FinTech Network

Smart Contracts – From Ethereum to Potential Banking Use Cases

With Contributions From:

ZERADO

Disclaimer:

Whilst every effort has been made to ensure the accuracy of the information contained in this publication, neither FinTech Network nor any of its affiliates past, present or future warrants its accuracy or will, regardless of its or their negligence, assume liability for any foreseeable or unforeseeable use made thereof, which liability is hereby excluded. Consequently, such use is at the recipient's own risk on the basis that any use by the recipient constitutes agreement to the terms of this disclaimer. The recipient is obliged to inform any subsequent recipient of such terms. Any reproduction, distribution or public use of this report requires prior written permission from FinTech Network.

FinTech Network

SMART CONTRACTS – FROM ETHEREUM TO POTENTIAL BANKING USE CASES

Contents

An Introduction – What Are Smart Contracts?

The phrase "smart contracts" was coined by computer scientist Nick Szabo all the way back in 1994, just as the first full text web search engines were beginning to be launched. This term emphasised the goal of bringing what Szabo called the "highly evolved" practices of contract law and related business practices to the design of electronic commerce protocols between strangers on the Internet. Szabo's 1994 description was as follows:

> *"A smart contract is a computerised transaction protocol that executes the terms of a contract. The general objectives are to satisfy common contractual conditions (such as payment terms, liens, confidentiality, and even enforcement), minimise exceptions both malicious and accidental, and minimise the need for trusted intermediaries. Related economic goals include lowering fraud loss, arbitrations and enforcement costs, and other transaction costs."*[1]

Smart contracts today have now developed in terms of technological innovation and legal construction but the definition of a "smart contract" is still materially the same as Szabo defined it over 20 years ago.

So, if blockchain is a "distributed ledger technology" then if two parties can have a shared distribution ledger that governs the whole process of creation, movement and management of money or cryptocurrency, then if those two parties also have a shared business logic they can then also create a "smart contract" between themselves.

Under a smart contract, if an actor from one party proposes a transaction and this is validated against the contract by a blockchain network, when there is consensus from the network then the transaction under the contract is finalised. Therefore the rules for how the contract is being evaluated are the same for both sides.

Smart contracts aim to provide security superior to traditional contract law and to reduce other transactional and administrative costs associated with contracting. Whilst it is unlikely that smart contracts will fully replace the traditional legal contract (in the near future at least) they can reduce the burden and the complexity of writing a new contract each time as the smart contract technology can be used to execute a number of terms of a contract between two parties automatically.

[1] https://en.wikipedia.org/wiki/Smart_contract#cite_note-tapscott2016-2

One real world implementation of a smart contract that gained mainstream coverage was The DAO, a distributed autonomous organisation for venture capital funding, which was launched with US $150 million in crowd funding in May 2016. The DAO was brought to the attention of the public when it was revealed that it had been hacked and drained of approximately US $50 million in cryptocurrency only three weeks later. This case is examined fully later on in this paper.

Thus the terms of a legal contract are then written in a programming code and this code is used to define the rules and consequences in the same way that a traditional legal document would, stating the obligations, benefits and penalties which may be due to either party in various different circumstances. This code is then automatically executed by a distributed ledger system without the further onerous input from either party.

Ethereum

Ethereum is one of the best examples of smart contracts in practice. It was first developed in 2013 with the aim to develop the nascent cryptocurrency technology. The idea was to build on existing concepts, such as Bitcoin, and improve upon transactional speed and overall security.

Ethereum, having raised approximately $25 million in 2014 from crowdfunding, then launched in June 2015. A new way of using blockchain technology was established, not to create cryptocurrency as Bitcoin does, but as a platform to build smart contracts. By using blockchain technology, Ethereum is used to construct contracts that self-execute upon completion of specified terms or if certain events happen. Ethereum is presently capable of 25 transactions per second.[2]

Ethereum is an open source smart contract protocol and is decentralised – representing a cultural shift of some of its predecessors (just as Bitcoin also was). Ethereum uses the “ether” to motivate a network of peers to validate transactions, secure the network and achieve consensus about what exists and what has occurred – thus enabling a smart contract to self-execute.

