Vanderbilt Journal of Entertainment & Technology Law

Volume 22
Issue 2 *Issue 2 - 2020*

Article 2

2020

The Very Brief History of Decentralized Blockchain Governance

Michael Abramowicz

Recommended Citation
Michael Abramowicz, The Very Brief History of Decentralized Blockchain Governance, 22 *Vanderbilt Journal of Entertainment and Technology Law* 273 (2020)
Available at: https://scholarship.law.vanderbilt.edu/jetlaw/vol22/iss2/2

The Very Brief History of Decentralized Blockchain Governance

Michael Abramowicz[*]

ABSTRACT

A new form of blockchain governance involving the use of formal games that incentivize participants to identify focal resolutions to normative questions is emerging. This symposium contribution provides a brief survey of the literature proposing and critiquing the use of such mechanisms of decentralized decision-making, and it evaluates early laboratory and real-world experiments with this approach.

TABLE OF CONTENTS

[*] Oppenheim Professor of Law, George Washington University. I am grateful to David Abrams and Omri Marian for helpful comments and to participants in workshops at Boston College and George Washington University. I am grateful to Amber Banks, Taylor Caleb, Caroline Hyde, Jin Yoshikawa, and the other editors at the *Vanderbilt Journal of Entertainment & Technology Law* for their excellent assistance in the publication process. All errors are my own.

I. INTRODUCTION

The Merriam-Webster dictionary illustrates the phrase "slower than molasses" with an example sentence about the workings of a legislature.[1] However slow legislatures may be in developing new legislation, the evolution of governance itself is far slower. It is a tribute to the genius of their designers that our democratic institutions still function, more or less, according to the same core procedures as existed when they were created, but it is also a testament to the challenges inherent in changing the rules by which other rules are created. Because the processes of governance lie at the core of any democratic government, any mistakes in developing new governance procedures can have adverse effects on substantive law. What's more, it is difficult to judge whether governance experiments are successful. We cannot run a randomized controlled trial in which half of state legislatures adopt one legislative procedure while the other half adopt another, and even if we could, it would likely be impossible to identify criteria for evaluating which half produced better laws.[2] Corporations can experiment more easily with governance than legislatures, but the incentives to do so are still limited.[3] It will rarely be possible to attribute a corporation's success or failure to a specific governance initiative rather than to a corporation's business model. And if a governance initiative were provably successful, most of the benefits would flow to copycats rather than to the original innovator.[4]

Yet in the past few years, there has been a flurry of experimentation with governance. This experimentation has taken place not in the legislature or in the boardroom but on the blockchain. The experiments are borne of necessity. Disputes about governance have sometimes led to "hard forks"[5] in blockchains and

[1] *See Slower than Molasses*, MERRIAM-WEBSTER, https://www.merriam-webster.com/dictionary/slower%20than%20molasses [https://perma.cc/7ZQV-YD8C] (last visited Oct. 17, 2019) ("People have complained that the legislature is moving/working *slower than molasses*.").

[2] For discussions of legal experimentation, see Michael Abramowicz et al., *Randomizing Law*, 159 U. PA. L. REV. 929, 986 (2011); Michael C. Dorf & Charles F. Sabel, *A Constitution of Democratic Experimentalism*, 98 COLUM. L. REV. 267, 267 (1998).

[3] On the slow pace of corporate governance innovation, see Michael Abramowicz, *Speeding up the Crawl to the Top*, 20 YALE J. ON REG. 139, 154 (2003); Lucian Arye Bebchuk & Assaf Hamdani, *Vigorous Race or Leisurely Walk: Reconsidering the Competition over Corporate Charters*, 112 YALE L.J. 553, 615 (2002); Marcel Kahan & Ehud Kamar, *The Myth of State Competition in Corporate Law*, 55 STAN. L. REV. 679, 738 (2002).

[4] On the implications of the lack of intellectual property protection in governance, see Ian Ayres, *Supply-Side Inefficiencies in Corporate Charter Competition: Lessons from Patents, Yachting and Bluebooks*, 43 U. KAN. L. REV. 541, 545 (1995).

[5] When a "hard fork" occurs in a cryptocurrency, the cryptocurrency becomes two different cryptocurrencies. The two cryptocurrencies share the same early history of transactions,

cryptocurrencies. This occurred most notably in the case of the hard fork of Bitcoin, the leading cryptocurrency by market capitalization, into Bitcoin Cash, after debate about the best way to scale Bitcoin to increase its transaction volume.[6] This hard fork left owners of bitcoins with ownership in two competing cryptocurrencies. On one hand, the availability of hard forks illustrates that there is a governance mechanism native to cryptocurrencies. If a cryptocurrency's value stems entirely from the community's belief that the cryptocurrency has value, then that value can be subdivided into child cryptocurrencies. On the other hand, a cryptocurrency may be more cumbersome to use and less valuable once split into pieces, so mechanisms that avoid hard forks may be preferable.

In principle, a blockchain, whether in the form of a cryptocurrency or not, can use any conventional governance mechanism. Indeed, many private companies have created "permissioned blockchains,"[7] wholly under their control and thus subject to change through ordinary governance procedures. But many blockchains, particularly cryptocurrencies, are implemented through open-source software.[8] The originator of a cryptocurrency project may control the repository for the software code, but in a typical licensing arrangement[9] anyone else may copy the software. And even if the software was not freely copyable, if the protocol the software implements is publicly known, others can implement the protocol in software of their own or borrow the best features of that software for a competing product. Moreover, cryptocurrency projects often reflect an anarcho-libertarian philosophy of decentralization. A blockchain is typically the result of a decentralized process for determining which transactions should be included on a ledger, and some may thus have

but their blockchains will reflect different transactions later in the history. *See, e.g.*, Jake Frankenfield, *Hard Fork (Blockchain)*, INVESTOPEDIA, https://www.investopedia.com/terms/h/hard-fork.asp [https://perma.cc/NW95-VW4K] (last updated Oct. 2, 2019).

[6] *See, e.g.*, Nathaniel Popper, *Some Bitcoin Backers Are Defecting to Create a Rival Currency*, N.Y. TIMES (July 25, 2017), https://www.nytimes.com/2017/07/25/business/dealbook/bitcoin-cash-split.html [https://perma.cc/B2V9-LBWK].

[7] *See, e.g.*, *The Difference Between Permissioned and Permissionless Blockchains*, SEPA FOR CORPORATES (Dec. 6, 2017), https://www.sepaforcorporates.com/thoughts/difference-between-permissioned-permissionless-blockchains/ [https://perma.cc/MBT5-F3TN].

[8] *See, e.g.*, *Bitcoin Core Integration/Staging Tree*, GITHUB, https://github.com/bitcoin/bitcoin [https://perma.cc/BA5E-AYP5] (last visited Oct. 25, 2019) (providing the Bitcoin repository).

[9] *See, e.g.*, *bitcoin/COPYING*, GITHUB, https://github.com/bitcoin/bitcoin/blob/master/COPYING [https://perma.cc/3MXT-NTQX] (last visited Oct. 25, 2019) (containing the content of the MIT license applicable to Bitcoin).

an ideological aversion to a centralized, hierarchical governance scheme for determining how the protocol that generates this process is defined.

