From ODR to ₿DR

A Template for Online Dispute Resolution in the Bitcoin Economy

W. Aaron Daniel

I.   INTRODUCTION: SOLVING FOR ENFORCEABILITY IN DISPUTE RESOLUTION.

Conflict is part of human nature. Civilizations are defined by how they resolve disputes. In the absence of institutionalized systems of dispute resolution, individuals are left to fend for themselves, resorting to violence to resolve interpersonal conflicts.

Although the civil justice systems of modern western societies abstract it away, violence nonetheless underpins those systems, as well. Civil justice systems resolve disputes by producing judgments. And, as Richard Susskind puts it in *Online Courts and the Future of Justice*, those judgments "differ from all other decisions in society — they are binding, enforceable, and backed ultimately by the coercive powers of the state."[1] In other words, judgments are binding and enforceable **because** they are backed by the state's monopoly on violence.

For civil justice systems to function, judgments must be enforceable. As a practical matter, "unless the judgment can be enforced, the dispute will continue," rendering the resolution process futile.[2] And unenforceability creates a negative

---

[1] Richard Susskind, ONLINE COURTS AND THE FUTURE OF JUSTICE 19 (2019).

[2] Nancy Rogers, Robert Bordone, Frank Sander, DESIGNING SYSTEMS AND PROCESSES FOR MANAGING DISPUTES 108 (2019) (hereinafter "Designing Systems").

feedback loop: without enforceability, "liability is merely symbolic, a status that risks undermining the legitimacy of the legal system;"[3] and without legitimacy, disputants are less likely to abide by court-rendered judgments.[4]

Alternative Dispute Resolution (ADR) systems, such as arbitration and mediation, share the same inherent vulnerability. Although private "[a]rbitration took its rise in the very infancy of Society" as "[c]ommunities created arbitration systems designed to quickly and efficiently determine disputes in accordance with local norms and accepted equitable principles," such extra-legal systems have nonetheless always existed in the shadow of the courts.[5] Arbitral awards are not self-executing. If a disputant refuses to comply, the other party must petition the courts to confirm and enforce the award, once again calling upon the coercive power of the state.[6]

Existing Online Dispute Resolution (ODR) systems are no different. Early advocates for resolving disputes through software and the internet recognized that challenges remained "to the enforcement of resolutions and decisions reached through

---

[3] Lea Shepard, *Creditors' Contempt*, 2011 B.Y.U.L. Rev. 1509, 1521.

[4] "At the heart of dispute resolution lies the concept of legitimacy, which is ultimately premised on trust — trust in the system, trust in the process, and trust in its fairness — and therefore a willingness to abide by outcomes." Orna Rabinovich-Einy & Ethan Katsch, *Blockchain and the Inevitability of Disputes: The Role for Online Dispute Resolution*, 2019 J. Disp. Resol. 47, 72 (2019).

[5] Amy J. Schmitz & Colin Rule, *Online Dispute Resolution for Smart Contracts*, 2019 J. Disp. Resol. 103, 115 (2019).

[6] *See* Riikka Koulu, LAW, TECHNOLOGY AND DISPUTE RESOLUTION: PRIVATISATION OF COERCION 71 (2019) ("ADR decisions struggle with accessing enforcement in those cases where the decision is not followed on a voluntary basis. Traditionally, ADR decisions had to resort to the state's enforcement mechanism, which meant that they were subordinated to ex ante control of due process before being enforced."); DESIGNING SYSTEMS at 408–09 (explaining enforcement mechanisms for arbitral awards).

ODR."[7] Unenforceability creates a "lack of incentives for participation by disputants."[8] This is because enforcement affirms the effectiveness of "a settlement process and reenforc[es] parties' incentives" to participate; but if a party can easily repudiate "its obligations under the settlement … this will eventually create disincentives to" participation.[9] And so, even ODR's effectiveness ultimately begins and ends at the courthouse steps.

Simply put, enforceability is essential to dispute resolution. And enforceability is derived from the coercive power of the state and its monopoly on violence.

In other words, all effective dispute resolution systems depend on a functioning state-run legal system. But this is, to put it mildly, problematic for the more than 4 billion people living outside the protection of the law without access to justice[10] or the 54% of the population that lives under some form of authoritarian rule[11]. Civil justice systems are failing to furnish the rule of law to most of humanity. State-run courts do not provide a sturdy base layer upon which to build accessible and fair dispute resolution systems.

---

[7] Orna Rabinovich-Einy & Ethan Katsh, *Technology and the Future of Dispute Systems Design*, 17 Harv. Negotiation L. Rev. 151, 162–63 (2012).

[8] *Id*.

[9] Ellen E. Deason, *Enforcing Mediated Settlement Agreements: Contract Law Collides with Confidentiality*, 35 U.C. Davis L. Rev. 33, 37–38 (2001).

