HARRY POTTER, ETHEREUM, AND THE BLOCKCHAIN: REVISED IMPLICATIONS AND CURRENT SHORTCOMINGS OF SMART CONTRACTS

By Ari Herbert[*]

Imagine a deal that can't be broken. Harry Potter fans will remember the "unbreakable vow": two wizards clasp arms, declare their promises, and whisper an incantation.[1] A silvery thread of light twists around the enclasped arms and then disappears. The spell is done. The deal can't be broken. This was a major plot tool in the Harry Potter series. But if self-enforcing agreements were real, our commercial world would be very different. Trusted intermediaries and legal enforcement procedures would be less needed.

Using blockchain (the same technology underlying Bitcoin), computer programmers are striving to make this a digital reality. They've built Ethereum, a new internet, which can host applications like Gmail and Facebook. Except on Ethereum, applications aren't hosted on company servers. Instead, applications are stored simultaneously on all computers running Ethereum. Like cream cheese spread on toast. In other words, it's decentralized.

This decentralized technology has many implications. Already mentioned is the possibility of self-executing agreements called "smart contracts." Yet so far, smart contracts have a narrower applicability than envisioned, and there are significant hurdles between present smart-contract use and widespread adoption. Nevertheless, smart contracts are on the rise.[2] Thus it's important to update the discussion of this promising commercial tool.

Part I of this Essay discusses the implications of smart contracts. In Subpart I.A, this Essay explains how blockchain and smart contracts work. This Essay continues in Subpart 1.B by raising the full gambit of possible benefits from smart contracts, both more and less plausible alike. Part II of this Essay then raises the obstacles that smart contracts face. In Subpart II.A, this Essay raises technological limitations, and Subpart II.B addresses the

* Associate, Quinn Emanuel Urquhart & Sullivan LLP; J.D. University of Texas, 2017.

1. J. K. ROWLING, HARRY POTTER AND THE HALF-BLOOD PRINCE 36–37 (2005).

2. *See* Confideal, *Confideal's Crusade to Harness the Power of Smart Contracts*, Bitcoin Mag., https://bitcoinmagazine.com/articles/confideals-crusade-harness-power-smart-contracts/.

legal and social limitations of smart contracts. Finally, this Essay concludes by giving an appraisal of the realistic potential for smart contracts and offering some modest suggestions for courts and regulators.

I. BLOCKCHAIN IS A DECENTRALIZED, ENCRYPTED RECORDING SYSTEM FOR TRANSACTIONS.

A. What blockchain is, and why it makes smart contracts possible.

Bitcoin was the first publicly accessible instance of blockchain technology.[3] Bitcoin was initially championed mostly by crypto-anarchists and libertarians. "Imagine it! A world where big banks run by the government can't manipulate your money." But at the time, the technology was more a novelty or experiment. Then, criminals began transacting with Bitcoin through the dark web.[4] Drugs, weapons, hit men. Sordid stuff. Eventually, Bitcoin took a turn for the better. The Winklevoss twins invested. Neighborhood coffee shops started accepting Bitcoin as payment (admittedly as more of a novelty). Most of all, the price sky-rocketed. But why? What is unique about blockchain? Three things.

First, blockchain technology uses cryptography. To better understand what that means, consider the following example. Andy wants to send his Bitcoin to Charlie. Andy and Charlie each have two unique codes ("keys"), one private and one public, that identifies them. By entering both his private and public keys, Andy creates a digital manifestation of consent, like a signature. Then, Andy identifies Charlie's public key in the public record of his Bitcoin. This proves the identities of the parties involved. It also shows that the party (or parties) intended to transact. Hence, the system is trustless in that intermediaries are no longer needed to verify the parties and their intent.

Second, blockchain technology runs on a distributed network,[5] similar to a public ledger. What this means is that no single computer is responsible for storing a master ledger of records. Rather, all of the computers running the blockchain program (called nodes) jointly share the job. Each node has a record of every transaction on the blockchain, so there's a low risk of tampering or

3 Matt Lucas, *The Difference Between Bitcoin and Blockchain for Business*, IBM: Blockchain Unleashed: IBM Blockchain Blog (May 9, 2017), https://www.ibm.com/blogs/blockchain/2017/05/the-difference-between-bitcoin-and-blockchain-for-business/.