Thus, the development of blockchains has led to two sources of demand for decentralized decision-making: first, a perceived need to coordinate developments of particular blockchains without hard forks, and second, the view that a decentralized system should be decentralized not only at the operational level but also at the level of governance. In addition, the entrepreneurial cryptocurrency ecosystem also generates interest in decentralized decision-making. When entrepreneurs witnessed initial coin offerings based on blockchain innovations generate tens of millions of dollars in capital,[10] they naturally sought to identify new potential blockchain innovations along many dimensions, of which governance is just one. Skeptics of cryptocurrencies may observe that cryptocurrencies are so innovative only because they are so devoid of underlying substance. Children playing in the schoolyard can fashion new rules for their games quickly because the stakes are so low. But whether cryptocurrencies were or are in a bubble, the froth has produced a great deal of thought and experimentation with decentralized governance.

By "decentralized governance," I mean a set of rules that allow some collective to produce discernible decisions without appointing individuals or entities to make those decisions. A direct democracy can represent a form of decentralized governance if there is some set of rules for identifying who is entitled to vote and some means of counting the votes to determine the result of the vote. Ownership of cryptocurrency and other blockchain assets is often obscured, so there is no simple way to implement the principle of "one person, one vote."[11] But some cryptocurrencies have experimented with the principle of "one token, one vote," through which those with greater ownership rights are given greater decision-making power.[12] Such voting arrangements are not my

[10] *See, e.g.*, Paul Vigna & Dave Michaels, *Are ICO Tokens Securities? Startup Wants a Judge to Decide*, WALL STREET J. (Jan. 27, 2019, 11:00 AM), https://www.wsj.com/articles/are-ico-tokens-securities-startup-wants-a-judge-to-decide-11548604800 [https://perma.cc/AW4K-4SPL] (including a list of the largest initial coin offerings in 2017).

[11] *See, e.g.*, Michael Abramowicz, *Cryptocurrency-Based Law*, 58 ARIZ. L. REV. 359, 363 (2016) (explaining why this is difficult with cryptocurrencies).

[12] Cryptocurrencies have also experimented with variations. One interesting variation is Dfinity, which creates a reputation network, in which the result of decisions depends on a combination of votes and on formal trust relationships. *See, e.g.*, Dominic Williams, *The DFINITY "Blockchain Nervous System"*, MEDIUM (Jan. 4, 2017), https://medium.com/dfinity/the-dfinity-blockchain-nervous-system-a5dd1783288e [https://perma.cc/C8NP-K6VL].

interest here, in part because they present a problem akin to that of majority shareholder oppression of minority shareholders.[13]

My focus in this Article is on a different approach to decentralized governance, in which not only are there no appointed officials but there are no votes either, at least as voting is conventionally conceived. The approach bases decisions on an algorithm that identifies *focal* resolutions of normative issues. A simple example can give the gist of this type of mechanism, which I describe further below. Suppose that I wish to decide whether to give a sizeable donation to the American Cancer Society or the Save the Wolves Foundation, and I do not want to split the donation between them. I solicit help from students in my class. I choose students at random and ask them one at a time to state which charity I should choose and to explain their choice. I promise to give each student (other than the last) $1 if that student announces the same answer as the *last* student I call on. I will stop calling on students at a random point—for example, if a coin that I flip lands on heads twice in a row. Whatever the last student says determines the charity to which I will donate.

Assuming that each student cares only about the dollar and not about which charity actually receives the money or about some other factor such as personal reputation, then the student should announce the charity that the student anticipates the last student will announce. But because the last student will not know that she is last, she too will be anticipating the reasoning of a later decision maker. If one knew that the last student would choose between the charities based on which was earlier in alphabetical order or based on some other arbitrary criterion, every other student would have an incentive to follow that same arbitrary criterion. But there are an infinite number of arbitrary criteria, so the normative criterion of which charity is actually better according to those participating in the game stands out. Thus, a student intent on winning the dollar will likely evaluate the relative merits of the charities, placing aside idiosyncratic beliefs. The student may then offer an explanation of why this choice is in fact focal to improve the odds that others conclude that the choice is a good one.

This process will always produce a clear result, in much the same way that legislative rules can lead to a conclusive determination of whether a bill has been enacted into law—excepting edge cases, such as when one might argue whether a particular legislator is rightfully a member of the body. And a blockchain is a decentralized system that can be used to record a series of transactions, such as the charity

[13] *See generally* Robert C. Art, *Shareholder Rights and Remedies in Close Corporations: Oppression, Fiduciary Duties, and Reasonable Expectations*, 28 J. CORP. L. 371, 372 (2003).

preference announcements, and it is possible for one to pay out the rewards (or collect the penalties) needed to provide participants with the relevant incentives. Thus, using the blockchain to identify focal resolutions of cryptocurrency-related issues may constitute one form of blockchain governance, and its merits or demerits must ultimately be compared with those of other forms of blockchain governance.

This Article's goal is to offer a history of this approach to decentralized governance. I was the first person to consider the possibility of decentralized governance systems along these lines two decades ago, well before the advent of Bitcoin and blockchain, and so I begin in Part II by summarizing the argument of my original article. In the past few years, the advent of blockchain led me to return to the topic, describing how this form of decentralized governance could be executed on the blockchain. In fact, it turned out to be unnecessary for me to return to the issue, as other commentators simultaneously recognized the possibility of similar types of mechanisms. Meanwhile, there have been experiments on similar mechanisms, both in the laboratory and in the real world, with mixed results. I describe these in Part III. After describing these experiments and projects, I conclude in Part IV by offering some recommendations for future designs and experiments.

II. DECISION-MAKING THROUGH SCHELLING POINTS

This Part provides a brief intellectual history of decentralized blockchain governance based on the identification of "Schelling focal points." Section II.A recounts what a Schelling point is and points out that individuals often informally coordinate on Schelling points but without producing quantifiable answers to normative questions. The formal games described in Section II.B give each player incentives to provide quantitative assessments on matters of opinion equal to the assessments that future players will make, and the process of soliciting such answers can thus result in an answer to the normative question posed. Section II.C describes various approaches that can result in the implementation of such a formal game in a cryptocurrency.

A. Informal Coordination with Schelling Points

The game theorist Thomas Schelling recognized the existence of "coordination games," in which each player's outcome depends on whether that player succeeds in making the same move as another player.[14] To illustrate the idea, he conducted a survey, largely of New York area residents, in which he asked each respondent what that person would do if the respondent needed to meet someone the next day in New York City but could not communicate a time or place. The majority of respondents chose Grand Central Station's information booth at noon.[15] Schelling's point was not that this was a game that the government should encourage individuals to play but rather that individuals in effect played such tacit coordination games in everyday situations, such as when a couple gets lost in a department store.[16]

Coordination around Schelling points occurs not just in the department store. David Friedman has argued that Schelling point coordination is central to social organization more broadly.[17] Friedman points out that Schelling points can serve to help resolve conflicts. In the absence of a Schelling point, there may be an infinite number of resolutions to a bilateral bargaining game, so "each proposal by one player is likely to call forth a competing proposal from another, slanted a little more in his own interest."[18] But if "there is one outcome that is seen as unique," the parties may readily agree to it rather than face continued bargaining, because a statement that a party insists on that resolution rather than one a small distance away becomes credible.[19] Moreover, even without the possibility of enforcement, contracts can create Schelling points. Though an unenforceable contract can always be renegotiated, the original agreement serves as a focal point, so each party may prefer that agreement to the alternative of continued bargaining.[20]

More ambitiously, Schelling points can be seen as the foundation of government itself. Hans Kelsen famously argued that every legal system has one basic norm, the *grundnorm*, from which the legitimacy of all other legal norms and conclusions follow.[21] Acceptance of the basic norm that the government's duly enacted rules are binding can be seen as the result of a Schelling game. Each person accepts the law as

[14] THOMAS C. SCHELLING, THE STRATEGY OF CONFLICT 54–57 (1980).