[10] *See* www.oecd.org/gov/delivering-access-to-justice-for-all.pdf, last visited Jan. 31, 2023. Another study of 179 states found that men do not have access to justice in 123 countries, and women do not have access to justice in 127. *See* https://ourworldindata.org/grapher/access-to-justice-women-row; https://ourworldindata.org/grapher/access-to-justice-men-row, last visited Jan. 31, 2023.

[11] *See* EIU DEMOCRACY INDEX, available at https://www.eiu.com/n/campaigns/democracy-index-2021/, last visited Jan. 31, 2023. By another measure, over 70% of the global population lives under a form of autocracy. https://ourworldindata.org/grapher/people-living-in-democracies-autocracies?stackMode=relative&country=~OWID_WRL, last visited Jan. 31, 2023.

Moreover, reliance on state coercion and violence is morally questionable. State-backed coercion conflicts with the right to individual self-determination and liberty.[12] Individuals did not, in fact, choose to sign a "Social Contract" assigning the state its monopoly on violence.

The standard response is that reliance on state coercion for enforcement is a necessary evil. The governed have tacitly consented to this state of affairs by living in society, goes the Lockian refrain. The alternative is anarchy.

But what if there was an alternative to existing dispute resolution systems that replaced enforcement by coercion with **voluntary consent**.

This paper proposes a voluntary solution to enforceability of judgments that is entirely separate from the state. This separation is achieved through the Bitcoin network, the most decentralized communication protocol for the transfer of value in human history. By anchoring a dispute resolution scripting logic layer into the Bitcoin network's immutable and global base layer, self-executing monetary judgments can be rendered that do not rely on the courts for enforcement. Disputants will be able to expressly contract in advance for such Bitcoin Dispute Resolution (₿DR) services,

---

[12] "When we speak of people as (generally) free or unfree, we can mean either that they are generally capable of acting or omitting to act as they please (de facto freedom) or that they are independent, sovereign beings, persons in actual and/or rightful control of their own choices." Joel Feinberg, *Autonomy, Sovereignty, and Privacy: Moral Ideals in the Constitution?*, 58 Notre Dame L. Rev. 445, 447 n.4 (1983). *See also* Art. 3, Universal Declaration of Human Rights, available at https://www.un.org/en/about-us/universal-declaration-of-human-rights ("Everyone has the right to life, liberty and security of person."); The Declaration of Independence ("[A]ll men are created equal, that they are endowed by their Creator with certain unalienable Rights, that among these are Life, Liberty and the pursuit of Happiness.").

either bilaterally or as part of a community's actual social contract governing rights and responsibilities of residents.

At a minimum, ฿DR can solve the enforcement problem that exists in most private ADR and ODR systems. And by relying on the open, borderless, interoperable, censorship-resistant properties of the Bitcoin network, ฿DR also has the potential to extend the rule of law to communities that do not have access to fair, reliable, and consistent state-run courts.

Furthermore, state-run courts will be ill-equipped to render enforceable judgments in the Bitcoin-based economies and communities of the future. An alternate, Bitcoin-native dispute resolution system will be required as Bitcoin adoption grows.

The remainder of this paper will proceed as follows. Part II will examine Bitcoin and describe why current court-based enforcement will not operate effectively in the Bitcoin societies of tomorrow.

Next, examples of existing cryptocurrency and traditional dispute resolution systems will be examined and critiqued in Part III. Proto-designs for ฿DR exist, however, they are not sufficiently scalable to anything more than bilateral contractual relationships and suffer from additional deficiencies. In the traditional ODR context, several examples of private dispute resolution systems that do not rely on courts to enforce decisions provide important lessons and demonstrate that private enforcement can occur at the community scale.

Incorporating lessons from these examples, Part IV will provide a schematic for a fully scalable ฿DR system based on the nascent open-source protocol FediMint[13], a scaling layer anchored into the Bitcoin network that, among many other things, introduces smart contracting capabilities.[14]

The paper will conclude in Section V by addressing drawbacks and trade-offs to the proposed ฿DR design.

II.   BITCOIN DISINTERMEDIATES CUSTODIANS AND COUNTERPARTIES, MAKING COURT ENFORCEMENT OF JUDGMENTS DIFFICULT FOR BITCOIN-BASED ECONOMIES.

A full explanation of exactly how Bitcoin works is beyond the scope of this paper.[15] Suffice it to say, Bitcoin has created a paradigmatic shift in property rights.

By storing wealth in Bitcoin, one need not rely on counterparties or the courts to protect one's property. This is because bitcoin[16] is a bearer asset that allows for self-custody with **no counterparty risk**.

---

[13] *See* www.fedimint.org.

