

Smart Contracts: Enforcing Trust through Code

Joel John

BBA (III), Symbiosis Centre for Management Studies, Symbiosis International University, Pune

Abstract

Shareholders believe in the fundamental ability of a corporate entity to produce long term profit and therefore invest capital towards it. Consumers believe that the produce supplied via retail outlets are of optimal quality and are therefore willing to spend money on it.. Trust therefore, is not only an emotion upon which human society is built but also a requisite for its optimal functioning. In the occurrences that this trust is broken or proven to be violated we see widespread disputes and the need for resolutions. Take for instance the massive dip in Nestlé's stock when it was proven that some of its produce had high amount of lead content in it. Markets react violently each time it detects volatility or a lack of trust in the functioning of organizations. In the age of automation, a certain amount of functions can be completely digitalized requiring little intervention from human beings. Placing our trust in machines that can function with no internal agenda's, susceptibility to human emotion or corruption through means of bribes can therefore be a means to attain the kind of utopian society we all seek to obtain over time.

Smart contracts - a means to enforce financial transactions through code that requires the occurrence of certain events taking place are one of the means to which we can obtain complete automation of agreements involving financial transactions. Where we otherwise depended on notaries, advocates and contracts - all of which are subject to time consuming processes, and heavy expenses in the case of dispute resolution, we can now rely on pieces of code that can function on basis of data relayed to it from trusted sources (Buterin, 2014). This can be as simple as an options contract that expires on a pre-set data to release of funds to a farmer on basis of remote satellite imagery of his crops. Using a blockchain, smart contracts and possibly artificial intelligence, organizations of the future will function with increased levels of transparency, performance optimization and faster decision making. As reference points we have looked at Nick Szabo's original writing on what a smart contract is, publicly available reports from leading audit firms, interviews and a number of books citing use cases for the emergent form of

technology. This paper aims to provide an introduction to smart contracts, its implications upon the functioning of certain industries and the possibilities they bring along

Introduction

A contract can be defined as an agreement with specific terms between two or more parties pertaining to the occurrence of an event, a financial transaction or trade (Legal Information Institute, n.d.). It has to be built upon mutual consent, capacity to fulfill, consideration of variables and ramifications if the said terms are not met. In the traditional sense, a contract is usually a legal document that allows an individual to seek third party resolution making if the terms of a contract are not met. Given the speed, efficiency and cost involved in hiring advocates and relying on the courts of a land, this can greatly hinder the pace of innovation and business. Although contracts have gone digital, and we often use PDF's instead of the traditional paper, their functionality has basically remained the same. In the age of blockchain (decentralized ledger that function on a peer to peer basis) based currencies and constant connectivity to the internet, such issues can be avoided through a smart contract.

A smart contract is a digitally signed, computable agreement between two or more parties. A virtual third party—a software agent—can execute and enforce at least some of the terms of such agreements. According to Nick Szabo (Gord, 2016) - a pioneer that first framed the phrase, a smart contract is a set of promises, specified in digital form, including protocols within which the parties perform on these promises. Here, a promise can be in regards to delivery of a certain amount of goods, rent every month or even the provision of a service. The specification in digital form refers to the use of code that will be enforce the rules upon which the contract has been made. In the case of a rental agreement, this can be a case where in an automatic transfer of funds is initiated from the wallet of the person residing in an apartment to that of an owner. Failure to initiate transfer due to lack of funds could possibly even result in a remote lock down of the house through a lock and key mechanism that is connected to the internet. Or, consider the case of an uber ride enforced through a smart contract. The funds could be locked automatically from the account of the traveler at the time the GPS coordinates of the rider matches with the

cab. Once the GPS coordinates of the rider matches with that of the destination, the smart contract would automatically release the funds to the cab owner. Such forms of trustless transactions that happen with the assistance of the internet are indicators of where businesses and financial transactions are headed in the future. Where we once relied on third parties to enforce trust and optimal release of funds, technology would step in to provide security, speed and efficiency for day to day transactions.