[15] *Id.* at 55 n.1.

[16] *Id.* at 54.

[17] *See* David Friedman, *A Positive Account of Property Rights*, 11 SOC. PHIL. & POL'Y 1 (1994).

[18] *Id.* at 7.

[19] *Id.*

[20] *See id.* ("In order for a Schelling point to provide a peaceful resolution to a conflict of interest, both parties must conceptualize the alternatives in similar ways—similar enough so that they can agree about which possible outcomes are unique, and thus attractive as potential Schelling points.").

[21] *See generally* HANS KELSEN, GENERAL THEORY OF LAW AND STATE (Anders Wedberg trans., 1945); Joseph Raz, *Kelsen's Theory of the Basic Norm*, 19 AM. J. JURIS. 94 (1974).

binding because each person anticipates that each other person will conclude that it is binding. The exception proves the rule: the grundnorm can change after a revolution.[22] The revolution is successful when it is *viewed* as successful or as having changed the grundnorm. The perception of success is success, because those with power have incentives to wield it in accordance with what they perceive as the new grundnorm.

More generally, Schelling points can explain coordination in contexts in which network externalities exist—that is, in which one participant's decision to participate in some activity (the network) heavily impacts how others make the same decision. A canonical example of network externalities is computer operating systems.[23] A user adopting an operating system often wishes to use the same one that others will use. It turns out, the focal point is not necessarily the operating system with the greatest market share, however, but the one that will have the highest market share in the future.

Cryptocurrencies themselves reflect this logic. What explains the market capitalization dominance of Bitcoin and, to a lesser degree, of Ethereum? It cannot be that they have more features than alternatives, because anyone can fork them at any time. It is because they are focal, in large part because Bitcoin was the first decentralized cryptocurrency and because Ethereum was the first to offer robust smart contracts. Others gain market share to the extent that they become focal—for example, by incorporating innovative features. Meanwhile, within a particular cryptocurrency, a blockchain is authoritative in large part as a result of a Schelling coordination game. Anyone can fork Bitcoin with software that reflects some new principle for determining the valid blockchain,[24] but the principle that Bitcoin uses to identify the valid blockchain (namely, the blockchain reflecting the greatest proof of work) is highly focal, because it was announced in advance as a core principle. Schelling point coordination thus determines the relative value of cryptocurrencies and also the valid blockchain within a particular cryptocurrency.[25]

[22] *See* N.W. Barber & Adrian Vermeule, *The Exceptional Role of Courts in the Constitutional Order*, 92 NOTRE DAME L. REV. 817, 842 (2016) (discussing the grundnorm and how it can change).

[23] *See, e.g.*, Thomas A. Piraino, Jr., *An Antitrust Remedy for Monopoly Leveraging by Electronic Networks*, 93 NW. U. L. REV. 1, 8–12 (1998) (discussing the relevance of network externalities to the Microsoft antitrust investigation).

[24] Indeed, the Bitcoin Cash fork announced new rules that thus led to the recognition of a different blockchain.

[25] *See, e.g.*, JOSHUA A. KROLL ET AL., THE ECONOMICS OF BITCOIN MINING, OR BITCOIN IN THE PRESENCE OF ADVERSARIES 2 (2013), https://www.econinfosec.org/archive/weis2013/papers/KrollDaveyFeltenWEIS2013.pdf [https://perma.cc/9V3A-PNF3] ("Participants must

B. Formal Coordination with Schelling Points

The use of Schelling points described above is informal: one does not choose where to meet in a department store or how much to value a cryptocurrency by processing numeric announcements according to some algorithm to produce a definitive answer. But it is possible to devise a formal game that gives participants incentives to find focal points. The goal of a formal game can be seen as converting numeric statements on a matter of opinion into an objective fact pursuant to some algorithm; the game can be said to work if that objective fact corresponds meaningfully to actual consensus opinion, even if individuals may have incentives to manipulate the game.

Such a game might occur in a single round. John Maynard Keynes famously described a contest in which "competitors have to pick out the six prettiest faces from a hundred photographs, the prize being awarded to the competitor whose choice most nearly corresponds to the average preferences of the competitors as a whole."[26] Keynes's worry that such a contest has no economic foundation is sound, but, depending on the precise rules, it may lead each competitor to try to find a focal point.[27] Thus, Keynes should perhaps receive credit for suggesting the possibility of an algorithm that might give each participant an incentive to suppress an individual opinion in favor of the perceived group consensus, but in fact he neither explained the precise algorithm of the competition he described nor evaluated the dynamics that would result from implementing it. This is because Keynes was skeptical that such a process could produce a meaningful answer. Keynes predated Schelling, and though his example highlights intuitions about focal points, the purpose of Keynes's argument was to express skepticism about markets without sufficiently strong underlying fundamentals. By implication, Keynes would be even more skeptical about an algorithm that relied on focal points alone.

An algorithm for a single-round game is easy to devise. On a binary issue, for example, each participant can be instructed to write down an answer, and the participants who reach the answer preferred by the majority can receive a bonus payment, perhaps at the expense of those who wrote down the minority answer. A formal Schelling game,

maintain consensus (1) on the rules to determine validity of transactions, (2) on which transactions have occurred in the system, and (3) that the currency has value.").

[26] JOHN MAYNARD KEYNES, THE GENERAL THEORY OF EMPLOYMENT, INTEREST, AND MONEY 156 (1936).

[27] This might not be so if the contest is winner takes all, in which case "one may have an incentive to deviate randomly from one's estimate of the consensus value." Michael Abramowicz, *Cyberadjudication*, 86 IOWA L. REV. 533, 545 (2001).

however, also may occur over multiple rounds. I described variations of such an algorithm in my 2001 article *Cyberadjudication*.[28] I assumed that in each round, a single gambler would volunteer to announce a number. The rules of the game ensure that the gambler "will always do best by trying to predict what will happen in the next round" and "will increase her winnings the further her own bet is from the average in the *previous* round."[29] In principle, the game could use real money to ensure that gamblers have strong incentives to predict what will occur in the next round.

I then gave an example of one approach that could satisfy these constraints. In this approach, the game is launched by auctioning a security corresponding to some normative question (e.g., "Plaintiff in Case X should win the lawsuit") to the highest bidder.[30] The purchaser at this initial auction would then be required to value this security according to some formula, such as a specification that $0 corresponds to certainty that the plaintiff should lose and $100 corresponds to certainty that the plaintiff should win. That valuation would entitle anyone else to either purchase the security at that price or sell short an identical security to the holder of the security. Someone who exercises either option is then subject to the same rule, valuing the option and entitling anyone else either to purchase or sell short at this price. At any time in the game, one can translate the most recent valuation into the corresponding resolution of the normative question. When the game ends (and, as in hot potato or musical chairs, no one knows exactly when that will occur), everyone is paid off based on the most recent valuation. That is, the current holder of the security receives the amount of the current valuation, but that valuation also determines how much the prior participant pays or receives, and so on back to the first participant. Anticipating this, if one participates in the game and believes that the final price will be higher, then one's incentive is to buy and announce a higher price; if one believes that the final price will be lower, then one's incentive is to sell short and announce a lower price. The greater the mispricing one observes, the greater the potential for profit; for example, if the current valuation is $3 and one believes one can persuade everyone else that the plaintiff is certain to win (for example, by producing some relevant evidence), then one can earn $97 in profit by announcing a valuation of $100.

[28] *See id.* at 544–45.

[29] *Id.* at 541. I also assumed that any one gambler's funds are small relative to the funds of those who could play the game and that the house places itself at a disadvantage as a way of subsidizing participation in the game. *Id.* at 542–43. Another important assumption is that participants do not know precisely when the game will end. *Id.* at 541 n.13.