[14] *See* Daniel Stabile, Kimberly A. Prior, Andrew M. Hinkes, DIGITAL ASSETS AND BLOCKCHAIN TECHNOLOGY: US LAW AND REGULATION 26 (2020) (Smart contracts "were originally described by Nick Szabo in 1997 as 'contractual clauses (such as collateral, bonding, delineations of property rights, etc.) which can be embedded in the hardware and software we deal with, in such a way as to make breach of contract expensive (if desired, sometimes prohibitively so)) for the breacher.' Smart contracts became a popular model for innovation with the adoption of blockchain systems that natively facilitate transfers of digital assets without reliance on centralized authorities. Smart contracts can automatically transmit value and data based upon the operation of 'if then' logic without the need for the software to interface with external systems or require external inputs. Likewise, smart contracts can be designed to execute the terms of a transaction upon the occurrence of some external event.").

[15] For those wishing to jump down the rabbit hole, see Yan Pritzker, INVENTING BITCOIN; Andreas Antonopolous, MASTERING BITCOIN, and Antonopolous ,THE INTERNET OF MONEY.

[16] Throughout this paper, "bitcoin" lowercase will refer to "the unit of currency," and capitalized "Bitcoin" will refer to the system or network. *See* Andreas M. Antonopoulos, Mastering Bitcoin (2018), available at

Unlike a physical bearer asset like gold, large amounts of which are very costly to defend (thereby introducing counterparty risk for security), bitcoin is trivially inexpensive to secure at the individual level. All that's required is a wallet (hardware or software) that stores private cryptographic keys used to transact on the blockchain.[17]

Moreover, transactions on the Bitcoin network are entirely decentralized and do not rely on trusted third-party intermediaries. Users send value through the protocol directly, peer-to-peer. Bitcoin achieves this with a distributed ledger that is updated and verified by thousands of computers (called nodes) throughout the world running Bitcoin's open-source software. A user broadcasts a transaction to the network by signing it with their wallet's private keys. Anyone can then compete to add this new transaction to the distributed ledger through the process of mining. But transactions that don't comply with Bitcoin's rules are rejected by the nodes that verify each block, thus preventing double-spends and maintaining the integrity of the ledger.

Because Bitcoin is both (i) a digital bearer asset that allows self-custody and (ii) a decentralized, permissionless, peer-to-peer network, it is the first truly seizure and censorship resistant store of value.

---

https://github.com/bitcoinbook/bitcoinbook/blob/develop/ch01.asciidoc ("the unit of currency is called "bitcoin" with a small b, and the system is called "Bitcoin", with a capital B.").

[17] The cryptography securing Bitcoin access is unfathomably difficult to breach. *See* Andreas Antonopolous, *Can Someone Guess My Crypto Private Key*, YouTube (Nov. 24, 2020).

Now imagine an economy that is based entirely on a Bitcoin standard, where everyone self-custodies their own wealth and transacts peer-to-peer. In this "hyperbitcoinized" economy, financial intermediaries would be obsolete. And without intermediaries, courts lose the traditional pressure point for enforcing money judgments.

Indeed, third-party financial intermediaries have become the linchpin of the civil justice system. Intermediaries facilitate the transfer of assets from judgment-debtors to judgment-creditors in satisfaction of compensatory damages awards. To collect assets from recalcitrant judgment-debtors, judgment-creditors can obtain from the courts a writ of garnishment. The judgment-creditor then serves this writ on a third-party in possession of the judgment-debtor's assets (usually a bank, custodian, or other financial services provider). These third-party intermediaries have no incentive to fight a writ of garnishment and will usually just wait to see if anyone objects, and then hand over the assets in their possession after all objections are resolved. After all, the writ of garnishment is enforcing a judgment entered after a full and fair opportunity for the third-party's customer to exculpate themselves. These highly regulated entities (also subject to the coercive power of the state) must respect the authority of the courts to adjudicate disputes.

Thus, because Bitcoin obsoletes these financial intermediaries, which have become essential to enforcement, Bitcoin is also in the process of disrupting the civil justice system. The court system is ill-equipped to enforce judgments against

individuals who maintain their wealth in Bitcoin, without resorting to increasingly aggressive coercion and substantially reduced due process.[18]

For this reason, alternative, Bitcoin-native methods of enforcement are needed to resolve disputes in Bitcoin-based economies and societies.

III.   LESSONS FROM EXISTING ODR SYSTEMS.

A.   Cryptocurrency-Based Dispute Resolution Systems.

1.   Bisq Network: Making Bitcoin Confiscatable.

The Bisq Network facilitates decentralized, peer-to-peer bitcoin exchanges for fiat and other cryptocurrencies through client software and a communication protocol.[19] Bisq is operated through what is known as a Decentralized Autonomous Organization, or DAO.[20] Instead of working for a centralized company, contributors collaborate (writing open-source code for the client software or performing operational roles) through the DAO, which rewards work with the BSQ token – a colored, or marked, bitcoin that can be exchanged for actual bitcoin (or other cryptocurrency assets) through

---

[18] Reduced due process could take the form of pre-judgment Mareva injunctions, which the U.S. Supreme Court has currently determined impermissibly deprives defendants of their property without due process. *See Grupo Mexicano de Desarrollo S.A. v. All. Bond Fund, Inc.*, 527 U.S. 308, 329 (1999). Or, jurisdictions could remove limitations on holding judgment-debtors in prison for failure to pay debts. Currently only about a third of U.S. states allow contempt against judgment debtors for refusal to turn over assets. *See Shepard, supra* at 1543.