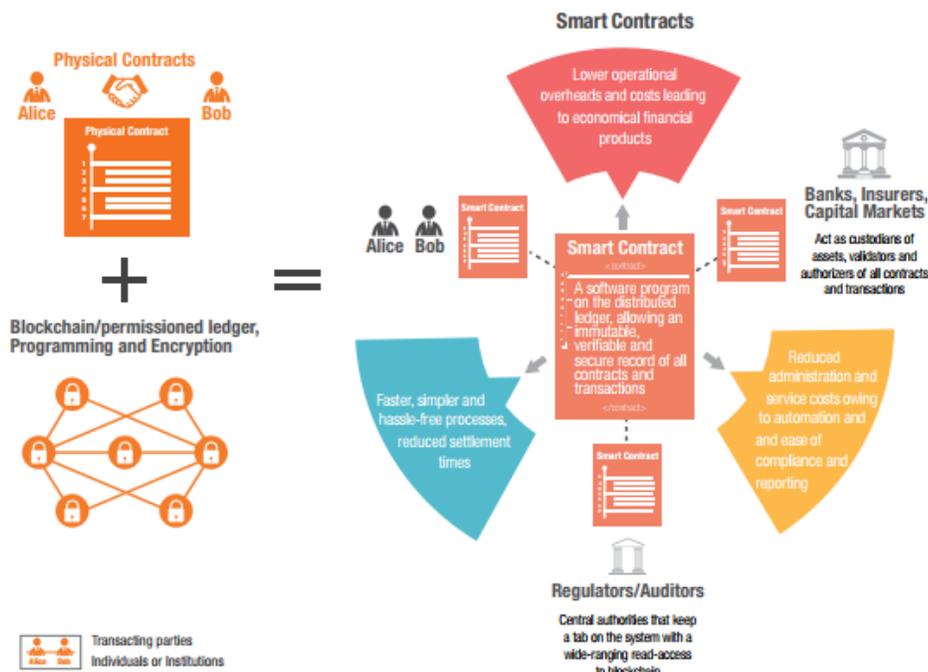


Image: A visual Comparison of traditional contracts with smart contracts

(Morrison, 2016)

While smart contracts are not legally accepted in countless nations around the globe, the level of trust and admiration they have obtained from technocrats round the globe have resulted in countless projects. The reason for this can be traced down the lack of understanding regulators possess, the lack of expertise they have over the subject matter and the lethargic fashion in which policy changes are made. The DAO(decentralized autonomous organization) for instance is an

example of a project that raised over 150 million dollars in smart contracts for the purpose of creating a decentralized crowdfunding platform with an entirely new approach to corporate governance that relied on the utility of a blockchain for voting and decision making. There are countless other examples of smart contracts being used for purposes ranging from medical insurance to in-game purposes. A few of them are discussed below.

1. Education

A major issue associated with conventional CV's and recruitment platforms like LinkedIn is the lack of ability to verify if stated claims are true or false. Even in the age of digitisation, conventional colleges rely largely on physical certificates and documents to convey grades to third parties. In the age of MOOC's (massive open online courses), online education is one of our last hopes of democratizing education and ensuring people from all walks of life have access to good quality education and in extension, opportunities. However, the cost of verifying claims made by applicants and ensuring produced certificates are from the right sources largely hinder the pace at which applications are processed in various colleges or organizations seeking to employ people. This can be resolved effectively through means of implementing smart contracts at different points. APPII (Allison, 2016), a UK-based technology start-up, is testing out a way of encapsulating verifiable recruitment-data within transparent, tamper-proof automated contracts run on the Ethereum blockchain. The smart contracts allow for the verification of the career profile (curriculum vitae or resume) of students and workers by their former, and current, employers and education providers. The system has been built on Ethereum by London based blockchain consultancy Applied Blockchain and aims to go live in the summer.. Given the scale at which education, employment and recruitment functions in nations like India, such systems can drastically reduce the costs, time and inefficiencies involved in the sector.

