GW Law Faculty Publications & Other Works

Faculty Scholarship

2019

The Very Brief History of Decentralized Blockchain Governance

Michael B. Abramowicz

George Washington University Law School, abramowicz@law.gwu.edu

Follow this and additional works at: https://scholarship.law.gwu.edu/faculty_publications

Part of the [Law Commons](#)

Recommended Citation

Abramowicz, Michael B., The Very Brief History of Decentralized Blockchain Governance (2019). The Very Brief History of Decentralized Blockchain Governance, Vanderbilt Journal of Entertainment and Technology Law (symposium contribution); GWU Law School Public Law Research Paper No. 2019-14; GWU Legal Studies Research Paper No. 2019-14. Available at SSRN: <https://ssrn.com/abstract=3366613>

This Chapter is brought to you for free and open access by the Faculty Scholarship at Scholarly Commons. It has been accepted for inclusion in GW Law Faculty Publications & Other Works by an authorized administrator of Scholarly Commons. For more information, please contact spagel@law.gwu.edu.

THE GEORGE WASHINGTON
UNIVERSITY LAW SCHOOL

GW Law School Public Law and Legal Theory Paper No. 2019-14

GW Legal Studies Research Paper No. 2019-14

The Very Brief History of Decentralized Blockchain Governance

Michael Abramowicz

The Very Brief History of Decentralized Blockchain Governance, Vanderbilt Journal of Entertainment and Technology Law (symposium contribution)

This paper can be downloaded free of charge from the Social Science Research Network: <https://ssrn.com/abstract=3366613>

The Very Brief History of Decentralized Blockchain Governance

Michael Abramowicz*

An emergent form of blockchain governance involves the use of formal games that give participants incentives to identify focal resolutions to normative questions. This symposium contribution provides a brief survey of the literature proposing and critiquing the use of such mechanisms, and it evaluates early laboratory and real-world experiments with this approach to decentralized decisionmaking.

Contents

I. INTRODUCTION	2
II. IDENTIFYING DECISIONS THROUGH SCHELLING POINTS	6
A. Informal Coordination with Schelling Points	6
B. Formal Coordination with Schelling Points.....	8
C. Schelling Points in Cryptocurrency	11
1. Autonocoin, SchellingCoin, and TruthCoin Proposals.....	12
2. The P+Epsilon Attack	14
III. EXPERIMENTATION WITH SCHELLING POINT DECISIONMAKING	17
A. Laboratory Experimentation	17
B. Augur	18
C. Token-Curated Registries	20

* 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. All errors are my own.

IV. RECOMMENDATIONS AND CONCLUSION21

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 process of 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 for 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 determining which half the states 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.

¹ See <https://www.merriam-webster.com/dictionary/slower%20than%20molasses> (“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 (2011); and Michael C. Dorf & Charles F. Sabel, *A Constitution of Democratic Experimentalism*, 98 COLUM. L. REV. 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 (2003); Lucian Arye Bebchuk & Assaf Hamdani, *Vigorous Race or Leisurely Walk: Reconsidering the Competition over Corporate Charters*, 112 YALE L.J. 553 (2002); and Marcel Kahan & Ehud Kamar, *The Myth of State Competition in Corporate Law*, 55 STAN. L. REV. 679 (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 (1995).

Disputes about governance have sometimes led to “hard forks” in blockchains and cryptocurrencies. This occurred most notably in the case of the hard fork of the leading cryptocurrency by market capitalization, Bitcoin, into Bitcoin Cash, following debate about the best way to scale Bitcoin to increase its transaction volume.⁵ 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,”⁶ wholly under their control and thus subject to change through ordinary governance procedures. But many blockchains, particularly cryptocurrencies, are implemented through open-source software.⁷ The originator of a cryptocurrency project may control the repository for the software code, but in a typical licensing arrangement,⁸ anyone else may copy the software. And even if the software were 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 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 decisionmaking: 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. Further generating interest in decentralized

⁵ See, e.g., Nathaniel Popper, *Some Bitcoin Backers Are Defecting to Create a Rival Currency*, N.Y. TIMES, July 25, 2017, available at <https://www.nytimes.com/2017/07/25/business/dealbook/bitcoin-cash-split.html>.