[30] *Id.* at 556–70.

In this instantiation of a formal Schelling game, the forced transaction rules are critical. They provide incentives for participants not to value too low or too high relative to the anticipated last valuation. Because the incentives for this last valuation are the same, at least so long as the last valuer does not know that the game is about to end, the game is entirely circular. But this does not mean that it is useless. Rather, participants must value relative to a focal point.

This is not, however, the only way to structure a multiround Schelling game. In my book *Predictocracy*,[31] I described a similar mechanism, which I called a "self-resolving prediction market."[32] A prediction market is a securities market in which the security will be redeemed at a price based on some event in the real world.[33] For example, popular prediction markets are used to forecast the probability that each candidate will be elected to a governmental position. Some prediction markets allow participants to trade with one another, and the most recent trading price can be translated into the market's prediction of the underlying event. Other prediction markets use automated "market maker mechanisms," in which participants trade against the sponsor of the market according to predetermined rules.[34] I defined a self-resolving prediction market as simply a prediction market with an automated market maker whose final value is the last transaction value at some time-to-be-determined, where the precise time is hidden from the players. A market design that rewards participants based on how close they are to the final price gives participants incentives not only to identify the focal point but also to influence it—for example, by introducing new legal or factual arguments.[35]

Placing aside the further question of whether it might be superior in any context to centralized approaches to providing adjudication, could a scheme like this be a viable mechanism for

[31] MICHAEL ABRAMOWICZ, PREDICTOCRACY: MARKET MECHANISMS FOR PUBLIC AND PRIVATE DECISION MAKING (2008).

[32] *Id.* at 290–94.

[33] *See, e.g.*, Kenneth J. Arrow et al., *The Promise of Prediction Markets*, 320 SCIENCE 877, 877 (2008).

[34] *See, e.g.*, Michael Abramowicz, *The Hidden Beauty of the Quadratic Market Scoring Rule: A Uniform Liquidity Market Maker, with Variations*, 1 J. PREDICTION MARKETS 111, 112 (2007).

[35] *See* ABRAMOWICZ, *supra* note 31, at 119–26. Participants can also have incentives to produce relevant arguments if the market concludes based on some realized state of the world (such as who wins an election), so long as the market is periodically resolved based on the current price. *See id.* at 119–26; Michael Abramowicz, *Deliberative Information Markets for Small Groups*, *in* INFORMATION MARKETS: A NEW WAY OF MAKING DECISIONS 112–13 (Robert W. Hahn & Paul C. Tetlock eds., 2006).

conducting adjudication? The most obvious concern is that while participants will have an incentive to look for a focal point, there is no guarantee that the focal point that participants settle on will be the correct resolution of the question associated with the market. A focal point might be affected by moral considerations independent of the legal questions posed. That is, if there is a "moral" focal point and a "legal" focal point, participants might see the ultimate focal point as a weighted average of these two focal points.[36] This is not necessarily a decisive objection, however. Maybe it is desirable for moral considerations to affect decision-making, and in any event, surely in actual adjudications, judges' perceptions of morality—or efficiency or the optimum for any other framework—affect their decisions. The "legal" focal point itself may reflect a weighting of different interpretive approaches, such as originalism and purposivism, representing different focal points.

One potential weakness of the scheme, however, is that numbers become focal for wholly arbitrary reasons. Perhaps a number will seem focal because it is a round number. I argued that this is unlikely because there are many numbers that have some focal attribute—prime numbers, well-known dates, and so forth—and so the question for participants is why a number should be focal in a particular instance of the game. But whether a game would be resolved by arbitrary focal points is ultimately an empirical question. In particular, in a Schelling game, participants and those affected by the decision may have incentives to create new focal numbers—for example, by announcing them loudly or by credibly committing to playing the Schelling game and betting on those numbers themselves. Yet this strategy creates incentives for others to push back to the original focal point. If *A* announces a manipulative number, then *B* can return to the original focal point in the next round. So long as each has only a small percentage of funds available to invest in the game, the question becomes what the broader set of participants will view as more focal.

C. Schelling Points in Cryptocurrency

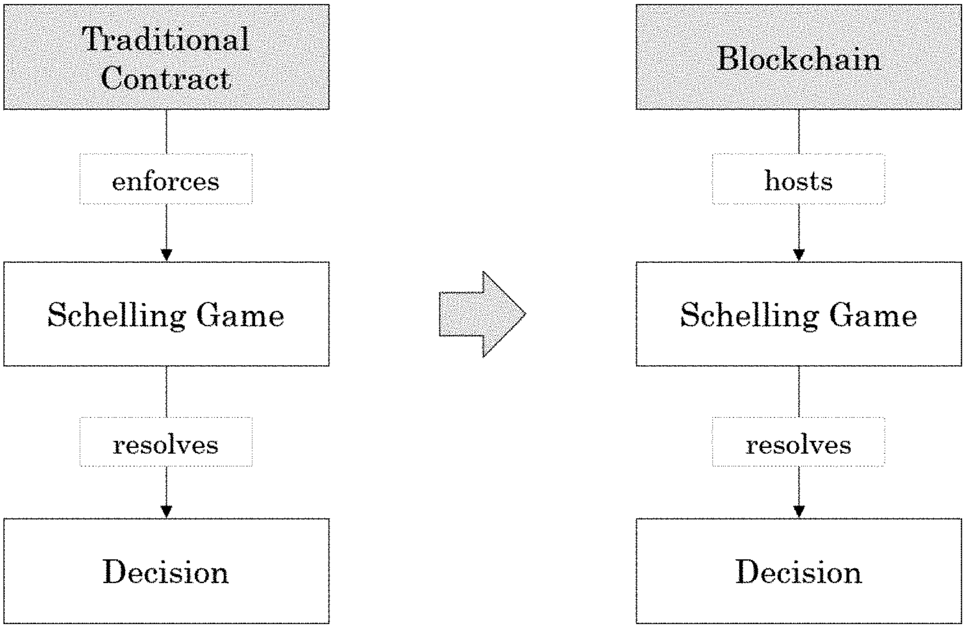
When I originally described the possibility that Schelling games might be used to perform decision-making, I assumed that these games would occur in the context of a conventional mechanism of governance. For example, a corporation might commit to make decisions based on prediction markets,[37] and such a promise could be enforced through

[36] Abramowicz, *supra* note 27, at 549–51.

[37] *See, e.g.*, Michael Abramowicz & M. Todd Henderson, *Prediction Markets for Corporate Governance*, 82 NOTRE DAME L. REV. 1343, 1346 (2007).

ordinary contracts in ordinary courts. A prediction market itself would be centralized, even though participants in the prediction markets could be dispersed. In *Predictocracy*, I mentioned that it might be possible "to have government decisions based entirely on decentralized prediction markets,"[38] but I did not describe how this might work. The advent of cryptocurrencies and the blockchain, however, establishes that at least some decisions—such as determining which ledger of transactions is the authoritative one—can be accomplished in a wholly decentralized way.