2. Loans

While talks of financial inclusion have been abundant in emerging economies, their progress have been largely hindered due to the pace at which humans function. Cost overheads in terms of labor, infrastructure and document verification added with the little income generated from those at the bottom of the pyramid give little incentive for private organizations to bother with setting up shop in remote parts of the world (Narasimhan, 2014). Smart contracts provide a framework to tackle this issue by drastically reducing the labor requirements for providing a number of financial services, making technology and inclusive part of the process and activating capital from remote parts of the globe through blockchain based currencies.

Consider the case of a micro loan requirement by an individual in a remote part of the globe. Assume that he is willing to provide collateral in terms of land ownership. Once an individual verifies the document and takes possession of the same on behalf of the bank, he can initiate a loan whose repayment conditions can be contractually enforced through code. Assume the individual deposits money in a quarterly fashion and over the course of the loan it is fully repaid. The code can deliver a text message to his personal phone number with an access code that can be submitted to the bank for receiving the collateral documents back from a central location.

By enabling the loan disbursement process to happen through a smart contract, banks can reduce the number of employees required to handle such loans, provide faster services, store documents pertaining to ownership at a central location and reduce infrastructure requirements and even have added sources of revenue. Consider the case of Credit Suisse that has been looking at the possibility of providing loans as a syndicate (Suisse, 2016) in collaboration with other banks. In the future, with the use of smart contracts, individuals could even look at trading mortgage backed loans on a blockchain. Unlike earlier where banks used to individually label the creditworthiness of these mortgages, individuals could look up the attached document and verify their worth and the value of the loan. Such systems could possibly even avert the kind of recession we saw in 2008

3. Internet of Things

Developments in the kind of hardware we use in our day to day operations have provided new ways for us to collect data and utilize it for the improvement of our lives. Simply put, the internet of things is the concept of basically connecting any device with an on and off switch to the Internet (and/or to each other). This includes everything from cellphones, coffee makers, washing machines, headphones, lamps, wearable devices and almost everything (Morgan, 2014). This also applies to components of machines, for example a jet engine of an airplane or the drill of an oil rig. This is particularly important in the case of blockchain and smart contracts as these internet of things can be used largely to rely upon for data from the sensors they possess. Consider the following use cases.

3.1 Cash on Delivery through a smart Contract

Consider a purchase that has to be made from an e-commerce firm. The rise of cash on delivery as a payment method has helped organizations like Flipkart garner market dominance over the course of the last decade. However, this has its inadvertent flaws. The lack of upfront payments gives individuals the ability to call off the order while the order is in transit. This puts the seller in an iffy position where ‘in he has to bear the cost of shipment if the individual chooses to call the order off during the time of transit. This can be circumvented through means of using the tracking mechanism available on most shipment platforms. Assume a smart contract is able to verify the shipment status of a purchase from the API’s (application programming interface) available with shipping platforms such as FedEx. Consider the fact that the said smart contract can be used to set up an escrow which is released upon time of delivery of the goods. Those making an order will have to put funds into the smart contract and initiate it with the seller. Assuming the buyer wishes to cancel order while the order is mid-way he has the ability to do so by means of calling the contract off. In such a case the contract can be released after deducting the amount used for shipping and a premium for the labor costs involved. Alternatively, if the produce is delivered effectively the funds can be automatically released post the shipment status saying “delivered”. This hedges both the buyer and the seller from risks and requires no third party to be involved. Additionally, if done on a blockchain, this stands as viable proof of the trade

made on the blockchain. Assume a use case where in both parties do not trust a third party shipping agent either. Then a GPS can be used to track the coordinates of the produce. Considering the buyer enters his GPS location for place of delivery, the smart contract can be released once the GPS coordinates match with the point of delivery. While this might have little to no implications for the average retail consumer, its implications can be huge in the B2B sector which is rife with issues regarding delay of payments. Assuming a penalty is charged for each day of delay in ensuring delivery, a seller has an added incentive to deliver the produce on time. Add an added bonus for each day the seller is able to deliver the produce in advance through a smart contract and verify it through a GPS and one would be able to bring forth much higher speeds to present day industrial processes.