⁶ See, e.g., *The Difference Between Permissioned and Permissionless Blockchains*, SEPA FOR CORPORATES (Dec. 6, 2017), available at <https://www.sepaforcorporates.com/thoughts/difference-between-permissioned-permissionless-blockchains/>.

⁷ See, e.g., <https://github.com/bitcoin/bitcoin> (providing the Bitcoin repository).

⁸ See, e.g., <https://github.com/bitcoin/bitcoin/blob/master/COPYING> (containing the content of the MIT license applicable to Bitcoin).

decisionmaking in blockchains is the entrepreneurial cryptocurrency ecosystem. When entrepreneurs witnessed Initial Coin Offerings based on blockchain innovations represented purely in code generate tens of millions of dollars in capital,⁹ 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.”¹⁰ But some cryptocurrencies have experimented with the principle of “one token, one vote,” through which those with greater ownership rights are given greater decisionmaking power.¹¹ Such voting arrangements are not my interest here, in part because they present a problem akin to that of majority shareholder oppression of minority shareholders.¹²

My focus in this Article is on a different approach to decentralized governance, in which not only are there no appointed officials, but also there are no votes, 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. Suppose that I plan to give a sizeable donation to either the American Cancer Society or the Save the Wolves Foundation, and I do not want to split the donation between them. I solicit help

⁹ See, e.g., Paul Vigna & Dave Michaels, *Are ICO Tokens Securities? Startup Wants a Judge to Decide*, WALL ST. J., Jan. 27, 2019, available at <https://www.wsj.com/articles/are-ico-tokens-securities-startup-wants-a-judge-to-decide-11548604800> (including a list of the largest initial coin offerings in 2017).

¹⁰ See, e.g., Michael Abramowicz, *Cryptocurrency-Based Law*, 58 ARIZ. L. REV. 359, 363 (2016) (explaining why this is difficult with cryptocurrencies).

¹¹ Cryptocurrencies have also experimented with variations. One interesting variation is Dfinity, which creates a reputation network, in which the result of decisions depend on a combination of votes and on formal trust relationships. See, e.g., Dominic Williams, *The DFINITY “Blockchain Nervous System,”* MEDIUM, Jan. 4, 2017, available at <https://medium.com/dfinity/the-dfinity-blockchain-nervous-system-a5dd1783288e>.

¹² See generally Robert C. Art, *Shareholder Rights and Remedies in Close Corporations: Oppression, Fiduciary Duties, and Reasonable Expectations*, 28 J. CORP. L. 371 (2003).

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 the 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 based 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 decisionmaker. 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 better by the lights of 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, and then offer any explanation designed to make others conclude that the choice is a good one.

This mechanism is not without its problems. Still, it is a decentralized process that will always produce a clear result, in much the same way as legislative rules can lead to a conclusive determination of whether a bill has been enacted into law, placing to the side edge cases, such as when one might argue whether a particular legislator is rightfully a member of the body. A blockchain is a system that can record a series of transactions, such as the charity preference announcements, and it is possible for cryptocurrencies to pay out the rewards (or collect the penalties) needed to provide participants with the relevant incentives. Thus, this is a potential form of cryptocurrency governance, and its merits or demerits must ultimately be compared with those of other forms of blockchain governance.

This Article's project 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 the blockchain, and so I will begin 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. After

describing these experiments and projects, I will conclude by offering some recommendations for future designs and experiments.

II. IDENTIFYING DECISIONS 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 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 end of the process of soliciting such answers can thus, by convention or rule, 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 depended on whether that player succeeds in making the same move as another player.¹³ 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 coordinate on a time or place. The majority of respondents chose Grand Central Station’s information booth at noon.¹⁴ Schelling’s point was not that this was a game that the government should encourage individuals to play, but rather that individuals effectively played such tacit coordination games in everyday situations, such as when a couple gets lost in an department store.¹⁵

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.¹⁶ 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

¹³ THOMAS C. SCHELLING, *THE STRATEGY OF CONFLICT* 54-57 (1980).

¹⁴ *Id.* at 55 n.1.

¹⁵ *Id.* at 54.