Figure 1. Elimination of Centralized Enforcement from Decentralized Decision-Making Mechanism



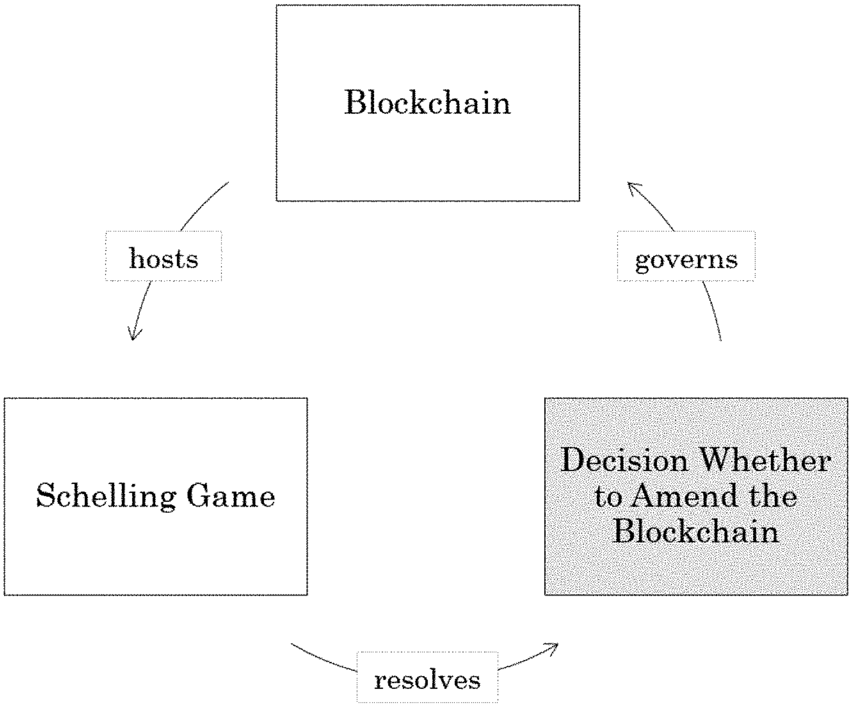
Thus, after the emergence of Bitcoin, I returned to my earlier work on Schelling points, explaining how it might be possible to implement a formal Schelling game on a decentralized cryptocurrency not controlled by any government.[39] Schelling games and cryptocurrencies are each designed to be decentralized, but each has a fundamental point of centralization. The Schelling games as I had previously described would ultimately be enforced by government-created courts enforcing contracts, and cryptocurrencies'

[38] ABRAMOWICZ, *supra* note 31, at 289.

[39] *See* Abramowicz, *supra* note 11, at 363–65.

software code would need to be maintained in a repository by some organization. But if a Schelling game is used to determine how a cryptocurrency supporting smart contracts evolves, decentralization comes full circle, with the cryptocurrency providing a platform for ensuring that Schelling game participants receive (or pay) the appropriate amounts and the Schelling game used to determine whether proposed amendments to the cryptocurrency software protocol should be accepted.

Figure 2.



Decentralization comes full circle—namely, blockchain-enforced Schelling games can decide the direction of the blockchain itself.

Unsurprisingly, given many cryptocurrency advocates' concerns about cryptocurrency governance and sympathy for decentralized decision-making approaches, I was not the only person to hit on the idea of using formal Schelling games to make decisions on a blockchain. In this Section, I describe several other proposals for integrating Schelling point decision-making into the blockchain, and then I address *P + Epsilon* attacks, a type of attack against Schelling point decision-making over which some commentators have raised a concern.

1. Autonocoin, SchellingCoin, and TruthCoin Proposals

In *Cryptocurrency-Based Law*, I offered an approach considerably simpler than the "forced transaction rules" and prediction market described above.[40] Suppose that a cryptocurrency faces a binary decision, such as whether to approve a new checkpoint—a point that all future versions of the blockchain must contain. A cryptocurrency could handle this by defining a transaction that initiates the question and then allowing holders of cryptocurrency to transfer cryptocurrency to designated addresses corresponding to "Yes" and "No." Once a round occurred in which there was a sufficiently low level of activity, the winning position would be declared to be the one with more total support. All of the currency spent would be allocated to the winners. Earlier supporters of the winning position would receive funds before later supporters, so participants would not be incentivized to pile onto the winning position. I explained how this approach would give each participant the incentive to choose a position consistent with what the *next* participant would be more likely than not to do.[41]

I expanded on this mechanism in an article suggesting the possibility of a cryptocurrency based on a concept that I termed "proof-of-belief."[42] I named the cryptocurrency "Autonocoin" to highlight that the cryptocurrency would be a self-governing, autonomous decentralized entity. With Autonocoin, all governance decisions would be made on the cryptocurrency itself. In addition to making binary decisions, the cryptocurrency could resolve questions of how much reward someone who contributed to the cryptocurrency should receive—for example, by contributing software or by marketing the cryptocurrency or adopting it for financial transactions.[43] Moreover, I explained how Autonocoin could be used to make the decision central to all cryptocurrencies: the determination of which is the correct blockchain. The principle would be that the correct blockchain is the one that has the most "proof of belief." A participant can sign transactions indicating that the participant thinks that a blockchain is authoritative, and other participants can sign transactions indicating

[40] *See id.* at 364–65.

[41] *Id.* at 390–95.

[42] *See* Michael Abramowicz, *Autonocoin: A Proof-of-Belief Cryptocurrency*, 1 LEDGER 119, 126 (2016).

[43] *See* Matan Field et al., Backfeed Protocol – The Objective Layer 1 (June 8, 2016) (unpublished manuscript), https://github.com/Backfeed/documents/blob/master/whitepaper_objective_protocol.pdf [https://perma.cc/7QQN-DY2C]. Another blockchain project that has recognized the importance of providing blockchain-based rewards for contributors to the project is Backfeed. *See id.*

the reverse. Autonocoin would embody a convention that these transactions determine which blockchain in fact is authoritative—that is, the one with the greatest degree of committed resources—and those who properly identify the correct blockchain earn a reward for expressing their proof of belief, while those who endorse the wrong blockchain lose their stakes. In general, there would likely be little controversy about the authoritative blockchain, given the existence of clear rules for determining which transactions a blockchain should include, but there might be edge cases that the Autonocoin mechanism could resolve.

At least two other commentators considered the possibility of Schelling point mechanisms at around the same time as me—and indeed published on the internet before the publication of my articles. One of these was Vitalik Buterin, the creator of Ethereum, who considered the possibility in a blog post.[44] Buterin considered using a Schelling game not to resolve a subjective question but an objective one, specifically about the current value of a unit of Ether cryptocurrency in terms of dollars. The ability to obtain this value would be useful because it would enable hedging in smart contracts. Although the value is in some sense objective, if a decentralized mechanism is needed for determining the correct value, then the smart contract requires third parties to report what they believe is the correct value; if there are differences in the value reported, then the analysis of which is correct is subjective. And thus, the determination of an objective value in a decentralized way requires Schelling point decision-making as much as the determination of a subjective value.

Buterin proposes the following mechanism: Users can submit hashes of transactions including their estimate of the ETH-USD price during the even-numbered block and can then cryptographically unveil their estimates during the subsequent block.[45] Once that block is complete, the submitted and revealed values would determine the answer, with "[e]very user who submitted a correctly submitted value between the 25th and 75th percentile gain[ing] a reward of N tokens."[46]

Around the same time, Paul Sztorc proposed a similar mechanism to accomplish the same problem of providing a means of

[44] Vitalik Buterin, *SchellingCoin: A Minimal-Trust Universal Data Feed*, ETHEREUM BLOG (Mar. 28, 2014), https://blog.ethereum.org/2014/03/28/schellingcoin-a-minimal-trust-universal-data-feed/ [https://perma.cc/HQ3G-DT3T].