[19] https://bisq.wiki/Main_Page

[20] https://bisq.network/dao/

the Bisq network.[21] BSQ is also a governance token that directs the DAO's collective

action through voting rights.

In order to preserve its decentralized and peer-to-peer nature, Bisq has designed

a system of resolving disputes between traders that involves minimal intervention from

DAO members and, importantly, is partially self-executing. At no point during a trade

are trader funds custodied by the Bisq DAO or its members. Instead, as part of every

trade, buyers and sellers lock up a percentage of the trade amount as a security

deposit, along with the bitcoin trade amount, in a time-locked, 2-of-2 multi-signature

escrow Bitcoin address, to which each of the traders has one key.[22] Both traders must

sign with their keys to release the funds as directed by the trade. If a dispute arises and

the traders do not sign the transaction before the time-lock expires, eventually the funds

are sent to a donation address controlled by DAO members (more on this shortly). Bisq

publishes a table of penalties for trading infractions, which are assessed out of the

escrow amounts and awarded to the wronged party through the dispute resolution

process, as follows.[23]

Bisq's dispute resolution system has three levels: trader chat, mediation, and

arbitration.[24] The first level, trader chat, is more appropriately considered dispute

avoidance than resolution.[25] The Bisq software includes an end-to-end encrypted

---

[21] https://bisq.wiki/Introduction_to_the_DAO; https://bisq.network/blog/bisq-dao-for-bitcoin-maximalists/.

[22] https://bisq.wiki/Introduction; https://bisq.wiki/Security_deposit

[23] https://bisq.wiki/Table_of_penalties; https://bisq.wiki/Trading_rules

[24] https://bisq.wiki/Dispute_resolution

[25] "the heart of both dispute resolution and dispute prevention lies in communication between parties as part of a decision-making process." Orna Rabinovich-Einy & Ethan Katsh, "Lessons from Online Dispute

trader chat function to facilitate early discussion of issues that may escalate into conflict.[26] Bisq's documentation encourages communication between traders and sets rules and best practices for using the chat function to avoid fraud and facilitate respectful and productive discussions towards completing trades.[27] Trader chat leverages the benefits of "asynchronous, text-based online exchanges," which allow "participants to be reflective" and "consider their comments before posting," further enabling a respectful line of communication conducive to resolving misunderstandings and completing trades.[28]

The trader chat function, along with Bisq's guidelines for effective communication, is an example of how dispute resolution or avoidance mechanisms can be integrated with "the site's (or community's) principal mission," which helps "prevent problems thereby enhancing trust in the site and improving its content and performance."[29]

Resolution for Dispute Systems Design," ONLINE DISPUTE RESOLUTION: THEORY AND PRACTICE, 59 (Mohamed Abdel Wahab, Daniel Rainey & Ethan Katsh, eds.) (2011). *See also* Susskind at 67.

[26] Id. *See also* Colin Rule & Chittu Nagarajan, *Crowdsourcing Dispute Reoslution Over Mobile Devices*, 5 (2011), available at http://colinrule.com/writing/mobile.pdf, last accessed Jan. 31, 2023 ("In face-to-face dispute resolution, third parties are often asked to engage a dispute long after it has escalated and become intractable. Many mediators must then labor mightily with the parties to de-escalate the matter and to undo much of the mistrust that has grown during the escalation. ODR was able to leverage the intimacy of technology to access disputes at a much earlier stage. In the eBay and PayPal context, the ODR systems we designed were available to buyers at the first inkling that a problem might exist. That enabled the ODR process to help the buyer diagnose the problem they were experiencing, and begin resolving it before escalation with the seller could take place.").

[27] https://bisq.wiki/Dispute_resolution

[28] Rule & Nagarajan at 4.

[29] Rabinovich-Einy & Katsh (2011) at 54.

The second level of Bisq's dispute resolution system is mediation.[30] Either trader can request mediation at any time once a trade has been initiated, which will initiate a chat tab directly between each trader and the mediator — but it ends the trader chat function between the two traders. Mediators are an operational role filled by DAO members, who must post BSQ bonds to ensure performance and fidelity, and which can be confiscated by vote of the DAO. The mediator takes information about the trade situation through the chat function and suggests a non-binding payout to resolve the dispute (sourced from the 2-of-2 multisignature Bitcoin address holding the security deposits and trade amount that the traders created at the beginning of the trade). The mediator may suggest that the breaching party pay a penalty to the wronged party based on the pre-published schedule of infractions (which include cancelling trades, requesting personal data, suggesting payment terms different from the agreed-upon trade, attempting communication outside of the Bisq client).[31] If both parties agree to the proposed resolution, they click a button that signs the transaction and releases the funds held in the 2-of-2 multi-signature address according to the resolution terms. If one party rejects the proposed resolution, the dispute is escalated to arbitration.