¹⁶ See David Friedman, *A Positive Account of Property Rights*, 11 *SOC. PHIL. & POL’Y* 1 (1994).

more in his own interest.”¹⁷ 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.¹⁸ Moreover, even without the possibility of enforcement, contracts can create Schelling points. Though an unenforceable contract can always be renegotiated, the original agreement is focal, and so each party may prefer that agreement to the alternative of continued bargaining.¹⁹

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.²⁰ Acceptance of the basic norm that the government’s duly enacted rules are binding can be seen as the result of a Schelling point game. Each person accepts the law as binding because each person anticipates that each other will conclude that it is binding. The exception proves the rule: The *grundnorm* can change after a revolution.²¹ The revolution is successful when it is *viewed* as successful, 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. A canonical example of network externalities is computer operating systems.²² A user adopting an operating system often wishes to use the same one that others will use. This is not necessarily the one 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

¹⁷ *Id.* at 7.

¹⁸ *Id.*

¹⁹ *Id.* at 3 (beginning explanation of why contracts may be useful in a state of nature, even though they are unenforceable).

²⁰ See generally HANS KELSEN, *THE GENERAL THEORY OF LAW AND THE STATE* (1945); Joseph Raz, *Kelsen’s Theory of the Basic Norm*, 19 AM. J. JURIS. 94 (1974).

²¹ 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).

²² 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).

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,²³ but the principle that Bitcoin uses to identify the valid blockchain (i.e., 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.²⁴

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.”²⁵ Keynes’ 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.²⁶ 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

²³ Indeed, the Bitcoin Cash fork announced new rules that thus led to the recognition of a different blockchain.

²⁴ See, e.g., Joshua A. Kroll et al., *The Economics of Bitcoin Mining, or Bitcoin in the Presence of Adversaries* 2 (2013), available at <https://www.econinfosec.org/archive/weis2013/papers/KrollDaveyFeltenWEIS2013.pdf> (“Participants must 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.”).

²⁵ JOHN MAYNARD KEYNES, *GENERAL THEORY OF EMPLOYMENT, INTEREST, AND MONEY* 156 (Harcourt Brace ed., 1936).

²⁶ This might not be so if the contest is winner-take-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).

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 point game, however, also may occur over multiple rounds. I described variations of such an algorithm, in my 2001 article *Cyberadjudication*.²⁷ I assumed that in each round, a single gambler would 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."²⁸ I then gave an example of one approach that could satisfy these constraints. In this approach, a security corresponding to some normative question (e.g., "Plaintiff in Case X should win the lawsuit") would be auctioned.²⁹ The winner of the auction would then be required to value this security, and 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. When the game ends, the current holder of the security receives the amount of the current valuation, which also determines the official resolution of the normative question, and the short sales are resolved based on this price.

In this instantiation of a formal Schelling point 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 multi-round Schelling point game. In my book *Predictocracy*,³⁰ I described a similar mechanism, which I called

²⁷ See *id.*

²⁸ *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.

²⁹ *Id.* at 556-70.

³⁰ MICHAEL ABRAMOWICZ, *PREDICTOCRACY: MARKET MECHANISMS FOR PUBLIC AND PRIVATE DECISION MAKING* (2008).

a self-resolving prediction market.³¹ 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.³² 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 pre-determined rules.³³ 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 change it, for example by introducing new legal or factual arguments.³⁴

Could a scheme like this be a viable mechanism for conducting adjudication, placing aside the further question of whether it might be superior in any context to centralized approaches to providing adjudication? The most obvious objection to the scheme 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 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.³⁵ This is not necessarily a decisive objection, however. Maybe it is affirmatively good for moral considerations to affect decisionmaking, and in any event, surely in actual adjudications, judges' perceptions of morality (or efficiency or the optimum for any other framework) affect their decisions.

Fatal to the scheme, however, would be numbers that become focal for wholly arbitrary reasons. Perhaps a number will seem focal because it is a round

³¹ *Id.* at 290-94.

³² See, e.g., Kenneth J. Arrow et al., *The Promise of Prediction Markets*, SCIENCE, May 15, 2008, available at <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.320.1811&rep=rep1&type=pdf>.

³³ See, e.g., Michael Abramowicz, *The Hidden Beauty of the Quadratic Market Scoring Rule: A Uniform Liquidity Market Maker, with Variations*, 1 J. PREDICTION MKTS. 111 (2007).