3.2 Car leasing

With millennials choosing to go more with rentals and less with ownership, cars connected to the internet provide a wide array of opportunities to integrate trust, transparency and blockchain based records. Consider this (DocuSign, 2015) example of a collaboration between DocuSign - a digital contract enabler and Visa - a global pay processing entity to build a car leasing prototype on top of a blockchain. Their vision is one where in cars are able to track distance driven, drivers financial status, financial records, driving records and the overall condition of the car on a blockchain. This proof-of-concept makes it easier and faster for customers to get out the door in their new car by bringing together smart contracts and payments so that customers can electronically sign all pertinent documents and seamlessly pay in one fully digital experience."

With all details stored on a blockchain - both a driver and the owner of the car will be able to verify the condition of the car or the eligibility of the driver to own the car. Considering payments - an individual will be able to lock up a certain amount of funds in a smart contract. The odometer positioned in the car can automatically relay the distance travelled and the smart contract could reduce funds from it. If the individual drivers lesser distance than earlier assumed, then the surplus funds and the security deposit could be given back to the drivers account. This has the added benefit of transparency in the sense that someone looking to

lease a car could now instantly verify how far the car has been driven, how often and by whom.

Conclusion

Smart contracts have the power to fundamentally disrupt how proof of ownership, transactions and legal enforcement of trade is facilitated. By reducing the amount of trust we put upon human operators and enforcing it through code, business can function fundamentally faster and produce substantially higher levels of profit through process automation. However, this transition towards smart contracts would take years, maybe decades to go mainstream and integrate with developing economies. Even as it stands right now, smart contracts have their susceptibility to being corrupted through a hack or leakage of funds. Additionally, individuals stand to hold no legal rights in the event that an issue occurs during the functioning of a contract. The removal of human parties to enable trust can turn to be a costly mistake if there is a technical glitch as with the case of an ethereum focused crowdfund. Due to a hack that was initiated against the system, individuals lost tokens worth millions of dollars and the community eventually collapsed and lost faith in the system. As it stands right now, smart contracts are utopian systems built for technocrats. Their integration towards existing systems can be slow, painful and excruciating. However, as they turn mainstream, they will bring along with them - a brand new way of building businesses. One, built upon trust, transparency, speed and efficiency.

References

- (2015, October 26). Retrieved from Docusign: <https://www.docusign.com/press-releases/docusign-showcases-smart-contracts-payments-prototype-built-for-visas-connected-ca>
- Allison, I. (2016, April 15). *IB TIMES*. Retrieved from Ibtimes.com: <http://www.ibtimes.co.uk/ethereum-based-system-cv-smart-contracts-save-recruiters-time-money-1555118>
- Buterin, V. (2014, 07 22). *Ethereum Blog*. Retrieved from Ethereum: <https://blog.ethereum.org/2014/07/22/ethereum-and-oracles/>

India, P. T. (2015, August 12). Retrieved from Business standard: http://www.business-standard.com/article/pti-stories/nestle-shares-dip-5-as-govt-files-case-against-maggi-115081200675_1.html

Legal Information Institute. (n.d.). Retrieved from Cornell: <https://www.law.cornell.edu/wex/contract>

Morgan, J. (2014, 05 13). Retrieved from Forbes: <http://www.forbes.com/sites/jacobmorgan/2014/05/13/simple-explanation-internet-things-that-anyone-can-understand/#4d74e3de6828>

Morrison, A. (2016). *Blockchain and smart*. PWC.

Narasimhan. (2014, August 24). *Opinion Column*. Retrieved from Thehindu.com: http://www.thehindu.com/opinion/columns/C_R_L__Narasimhan/the-challenge-of-financial-inclusion/article6345276.ece

Suisse, C. (2016, 09). Retrieved from Credit Suisse: <https://www.credit-suisse.com/articles/media-releases/2016/09/en/blockchain-demonstration-shows-potential-loan-market-improvements.html>