guy in your office who fixes the system when it goes down. What does he know? How does he know it? Any time you see a network system, from cutting-edge databases to networks of commodities trading, there is someone like that or some tight group of elites who feel out the inside of the systems with a fidelity most of us will never achieve. Just what are they up to?" Ramo, 177-178. Later, Ramo expresses his concern that technology will supplant humans because humans will come to rely on technology for its data processing power while not understanding how technology, in particular artificial intelligence – representational and predictive – arrives at its conclusions. See also, *Id.*, at 276-308 (generally).

[15] "[We should] rely on ourselves, to use the inheritance of the Enlightenment – the revolution that made us citizens and not subjects – to ensure that we're not made subjects yet again, by forces we can't understand and won't manage to control. In trading our liberty for convenience, we are spending that inheritance too fast now, too blindly. […] We need men and women who can confidently command networks in a fight against network dangers." Ramo, 298-299.

Perspective

Peter Thiel, the former CEO of Paypal and now a partner at Founders Fund, lends an insider's perspective to the advent of new technologies: "The most valuable businesses of coming decades will be built by entrepreneurs who seek to empower people rather than try to make them obsolete."[16] He continues:

> "[…]computers are far more different from people than any two people are different from each other: men and machines are good at fundamentally different things. People have intentionality – we form plans and make decisions in complicated situations. We're less good at making sense of enormous amounts of data. Computers are exactly the opposite: they excel at efficient data processing, but they struggle to make basic judgments that would be simple for any human.
>
> "To understand the scale of this variance, consider another of Google's computer-for-human substitution projects. In 2012, one of their supercomputers made headlines when, after scanning 10 million thumbnails of YouTube videos, it learned to identify a cat with 75% accuracy. That seems impressive – until you remember that an average four-year-old can do it flawlessly." [17]

The Law Offices of Eric Lewin
Level 1, Devonshire House | 1 Mayfair Place | London W1J 8AJ | United Kingdom | www.ericlewin.net

[16] Thiel, Peter, Zero to One: Notes on Startups, or How to Build the Future, Penguin Random House UK (2014), 141.
[17] *Id.*, at 143.