Arbitration is the third and final level of Bisq's dispute resolution process. The arbitrator role is similarly filled by a bonded DAO member. Once the mediator's suggestion is rejected, or the time-locked escrow address expires, the disputed funds are sent to the donation address and arbitration is initiated.[32] Much like with mediation,

---

[30] https://bisq.wiki/Dispute_resolution.

[31] https://bisq.wiki/Table_of_penalties

[32] https://bisq.wiki/Dispute_resolution

the arbitrator will assess the details of the case through chat. But unlike mediation, there are no additional penalties. Whichever party the arbitrator sides with receives only their security deposit back, and the bitcoin funds, if so entitled. Thus, "the total arbitration payout will be **less** than the mediation payout."[33] This design is intended to incentivize resolution at mediation (or earlier) and discourage resort to arbitration, which Bisq views as being reserved "for extreme circumstances."[34]

Bisq's intent to incentivize resolution earlier in the process, apart from being laudable in and of itself, is likely also derived from the fact that arbitration outcomes are not enforced automatically. By the time of arbitration, the 2-of-2 time-locked escrow address has expired and the funds have been deposited to an address controlled by the DAO. The arbitrator must, therefore, **personally** reimburse the party in whose favor the arbitrator decides, and then seek repayment from the DAO treasury, by vote of all the Bisq-holding DAO members.[35] This introduces a level of centralization and intervention that is antithetical to the purpose of the Bisq network, which is intended to be peer-to-peer and decentralized, with funds never flowing through the DAO or its members.

Although the final level of dispute resolution in Bisq requires human intervention and control to execute fully, Bisq is correct to describe its process as an attempt to "make[] bitcoin confiscatable, enabling a sort of mutually assured destruction to drive

---

[33] https://bisq.wiki/Dispute_resolution

[34] Id.

[35] Id.

dispute resolution on Bisq without trusted third parties."[36] It is an attempt to overcome Bitcoin's seizure resistance to remedy wrongs – but only where the aggrieved party and perpetrator have voluntarily assented to this system in advance. It is a system built on consent, not coercion.

Bisq's dispute resolution system is a useful prototype for understanding how to make judgments enforceable through Bitcoin, but because it is tied into an app and network that has a specific, limited purpose (trading), it is not scalable in its existing form.

2. Kleros: Crowdsourced Arbitration.

Kleros is dispute resolution service that uses crowdsourced decision-making instead of a single neutral third-party arbitrator or mediator. The system is designed primarily to resolve conflicts related to blockchain activity, but also resolves "off-chain," real world disputes mostly involving freelance and work-for-hire contracts.[37] Kleros is built on the Ethereum blockchain. It is not Bitcoin based and does not interface with Bitcoin at any level.

---

[36] https://bisq.wiki/Dispute_resolution.

[37] https://kleros.gitbook.io/docs/products/court

To use Kleros, disputants must enter into a smart contract and designate Kleros as their arbitrator within the contract.[38] Users access Kleros's platform through a web-app interface, or front-end.[39]

Kleros's crowdsourcing design works by enlisting anonymous "jurors" who stake a certain number of Kleros's own token, "Pinakion," to demonstrate interest in being randomly selected for cases.[40] The disputants then present their cases to the jurors asynchronously, submitting evidence and statements through the app, and jurors secretly commit to vote for one particular party.[41] Jurors are unable to communicate with one another (in fact, they are penalized for doing so), and they must provide justification for their votes to the parties.[42]

Once the voting is closed, the votes are revealed, and the party with the majority of juror votes prevails.[43] The jurors in the minority (designated "incoherent") are penalized with the loss of their staked Pinakion tokens, which are transferred to the jurors in the majority (those designated "coherent").[44] "Coherent" jurors are also

---

[38] Kleros White Paper, https://kleros.io/static/whitepaper_en-8bd3a0480b45c39899787e17049ded26.pdf ("Smart contracts have to designate Kleros as their arbitrator.").
https://kleros.gitbook.io/docs/integrations/types-of-integrations/1.-dispute-resolution-integration-plan/smart-contract-integration

[39] https://court.kleros.io/

[40] Schmitz & Rule at 118–19. https://kleros.gitbook.io/docs/pnk-token.

[41] Id.

[42] Id.

[43] Id.