The “Ethereum Virtual Machine” (EVM) is where the smart contracts run in Ethereum. It provides a more expressive and complete coding language than Bitcoin for scripting and is also a Turing Complete programming language – meaning that it can encode any computation that can be conceivably carried out. The Ethereum blockchain records transfers of native cryptocurrency called “Ether.”

Any possible asset, such as a house or a bond, can be represented in the form of a token and consequently traded on a blockchain using Ethereum. This could start to disintermediate some of the existing online marketplaces and services providers that have grown up recently and reduce administrative costs and transaction times.

[2] http://www.ibtimes.co.uk/how-are-banks-actually-going-use-blockchains-smart-contracts-1539789

Benefits

One of the main benefits of using Ethereum is the tighter security. Where every participant is a client and a server at the same time, this allows Ethereum to increase its network's security and resilience – arguably far beyond that of competitors such as Bitcoin. This is because in other systems, the entire network is handled by a single server entity and thus it becomes a weak point and far more able to be exploited by potential attacks and hacks.

As Ethereum is a decentralised network, it is very resistant to such hacker attacks and has, potentially, zero downtime – even if some parts of the network go down. The transaction log becomes robust as the integrity of the data is verified, stored and protected. Records can be accessed by anyone on the network, are easily traceable and are virtually unalterable – therefore, Ethereum has inbuilt checks and balances to ensure that transactions are near 100% accurate.

Ethereum has become the best way to ensure that applications work efficiently and correctly. As the blockchain network behind the application, using Ethereum, executes an order or transaction by itself, verifies the output(s) by itself and distributes the value between participants by itself there is no need to have separate blockchains for each application or to have costly central administrative processes for monitoring and execution.

The DAO

However, the issue of applying logic and ensuring that the code is followed did lead to a major problem for some investors using Ethereum in June 2016. Investors in the DAO (a digital decentralised autonomous organisation), a form of investor-directed venture capital fund, lost their investment to hackers who had exploited a vulnerability in the DAO code to enable them to siphon off one-third of the DAO's funds to a newly created subsidiary account (thought to be worth about $50 million). The DAO's fund Ether value as of 21 May 2016 had been more than $150 million, representing nearly 14% of all ether tokens issued to that date[3] .

The hack wiped $700 million off the book value of the Ethereum economy. To try to restore confidence and provide an opportunity for the DAO investors to recover their lost investments, the Ethereum Foundation proposed changing the underlying Ethereum code rules, introducing the equivalent of a constitutional amendment to freeze the account to which the DAO's funds were being diverted.

However, the Ethereum Foundation couldn't impose this solution as it required those operating the computers that run the distributed network system to decide whether to adopt the changed code: If a majority of them did, only then the proposal would take effect.

At the time there was huge debate about this issue. If the proposal was to be adopted and take effect then this would undermine Ethereum's bedrock principle that smart contracts will run exactly as programmed, without third-party interference. However, if the code was not to be adopted then the DAO would likely have collapsed and this would have shattered the confidence in the rest of the Ethereum platform.

[3] https://en.wikipedia.org/wiki/The_DAO_(organization)

In the end, the Ethereum community decided to adopt the proposal and to "hard-fork" the Ethereum blockchain to restore virtually all funds to the original contract, ensuring the investors did not lose their money. This was controversial, however, and led to a fork in Ethereum, where the original un-forked blockchain was maintained as Ethereum Classic, thus breaking Ethereum into two separate active cryptocurrencies.

Nevertheless, it was a good early test to see if investors would want to be part of a truly decentralised economy, with no central authority to impose sanctions and redress if problems occur.