³⁴ 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 ABRAMOWICZ, *supra* note 30, at 119-26; Michael Abramowicz, *Deliberative Information Markets for Small Groups*, in INFORMATION MARKETS: A NEW WAY OF MAKING DECISIONS 101 (Robert W. Hahn & Paul C. Tetlock eds., 2006).

³⁵ Abramowicz, *supra* note 26, at 549-51.

number. I argued that this seems 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 it is ultimately an empirical question. Meanwhile, in a Schelling point game, participants and those affected by the decision may have incentives to create new focal numbers, for example by announcing them loudly or by committing credibly to playing the Schelling game and betting on those numbers themselves. Yet this strategy creates incentives for others to push 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 point games might be used to perform decisionmaking, I assumed that these games would occur in the context of an existing government. For example, a corporation might commit to make decisions based on prediction markets,³⁶ and such a promise could be enforced through 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,”³⁷ 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.

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 point game on a decentralized cryptocurrency not controlled by any government.³⁸ Schelling point games and cryptocurrencies are each designed to be decentralized, but each has a fundamental point of centralization. The Schelling point games as I had previously described would ultimately be enforced by government-created courts enforcing contracts, and cryptocurrencies’ software code must be maintained in a repository by some organization. But if a Schelling point game is used to determine how a cryptocurrency supporting smart contracts evolves, decentralization comes full circle, with the cryptocurrency providing a

³⁶ See, e.g., Michael Abramowicz & M. Todd Henderson, *Prediction Markets for Corporate Governance*, 82 NOTRE DAME L. REV. 1343 (2007).

³⁷ ABRAMOWICZ, *supra* note 30, at 289.

³⁸ See Abramowicz, *supra* note 10.

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.

Unsurprisingly, given concerns about cryptocurrency governance and a sympathy among many cryptocurrency advocates for decentralized decisionmaking approaches, I was not the only person to hit on the idea of using formal Schelling point games to make decisions on a blockchain. The next section describes several proposals for integrating Schelling point decisionmaking into the blockchain, and I then turn to a concern that attacks against Schelling point decisionmaking would make it untenable.

1. Autonocoin, SchellingCoin, and TruthCoin Proposals

In describing a blockchain-based Schelling point coordination game, I offered an approach considerably simpler than the “forced transaction rules” and prediction market that I had described earlier. Suppose that a cryptocurrency faces a binary decision, such as whether to approve a new checkpoint. 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 winner would be declared to be the position 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 there would be no incentive 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.³⁹

I expanded on this mechanism in an article suggesting the possibility of a cryptocurrency based on a concept that I termed “proof-of-belief.”⁴⁰ 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.⁴¹ Moreover, I explained how Autonocoin could be used to

³⁹ *Id.* at 390-95.

⁴⁰ See Michael Abramowicz, *Autonocoin: A Proof-of-Belief Cryptocurrency*, 1 LEDGER 119 (2016).

⁴¹ Another blockchain project that has recognized the importance of providing blockchain-based rewards for contributors to the project is Backfeed. See Matan Field et al., *Backfeed Protocol—The*

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 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.⁴² 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 decisionmaking as much as 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 even-numbered block and can then reveal cryptographically unveil their estimates during the subsequent block.⁴³ Once that block is complete, the submitted and revealed values would determine the answer, with “[e]very user who submitted a correctly

Objective Layer (June 8, 2016), available at https://github.com/Backfeed/documents/blob/master/whitepaper_objective_protocol.pdf.

⁴² Vitalik Buterin, *SchellingCoin: A Minimal-Trust Universal Data Feed*, <https://blog.ethereum.org/2014/03/28/schellingcoin-a-minimal-trust-universal-data-feed/> (Mar. 24, 2014).

⁴³ This mechanism allows users to keep their decisions anonymous during the first round.

submitted value between the 25th and 75th percentile gain[ing] a reward of N tokens.”⁴⁴

Around the same time, Paul Sztorc proposed a similar mechanism to accomplish the same problem of providing a means of incorporating facts about the real world into a cryptocurrency.⁴⁵ 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.⁴⁶ Sztorc recommends the determination of the plurality decision using an algorithm based on matrix algebra,⁴⁷ and he explains why his system gives participants the incentive to find Schelling points.⁴⁸

2. *The P+Epsilon Attack*

In a later blog post, Buterin describes a potential attack on Schelling points coordination schemes conceived by Andrew Miller.⁴⁹ 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*, 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*.⁵⁰ Mesa offered to buy Unocal with a two-tier tender offer. The first tier of the offer was for just over 50% of the company. Shareholders successfully tendering would receive this amount, and Mesa would then use its majority interest to effect a second tier of

⁴⁴ Buterin, *supra* note 42.