[45] *Id.* This mechanism allows users to keep their decisions anonymous during the first round. *Id.*

[46] *Id.*

incorporating facts about the real world into a cryptocurrency.[47] He suggested that the currency include, in addition to the store of value, VoteCoins, whose ownership changes as a result of voting activity. VoteCoins are gained by voting with the plurality on disputed decisions and lost by not voting or voting different from the plurality.[48] Sztorc recommends the determination of the plurality decision using an algorithm based on matrix algebra,[49] and he explains why his system gives participants the incentive to find Schelling points.[50]

2. The P + Epsilon Attack

In a later blog post, Buterin describes a potential attack conceived by Andrew Miller against Schelling point coordination schemes.[51] Buterin considers a simple coordination game in which one is rewarded with *P* coins if one votes for the same result as the majority. An attacker, however, credibly commits—perhaps using an Ethereum contract—to pay *X*, which exceeds *P* by a small amount *Epsilon* (*P* + *Epsilon*), to each participant if (1) the participant voted the incorrect answer, and (2) the majority voted the *correct* answer. Thus, the participant will be better off voting the incorrect answer if the majority votes the correct answer (because of the higher payment) and will also be better off voting the incorrect answer if the majority votes the incorrect answer (because of the baseline rules of the coordination game). If everyone reasons along similar lines, each player will vote the *incorrect* answer, thus sabotaging the game. Making the attack more attractive is that the attacker does not need to pay the money, because the money only needs to be paid if the majority votes for the correct answer.

Though Buterin and Miller do not mention it, similar mechanisms exist in the real world, as illustrated in the case of *Unocal v. Mesa Petroleum*.[52] Mesa offered to buy Unocal with a two-tier tender offer. The first tier of the offer was for just over 50 percent of the company. Shareholders successfully tendering would receive this amount, and Mesa would then use its majority interest to effect a

[47] PAUL SZTORC, TRUTHCOIN: PEER-TO-PEER ORACLE SYSTEM AND PREDICTION MARKETPLACE 11–12 (2015), http://www.truthcoin.info/papers/truthcoin-whitepaper.pdf [https://perma.cc/G883-FPPH].

[48] *Id.* at 3.

[49] *Id.* at 13.

[50] *Id.* at 13–14.

[51] Vitalik Buterin, *The P + Epsilon Attack*, ETHEREUM BLOG (Jan. 28, 2015), https://blog.ethereum.org/2015/01/28/p-epsilon-attack/ [https://perma.cc/X2SF-QB42].

[52] Unocal Corp. v. Mesa Petroleum Co., 493 A.2d 946, 949–51 (Del. 1985).

second tier of lower value to buy out the remaining shares. A shareholder's incentive is always to tender in this situation, regardless of the value of the first tier relative to the current value of the first. If the tender offer is successful—that is, at least half of the shares are tendered—then it is better to have as many shares as possible redeemed in the first tier. If the tender offer is not successful, then it does not matter whether one tendered. If every shareholder reasons accordingly, then any two-tiered tender offer will succeed, at least assuming that the courts do not interfere with it.

But attacks can generate counterattacks, and *Unocal* features one: the counter tender offer. Unocal announced that if Mesa's tender was successful, then Unocal would buy back the rest of the stock for an amount greater than offered in the first tier of the tender offer.[53] This reverses the optimal strategy for shareholders by making the alternative to tendering more attractive than tendering. If the tender offer is successful, then it is better not to have tendered, since one will receive more from the company. In the context of Schelling games, we must thus ask both whether a game can be designed to prevent the *P + Epsilon* attack and whether the game can be saved with counterattacks.

Buterin considers approaches that might defeat the *P + Epsilon* attack. He suggests that instead of having a single-round game, the game might occur over multiple rounds, with round *N* determining the payouts in round *N* – 1. "Theoretically," Buterin argues, "this requires an attacker wishing to perform a cost-free attack to corrupt not just one round, but also all future rounds, making the required capital deposit that the attacker must make unbounded." But this approach is not sufficient to prevent a *P + Epsilon* attack. If an attacker commits funds to pay out once, then so long as the payouts never have to be made, the funds will be available for each successive round. An attacker need only have the funds available for the first round, since the beauty of the attack, like Unocal's response to Mesa's tender, is that the money does not actually need to be paid.

Buterin completes his counterattack as follows. Crediting Storcz's TruthCoin, Buterin recognizes that if the amount at stake increases with the degree of contention, then the size of the bribe needed to corrupt successfully might have to be very high, as the attacker would need to be able to establish enough capital to make a payout in some future round in which the total amount at stake is unbounded. Suppose, for example, that if there is sufficient voting on the losing answer, then voting is simply extended to another round with

[53] *Id.* at 949–50.

higher stakes, and so on forever. So long as a counterattacker anticipates that eventually the stakes will be higher than the attacker's payment commitment, the attack will fail in the first round, and the attacker will need to pay out right away. Thus, for the attack to succeed, the attacker must establish that it "is capable of pulling off a 51% attack"[54]—that is, that it has more money than all other participants in the game.

Interestingly, even in a one-round game, a *P + Epsilon* attack could generate a counterattack without ever increasing costs on both sides. Suppose that the correct answer is "Yes" and that in the absence of an attack, a voter would receive 1 for voting with the majority or −1 for voting against the plurality. The attacker promises to pay "No" voters 2 if "Yes" wins. A counterattacker might then credibly commit to paying "Yes" voters 2 if "No" wins. The extra incentives cancel out, and so the ordinary logic of the Schelling game returns but with far more voters participating, since the voters will earn a profit no matter who wins. The attacker might then increase its offer, to protect its original investment, but so might a counterattacker. So long as the counterattacker can match any increased offers by the attacker, the counterattacker should expect to win this battle (and pay out nothing) if the underlying logic of the Schelling game is correct. This can be profitable for the counterattacker if the counterattacker puts money on "Yes," so a counterattacker would have a built-in advantage over an attacker. Of course, a counterattacker might not emerge, but the mere possibility of a counterattack means that the attack may fail and result in a substantial payout.

The counterattacker's advantage depends on the correct Schelling point emerging once the attacker is neutralized. One might argue that those promoting the correct answer (the counterattackers) are no more likely to succeed than those promoting the incorrect answer (the attackers). But there is a strong argument that a counterattack is likely to fail: those defending the correct answer are likely to have a vested interest in the success of the cryptocurrency. If the cryptocurrency is attacked successfully, especially with an attack that ultimately costs the attacker nothing, then the Schelling game mechanism will not be trusted, and if the cryptocurrency itself relies on the Schelling mechanism, then the cryptocurrency itself is likely to fail. At least, this is the likely result if such attacks were successful a significant percentage of the time. Even if the payments from the attacker and counterattacker are *in name* symmetric, they are *in fact* asymmetric if a successful counterattack lowers the value of the

[54] Buterin, *supra* note 51.

cryptocurrency. This provides a built-in incentive for participants to favor the counterattacker over the attacker, and this in turn creates an incentive for counterattackers to emerge. With Schelling games, other counterattacks are possible. Buterin notes that participants might, via credible commitments, agree to vote with probability just over 0.5 on the correct answer and probability just under 0.5 on the incorrect answer, allowing the correct answer to prevail and to still generate part of the bribe.[55] In any event, as Buterin seems to concede, with a multiround game in which the stakes rise over time, no counterattack of this sort is needed. Consider, for example, the forced transaction rules described in Section II.B. With those rules, one will have the incentive to force a sale or purchase of a security if one believes that the ultimate price is more likely to be on one side of the current valuation than the other. Similarly, with the simple rules identified in the previous Section for Autonocoin, one will always have an incentive to place another bet on a binary issue if one expects that one is more likely to prevail than not if challenging the last decision. The attack will fail if more money is placed on the correct answer than the incorrect answer, and the ability of participants to wager more than the amount promised by the attacker is likely to make the attack fail. A caveat is that a genuine 51 percent attack—or perhaps even an attack by a player with a plurality of voting shares—might succeed, but those with large interests will generally be those least likely to want to attack the system.[56]