4 Keith Kirkpatrick, *Financing the Dark Web*, 60 Comm. of the ACM 3, 2122 (March 2017), https://cacm.acm.org/magazines/2017/3/213816-financing-the-dark-web/fulltext.

5 *See* Nolan Bauerle, *How Does Blockchain Technology Work?*, CoinDesk, https://www.coindesk.com/information/how-does-blockchain-technology-work/ (offering the tree-falling-in-the-woods thought experiment as a way to understand a benefit of blockchain).

loss. A useful analogy is the familiar thought experiment: if a tree falls in the woods and no one is around to hear it, does it make a sound?[6] If you put one person in the woods with recording equipment, you are trusting that one person's recording. So you need to vet that one person to ensure they are reliable. Instead, having many people in the woods, each with their own recording equipment, reduces the need for vetting. If the majority of people were able to record the falling tree, there's a consensus on whether the tree made a sound.

Third, blockchain technology incentivizes participation. Returning to the previous example, how do you get all those people to go to the woods? One way is to offer a reward. Blockchain technologies build a reward program into the system. With Bitcoin, for example, participating computers maintain records by working complicated math problems showing the origin of a particular Bitcoin, called proof-of-work problems. Anytime a new Bitcoin is discovered through this process, the discovering computer is awarded ownership.

In sum, blockchain technology is a trustless, decentralized public ledger. It has a number of implications and uses. Bitcoin and other crypto currencies are the most known and discussed use of blockchain. But that's not all. In Sweden and the Republic of Georgia, blockchain programs are being established by the government as official property-title recording systems, replacing the old central databases.[7] Then, of course, there are smart contracts.

The term "smart contract" was first coined by Nick Szabo, one of the early originators of the idea.[8] He described smart contracts as "a set of promises, specified in digital form, including protocols within which the parties perform on the other promises."[9] In other words, it's a meeting of the minds—just like any contract—that, atypically, is memorialized in code. And the contract self-executes based on any number of pre-programmed conditions. This means the contract self-enforces. Today, smart contracts are possible

6 *See id.*

7 Laura Shin, *The First Government to Secure Land Titles on The Bitcoin Blockchain Expands Project*, Forbes (Feb. 7, 2017), https://www.forbes.com/sites/laurashin/2017/02/07/the-first-government-to-secure-land-titles-on-the-bitcoin-blockchain-expands-project/#3ac3918d4dcd (discussing the Republic of Georgia); Joseph Young, *Sweden Officially Started Using Blockchain to Register Land and Properties*, The CoinTelegraph (July 6, 2017), https://cointelegraph.com/news/sweden-officially-started-using-blockchain-to-register-land-and-properties (discussing Sweden).

8 Michael Gord, *Smart Contracts Described by Nick Szabo 20 Years Ago Now Becoming Reality*, Bitcoin Mag (Apr. 26, 2016), https://bitcoinmagazine.com/articles/smart-contracts-described-by-nick-szabo-years-ago-now-becoming-reality-1461693751/ (citing Nick Szabo, *Smart Contracts*, Extropy (1996)).

9 *Id.*

within a blockchain system. But the Bitcoin platform can't sustain smart contracts. Enter Ethereum.[10]

Ethereum hosts services and applications like the ones accessible already through the internet. Except the applications aren't hosted on company servers that users access on demand. Instead, Ethereum is a blockchain platform. Blockchain nodes running Ethereum jointly host all applications. This could, if widely adopted, decentralize the internet and eliminate currently necessary middlemen. Similar to Bitcoin, Ethereum has its own crypto currency called Ether. But Ether is merely a facilitating currency for the central purpose of Ethereum: building applications and creating contracts on a platform akin to a new internet. The Ethereum platform allows blockchain transactions that are significantly more complicated than the transfer of currency. Using smart-contract-specific programming languages, such as Solidity,[11] programmers can incorporate sophisticated conditions into code. The conditions, when met, cause a transfer. Thus, by agreeing at the outset to the provisions of a code, parties effectively agree to terms of a contract. And these smart contracts are publicly recorded and stored on the blockchain across all nodes.[12] So to the extent that the parties' assets and value are stored within Ethereum, a self-executing contract is also self-enforcing.