⁴⁵ Paul Sztorc, *Truthcoin: Peer-to-Peer Oracle System and Prediction Marketplace* (Dec. 14, 2015), available at <http://www.truthcoin.info/papers/truthcoin-whitepaper.pdf>.

⁴⁶ *Id.* at 3.

⁴⁷ *Id.* at 13.

⁴⁸ *Id.* at 13-14.

⁴⁹ Vitalik Buterin, *The P + epsilon Attack*, <https://blog.ethereum.org/2015/01/28/p-epsilon-attack/>.

⁵⁰ 493 A.2d 946 (Del. 1985).

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 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 Mesa would buy back the rest of the stock for an amount greater than offered in the first tier of the tender offer.⁵¹ 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 $P + \textit{Epsilon}$ attack and whether the game can be saved with counterattacks.

Buterin considers approaches that might defeat the 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 that response is not sufficient. So long as 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 to have the attack available on each 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, however, salvages his counterattack. 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 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

⁵¹ *Id.* at 949-50.

succeed, the attacker must establish that it “is capable of pulling off a 51% attack,”⁵² i.e. that it has more money than all other participants in the game.

Interestingly, even in a one-round game, a $P + \textit{Epsilon}$ attack could generate a counterattack with ever increasing resources 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 nominally symmetric, they are in fact asymmetric, if a successful counterattack lowers the value of the 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 still to generate part of the bribe.⁵³ In any event, as Buterin seems to concede, with a multiple-round game in

⁵² Buterin, *supra* note 49.

⁵³ *Id.*

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% 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.⁵⁴

III. EXPERIMENTATION WITH SCHELLING POINT DECISIONMAKING

Part II provided 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 into an attacker who promises a bonus to those who support the wrong answer. But we must be cautious in this conclusion. Schelling point games can have multiple Nash equilibria, and the prediction of which equilibrium will emerge is as much psychology as mathematics. Thus, the fate of Schelling point decisionmaking is an empirical matter. This Part describes some tentative evidence. To date, there has been no large-scale in the field experimentation with Schelling points built into a cryptocurrency, so the ultimate answer is unclear.

A. Laboratory Experimentation

A first line of evidence comes from a laboratory experiment on self-resolving prediction markets markets⁵⁵ by Kristoffer Ahlstrom-Vij.⁵⁶ The

⁵⁴ 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.* (section describing “Further Consequences”). 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.

⁵⁵ *See supra* text accompanying note 31.

⁵⁶ Kristoffer Ahlstrom-Vij, *Self-Resolving Information Markets: A Comparative Study* (2018)

experimenter recruited 1,000 participants and provided them with education about how prediction markets work.⁵⁷ 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 an 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.⁵⁸

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).⁵⁹ 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.⁶⁰ 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 participants are given an external incentive to manipulate the market and other participants know that such manipulation is possible.⁶¹ 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

A real-world experiment lies in the Augur project.⁶² This project uses Ethereum-based smart contracts to implement and resolve prediction markets.

(unpublished manuscript, on file with author).

⁵⁷ For a detailed description of the methodology, see *id.* at 6-8.

⁵⁸ *Id.* at 12.

⁵⁹ *Id.* at 8-12.

⁶⁰ *Id.* at 13.

⁶¹ *Id.*

⁶² See <https://www.augur.net/> (last visited Feb. 13, 2019).

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.⁶³ The problem facing Augur is the same as the problem Buterin noted in his SchellingCoin blog post.⁶⁴ 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 point games.⁶⁵ 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,⁶⁶ in which case the market is to be resolved with a special “invalid” answer being correct. Indeed, some participants in the project were motivated by a desire to ensure that the Augur prediction markets were *not* Schelling point games, which they regarded as being indeterminate.⁶⁷ 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 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.”⁶⁸ 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

⁶³ <https://bitcoinexchangeguide.com/augur-rep-coin-market-cap-is-148-million-with-less-than-40-active-users/>

⁶⁴

⁶⁵ Jack Peterson et al., *Augur: A Decentralized Oracle and Prediction Market Platform* (July 12, 2018), available at <https://www.augur.net/whitepaper.pdf>.

