Ryan Inglis, MBA 590 (616)

Smart Contracting and the Digital Supply Chain Revolution

The notion of a contract can be traced back as far as ancient Greece. Laws existed and were enforceable in court, but society at large was substantially different than the world we live in today. In particular, the methods and means of long distance communication were complicated and unreliable, such as light signals or pigeon carriers[1]. As a result, maintaining a contract between two parties in separate regions was likely very difficult to maintain and enforce. As time marched on and societies grew, so too did their ability to maintain and communicate contracts. However, up until very recently contracts were largely a paper affair. The documents could be signed, copied, and distributed through the postal service or other couriers, but still required some form of verbal or written communication during execution or disputes.

Fast forward to the year 2018 where we live in a digitally connected world. Individuals are able to send and receive real time data from virtually any location around the globe. Contracts can still be created and distributed on paper, but innovations in technology have paved the way for automated solutions. Smart contracting is a method of automatically executing conditions or terms through digital means, but to fully understand the technology and the future of this burgeoning industry we have to start with the advent of computer networks in the 20th century.

In its simplest state, a computer network is two or more computers linked together for the purpose of sharing information. Technically this type of transmission can be traced all the way back to the 1930's, but most experts agree the first use of modern computer networking coincided with invention of the modem[2]. Modems allow computers to talk over phone lines by converting digital data into sounds, and sounds into digital data. By 1970 this technology had enabled various types of computers to connect within a local network, and by the early 1990's we were connecting individual networks together to form larger networks. This "network of networks" is what we now call the internet and allows us to share information around the world.

So what does all this have to do with smart contracting? In 1994, Nick Szabo realized that computer networks could be used to manage and automate contracts. By converting the contract into computer code, the information can be decentralized, automated, and monitored by the network of computers[3]. Because each computer has access to a copy of the digital ledger, there is an inherent benefit of checks and balances when transactions take place. If one computer fails to adhere to the process specified in the code, the other nodes are immediately notified. This decentralized shared database is commonly referred to as blockchain technology.

So in essence, smart contracts can utilize blockchain technology to exchange information, goods, or services without overhead fees or extensive human interaction[3]. And on the surface it would appear that there's a lot to like about smart contracting and leveraging the use of blockchain technology. It has the potential to increase governance and speed up transactions through adherence to the specified code. The technology is largely autonomous and doesn't require constant surveillance. But the devil is in the details, and when it comes to smart contracting this means creating a contract that can be converted into digital code without loopholes or gaps.

The term "DAO", decentralized autonomous organization, is used to describe the computer code that manages smart contracts[11]. The basic idea is that a group of programmers write the code which will run the DAO, and then stakeholders buy into the DAO for voting rights on proposals. Back in 2016, one particular DAO with a substantial amount of funding was hacked. Without going into the technical details, there was an omission of code which unintentionally created a loophole in the smart contract. The developers made a critical error in determining what would happen if a certain set of variables appeared in the program. The hacker realized this security gap and was able to siphon funds from the DAO by creating what was essentially a duplicate DAO. Within weeks approximately $50 million USD in cryptocurrency was swept into the duplicate account[4].

The issue of hacking and cryptocurrency management brings us to the legal challenges involved with deploying a new technology. The ability to develop new systems, programs, and hardware is happening at a rate which far surpasses legislation. At the time of writing this, the federal Electronic Signatures in Global and National Commerce Act (ESIGN Act) and the Uniform Electronic Transactions Act (UETA) are in place[5]. But in the context of the DAO hack these federal programs don't provide the guidance or precedence needed to take legal action. Is the hacker really committing a crime by finding a loophole in the code? Or are the programmers responsible for damages equal to the amount of funds lost? What responsibility do the stakeholders have to ensure that the code meets the organization's needs? Max Raskin from the Georgetown Law Technology review writes, "It is too speculative at this point to see how the governments will respond to smart contracts because these technologies have yet to reach a level that requires a government response"[6].

This brings us to the current state of smart contracting and what the future may hold. To understand what the technology is capable of it's important to emphasize the fact that the technology isn't just used for contracts in the traditional sense. It doesn't have to be limited to an exchange of currency or goods between two parties. With enough programming the potential for smart contracts is virtually limitless. Max Raskin provides an example of smart contracts impacting constitutional amendments. He pens, "Smart contracts could be used to

encode certain constitutional principles into armaments, such that weapons would not work if certain conditions were not met, e.g. if Congress does not declare war, weapons will not function on foreign soil"[6]. Personally I do not foresee this happening in the immediate future, but the point is well taken. If smart contracts exist to execute a set of rules automatically, it's possible to imagine a world where much of life is controlled and automated. Jerry Cuomo, Vice President of blockchain Technologies at IBM was quoted as saying, "Think about getting carded at a bar. From an identity perspective, I can imagine a blockchain managing verification of a citizen's identity. A smart contract could ensure something like my daughter going out for her 21st birthday and the bouncer only being able to see her age, not her address. blockchain could set up a centralized identity verification system that could make the world safer for dads like myself"[7].