Smart Contracts in Banking

A Capgemini Consulting paper "Smart Contracts in Financial Services: Getting from Hype to Reality " (October 2016) states that:

> *"Smart contracts, enabled by blockchain or distributed ledgers, have been held up as a cure for many of the problems associated with traditional financial contracts, which are simply not geared up for the digital age. Reliance on physical documents leads to delays, inefficiencies and increases exposures to errors and fraud. Financial intermediaries, while providing interoperability for the finance system and reducing risk, create overhead costs for and increase compliance requirements."*[4]

Thus, there are multiple cases where financial institutions (especially banks) could benefit from the adoption of smart contracts in their day-to-day operations. Banks can benefit from the reduced administrative costs and be relieved of the burdens of verification and the monitoring of data. The Capgemini report anticipates that banks using distributed ledgers and smart contracts could go mainstream "early in the 2020s".

Mortgages

Banks and financial institutions, using smart contracts, could potentially save a huge amount of money through lowered processing costs.

Mortgages typically require the collation and verification of a huge amount of property and financial data by all parties involved in the transaction. This complex system builds in additional cost and delay into the process.

Smart contracts could reduce the cost and time involved in the mortgage process through automation, shared access to electronic versions of verified physical legal documents between trusted parties and access to external sources of information such as title deeds and Land Registry records.

This saving can then be passed on to the consumer who could benefit from better lending and interest rates, making home ownership more affordable. The Capgemini paper estimates that "consumers could potentially expect savings of $480 to $960 per loan" and that banks would also be able to "cut costs in the range of $3 billion to $11 billion annually" by lowering processing costs in the origination process in the US and European markets.

[4] https://www.capgemini-consulting.com/blockchain-smart-contracts

Clearing and Settlement

The opportunity to streamline banks' clearing and settlement processes with smart contracts is immense. More than 40 global banks have already participated in a consortium that has tested smart contracts for clearing and settlement activity and many of those banks have already progressed to pursuing their own individual further trials.

Smart contracts can take over the onerous administrative task of managing approvals between participants, calculating trade settlement amounts and then transferring the funds automatically once the transaction embedded within the smart contract has been verified and approved.

For example, in 2015, the Depository Trust & Clearing Corporation (the American post-trade financial services company providing clearing and settlement services to the financial markets) processed over $1.5 quadrillion worth of securities, representing 345 million transactions.[5] Utilising smart contracts to automate part or parts of this process could generate a substantial saving.

Santander Bank's innovation fund, Santander Innoventures, expects blockchain technology to lead to $15 – $20 billion in annual savings in infrastructure costs by 2022.[6]

The Australian Securities Exchange is also working on a smart contracts post-trade platform to replace its equity settlement system.

KYC

Smart contracts can incorporate a KYC element utilising the blockchain. KYC is an expensive element of on-boarding a new client and each bank must create their own KYC, resulting in a high cost of customer acquisition and a long process for a customer to open a new account at a new bank (for example).

Customer information can be checked and verified against approved central records by the blockchain network. Blockchains remove the need to trust a third party by trusting the network-approved and verified dataset thus enabling a smart contract that relies on KYC information to be verified as a condition precedent to be executed automatically.

Smart contracts can also make provision for a situation where the customer changes their address, currently an administrative issue that can cause significant delay. The coding in the smart contract would require the customer to be notified automatically that they need to resubmit their proof for it to be acceptable again by the participating bank without having to require the bank to do this manually.

Bonds

Due to the ability of blockchain to execute complex computation, there is the capability to use smart contracts to set up and manage "smart bonds". The coding of the legal requirements in a smart bond would mainly be in the area of permission i.e. to define detailed rules about who is allowed and not allowed to hold this bond.

[5] www.dtcc.com/annuals/2015/index.php#performance-dashboard
[6] http://santanderinnoventures.com/wp-content/uploads/2015/06/The-Fintech-2-0-Paper.pdf

In a recent trial UBS produced a smart-bond, in which risk free interest rates and payment streams were fully automated, creating a self-paying instrument. UBS's experiment uses the Bitcoin blockchain

The idea of a smart bond is a financial instrument which automatically pays out at given intervals. Szabo said that "bonds are a good example of a financial instrument suited to smart contracts because they could be backed by other assets that exist on the blockchain, if the bond issuer itself fails to make a payment".