B. The range of smart-contract implications.

Such smart contracts have a number of implications. First, there's the possibility of disintermediating contracts.[13] Blockchain currency disintermediates personal and consumer finance by eliminating middlemen like banks and clearing houses, reducing associated costs. Likewise, smart contracts could eliminate contractual middlemen like lawyers, title companies, lenders, arbitrators, and countless other transaction-specific intermediaries.

Second, some have speculated that since self-executing contracts are effectively self-enforcing, the need for courts may be eliminated if parties are unable to breach.[14] And even if the need for enforcement or remedies are not rendered unnecessary by smart contracts, the smart contracts themselves could contain code providing for particular remedies or enforcement mechanisms that

10 Ethereum Project, https://ethereum.org/.

11 *See generally* Ryan Molecke, *How to Learn Solidity: The Ultimate Ethereum Coding Guide*, Blockgeeks, https://blockgeeks.com/guides/how-to-learn-solidity/ (providing a step-by-step process for learning Solidity).

12 *See* Alyssa Hertig, *What is Ethereum?*, CoinDesk, https://www.coindesk.com/information/what-is-ethereum/.

13 *See generally* Joshua A.T. Fairfield, *Smart Contracts, Bitcoin Bots, and Consumer Protection*, 71 WASH. & LEE L. REV. ONLINE 35, 40 (2014).

14 *See, e.g.*, *id.* at 38–41; Trevor I. Kiviat, Note, *Beyond Bitcoin: Issues in Regulating Blockchain Transactions*, 65 DUKE L.J. 569, 605–07 (2015).

automatically occur on certain conditions. This would be similar to a liquidated damages clause, except it would be self-enforcing.

Third, smart contracts and blockchain could make possible the return of consumer commercial contracts with dickered terms. Currently, everyday contracts—e.g., digital terms of service for companies like Spotify—are filled with boilerplate provisions. There's no way to alter or decline particular provisions. In effect, consumers' only choice is take it or leave it. But with smart contracts that self-execute and self-enforce, the possibility for programmed-in conditions might enable variable price structures for goods or services depending on a number of terms that are accepted or rejected.[15] Consumer choice could be effectuated by automated agents programmed into the blockchain to behave according to consumer-set preferences.[16]

Fourth, smart contracts could also incorporate external information to increase the scope of their applicability. Through contractual reference to particular outside sources referred to as "oracles," parties can contract on the basis of outside information, which the smart contract will draw into its enforcement and execution protocol at the contractually determined time.[17] For example, parties could stipulate that their transaction would be for the market price of a given commodity on a particular date, as listed under a specific exchange. The smart contract would be programmed to pull the market rate listed under the specified exchange on the date set in the contract.

As blockchain innovators continue to experiment, even more uses and potentials for smart contracts may emerge. Yet future potentials aside, smart contracts have real hurdles blocking their path.

II. IMPLEMENTING SMART CONTRACTS WOULD REQUIRE OVERCOMING SIGNIFICANT TECHNOLOGICAL, LEGAL, AND SOCIAL CONSTRAINTS.

Smart contracts' promises are enticing. But those promises remain unfulfilled because of two major roadblocks. First, there are technological limitations that make broad implementation of smart contracts costly. Computer power must improve in order to make smart contracts sensible for smaller, consumer transactions. Currently, smart contracts are implementable only for larger scale transactions in a narrow scope of industries. Second, smart contracts have so far failed to meet social needs and to replace legal guarantees.

15 *See* Fairfield, *supra* note 13, at 41–44.
16 *Id.* at 44–46.
17 Kiviat, *supra* note 14, at 606–07.

A. Technological constraints.

Three technological constraints prevent large-scale adoption of smart contracts. First, computations and transactions are relatively expensive when carried out with blockchain technology. Normally, one computer carries out a computation. But with blockchain technology, every node running the system is responsible for the transaction. So every node must run the computations, which uses many times the computing power. With Bitcoins, the transactions are simple, and so the costs are relatively low. But with smart contracts run on Ethereum, the transactions—and hence, computations—are significantly more complicated. Every Ethereum node, using a feature called the Ethereum Virtual Machine or EVM, must record, read, and carry out every smart contract.[18] Nick Szabo views requirements like these as "necessary tradeoffs, sacrificing performance in order to achieve the security necessary for independent, seamlessly global, and automated integrity . . . ."[19] Regardless, the computer power required is immense. But that's not all.