[44] Id. https://blog.kleros.io/become-a-juror-blockchain-dispute-resolution-on-ethereum/ White Paper at 6–7.

separately paid in ethereum from arbitration fees that the disputants pay to the Kleros

court protocol, with fees rising as a dispute is appealed.[45]

This crowdsourcing model is based on the game theory concept of "Schelling

points."[46] The jurors must guess what most of their peers will decide and vote

accordingly. The theory behind this model is that jurors with financial stake will seek to

maximize their financial interests by voting coherently and sincerely.

But resolving disputes through Schelling points does not incentivize the jurors to

vote for the **correct legal result**, only the most likely to be **popular**.[47] Indeed,

blockchain-based arbitration platforms like Kleros do not provide any legal structure or

guidance to jurors, nor do they apply any particular jurisdiction's laws, or even any

model codes.[48] Contrast this formlessness to Bisq's clearly published trader rules and

schedule of penalties for infractions, which guide the neutral's decision-making.[49] And,

in state-run civil courts, jurors are handed sheets of instructions explaining the relevant

laws that pertain to the dispute, as well as verdict forms that constrain how jurors must

apply those laws in resolving the dispute. Kleros's jurors, on the other hand, lack any

---

[45] Id.

[46] Kleros White Paper, at 2

("Thomas Schelling described focal point(s) for each person's expectation of what the other expects him to expect to be expected to do. The Schelling Coin uses this principle to provide incentives to a number of agents who do not know or trust each other to tell the truth.") (internal quotation marks omitted);

[47] *See* Michael Buchwald, *Smart Contract Dispute Resolution: The Inescapable Flaws of Blockchain-Based Arbitration*, 168 U. Penn. L. Rev. 1369, 1404–05.

[48] Id. at 1406.

[49] Of course, Bisq's dispute resolution process is designed to be integrated into a specific use case — trading — and thus must anticipate only a small universe of potential dispute types; whereas, Kleros is attempting to scale dispute resolution as a service for many varied contexts and disputes.

such guidance and so must cast votes based on their own beliefs about the merits of the dispute, while also guessing at other jurors' beliefs. This leads to consideration of factors irrelevant to the merits of the dispute, as jurors attempt to discern what other jurors will think is a "fair" outcome. But what is perceived as "fair" may not accurately reflect what the disputants actually contracted for.

As one critic put it:

> On-chain, a juror is specifically incentivized to incorporate extraneous and frankly irrelevant factors. In the B2C context, the juror must ask: will a narrative built around evil corporations pull at the heartstrings of her fellow jurors? As correctly envisioned and predicted by on-chain application developers, such a consideration does in fact require game theory-like tactics. However, the focus of the game incorrectly shifts to incentivize a juror to vote for an outcome that diverges from the "right" legal result. Out of economic self-interest, the juror must instead predict how co-jurors will vote — effectively replacing the disputant as the proverbial prisoner in a dilemma. This system forces the decisionmaker to care more about her own well-being than the well-being of the disputants. When such a swap occurs, a juror with a perfect understanding of contract law, which assumes consumer readership for good reason, may veer away from a straightforward legal analysis.[50]

Because this incentive model will invariably produce legally or contractually arbitrary outcomes, it risks its own legitimacy in the eyes of its potential users, thereby disincentivizing use. Moreover, without a structure to guide resolution, outcomes will be inconsistent on a case-by-case basis, again, diminishing legitimacy.[51]

And the token-based incentive structure itself is likewise problematic. Practically speaking, requiring jurors to obtain and stake a bespoke token issued by the dispute

---

[50] Buchwald at 1405–06.

[51] Id. at 1406–07.

resolution provider introduces friction to juror participation. This friction is, of course, by design to discourage incoherent or arbitrary voting and prevent Sybil attacks, where a single juror could pseudonymously create large numbers of juror accounts to control the outcome of cases. [52] But for the average person, obtaining an esoteric token is not intuitive or user friendly, and requires jurors to go outside the Kleros app to various Decentralized Exchanges (DEXs) or centralized exchanges where jurors can purchase the token with eth or fiat.[53] This limits the pool of potential jurors to very technologically savvy individuals with disposable incomes. And, there is no bright line on how much of the token must be staked to prevent attacks and ensure integrity of the dispute resolution process. Indeed, Kleros recently initiated a "Juror Incentive Program" in an attempt to attract more jurors to the system and increase the number of staked tokens.[54] In effect, this program involved airdropping new tokens to staking jurors every month, thereby increasing the supply of the token (and, in turn, debasing the value of held tokens).

For the developers and contributors to the Kleros project, issuing a token presents unnecessary regulatory risk. Although the Kleros token may be either a so-called "utility" or "governance" token, these categories are not legally significant and may not ultimately shield the token from being categorized as a security by relevant regulators.[55] Moreover, by issuing their own token, the Kleros development team

---

[52] See Kleros White Paper at 4.