⁶⁶ *Id.* at 1.

⁶⁷ See Augur game-theory discussion forum, <https://discordapp.com/channels/378030344374583298/384145958902169630> (search for “Schelling”).

⁶⁸ Peterson et al., *supra* note 65, at 5.

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.⁶⁹

This process bears a substantial resemblance to a multi-round Schelling point 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. 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. Yet this is unlikely, for the reasons explored above. With so much at stake, participants would have incentives to choose the correct answer (or the answer they think that most would think better, in the case of a genuinely close question). It certainly could not be manipulated using the REP currency itself, since no one would want to choose an option that would pay them more of this currency if the success of that option would simultaneously make such currency worthless.⁷⁰

A mechanism designed to resolve Schelling points on subjective questions could use the same mechanism. 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 source of evidence about Schelling point games may emerge from token-curated registries, should they attract sufficient interest.⁷¹ A token-curated

⁶⁹ The paper states a lesser penalty, *see id.* at 6, but a new version of Augur includes this provision to ensure that all participants will have an incentive to participate in the fork.

⁷⁰ On the possibility that one blockchain could be used to manipulate another, see Matteo Leibowitz, *The Power of Prediction: An Experiment in Vote Buying*, <https://www.theblockcrypto.com/2019/01/31/the-power-of-prediction-an-experiment-in-vote-buying/>.

⁷¹ See Mike Goldin, *Token-Curated Registries 1.0* (Sept. 14, 2017), available at <https://medium.com/@ilovebagels/token-curated-registries-1-0-61a232f8dac7>; Mike Goldin, *Token-Curated Registries 1.1, 2.0 TCRs, new theory, and dev updates* (Dec. 4, 2017), available at <https://medium.com/@ilovebagels/token-curated-registries-1-1-2-0-tcrs-new-theory-and-dev->

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 counter-bond. 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 give each participant an incentive to seek the focal-point solution.⁷²

Token-curated registries are in their infancy, with relatively at stake. Alex Tabarrok has offered some skepticism about the mechanism, noting that “[t]he truth is a Schelling point but it is rarely the only Schelling point.”⁷³ 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.⁷⁴ 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 100 publishers), 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

[updates-34c9f079f33d](#).

⁷² Goldin, *Token-Curated Registries 1.1*, *supra* note x (“It is likely that one or more Schelling points will emerge.”)

⁷³ Alex Tabarrok, *When Can Token Curated Registries Actually Work?*, (Nov. 1, 2018), <https://medium.com/wireline/when-can-token-curated-registries-actually-work-%C2%B9-2ad908653aaf>.

⁷⁴ See Carlo Gutierrez, *adChain Registry: Blockchain to Prevent Fraud in Digital Advertising* (Aug. 31, 2018), available at <https://www.altoros.com/blog/adchain-registry-blockchain-to-prevent-fraud-in-digital-advertising/>.

decisionmaking is scarce. The goal of this short symposium contribution has been to explain the logic of formal Schelling point games and explore the critiques of decisionmaking 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 decisionmaking. Whether this occurs will depend in part on whether resolving disputes in this way rather than through conventional approaches has value, a subject to which this short piece does not contribute.⁷⁵

Nonetheless, the literature at least can allow for development of recommendations about the design of Schelling point decisionmaking. A variety of mechanisms may give parties incentives to seek out focal point resolutions of normative questions, but any successful mechanism, at its core, 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,⁷⁶ or continue so long as participants are willing to charge previous assessments with higher stakes.⁷⁷

⁷⁵ For discussion of potential applications of Schelling-point games, see Abramowicz, *supra* note 10, at 404-19.

⁷⁶ A cryptocurrency can itself generate random numbers beyond the control of individual participants. See Philipp Schindler et al., *HydRand: Practical Continuous Distributed Randomness* (2018), available at <https://eprint.iacr.org/2018/319.pdf>.

⁷⁷ 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* (May 24, 2016) ("Fix 3: Require "double tap" validation"), available at https://medium.com/@dominic_w/how-the-daos-first-proposal-should-fix-critical-holes-and-secure-150mm-550186668cab.