Second, there remains some risk of mistakes, hacks, and fraud in blockchain. Mistakes are magnified by the blockchain. As Professor Bill Maurer of UCI notes: "Cryptography is brittle: if even a single bit is changed (or "rots") the hash function[, which maps unique keys to their respective owners,] no longer precisely refers to the contract, leaving only a nearly-impossible mathematical needle-in-the-haystack search as redress (formally, "code cracking")."[20] And hacks can be even worse.

One type of potential hack is a 51% attack. If the majority of nodes in a blockchain system agree on a particular record of affairs, that record is the consensus view and thus controls.[21] So if hackers could convince 51% of the nodes running Ethereum to believe in a fabricated state of affairs, the hackers could alter digital property at will. In 2016, someone hacked an immensely valuable Ethereum smart contract called the DAO—Decentralized Autonomous Organization.[22] The DAO was a smart contract programmed to run like an investment fund, except it was decentralized and funded with Ether. Anyone could contribute to the fund. The more someone contributed, the more control that person had over the

18 *See* Hertig, *supra* note 12.

19 Nick Szabo, *Money, Blockchain, and Social Scalability*, Unenumerated: An Unending Variety of Topics (Feb. 9, 2017), http://unenumerated.blogspot.com/search?updated-max=2017-02-23T23:48:00-08:00&max-results=11.

20 Quinn DuPont & Bill Maurer, *Ledgers and Law in the Blockchain*, King's Review, at 7 (June 23, 2015), http://kingsreview.co.uk/articles/ledgers-and-law-in-the-blockchain/.

21 *Id.*

22 Klint Finley, *A $50 Million Hack Just Showed That the DAO Was All Too Human*, Wired (June 18, 2016), https://www.wired.com/2016/06/50-million-hack-just-showed-dao-human/.

fund. It was a skin-in-the-game experiment to show that Ethereum smart contracts could even replace the role of trusted financial institutions. But it all went awry when a still-unknown hacker stole $55 million worth of Ether from the fund. It's not clear what sort of hack was used, and the money remains missing.[23] But Ethereum's solution was to duplicate the entirety of the blockchain, creating two parallel copies of Ethereum: one from before the theft occurred and one from after.[24]

This is called a hard fork.[25] It presents a vexing philosophical question for blockchain proponents. The central premise of blockchain is that it's trustless. But if fraud and thievery requires the intervention of an administrator, how is Ethereum any different from present payment systems with intermediaries? How is it still trustless? Now, there are two versions of Ethereum. The first is still called Ethereum, and it is the corrected blockchain in which the theft never occurred. The second is called Ethereum Classic, where the theft did occur.[26] By and large, the Ethereum community ignores Ethereum Classic in favor of Ethereum. So in that sense, DAO never lost its money. This solution depends on the existing community's willingness to accept the hard fork to switch tracks and go along with the remedial version of Ethereum. And this isn't the only compromise to the trustless element of blockchain.

Third, the need for smart contracts to incorporate external information from oracles[27] is itself a shortcoming. The accuracy of the external source requires vetting and trust. From a theoretical standpoint, possible inaccuracy doesn't present a contract problem. So long as the parties to a smart contract jointly and knowingly rely on a particular external source, then the possible inaccuracy of the source is a risk they've allocated in their bargain. But from a practical standpoint, contracting parties routinely seek out trusted institutions for intermediaries. These trusted institutions are usually regulated and heavily vetted, so parties are unlikely to be content with significant inaccuracy risks. Likely, parties will ultimately rely on trusted intermediaries,[28] undermining at least some (if not much) of blockchain's appeal. Then, there are the complications and costs of using a trusted intermediary. Ensuring that an intermediary can be trusted is expensive. This raises the transaction costs for smart contracts.

23 Matthew Leising, *The Ether Thief*, Bloomberg (June 13, 2017), https://www.bloomberg.com/features/2017-the-ether-thief/.