[53] https://blog.kleros.io/how-to-buy-pnk-on-bitfinex-exchange/

[54] https://forum.kleros.io/t/kip-46-extension-of-juror-incentive-program/669

[55] *See*, *e.g.*, *Report of Investigation Pursuant to Section 21(A) of the Securities Exchange Action of 1943: The DAO, SEC Release No. 81207* at 13-14 (2017), https://www.sec.gov/litigation/investreport/34-81207.pdf (advising that governance tokens may still be securities, explaining "[a]lthough DAO Token

introduced incentives that are orthogonal to the goals of the project, namely, to resolve

disputes in a fair and decentralized way. The Kleros team retained a portion of the

tokens during the so-called "Initial Coin Offering."[56] Beyond having a financial incentive

in the form of a functioning and successful dispute resolution protocol, they also have

financial incentives stemming from the value of their tokens. While a functioning and

successful dispute resolution protocol may drive up the price of the tokens, it's not

necessary to increase token price, as these tokens trade on the open market with thin

liquidity.[57] This presents a scenario for misaligned incentives between developers,

users, and jurors.[58]

Where Kleros succeeds, however, is in its automatic enforcement of decisions

and its voluntary nature. Because it leverages the smart contracting functionality of the

---

holders were afforded voting rights, there voting rights were limited. DAO Token holders were substantially reliant on the managerial efforts of [issuing entity], its co-founders, and the Curators."); *In the Matter of Munchee Inc.*, No. 3-18304 at 9 (SEC Admin. Proceeding Dec. 11, 2017), https://www.sec.gov/litigation/admin/2017/33-10445.pdf (determining utility tokens may still be securities; "Even if MUN tokens had a practical use at the time of the offering, it would not preclude the token from being a security. Determining whether a transaction involves a security does not turn on labeling – such as characterizing an ICO as involving a 'utility token' – but instead requires a assessment of 'the economic realities underlying a transaction.'" (internal citations omitted).

[56] https://blog.kleros.io/kleros-token-sale-frequently-asked-questions/ represents it to be 18% of the 1,000,000,000 token supply.

[57] Recall, Kleros directs its jurors to various exchanges where they can purchase the token. https://blog.kleros.io/how-to-buy-pnk-on-bitfinex-exchange/.

[58] Allen Farrington has described those "DeFi" incentives thus:

> Given VCs have immediate and total exit liquidity, their incentives are to not to nurture a highly uncertain business for as long as it takes to stabilize its return profile, but to maximize i) the amount of tokens they are allocated for free as early as possible and, ii) the price at which they can unload it as quickly as possible. Given protocol developers (the equivalent of companies) are similarly directly exposed to the immediate price rather than the long-term value of the capital they are responsible for creating, their incentives are equally aligned with VCs and misaligned with buyers and holders of the token.

Allen Farrington & Anders Larson, *Green Eggs and Ham: Decentralized Finance: The Good, The Bad, and the Ugly*, 18 (2022), available at https://www.uncerto.com/green-eggs-and-ham.

Ethereum blockchain, Kleros's decisions are self-executing and deliver value from the liable party directly to the injured party, peer-to-peer. There is no need to confirm or enforce Kleros's decisions through the state-run court system. And because parties must agree to use Kleros ex ante when entering into smart contract transactions, just like parties to traditional contracts can choose to arbitrate disputes before the American Association of Arbitrators, for example, it is entirely consensual and voluntary.

B. "Community Court" ODR Examples

1. eBay India's Community Court.

The archetypal example of efficient and successful ODR is eBay's dispute resolution system. Over the years it has undergone many revisions and adjustments, and different models are deployed in different geographic areas. Generally, to keep costs of adjudication low (due to the low-value nature of eBay transactions), eBay has used levels of dispute resolution, "which held open the possibility of an appeal to a human mediator but that had a required first step of a software-driven process that could lead to settlement without any human third-party intervention."[59] And because eBay manages the flow of money between the parties through its subsidiary, PayPal, it has developed its own enforcement process without the necessity of state-run courts.[60]

---

[59] Rabinovich-Einy & Katsh (2012) at 169.

[60] DESIGNING SYSTEMS at 118.

One specific design used by eBay was the "Community Court" in India.[61] This system used crowdsourced decision-making (like Kleros).[62] If a seller thought they received an undeserved review from a buyer, they could log into the Community Court and explain their case.[63] The system allowed the seller to upload evidence in the form of images, text, or other files. The Community Court would then automatically contact the buyer and provide them with the same opportunity and ability to respond to the seller's submission. The seller was afforded a text-based rebuttal.[64]

After the submissions were completed, the Community Court randomly selected a panel of 21 jurors.[65] Jurors were required to apply for the position and meet eligibility criteria based on their history on eBay.[66] After they reviewed the buyer/seller submissions, each juror was asked if they agreed with the buyer, the seller, or if they could not make a decision.[67] If the majority agreed with the seller, then the case was decided in the seller's favor and the feedback would be removed from eBay's system. If the majority disagreed with the seller, then the feedback would stand.[68]

---

[61] "eBay India's Community Court leveraged the best judgement of other eBay users to decide whether a contested eBay review should be deleted." Schmitz & Rule at 117.

