Blockchain Based Smart Contracts: An Overview

February 13, 2019 | By Ibrahim Shehata

Introduction

There have been a few news headlines lately reporting how blockchain technology and smart contracts will have an astounding added business value. For instance, McKinsey reports that blockchain-based smart contracts can save nearly $50 Billion in B2B transactions. [1] Furthermore, Accenture suggests that blockchain-based smart contracts can save the banking industry up to 70% in central financial reporting. [2] Maybe, that's why Gartner has made a bold prediction that 25% of global organizations will use blockchain-based smart contracts by 2022. [3] All of these headlines have one thing in common; they are not taking about cryptocurrency but they are all taking about smart contracts that will be based on the blockchain. This invites to delve further into the notion of blockchain-based smart contracts and try to make the most sense of such a new phenomenon and its implications in our world.

Definition & Types of Smart Contracts (Strong Smart Contracts vs. Weak Smart Contracts)

Smart contracts have been defined as "agreements wherein execution is automated, usually by computers. Such contracts are designed to ensure performance without recourse to the courts. Automatio ensures performance, for better or worse, by excising human discretion from contract execution." [4] This type of smart contracts has been labeled as a strong smart contract whereby human intervention is expunged. [5] In other words, these smart contracts are self-executing or self-enforcing. The problem with these strong smart contracts is that they would run the imminent risk of technical bugs. Further, natural language processing in artificial intelligence has not yet been developed to encode vague or complex contractual clauses. Therefore, the realm of these smart contracts in any way would not be able to extend to more than simple standard agreements.

To the contrary, a weak smart contract can be defined as: "an automatable and enforceable agreement. Automatable by computer, although some parts may require human input and control. Enforceable either by legal enforcement of rights and obligations or via tamper-proof execution of computer code." [6] This definition is sufficiently clear as it covers both "'smart legal contracts' (where the agreement is a legal agreement, at least some of which is capable of being implemented in software) and 'smart contract code' (which is automated software that may not necessarily be linked to a formal legal agreement)." [7] The word "automatable" was used rather than "automated" to clarify that in practice, there are usually some parts of the smart contract that require human intervention. [8]

We should note that our discussion here concerns the use of smart contracts which are based on the blockchain, as smart contracts do not have to be based on the blockchain in the first place. Also, it's essential to note that smart contracts based on a certain type of blockchains will inherit the features of such blockchain. In this regard, a strong smart contract based on a public permissionless blockchain would be transparent, would require cryptocurrency, and would have low scalability. By contrast, a weak smart contract on a private permissioned blockchain would be confidential, would not require cryptocurrency and would have very high scalability (see figure 1. A comparison of the various types of blockchains and their distinctive features)

Public Permissionless	Public Permissioned	Private Permissionless	Private Permissioned
Anyone Can Join & Read the Data (Anonymous Identity)	Anyone Can Join & Read the Data (Anonymous Identity)	Only Participants with Known Identity Can Join & Read the Data	Only Participants with Known Identity Can Join & Read the Data
All of Participants Can Write the Data	Only Pre-Designated Participants Can Write the Data	All of Participants Can Write the Data	Only Pre-Designated Participants Can Write the Data
Data is Transparent	Data is Transparent	Data is Confidential	Data is Confidential
Requires Native Assets (Cryptocurrency)	Requires Native Assets (Cryptocurrency)	Does not Require Native Assets	Does not Require Native Assets
Low Scalability	Moderate Scalability	High Scalability	Very High Scalability

Figure 1. A comparison of the various types of blockchains and their distinctive features

Limitations of Smart Contracts

We turn now to exploring the limitations usually associated with smart contracts (both types: strong and weak) and how they can be addressed:

1. Legal Effects:

The binding effect of smart contracts depend on three main factors: (1) the specific use case; (2) the type of smart contract being used (i.e. strong or weak smart contract); (3) the law applicable to the contract. [9] In this regard, some states like Delaware, Tennessee and Arizona have passed legislation to recognize the legal effects of smart contracts. [10] Therefore, smart contracts encoded entirely in compute code and stored on the blockchain will be producing legal binding effects in such jurisdictions, even if they are strong smart contracts. The question then is what about uncertainty in the remaining jurisdictions? A “Ricardian Contract” which is a contract that has two versions, one of them is in normal word text, while the other is in compute code [11] might reduce such uncertainty.

2. Coding Limitations:

Whenever coding limitations are mentioned in the sphere of blockchain-based smart contracts, the incident of the decentralized autonomous organization (“DAO”) comes to our minds. The DAO was formed in 2016 to create an investing fund that “would not be controlled by any one individual, but by shareholders voting based on their stakes on a blockchain.” [12] The entity was able to collect funds worth $150 million. Soon thereafter such money was raised, a hacker was able to steal about around $40 million from the DAO. The hacker “did not “hack” the code in a malicious way, but rather used the terms of the existing smart contracts to accomplish something others later found objectionable.” [13] The hacker simply exposed a loophole or a bug in the smart contracts of the DAO.

Further, a 2016 study of Ethereum smart contracts revealed that there are at least 100 errors per 1,000 lines of code. [14] This is such a revealing study that depicts the imperfect reality of computing and smart contracts. According to Deloitte, it will be essential “to apply methodologies such as the Secure Software Development Life Cycle (S-SDLC) in order to minimize the threat of a critical bug during the life cycle smart contracts”. [15] Therefore, we recommend the use of weak smart contracts and to be based on a private permissioned blockchain as it can enable the parties to regularly cure any bugs that might arise. [16] This is because the parties to a weak smart contract on a private permissioned blockchain can request a computer engineer to deal with the coding limitations of their smart contract on a temporary basis and for a specific task without comprising the confidentiality of the data lodged on such blockchain.