24 Finley, *supra* note 22.

25 *Id.*

26 Ameer Rosic*, What Is Ethereum Classic? Ethereum vs. Ethereum Classic,* BlockGeeks (June 2017), https://www.blockgeeks.com/guides/what-is-ethereum-classic/.

27 *See* Kiviat, *supra* note 14, at 606–07 and accompanying text.

28 *See* Oraclize, *About,* http://www.oraclize.it/#about.

Even so, there's still the possibility that the transaction costs will remain substantially lower than current payment systems—low enough to still be attractive. As Nick Szabo has noted, while "blockchain itself cannot possibly come anywhere near Visa transaction-per-second numbers and maintain the automated integrity that creates its distinctive advantages versus these traditional financial systems . . . ," a "less trust-minimized" third party can be relied on to carry a significant load.[29]

B. Legal and social constraints.

There are even more social and legal constraints to smart contract implementation. The initial most requirement is threshold. There must be a sufficient population using Ethereum for it to matter. Your next-door neighbor Joe might use Ethereum to register the title to his house, but that only protects his interest in the house if the government recognizes the title system. Joe may be willing to contract out his services through Ethereum, but that only benefits him if there are customers seeking out services through Ethereum. There must be a sufficient using Ethereum in the first place for other users to get onboard.[30] That's the risk of attracting users.

There's also the risk of losing users. If (or maybe when) there's a new, better alternative to Ethereum, the community using Ethereum may abandon it. Professor Maurer rightly observes that "high technology is famously faddish, so whether the network of miners will keep your Ethereum marriage contract as long as your love remains is an open question."[31] The records—in fact, the entire system—is premised on the idea that there is a community of users providing a system of nodes that maintain the network. The more nodes, the stronger the system. If users abandon Ethereum, the strength and reliability of the contracts and property rights recorded on Ethereum would quickly fade. This long-term risk blocks serious entrants.

Also somewhat problematic is competing platforms. If there are competing blockchain platforms on which smart contracts can be made, there may be a need for cross-platform transactions. This means additional intermediaries, which increase the cost as well as the potential vulnerability. If a smart contract exists across two platforms, there are two points of attack. On the other hand,

29 Nick Szabo, *Unenumerated: Money, blockchains, and social scalability*, BLOGSPOT (Feb. 9, 2017), http://unenumerated.blogspot.com/2017/02/money-blockchains-and-social-scalability.html.

30 *See generally* Malcolm Gladwell, *The Big Man Can't Shoot*, Revisionist History Podcast, https://www.revisionisthistory.com/episodes/03-the-big-man-cant-shoot/ (explaining threshold theory through the example of Wilt Chamberlain and free-throw shooting).

31 DuPont & Maurer, *supra* note 20, at 7.

intermediaries for cross-platform transactions may be a necessary cost that is relatively inexpensive in comparison to the complex system of trusted parties in contemporary commercial life.

Finally, there are practical competence issues preventing widespread use of smart contracts. Using Ethereum requires the technological know-how. Users need to download a browser like Mist to actually use Ethereum.[32] Eventually, of course, browsers may advance to a more user-friendly point. Users also need to store their currency. Often, this is a "wallet": a digital service or physical device that stores crypto currency keys. These, too, present security risks. Hackers can steal keys from digital wallets, and users can lose physical wallets. Without the private keys, the respective crypto currency is useless and unrecoverable. With traditional money, someone who loses access to their online banking account merely needs to call or go to their bank and offer sufficient proof of identity to recover access. No big deal.

C. Due to constraints, smart contracts are viable in limited circumstances, and regulators and courts should seek to help the technology overcome some of these legal and social constraints.

Computer scientists are building this new future. Ultimately, they are the ones that must solve the technological and social constraints that smart contracts currently face, and they're already working toward that goal. Ethereum developers have begun a series of planned hard forks to buttress the security of the system and to further the development of Ethereum.[33] Vitalik Buterin, Ethereum co-founder, has publicly recognized the interest from and entrance by many major companies. This includes a number of "multi-billion dollar financial institutions . . . [and] Fortune 500 conglomerates . . . like JPMorgan, Microsoft, Intel and BBVA."[34] Buterin has noted that applications like Reddit, United Nations world food programs, and global prediction markets are all ready to join Ethereum but for the social scalability issues that Ethereum faces.[35] Hence the hard fork series.