Despite the fact that there are limitless opportunities for smart contracts and blockchain, it's much more probable that we will see the technology gain popularity in the Internet of Things (IoT). IoT devices are typically standalone products that are web connected via Wi-Fi and continuously transmit information. The purpose being to improve both the device functionality as well as the information provided to the service provider. Christidis and Devetsikiotis provide a simple example in the IEEE access journal, noting "Consider the following setup to get an understanding of how this could work. All the IoT devices of a manufacturer operate on the same blockchain network. The manufacturer deploys a smart contract that allows them to store the hash of the latest firmware update on the network. The devices either ship with the smart contract's address baked into their blockchain client, or they find out about it via a discovery service (see Section IV). They can then query the contract, find out about the new firmware, and request it by its hash via a distributed peer-to-peer filesystem such as IPFS"[8]. Building off the prior example, I can foresee significant benefits to the energy industry by using smart contracts to operate IoT devices. Suppose you want to reduce your energy consumption at a manufacturing location. Energy costs are largely driven by "peak" and "off-peak" hours, meaning that consumption cost is linked with the time of day. It's possible that blockchains and smart contracts could dictate that the plant should tap into energy reserves during peak hours while building and storing energy during off peak hours. Taking it a step further, it's realistic to think that plants could share energy between facilities as needed to minimize waste and optimize efficiency.

But perhaps what is of most interest to me is the combination of IoT, blockchain, smart contracts, and supply chain management. It seems particularly pertinent due to the constant motion of supply chains and the need for timely and accurate information within each step of the replenishment process. Consider the common scenario where the actual demand for a product greatly exceeds the forecasted demand. The supplying distribution center doesn't have sufficient stock, so it creates an order on the manufacturing plant to build more products.

The manufacturing manager at the plant realizes he doesn't have enough components, so he asks purchasing to order more from the supplier. Meanwhile, the planning team is looking for inventory at other local and regional warehouses in the event material can be transferred to fulfill the large order. The supplier gets inundated with unexpected orders and begins expediting shipments with the transportation provider. Maybe the transportation provider begins re-routing cargo ships, or in an extreme scenario perhaps even using air transport to reduce the replenishment lead-time. In our current world, much of this is being done manually or must be triggered by human interaction. This hand off of tasks creates delays in the process and limits end to end visibility.

Now let's reimagine the same scenario with the new technology in place. The smart contract recognizes that the demand has exceeded the forecast and automatically launches the appropriate orders on the manufacturing facility, which in turn automatically triggers the order on the supplier. Upon shipment, the carrier automatically broadcasts that the material is in transit to the warehouse, which can then prepare to receive the inventory. The inventory is automatically signed for upon receipt and the process is closed. Each step of the way there is a time stamp or signal generated such that each node in the blockchain is synchronized. In the event two nodes both claim to have the inventory simultaneously, its clear there was a breakdown in either the supply chain management or perhaps a loophole in the smart contract. But the amount of time wasted manually moving information from one department to another would be entirely eliminated, and as is the chance of user error. The holy grail of balancing inventory, lead times, and order fill rates might actually be viable.

But actually realizing this digital automation scenario is much more complicated than simply creating a smart contract. There must be the requisite technologies in all areas of the supply chain to collect and supply data. Although several companies have started down this path, few have end to end capability. For starters, it would require sensors in the manufacturing facilities that could monitor production activity. From there, a radio frequency identification system (RFID) would likely need to be in place to keep track of inventory moving in and out of the facility. The fleets used for transportation of goods would require constant GPS, both on land and ocean. And in an ideal state, the company's suppliers and partners would have similar technology such that an asset could be tracked from work in progress at the manufacturing facility all the way to the end customer. Adding artificial intelligence or predictive analytics to this equation may highlight shortcomings or opportunities to be had.

But this combination of hardware, software, and blockchain technology is probably the single largest hurdle firms are currently facing. As was mentioned earlier, this technology is so new that there's little to no legislation surrounding its use. It's one thing to implement one of the systems previously mentioned, but pioneers who wish to pursue the end to end digital

revolution are facing an extremely high risk, high reward scenario. The upshot being if they are capable of implementing the technology across the board, they will have a distinct competitive advantage for the next several years. The downsides being the volatility of the industry, high cost of implementation, and industry uncertainty. In many ways the smart contracting and IoT scenario is reminiscent of the early days of personal computers. Competitors are flooding into the market with similar but slightly different products and software, and it's unclear what will become the industry standards. This could lead to firms severing existing relationships with suppliers that fail to see the synergy in adapting similar digital solutions, but also long term partnerships or joint ventures where the firms can share the costs and risks associated with overhauling the supply chain technology.