III. EXPERIMENTATION WITH SCHELLING POINT DECISION-MAKING

Part II provides theoretical arguments suggesting that participants in Schelling point coordination games are likely to seek out the focal points corresponding to the normative questions posed, rather than to latch onto other focal points or to give in to an attacker who encourages others to support the wrong answer. But we must be cautious in this conclusion. Schelling games can have multiple focal points, and the prediction of which focal point will emerge is as much psychology as mathematics. Thus, the fate of Schelling point

[55] *Id.*

[56] Indeed, this may help explain why a similar hypothetical attack is not deployed on Bitcoin. Buterin notes that an attacker could create a Bitcoin fork with a double-spend transaction. *See id.* The attacker could then promise to pay more than the typical mining reward for a miner who successfully mines a block on the fork with the double-spend transaction, if that fork ends up not becoming the official fork. The theory is that everyone would mine on the unofficial fork, and the money would not need to be paid. But such an attack has never been attempted. And it is likely that miners would ignore it because, if it worked, it ultimately would doom Bitcoin itself.

decision-making is an empirical matter. This Part describes some preliminary observations. To date, there have been no large-scale field experiments with Schelling points built into a cryptocurrency, so the ultimate answer is unclear.

A. Laboratory Experimentation

The first piece of evidence comes from a laboratory experiment on self-resolving prediction markets[57] by Kristoffer Ahlstrom-Vij.[58] The experimenter recruited one thousand participants and provided them with education about how prediction markets work.[59] The subjects participated in a game in which they were given incentives to predict the proportion of black balls in an urn with black-and-white balls. Each subject would receive information in the form of balls drawn from the urn; in any single market run, each participant would receive a different random selection of balls. The subjects were randomized either to a treatment group, using self-resolving prediction markets, or to a control group, using prediction markets that resolved based on the actual number of black balls in the urn. The experimenters verified that the members of the treatment group in fact understood that their payouts would depend on later market prices, not on the number of black balls actually in the urn.[60]

Ahlstrom-Vij assessed whether the results of the self-resolving prediction markets were similar to those of the non-self-resolving markets. Indeed, they were, with similar results in both volatility and in accuracy (indeed, slightly better in accuracy though not significantly better).[61] Ahlstrom-Vij interprets this to be evidence in favor of a "face value hypothesis"—namely, that participants in self-resolving prediction markets will in fact pay attention to the questions posed, rather than to any arbitrary focal point.[62] This is, as Ahlstrom-Vij recognizes, a tentative conclusion. Perhaps the experimental subjects, though understanding how self-resolving markets work, did not recognize the arbitrariness of the focal point. Or, perhaps the result would be different if subjects were given an opportunity to communicate with one another. Ahlstrom-Vij notes that a promising direction for future work would be to run a similar experiment but in which some

[57] *See* ABRAMOWICZ, *supra* note 31, at 290–94.

[58] Kristoffer Ahlstrom-Vij, *Self-Resolving Information Markets: A Comparative Study*, 13 J. PREDICTION MARKETS (forthcoming 2019).

[59] For a detailed description of the methodology, see *id.* (manuscript at 5–7).

[60] *Id.* (manuscript at 6).

[61] *Id.* (manuscript at 7, 10).

[62] *Id.* (manuscript at 11).

participants are given an external incentive to manipulate the market and other participants know that such manipulation is possible.[63] Nonetheless, the study provides some reason to think that at least absent efforts to move participants from the focal solution, participants will naturally compete on the assumption that all others are looking for the same focal point.

B. Augur

The next piece of evidence is how the Augur project resolves internal disputes.[64] This real-world project uses Ethereum-based smart contracts to implement and resolve prediction markets. Thus, decentralized participants can bet on the result of events, including political elections and sports competitions. The project includes its own coin, REP, with a current market capitalization of over $100 million.[65] The problem facing Augur is the same as the problem Buterin noted in his SchellingCoin blog post.[66] The smart contracts predicting events must be resolved based on events in the outside world, so the decentralized system must employ some attack-resistant mechanism for incentivizing and processing reports of what in fact happened in the outside world.

The designers of Augur in fact do everything that they can to resist allowing Augur to serve as a general mechanism for Schelling games.[67] The Augur rules require the creator of a market to post a "validity bond," which will be lost if the market turns out to be ambiguous, in which case the market is to be resolved with a special "invalid" answer being correct.[68] Indeed, some participants in the project were motivated by a desire to ensure that the Augur prediction markets were *not* Schelling games, which they regarded as being indeterminate.[69] Yet the designers appear to have recognized that there might be disputes and that no linguistic standard can eliminate all ambiguity. For example, there might be a weak argument that a market

[63] *Id.* (manuscript at 12).

[64] *See* JACK PETERSON ET AL., AUGUR: A DECENTRALIZED ORACLE AND PREDICTION MARKET PLATFORM 5 (2018), https://www.augur.net/whitepaper.pdf [https://perma.cc/KFB4-D7BM].

[65] *Augur (REP) Coin Market Cap Is $148 Million with Less than 40 Active Users*, BITCOIN EXCHANGE GUIDE (Sept. 13, 2018), https://bitcoinexchangeguide.com/augur-rep-coin-market-cap-is-148-million-with-less-than-40-active-users/ [https://perma.cc/5M7R-S3HE].

[66] *See* Buterin, *supra* note 44.

[67] *See* PETERSON ET AL., *supra* note 64, at 1, 3.

[68] *Id.* at 2, 11.

[69] *See* Augur game-theory discussion forum, https://discordapp.com/channels/378030344374583298/384145958902169630 (search for "Schelling").

has a latent ambiguity, and then the question becomes whether it is ambiguous enough to make the "invalid" answer correct.

Thus, there will be at least some circumstances in which Augur *does* need to resolve questions that ultimately involve some subjective component. The mechanism works as follows: While the underlying bet in Augur is of Ethereum cryptocurrency, the separate REP token is used to encourage accurate reporting of event outcomes. In every seven-day period, all REP holders who participate in the reporting process by reporting outcomes receive rewards for doing so. After an initial report is received, there occurs "a 7-day period during which any REP holder has the opportunity to dispute the market's tentative outcome."[70] The dispute requires placing a bond against the tentative outcome; if the sum of such bonds exceeds some threshold, then the tentative outcome is successfully disputed. But then this resolution itself can be successfully disputed by placing even higher bonds. Eventually, when the dispute size exceeds some threshold, Augur goes into a fork state, with a separate fork for each resolution. Each Augur participant must choose a fork, and the fork that receives the greatest number of contributions survives, and all money invested in any other fork is forfeited.[71]

This process bears a substantial resemblance to a multiround Schelling game, in particular to the proof-of-belief system embodied by the Autonocoin proposal. At least in the fork round, each participant has an incentive to place REP currency on the fork that other participants are most likely to choose. At the same time, the Augur design is intended to make such a fork exceedingly rare, requiring a dispute—rare in the first place—to escalate over multiple rounds. To date, no fork has occurred.[72] Nonetheless, all incentives in Augur are ultimately based on the possibility of such a fork. An obviously incorrect choice in a fork round would likely doom confidence in the Augur project. This is unlikely, because an incorrect choice, if recognized as such by others, would cause participants to lose money. With so much at stake, participants have an incentive to choose the correct answer, or the answer they think that most would think better, in the case of a

[70] PETERSON ET AL., *supra* note 64, at 5.