Still, there are two minor remedies regulators and courts can implement, respectively. First, regulators can update the UCC to clearly recognize the enforceability of smart contracts. At first glance, it appears that the UCC already captures a great deal of potential smart-contract transactions. Under UCC § 2-206, "an offer

32 *See* Alyssa Hertig, *How to Use Ethereum*, CoinDesk, https://www.coindesk.com/information/how-to-use-ethereum/.

33 Joseph Young, *First Iteration of Ethereum Metropolis Hard Fork to Appear Monday*, CoinTelegraph (Sept. 17, 2017), https://cointelegraph.com/news/first-iteration-of-ethereum-metropolis-hard-fork-to-appear-monday.

34 *Id.*

35 *See* Vitalik Buterin (@VitalikButerin), Twitter (Aug. 10, 2017, 12:27 AM), https://twitter.com/VitalikButerin/status/895547081976303617.

to make a contract shall be construed as inviting acceptance in any manner and *by any medium reasonable in the circumstances . . . .*"[36] So, some may reason, maybe smart contracts shouldn't face much difficulty in getting court recognition. In which case, if a dispute arises—perhaps out of fraud—a plaintiff would have the full host of remedies available to him or her. But there is significant ambiguity about how Bitcoin and crypto currency should be categorized under the UCC. Jeffrey Snyder of Bilzin Sumberg speculates that there are plausible arguments to classify Bitcoin, for example, as either a security under Article 8 of the UCC or a commodity under the Commodity Exchange Act.[37] Some additional comments or clarification recognizing the enforceability of smart contracts would provide a safety net for transactions gone wrong, making experimentation with Ethereum less risky.

Second, if the UCC fails, courts can stand ready with the law of restitution for unjust enrichment. If smart contracts are not even recognized as contracts (as opposed to merely being held unenforceable), restitution provides yet another safety net. Restitution law starts with the premise that unjust enrichments occur from time to time.[38] Somebody gets something that didn't belong to him or her. When no contract existed and no tort was committed (i.e., there was no conversion), the law of restitution provides an alternate theory for recovery. In the case of smart contract mistakes, the plaintiff can seek—assuming a contract is not recognized[39]—restitution: "Give me the money equivalent of the windfall you received, defendant." Of course, the issue with this proposal is that it only becomes viable when something goes wrong, parties end up in court, and the plaintiff *realizes* there's an unjust enrichment theory. Nonetheless, courts may be capable of providing some assurances to otherwise-hesitant blockchain entrants.

CONCLUSION

While smart contracts offer great promise for a decentralized and democratized commercial world, there remain hurdles to be vaulted. The technology continues to improve as blockchain-based-crypto-currency exchange rates continue to sky-rocket. While the programmers focus on improving the technology and ecosystems, the

36 U.C.C. § 2-206(1)(a) (Am. Law Inst. & Nat'l Conference of Comm'rs on Unif. State Laws 2014) (emphasis added).

37 Jeffrey I. Snyder, *Does Bitcoin constitute currency under the UCC?*, Lexology (Oct. 16, 2014), https://www.lexology.com/library/detail.aspx?g=db12a442-5a77-4255-bb87-0fe093a62a31.

38 *See generally* RESTATEMENT (THIRD) OF RESTITUTION & UNJUST ENRICHMENT (Am. Law Inst. 2010) (explaining that liability in restitution derives from unjust enrichment); WARD FARNSWORTH, RESTITUTION (2014) (defining restitution as an action to recover a defendant's unjust enrichment).

39 *See generally* U.C.C. § 1-103 (providing that the UCC governs all contracts).

lawyers ought to focus on creating a legal and regulatory environment to enable these technologies to flourish. Future legal areas of interest may be on the applicability of the UCC to blockchain technologies. Yet regulators should move slowly and cautiously. Had regulators hastily attempted to classify Bitcoin and its competitors early on as a currency or security interest, they might have unintentionally cabined the entire blockchain technology in an ill-fitting regulatory framework. In this field, regulation should be reactive, not proactive.