The Potential of Blockchain Technology for the Conclusion of Contracts

Nikolas Guggenberger

I. Introduction

Blockchain technology has attracted significant media attention in the financial sector and beyond and significant investments. Agencies and institutions on a national, European as well as international level have dedicated significant work and numerous reports to the subject matter. The legislature has refrained from heavily regulating the immature technology. As of now the full impact of Blockchain technology on the economy – especially its potential for smart contracts – is far from foreseeable.

II. Technology

The concept of Blockchain technology as it is presently understood is based on the ideas of Satoshi Nakamoto, the unknown author of the paper ‘Bitcoin: A Peer-to-Peer Electronic Cash System’\(^1\) published in 2008.\(^2\) His paper eventually led to the creation of the most successful virtual currency system to date, Bitcoin. Blockchain is a decentralised database that is jointly maintained by a network of participants, in the Bitcoin context called ‘miners’.\(^3\) In the Bitcoin architecture, these miners validate transactions for which they are rewarded with newly issued coins and, potentially, with transaction fees.\(^4\) Indeed, it is only the first entity solving a math-

---

1 Available online under bitcoin.org/bitcoin.pdf (accessed 22 December 2016).
4 See A Badev/M Chen, ‘Bitcoin: Technical Background and Data Analysis’ (2014) Finance and Economics Discussion Series 1, 14–15. The paper is avail-
ematical problem (by randomly guessing solutions) that gets to determine the next ‘block’ and receives the compensation. The network and its ‘block-building’ therewith are based on a ‘voting system’ in which the employment of computing power (at least over time via increased probabilities) translates to influence in the decision-making process. Hence, within the ‘proof-of-work system’ governing Bitcoin the competition for influence in the gestalt of computing power and the electricity to be invested serves as a threshold for manipulation and safeguards the integrity of the system. Individual transactions are validated and secured by private/public key encryption.

The concept is based on a combination of cryptography, economic incentives and game theory. Neither of these elements were novelties per se, yet the combination thereof shaped a unique scheme which have contributed to its phenomenal success. As a result, Blockchain technology replaces trust and allows for ‘pseudonymous’ transactions without intermediaries.

The characteristics and the enormous potential of this technology have spurred the development of potential business models and opportunities of its employment for the public good. The potential impact ranges from all sorts of transfer of (digital) value, to reliable supply chain management and the operation of registries – most of which is in some respect related to automated contracts or regulation.

---

5 Nakamoto (n 2) 3.
6 Badev/Chen (n 3) 14.
III. Smart Contracts

Smart contracts are no novelty. The term goes back at least to a 1994 publication by Nick Szabo in which he describes a smart contract as ‘computerized transaction protocol that execute the terms of a contract’\(^{11}\). As existing examples he describes payment systems as well as network bandwidth management.\(^{12}\) Later he draws parallels to ‘the humble vending machine’ as a ‘primitive ancestor of smart contracts’\(^{13}\), exemplifying that even in 1994 Szabo described a phenomena whose fundamental principles were far from discretely novel, but had already been embodied in traditional machinery – yet had not been brought to their full potential in the unfolding digital age.

Retrospectively, the observations were visionary, especially because they linked the disruptive potential of smart contracts to ‘digital cash protocols’\(^{14}\) – technology that had already been developed, but whose rise to a fully-fledged and functioning ecosystem only started with the launch of Bitcoin in 2009.\(^{15}\) It is the interdependence between the full potential of the automation of the execution of contracts and the existence of a system that allows for transactions of digital value without intermediaries that has recently centred the attention on smart contracts. Despite the enormous success of Bitcoin and other similar networks (most prominently Ethereum\(^{16}\)), and the technological advances, we are far from having experienced the full potential of the merger of smart contracts and blockchain technology.