[71] The paper states a lesser penalty. *See id.* at 6. However, a new version of Augur includes this provision to ensure that all participants will have an incentive to participate in the fork. *See* Siamak Masnavi, *An Overview of Main Features of Augur Version 2 and What They Mean*, CRYPTOGLOBE (Apr. 10, 2019), https://www.cryptoglobe.com/latest/2019/04/an-overview-of-the-main-features-of-augur-version-2-and-what-they-mean/ [https://perma.cc/CWC2-WM7W].

[72] At least one software project has adapted the Augur source code, but this did not result in a fork of REP. *See* Paul Fletcher-Hill, *AugurLite Follow-Up*, MEDIUM (May 21, 2019), https://medium.com/veil-blog/augurlite-follow-up-59fefaf240c9 [https://perma.cc/7LJS-JYQ2].

genuinely close question. It certainly could not be manipulated using the REP currency itself, since it would be irrational to choose an option that would pay a theoretical attacker more of this currency if the success of that option would simultaneously make such currency worthless.

A mechanism designed to resolve Schelling points on subjective questions could use the same approach. But forks might turn out to be considerably more common, and thus a lower cost resolution is useful. Nonetheless, any Schelling point mechanism that allows those confident that an outcome is wrong to wager an ever-increasing amount of money on the opposite solution should provide similar incentives. It will be rare for disputes to involve a significant portion of the available cryptocurrency, but the possibility of such disputes serves as a disciplining mechanism for participants.

C. Token-Curated Registries

A final piece of evidence about Schelling games may emerge from token-curated registries, should they attract sufficient interest.[73] A token-curated registry is simply a list of entities that meet some criterion, such as a "top colleges" list or "best tourist attractions in Nashville" list. After initial token distribution, anyone can apply to add an entry to a token-curated registry by depositing a token bond of a minimum size. An existing holder of the token may then challenge the application by putting up a counterbond. Other token holders may then assign their tokens to either a "Yes" or "No" vote, and the side with more total investment earns the tokens of the side with less total investment. This is a cursory description, but the core structure should by now be familiar. The goal is to incentivize each participant to seek the focal point solution.[74]

Token-curated registries are in their infancy, with relatively little at stake. One economist has offered some skepticism about the mechanism, noting that "[t]he truth is a Schelling point but it is rarely

[73] *See* Mike Goldin, *Token-Curated Registries 1.0*, MEDIUM (Sept. 14, 2017), https://medium.com/@ilovebagels/token-curated-registries-1-0-61a232f8dac7 [https://perma.cc/77B9-L9WK]; Mike Goldin, *Token Curated Registries 1.1, 2.0 TCRs, New Theory, and Dev Updates*, MEDIUM (Dec. 4, 2017), https://medium.com/@ilovebagels/token-curated-registries-1-1-2-0-tcrs-new-theory-and-dev-updates-34c9f079f33d [https://perma.cc/W8YG-HWUK] [hereinafter Goldin, *Token Curated Registries 1.1*] ("It is likely that one or more Schelling points will emerge.").

[74] Julian Martinez, *Token Curated Registries: An Experiment in Game Theory, Part 1*, CRYPTODIGEST (Mar. 12, 2018), https://cryptodigestnews.com/token-curated-registries-an-experiment-in-game-theory-part-1-3b46a884a3f3 [https://perma.cc/JG75-SPFD].

the only Schelling point."[75] An early token-curated registry called *Adchain* seeks to identify "real publishers" as a way of distinguishing these from publishers of fake content that seek to defraud internet advertisers.[76] Yet the process resulted in Facebook and the *New York Times* being refused admission as a result of moral concerns among participants. This is not necessarily inconsistent with a search for focal points, but it seems to indicate that participants considered moral issues separate from the goals of the registry creator. At this point, however, the registry is quite small—consisting of a motley group of only about one hundred publishers[77]—and it may be difficult for a project capitalized entirely by its own (potentially worthless) token to generate enough interest to give participants robust incentives. If the group were larger and the list came to be taken seriously, then participants would have an incentive to protect their investment, likely by making choices according to the interests of advertisers rather than according to their own moral lights. Should a token-curated registry be capitalized at least partly with a valuable token (such as Ethereum), better evidence on the viability of Schelling point schemes may be generated.

IV. RECOMMENDATIONS AND CONCLUSION

The preliminary experiments in the last Part have primarily occurred over the past year, and thus evidence of the viability and scalability of Schelling point decision-making is scarce. The goal of this short symposium contribution has been to explain the logic of formal Schelling games and explore the critiques of decision-making systems predicated on them. A full empirical evaluation will have to wait for the day, should it come, when significant venture capital is staked behind some system relying on Schelling point decision-making. Whether this occurs will depend in part on whether resolving disputes in this way rather than through conventional approaches has value—a subject which this short piece does not address.[78]

[75] Alex Tabarrok, *When Can Token Curated Registries Actually Work?*, MEDIUM (Nov. 1, 2018), https://medium.com/wireline/when-can-token-curated-registries-actually-work-%C2%B9-2ad908653aaf [https://perma.cc/YT6Z-K7SS].

[76] *See* Carlo Gutierrez, *adChain Registry: Blockchain to Prevent Fraud in Digital Advertising*, ALTOROS (Aug. 31, 2018), https://www.altoros.com/blog/adchain-registry-blockchain-to-prevent-fraud-in-digital-advertising/ [https://perma.cc/72MR-5YSZ].

[77] *See* Barry Levine, *MetaX Launches a Blockchain-Based Whitelist of Websites*, MARTECH TODAY (May 1, 2018, 9:00 AM), https://martechtoday.com/metax-launches-a-blockchain-based-whitelist-of-web-sites-214885 [https://perma.cc/RG7Z-553U].

[78] For discussion of potential applications of Schelling point games, see Abramowicz, *supra* note 11, at 404–19.

Nonetheless, the literature is sufficiently mature that I can at least offer tentative recommendations about the design of Schelling point decision-making. A variety of mechanisms may give parties incentives to seek out focal point resolutions of normative questions, but any successful mechanism must ensure that each participant makes a bet that will pay off better if it is the same as any bet announced by future participants. In addition, a mechanism must allow participants to place ever-larger challenges to the current resolution, thus providing financial incentives for third parties to study the relevant issue and to contribute to the focal resolution. Typically, the game will proceed in rounds, with participants in any round anticipating some probability that attempting to move the focal point resolution will lead to a challenge in the next round. The process may end with some probability after each round,[79] or continue so long as participants are willing to charge previous assessments with higher stakes.[80] Further experimentation, both in the laboratory and in the real world, may determine whether Schelling point decision-making consistently identifies focal point resolutions and whether there are contexts in which such decision-making may be preferable to more traditional centralized governance.

[79] A cryptocurrency can itself generate random numbers beyond the control of individual participants. *See* PHILIPP SCHINDLER ET AL., HYDRAND: EFFICIENT CONTINUOUS DISTRIBUTED RANDOMNESS 2 (2018), https://eprint.iacr.org/2018/319.pdf [https://perma.cc/YM5F-B8C9].

[80] For discussion of a voting regime in which voting continues when a second round confirms the previous round without great controversy, see Dominic Williams, *Fixes the DAO's First Proposal Can Introduce to Secure $150MM*, MEDIUM (May 24, 2016), https://medium.com/@dominic_w/how-the-daos-first-proposal-should-fix-critical-holes-and-secure-150mm-550186668cab [https://perma.cc/336P-WUJP] ("Fix 3: Require 'double tap' validation").