3. Complex Contractual Clauses:
We are many years away from a code that can determine subjective legal criteria. For example, there is no yet a code that would be able to determine whether a party satisfied its duty of care. [17] Currently, smart contracts can only automate simple standards of agreement that are purely objective. For example, 'Material Adverse Effect' and 'Best Reasonable Efforts' usually have a number of different meanings that usually change over time depending on the latest trend in case law. [18] These terms are not susceptible to encoding within smart contracts. The problem highlighted by these terms is that smart contracts may not be able to encode "the subtlety and richness of contracts written in natural language or to cater for the exercise of discretion given to one party." [19] Therefore, the solution would be the inclusion of oracles. Oracles might be able to determine or update obligations based on the subjective and arbitrary judgment of certain individuals. In this way, parties can rely on "the deterministic and guaranteed execution of smart contracts for objective promises that are readily translatable into code." [20]

Accordingly, parties can choose an oracle to assess terms of the contract that cannot easily be encoded into a smart contract, if they require a subjective assessment of real-world events. [21] Even though the use of such oracles might reduce the efficacy of smart contracts, a smart contract could still "deliver value to businesses by coordinating the various stages of the transaction by process automation." [22] It must be noted that the inclusion of oracles would only be viable in weak smart contracts, as strong smart contracts by definition eliminate human intervention.

Conclusion
In conclusion, a smart contract would be more business-friendly if it takes the form of a weak smart contract rather than a strong smart contract. In that way, the weak smart contract would have a computer code with some "automated" parts [23] and other "automatable" parts. Therefore, humans would be able to intervene in such weak smart contracts to fix any coding limitations (i.e., software bugs) which are exceedingly recurring as we have shown above. Also, weak smart contracts can be able to assign the interpretation of ambiguous or complicated contractual clauses or the resolution of any disputes between the parties to such smart contracts to oracles as we have explained above. Further, one way to avoid the legal uncertainty surrounding the use of blockchain-based smart contracts in some jurisdictions would be drafting a dual text-code form (Ricardian Contract) of such weak smart contracts. This will definitely offer more legal predictability when it comes to the use of these weak smart contracts.

Notes
[1] Available at: https://www.mckinsey.com/industries/financial-services/our-insights/blockchain-in-insurance-opportunity-or-threat
[2] Available at: https://www.accenture.com/us-en/insight-banking-on-blockchain
[3] Available at: https://www.gartner.com/smarterwithgartner/why-blockchains-smart-contracts-arent-ready-for-the-business-world/ [4] M. Raskin, The Law and Legality of Smart Contracts (2017)
[5] Id
[6] Clack, C., Bakshi, V. & Braine, L. (2016, revised March 2017). Smart Contract Templates: foundations, design landscape and research directions
[7] Id
[8] Id
[9] Ibrahim Mohamed Nour Shehata, 'Arbitration of Smart Contracts Part 1 – Introduction to Smart Contracts', Kluwer Arbitration Blog, August 23 2018, http://arbitrationblog.kluwerarbitration.com/2018/08/23/arbitration-smart-contracts-part-1/
[10] Id
[11] Ian Grigg, "The Ricardian Contract," in Proceedings of the First IEEE International Workshop on Electronic Contracting, ed. Ming-Chien Shan, Boualem Benetallah, and Claude Godart (Piscataway, NJ: IEEE, 2004), 25–31, http://iang.org/papers/ricardian_contract.html.
[12] Raskin, The Law and Legality of Smart Contracts (2017); pp.337

[13] Id
[14] David Zaslowsky, “What To Expect When Litigating Smart Contract Disputes” Law360 April 4, 2018
[15] https://dupress.deloitte.com/dup-us-en/focus/signals-for-strategists/trends-blockchain-bitcoin-security-transparency.html
[16] https://www2.deloitte.com/content/dam/Deloitte/ie/Documents/Technology/IE_C_BlockchainandCyberPOV_0417.pdf
[17] Stuart D. Levi and Alex B. Lipton, “An Introduction to Smart Contracts and Their Potential and Inherent Limitations,” Skadden, Arps, Slate, Meagher & Flom LLP and Affiliates, May 7, 2018. https://www.skadden.com/insights/publications/2018/05/an-introduction-to-smart-contracts
[18] http://www.nortonrosefulbright.com/knowledge/publications/137955/smart-contracts-coding-the-fine-print
[19] Id
[20] Michael del Castillo, “Lawyers Be DAMNed: Andreas Antonopoulos Takes Aim at Arbitration with DAO Proposal,” CoinDesk, May 26, 2016, http://www.coindesk.com/damned-dao-andreas-antonopoulos-third-key/ See also Michael Abramowicz, “Cryptocurrency-Based Law,” Arizona Law Review 58 (2016): 359–420 (explaining how blockchains could help facilitate peer-to-peer arbitration, which could lower transaction costs of commercial relationships and increase trust between parties)
[21] Id
[22] http://www.nortonrosefulbright.com/knowledge/publications/137955/smart-contracts-coding-the-fine-print