This merger promises to reduce transaction costs significantly by eliminating multiple layers of intermediaries present in the current system. Furthermore, it has the potential to provide more security, a higher degree of privacy and finality of transactions.\(^{17}\) On the technical side, it is especially

\(^{11}\) N Szabo, ‘Smart Contracts’ (1994).
\(^{12}\) ibid.
\(^{13}\) N Szabo, ‘Formalizing and securing Relationships on Public Networks’ (1997) 3.
\(^{14}\) Szabo (n 11).
\(^{16}\) www.ethereum.org (accessed 22 December 2016).
the resilience of decentralised systems that is prominent: the Blockchain approach aims at eliminating single points of failure in databases.\textsuperscript{18}

IV. Regulatory State of Play in the EU

Just as the technology itself, regulation in the field of virtual currencies and Blockchain technology is at a very early stage. In light of the potential benefits of blockchain technology, the European Parliament has clearly emphasised that it does not intend to ‘stifle innovation’\textsuperscript{19}. Yet, the institutions agree that no potential comes without risks. The prevailing risk factor in the political discourse is the technology’s potential exploitation for criminal conduct.\textsuperscript{20}

1. Reports and assessments

Since 2012, European institutions and authorities have published numerous reports on virtual currencies and, especially recently, on the underlying blockchain technology.\textsuperscript{21} Financial markets and banking supervisors first picked up on the phenomena. Naturally, most of the agencies and institutions focused on their specific mandate when conducting their studies.

\begin{enumerate}
\item Kaulartz (n 8) 476.
\item European Parliament (n 10) [14].
\end{enumerate}
The European Central Bank (ECB) alone published two comprehensive reports focusing on monetary policy implications of virtual currencies as well as various shorter papers, with at least one shifting the focus towards the employment of the technology beyond virtual currencies. In its reports focusing the monetary policy, the ECB expressed that it at least ‘presently’ (2012–2015) does not fear a limitation of the impact of monetary policy rooted in a competition by virtual currencies.

After its initial early and very explicit warning of consumers against using virtual currencies in general, the European Banking Authority (EBA) published a comprehensive report with a list of 82 individual risks that it associated with virtual currencies. Amongst other measures the EBA called for the implementation of customer due diligence rules in the blockchain network, a mandatory incorporation in a EU Member State, a structural separation of exposures to virtual currencies and regulated banking activities to shield off the risks thought to be associated with virtual currencies, mandatory capital requirements, the establishment of evidence for sufficient IT security and the implementation of guarantees for unauthorised transactions.

24 ECB, ‘Virtual Currency Schemes – a further analysis (February 2015) 26; yet, the ECB’s opinion on the Commission’s proposal to amend the AMLD seems more critical of virtual currencies as a phenomenon, possibly suggesting a certain level of suspicion towards potential future competition.
25 EBA, ‘Warning to consumers on virtual currencies’ (n 21).
26 EBA, ‘Opinion on “virtual currencies (n 21) [64–146].
27 ibid [156–157].
28 ibid [159].
29 ibid [169].
30 ibid [164].
31 ibid [166].
32 ibid [167–168].
a) European Parliament Resolution

The European Parliament picked up the subject in 2015 and started working on its own-initiative report titled ‘Virtual currencies’. After an expert hearing in the Committee for Economic and Monetary Affairs (ECON), Jakob von Weizsäcker, the Parliament’s Rapporteur, published a draft report on virtual currencies in February 2015.\(^{33}\) The report was grounded on the assessment that Blockchain is a nascent technology, that the understanding of said technology and its applications are limited, and that prohibitive legislation at this early stage is prone to limiting the technology’s potential. The Rapporteur aimed at striking a balance between allowing for breathing space for a new technology and concerns over potential new systemic implications of rapidly growing applications and the ability to respond appropriately.\(^{34}\) After the ECON Committee had adopted the report with an overwhelming majority, the Rapporteur explained: ‘To avoid stifling innovation, we favour precautionary monitoring instead of preemptive regulation. But, IT innovations can spread very rapidly and become systemic.’\(^{35}\) This approach was successfully upheld in plenary, again with a broad majority in May 2016\(^{36}\). Following its initial assessment, the European Parliament in the final resolution ‘call[ed] on the Commission to establish a taskforce to actively monitor how the technology evolves and to make timely proposals for specific regulation if, and when, the need arises’.\(^{37}\)

The Parliamentary Resolution contains a comprehensive set of potentials and risks associated with the employment of virtual currency schemes, ranging from hopes to cut transaction costs, especially for cross-border transfers, enhancing resilience of payment infrastructures and en-

\(^{33}\) European Parliament Committee on Economic and Monetary Affairs, ‘Draft Report on virtual currencies’ (2016/2007(INI)).