Given the complexity of implementing a full network solution, most firms are addressing each segment of the supply chain individually. A press release from GTNexus released in April of 2016 cites Capgemini research showing that 70% of 337 executives interviewed said they have started a formal digital supply chain transformation effort, but that over 30% of the respondents said they are "dissatisfied" with progress so far[9]. Still, there are opportunities at a much smaller scale that can be addressed relatively quickly with a knowledgeable team. Smart contracts are an excellent solution for supply chain processes such as Requests for Proposals (RFP), Requests for Quotes (RFQ), or payments to suppliers. RFID can be piloted in a single warehouse with limited inventory prior to making it a full scale solution. And most major transportation providers are able to provide GPS tracking or at least delivery confirmations through Electronic Data Interchange (EDI) or Application Programming Interfaces (API).

Finally, moving forward with these technologies will have an impact on the number and type of employees that are needed in the workplace[10]. Some managers may not be trained or capable of leveraging the technologies full capabilities, and some individual contributors may no longer be necessary. The senior manager who started prior to desktop computers being commonplace in the business may struggle to adapt. The finance clerk who was previously responsible for tracking accounts payable transactions may be looking for new work. Firms which are successful in digital revolutions will demonstrate as much competency in business transformation as they do in technical knowledge.

In closing, the past 30 years have marked an era of intense technical and digital growth. The advent of computer networks and smart contracts has the potential to revolutionize the ways business is conducted. The rate of new technologies being introduced in the marketplace is expanding at an exponential rate and shifts in industry best practices are imminent. However, despite the bright future firms face a number of roadblocks in legislation, deployment, standardization, and talent management. In the supply chain industry, firms are electing to take individual steps, preferring to implement technology within specific processes

in lieu of end to end system overhauls. As the smart contract and IoT industries mature, I expect we will see a convergence around a common set of tools. As the tools become increasing commonplace, so too will technologically savvy supply chain managers who are capable of extracting maximum value from the solution. And finally, when manufacturers, suppliers, and distributors agree to leverage their combined digital expertise to revolutionize the supply chain, will we see governmental action to establish and enforce the appropriate legislation.

Sources:

1) Saunders, Jen. “How They Communicated in Ancient Greece.” https://classroom.synonym.com/communicated-ancient-greece-5916.html.

2) “Timeline of Computer History.” *Networking and the Web*, http://www.computerhistory.org/timeline/networking-the-web/.

3) Rosic, Ameer. “Smart Contracts: The blockchain Technology That Will Replace Lawerys.” *Blockgeeks*, 15 Jan. 2017, https://blockgeeks.com/guides/smart-contracts/.

4) Bulters, Jeroen, and Jacob Boersma. “blockchain Technology – the Benefits of Smart Contracts.” *Deloitte*, 16 Nov. 2017, https://www2.deloitte.com/nl/nl/pages/financial-services/articles/3-blockchain-the-benefits-of-smart-contracts.html.

5) Adlerstein, David M. “Are Smart Contracts Smart? A Critical Look at Basic blockchain Questions.” *Coindesk*, 26 June 2017, https://www.coindesk.com/when-is-a-smart-contract-actually-a-contract/.

6) Raskin, Max. “The Law and Legality of Smart Contracts.” *Georgetown Law Technology Review*, 1 Apr. 2017, https://www.georgetownlawtechreview.org/the-law-and-legality-of-smart-contracts/GLTR-04-2017/.

7) Marvin, Rob. “blockchain in 2017: The Year of Smart Contracts.” *PCMag*, 12 Dec. 2016, https://www.pcmag.com/article/350088/blockchain-in-2017-the-year-of-smart-contracts.

8) Christidis, Konstantinos, and Michael Devetsikiotis. “blockchains and Smart Contracts for the Internet of Things.” *IEEE Xplore*, 3 June 2016, http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=7467408.

9) “The Current and Future State of Digital Supply Chain Transformation.” *GTNexus*, 4 Apr. 2016, https://capgemini.com/consulting/wp-content/uploads/sites/30/2017/07/digital_transformation_report_capgemini-consulting_0.pdf

10) Michel, Roberto. “The Evolution of the Digital Supply Chain.” *Logistics Management*, 5 May 2017, https://www.logisticsmgmt.com/article/the_evolution_of_the_digital_supply_chain.

11) Sigel, David. “Understanding the DAO Attack.” *Coindesk*, 25 June 2017, https://www.coindesk.com/understanding-dao-hack-journalists/.