However, there may be an issue with smart bonds that would first need to be addressed and resolved before it becomes workable. If an issuer of the smart bond does not have sufficient funds to pay the bond coupon on time how can the smart contract coding be written to resolve this type of situation? A smart contract cannot be written so that real world assets are seized or so that the bond issuer is taken to court. The smart contract can only highlight that the payment is overdue and calculate the interest payable.

The smart contract would need to be written and managed in a way that, to ensure there are sufficient funds to pay the coupon, it could lock up those funds under the control of the smart contract representing the smart bond. However, to lock up the funds in this way would mean that the issuer could not use them for anything else so that there would not be any point to issuing the bond in the first place. This could be a problematic issue to resolve.

In December 2016 Barclays Bank released a second research paper[7] on its Smart Contract Templates initiative. The paper looks closely at legally-enforceable smart agreements, examining some essential requirements and potential design options.

This new paper lists five essential requirements for well-written and coded smart legal agreements:

1. Methods to create and edit smart legal agreements, including legal prose and parameters.

2. Standard formats for storage, retrieval and transmission of smart legal agreements.

3. Protocols for legally executing smart legal agreements (with or without signatures).

4. Methods to bind a smart legal agreement and its corresponding smart contract code to create a legally-enforceable smart contract.

5. Methods to make smart legal agreements available in forms acceptable according to laws and regulations in the appropriate jurisdiction.

Barclays aim to "support the financial industry in exploring how legal prose can be connected with parameters and code, and trade associations when reviewing existing data standards to take account of the features of smart legal agreements."

[7] Available at: https://arxiv.org/pdf/1612.04496.pdf

Potential Problems with Smart Contracts

Conceptual Misalignment

Many legal scholars perceive smart contracts to be neither smart, nor contracts. One way to describe them, is "electronically enforced real-time agreement" – the idea that some of the provisions of the contract are enforced automatically in software. An alternative point of view, formed during workshops with participants from both law theory, and computer science backgrounds, is that smart contracts are never going to be possible.

The reasoning is based on the juxtaposition between Halting Problem, that is the infeasibility of determining, from the description of an arbitrary computer program and its input, whether the program would complete successfully or not. Contrasting that with Meeting of Minds, a legal concept wherein a contract is only valid when parties are able to fully understand its consequences, whether by themselves or through seeking legal advice. Smart contracts can (and occasionally do) appear straightforward, however, fundamentally, any platform capable of expressing arbitrary code, is thus capable of covertly introducing complexities that prevent the formation of Meeting of Minds.

One of London's leading Blockchain Consultancies, Zerado, has proposed an alternative term, Dumb Contract, to describe a system which, by design, eliminates the Turing-Completeness (and the Halting Problem). In layman's terms, this can be described as "If-Then" contracting, where a simple, linear flow of conditions leads to a deterministic outcome. Such designs are popular in the safety-critical industries, such as aviation, automotive or nuclear engineering, precisely to enable formal verification of the contractual code against specification for all possible inputs. Recent formal validation of Estonian GuardTime system, conducted by the Galois consultancy upon request from US Department of Defense, highlights such demand.

Inflexibility

Smart contracts written as software programs on distributed ledgers would mean that the contracts, once agreed upon, cannot easily be modified. This was the main issue that the Ethereum Foundation had to resolve once the DAO account had been hacked and the money transferred to another account. Once a problem arises, it is very difficult to rectify it as the smart contract transaction has to be completed before any change can be made.

In traditional legal contracts, there is always the provision that a contract can be amended, novated or terminated before the contractual goal is complete. A smart contract would need similar mechanisms to ensure flexibility and commerciality (in the more complex contractual transactions).

Contractual Secrecy

In traditional contractual documents there is often a non-disclosure clause that both parties will keep information (particularly commercially sensitive terms such as pricing) confidential. In a smart contract that is executed on a blockchain or distributed ledger, this information will be available to all parties on the blockchain. An issue of confidentiality can therefore arise for more comprehensive smart contracts.