\(^{34}\) ibid Explanatory Statement 2.c).


\(^{37}\) ibid.
suring a high degree of privacy to concerns relating to the criminal abuse of pseudonymous structures, the energy consumption of proof of work models, sufficient consumer protection and the absence of reliable governance structures. The resolution encourages the public sector to test Blockchain-based systems and urges to include the technology in a broader regtech agenda, namely to ‘reduce the sizeable VAT gap in the Union’. The Parliament endorsed the Commission’s suggestions to include exchange platforms in the scope of the Anti Money Laundering Directive (AMLD). Interestingly, the resolution remains silent with respect to wallet providers. In paragraph 20, Parliament explicitly mentions enhancing interoperability and ‘the promotion of a universal and non-proprietary electronic wallet’ as means to increasing ‘competition and lowering transaction costs’. Conditional on reaching systemic importance the European Parliament suggests developing stress tests for the block chain based applications. With the adoption of the final resolution in May 2016 the ball was back in the Commission’s court.

b) Commission Proposal for Amendments to the AMLD

Slightly later than originally planned the Commission came forward with its suggestions to amend the AMLD on 5 July 2016. The Commission in its proposal maintained its original suggestions in the action plan and recommended an inclusion of virtual currency exchange platforms as well as custodian wallet providers in the scope of the AMLD by including them in the list of obliged entities. As a result of this inclusion both exchange

38 European Parliament (n 10).
39 ibid [12–13].
40 ibid [13].
42 European Parliament (n 10) [19].
43 ibid [20].
44 ibid [22 iv].
45 European Commission, COM(2016) 50 final (n 20).
platforms and custodian wallet providers would be required to comply with ‘know your customer’ rules (KYC), to report suspicious transactions and to ensure that their managers are ‘fit and proper’.\textsuperscript{47}

The Commission implicitly defined virtual currency exchange platforms as ‘providers engaged primarily and professionally in exchange services between virtual currencies and fiat currencies’\textsuperscript{48}. The inclusion of wallet providers is limited to such ‘wallet providers offering custodial services of credentials necessary to access virtual currencies’.\textsuperscript{49} In the impact assessment the Commission clarifies that it intended to include services relying on multi-signature technology.\textsuperscript{50}

Not less importantly, for the first time EU legislation would include a legal definition of virtual currencies, defining them as ‘a digital representation of value that is neither issued by a central bank or a public authority, nor necessarily attached to a fiat currency, but is accepted by natural or legal persons as a means of payment and can be transferred, stored or traded electronically’.\textsuperscript{51} Noteworthy in this respect is the exclusion of local currencies from the aforementioned definition in recital 8.

The Member States are called upon to ensure that the entities in question are either registered or licensed. It is up to the Member States to specify the requirements, to set up new processes and to dedicate competent authorities. Despite the undoubtedly cross-border nature of the business there will be no possibility for passporting. The directive is only a minimum standard allowing Member States to go beyond the requirements laid out in the directive – a fact that would not have excluded passporting as such.
2. EBA Opinion, ECB Opinion and Council Approach

On 11 August 2016, the European Banking Authority published its Opinion on the recent Commission proposal. In general terms the EBA ‘welcomes the Commission’s proposal’ to extend the scope of the AMLD, laying out that this would ‘be an important step to mitigate some of the financial crime risks arising from the use of virtual currencies’52. The EBA expresses that – due to the urgency of action – the Commission was right in limiting itself to amendments to the AMLD and calls for the launch of a comprehensive review of the regulatory regime in light of its 2014 suggestions as soon as possible.53 In its Opinion, the EBA expresses concerns relating to the perceived level of regulation deviating from the actual level of regulatory safeguards.54 The authority points out that passporting is not possible across the Union and that obliged entities may have ‘to be registered or licensed in each Member State in which they intend to provide VC-related services’55 and suggests to ease the exchange of information between authorities56. Based on the lack of specific sectorial regulation, the EBA recommends further clarification with respect to the ‘fit and proper’ criterion for managers.57 The EBA emphasises that nationally differing regulatory regimes based on ‘a choice between a licensing or a registration regime […] risks […] undermining the aims of the Directive’58 and, therefore, proposes to opt for the one deemed appropriate.59

Just one day after the EBA, on 12 October 2016, the European Central Bank issued its own Opinion60 on the AMLD-proposal. While the ECB expresses support for the inclusion of exchange platforms and custodian

52 EBA, EBA/Op/2016/07 (n 21) [8].
53 ibid [19].
54 ibid [22].
55 ibid [27].
56 ibid [30].
57 ibid [31–33].
58 ibid [37].
59 ibid [38].
wallet providers in the AMLD, the tone the ECB chooses certainly differs from the Commission’s. In this sense the ECB even goes as far as advising ‘Union legislative bodies’ to ‘take care not to appear to promote the use of privately established digital currencies’.\(^{61}\) The ECB articulates concerns relating to the volatility of virtual currencies, their lacking guarantee to remain interchangeable for goods or fiat currency in the future and their abstract potential to diminish the effectiveness of monetary policy.\(^{62}\) On substance the ECB specifically suggests deleting the perceived endorsement of the usage of virtual currencies in recital 7 as well as a modification of the definition of virtual currencies: According to the ECB’s proposal, it should be pointed out that virtual currencies do not have the legal status of currency or money and indeed might be used for purposes other than payments.\(^{63}\)

The latest version discussed in the Council, dated as of 14 November 2016, incorporates the core of the ECB suggestions and changes the proposed definitions for exchange platforms and custodian wallet providers.\(^{64}\) It is no longer required that exchange platforms primarily or professionally act as such. The definition of custodian wallet providers, now an explicit definition complementing Art 3 AMLD, clarifies that any provision of services to safeguard private cryptographic keys is sufficient. Especially with respect to multi-signature services this seems to reflect the original intent articulated in the impact assessment of the Commission.\(^{65}\) The definition of virtual currencies suggested by the Presidency is very explicit in distinguishing virtual currencies from regulated types of currencies and money.\(^{66}\)

---

61 ibid [1.1.2].
62 ibid.
63 ibid Annex.
65 European Commission, Inception Impact Assessment (n 50) [A. (iii)].
IV. Observations

While reasonable on substance in terms of the material requirements and the respective burden on the virtual currency ecosystem, the approach currently taken by the EU legislative bodies suffers from a serious flaw: it creates a legally fragmented regulatory regime where a full harmonisation on substance combined with a one-stop-shop European regulator would be appropriate. The EBA in its Opinion rightly points out that virtual currency transactions are not bound by national borders and therefore cannot be treated as if they were. Yet, the EBA’s suggestions relating to the exchange of information are far from sufficient to mitigate the apparent problem, both with respect to the effectiveness of the new rules and with respect to the regulatory burden, especially on nascent start-ups. The problem becomes worse when taking into account that passporting in will not be possible.

One could have and should have learned from the situation in the United States where payments in general and virtual currencies specifically are regulated (or not-regulated) on a state level and where this circumstance has been identified as a significant disadvantage. The field of virtual currencies would have been (and currently still is) an excellent opportunity for building up functional and efficient European regulatory structures where legacy problems do not hinder such efforts. Relying on minimum harmonisation on substance and procedure, entrusting the execution of the rules with national authorities and passing on creating appropriate passporting rules is a missed chance in terms of industrial policy and will be looked back upon as a painful mistake. Therefore – where a global approach would be appropriate, but not in sight – let us at least opt for a genuinely European solution.

---

67 EBA, EBA/Op/2014/08 (n 21) [173].
69 EBA (n 67).
1. Smart Contracts

In accordance with the aforementioned original definition by Nick Szabo, smart contracts are protocols whose execution of a pre-defined outcome is triggered by certain predefined conditions. It is important to note that smart contracts need a link to their built-in condition functioning as a trigger. This link usually is a trusted source or set of sources of information commonly called ‘oracle’. Based on Blockchain technology smart contracts then allow for any sort of direct transactions without intermediaries. This entails both, enormous chances and challenges for a legal system that was (at least originally) certainly not designed for these phenomena.

2. Chances

In general, advantages of smart contracts are seen related to the speed of their potential execution, the transaction costs, the finality of their execution and the reliance upon its execution. The automation of the execution and the potential to ‘lock-in’ value released upon performance has the capacity to substitute trust between the parties to the contract which traditionally has especially been based on reputation the threat of enforcement with the help of public authorities. Smart contracts are thought to be able to provide full transparency or a high degree of privacy.