This issue can be addressed in two different ways: (1) the information can be shared by use of advance cryptographic structures ensuring that only the parties who are required to know the sensitive or confidential information have access to it and/or (2) a concept of "zero knowledge proofs" is being explored to devise a way to separate the way of verifying a transaction from seeing the content of a transaction.

Legal Jurisdiction

As smart contracts are run on a decentralised distributed ledger network, there may be the issue of legal jurisdiction if a problem arises and some form of court or authority is required to intervene. As this technology and concept is so new there are very few courts or authorities that are set up to recognise the legality of financial smart contracts. The US states of Vermont and Delaware have both recently taken steps to address this issue. However, up to now there is still the issue of enforceability and jurisdiction with a smart contract due to its decentralised nature.

However, if the smart contract and coding is correctly set up there should not, of course, be any issue with the correct application of a transaction through a smart contract. The use of logic and simple terminology should ensure that very simple transactions are effected correctly and efficiently.

In addition, start-ups such as CommonAccord are working on a system that auto-translates legal documents into smart contracts, simplifying their interpretation by both lawyers and developers and obviating the need for "legalese."

Smart contracts could also embed dispute resolution mechanisms and jurisdiction clauses to reduce friction and give certainty. For example, a smart contract could include a clause that delegates a matter to an external arbitrator if the parties involved disagree about the contract (as is also standard in a traditional legal contract).

Conclusion

Blockchain based smart contracts can offer many benefits for a wide range of applications for banks. If properly implemented banks can benefit from reduced risk, real-time accurate and verified transactions, fewer intermediaries and lower costs.

In order for smart contracts to come to market in a shorter time they need to be accessible and understandable by businesses. Where processes (and banking processes) are capable of automation then smart contracts could be important to reduce costs and time lag of transactions. However, it remains to be seen whether all the other issues can be overcome to allow for traditional legal contracts to be coded into smart contracts.

Additional Sources

https://www.fastcompany.com/3035723/app-economy/smart-contracts-could-be-cryptocurrencys-killer-app

http://www.blockchaintechnologies.com/blockchain-smart-contracts

http://www.coindesk.com/making-sense-smart-contracts/

http://blogs.lexisnexis.co.uk/futureoflaw/2016/09/what-makes-a-smart-contract-smart/

https://www.cryptocompare.com/coins/guides/what-is-ethereum/

https://cointelegraph.com/ethereum-for-beginners/what-is-ethereum

http://www.pcworld.com/article/3086211/a-blockchain-smart-contract-could-cost-investors-millions.html

https://dupress.deloitte.com/dup-us-en/focus/signals-for-strategists/using-blockchain-for-smart-contracts.html#endnote-14

http://uk.businessinsider.com/smart-contracts-pose-enforceability-issues-2016-11

http://www.coindesk.com/three-smart-contract-misconceptions/

http://www.ibtimes.co.uk/barclays-gets-into-nuts-bolts-smart-contract-templates-1596874

http://blog.mastek.co.uk/smart-contracts-benefits-and-use-cases

https://re-publica.com/en/dub16/session/blockchain-smart-contracts-future-law

http://smartbonds.co/

SPECIAL THANKS

FinTech Network would like to thank Imogen Bunyard (Zerado), Tomasz Mloduchowski (Zerado), Laura Bailey (Zerado) and Will Taylor for their assistance with this whitepaper.

ABOUT FINTECH NETWORK

FinTech Network

We exist to facilitate and advocate the adoption of innovative and disruptive financial technologies. We do this by uniting the most influential figures in the industry to challenge the status quo and improve traditional banking systems. This happens through our industry leading conferences and original content.

W: www.fintecnet.com

dmurphy**@**fintecnet.com

Join the Banking & FinTech Connect
Group on **LinkedIn**

UK Telephone: +44 (0)203 468 9461

Follow FinTech Network on **Twitter**