The use cases for the employment of smart contracts based on Blockchain or Blockchain-like infrastructures appears to be almost unlimited. Areas which have already been identified as potential beneficiaries of the

---

71 ibid 10.
employment of smart contracts relate to the Internet of Things, to privacy and identity management, to electricity grid management, to industry 4.0 infrastructure and to digital rights and supply chain management. From settlement to reconciliation and from derivatives to loan agreements, the financial sector seems to be especially prone for disruption. The potential of smart contracts becomes greater the more objective and reliable the ‘triggers’ in a contract are (representations and warranties, covenants, conditions for default and breach as well as remedies).

An example for an issue well suited to be addressed via smart contracts is the distribution of compensation resulting from the exercise of flight passenger rights. To a large extent this concerns a B2C environment: rather small claims and a large number of potential creditors. The main criteria for the validity of a claim, delays or cancellations, are comparably objective. The condition triggering a pay-out can be verified (rather) reliably by oracles. Yet this very example also shows that there is no claim simple enough to be determined only by objective criteria: an airline does not owe compensation in cases of force majeure which certainly challenges the automation.

3. Challenges

First and foremost a smart contract can only be based on objective criteria. Of course, objective criteria might contain elements of or fully constitute judgements of others. Still, despite the possibility to outsource judgement and the employment of discretion to oracles, each and every individual contract as such is governed by overarching principles and legal concepts whose application itself require judgement and discretion.

Putting aside potential advances in artificial intelligence, a smart contract can only reflect the knowledge and capabilities of the coder at the

75 Kaulartz/Heckmann (n 17) 620.
78 Wright/De Filippi (n 70) 26.
A fully automated smart contract is therefore incapable of including future changes in the law or reality as well as incorporating abstract legal consequences such as equity.

This leads to an inherent tension between automation and efficiency on the one hand and flexibility and equity on the other. Smart contracts in this sense are not law. Smart contracts are simply a form of execution which might or might not deviate from the law just as any other act in reality can. Smart contracts can only automate typical and probable scenarios. While the employment of smart contracts does not guarantee the enforcement of ‘the law’, they are a suitable means to adjusting the default risk allocation amongst contractual parties.

VI. Conclusions

The recent Commission proposal on the extension of the AMLD is reasonable on substance. The suggestions by the ECB and the EBA as well as the amendments presently discussed in the Council can contribute to the clarity of the rules. Yet, in terms of industrial policy as well as to avoid undue burden on a nascent technology, this proposal constitutes a missed chance. Instead of relying on national regimes and various national competent authorities, the Commission should have opted for a one-stop-shop single regulator on an EU level enforcing a fully harmonised set of rules. The legislative measure of choice would be a regulation instead of a directive. While promising more effectiveness on substance, harmonising the regulatory standards and entrusting them with a single regulator on an EU-level would still entail a major industrial policy opportunity for Europe.

Smart contracts based on Blockchain have the potential to automate standardised transactions and significantly lower transaction costs. They can – to a certain extent – create certainty and finality and ease the practical enforcement of small claims. The need for flexibility and equity, how-

79  Raskin (n 73) 7.
80  Wright/De Filippi (n 70) 26.
81  Raskin (n 73) 22.
ever, severely limits contractual automation. Rights and defences based on discretionary judgments and equity will have to be safeguarded.

The potential to easily redistribute risks associated with the enforcement of contractual or legal obligations is powerful, both as a tool for contractual parties seeking to perpetuate their bargaining power and as a tool for regulators to ensure the practical enforcement of protective regulation or small claims. Smart contracts have the potential to replace existing intermediaries and gatekeepers, but not yet courts or other official dispute resolution mechanisms. Still, public courts and the traditional judicial system will have to transform to keep up with the technology.

This innovation cycle calls for an active and engaging state as opposed to one that is either prohibitive or passive. A comprehensive roadmap is urgently needed and should explore options for official virtual currencies (as currently done, for example, in the UK and Sweden) and efforts to further open up innovations surrounding application process interfaces (API) should not be hindered, especially at this early stage. Yet, a ‘do no harm’-approach will certainly not be sufficient to foster innovation in the long run and to guarantee a fair and inclusive environment.