[62] *Id.*

[63] Rule & Nagarajan at 6-7; Colin Rule and Harpreet Singh, "ODR and Online Reputation Systems," ONLINE DISPUTE RESOLUTION: THEORY AND PRACTICE 192-93 (Mohamed Abdel Wahab, Daniel Rainey & Ethan Katsh, eds.) (2013), available at http://www.ombuds.org/odrbook/rule_singh.pdf, last visited Jan. 31, 2023; DESIGNING SYSTEMS at 118–120.

[64] Rule & Nagarajan at 6-7.

[65] Id.

[66] Id.

[67] Id.

[68] Id.

The Community Court prevented fraud and collusion by "assigning cases out to jurors on a first-come, first-served basis" and limiting juror access to the case and materials for a limited period of time.[69] The Community Court system also ensured that jurors have never transacted with the disputing buyers/sellers.[70] eBay would continually monitor outcomes and juror voting data to check to consistency and coherence. "If a juror display[ed] some concerning patterns," the Community Court would "refer them cases that have already reached an outcome (for example, more than half have already voted one way or another, so the resolution is already known) as a test," and eBay could eventually just stop referring problematic cases to jurors altogether.[71]

Although it was a crowdsourced system like Kleros, the eBay Community Court did not rely on financial incentives to encourage juror participation. The designers originally thought there would be a shortage of eligible jurors, but after three years of operation, they found "the eBay Court has had more than enough jurors apply, and as of yet the platform has not needed to compensate jurors for their service in order to keep them engaged."[72] The designers attribute this to the unique nature of eBay, which "has long had an active community with extremely engaged users."[73] The Community Court has been well received in India, with users supporting its continued existence.[74]

---

[69] Id. at 7.

[70] Id.

[71] Id.

[72] Rule & Singh at 193.

[73] Id.

[74] Id.

The eBay Community Court thus demonstrates that effective crowdsourced dispute resolution can be accomplished, at least on a limited basis, without financial incentive schemes if embedded within a community with shared norms and customs.

2. Mobile Jirga.

The "Mobile Jirga" or "M-Jirga" program was a proposed dispute resolution design based on the strategy of leveraging mobile technology to "leapfrog costly intermediary steps and move right to the most modern systems" for the developing world.[75] Over a decade ago, local communities in Afghanistan explored partnering with American lawyers and dispute systems designers to pilot a mobile telephone-based dispute resolution system.[76] Although international aid organizations and the U.S. government were attempting to strengthen the rule of law through the state-run courts of the Karzai administration, they were falling short.[77] The Taliban were seen by many in Afghanistan as delivering more efficient and fair justice than the American-backed government.[78] This was in part because the Taliban were using the traditional, informal dispute resolution systems known to many Afghans, the "Jirga."[79] Afghans also preferred the Jirga was because it was local, and travel in Afghanistan was difficult,

---

[75] Rule & Nagarajan at 2.

[76] Id. See also https://www.wired.com/2010/10/can-cellphones-bring-justice-in-afghanistan/.

[77] Id.

[78] Id. Rule & Nagarajan at 10.

[79] Rule & Nagarajan at 10.

making it hard to reach formal courts, or for legal professionals to reach many areas outside of Kabul.[80]

Colin Rule (eBay's chief dispute resolution designer) and Chittu Nagarajan, two of the M-Jirga designers, described the traditional Jirga process this way:

> To convene a jirga, one or both of the parties to a dispute formally invite tribal elders to attend. Usually food is provided for the elders who attend (e.g. a cow or a sheep is killed for the occasion). The size of the jirga panel varies depending on the nature and seriousness of the issue. If six or more men are asked to mediate a dispute between individuals in different villages or tribes, half of the panel will be drawn from one side and half from the other in order to keep balance between the parties.
>
> To solve a dispute, the men on the jirga panel (it is almost always men) gather in a mosque or under a tree and discuss the situation in depth. During the proceedings, all members of the panel have equal say, but in practice everyone pretty much accepts the solution chosen by the most influential and respected members. Every member is entitled to state his point of view and make suggestions. It is considered very important for the atmosphere of the discussion to remain calm and respectful.[81]

Decisions are rendered orally and no record is kept of the adjudication.[82] Jirga decisions implement restorative justice, not retributive, and so "there's no question of punishment or jail time in the outcomes rendered," somewhat obviating the need for enforcement through coercion.[83]

The M-Jirga proposal attempted to administer the same Jirga process through mobile phone technology. Rule and Nagarajan described its operation as follows:

---

[80] Rule & Nagarajan at 9.

[81] Id. at 10.

[82] Id.

[83] Id. at 11.

Disputants could call a special number on their mobile phone to begin the process. The hotline number could be advertised around the country on posters or leaflets, or provided at the USAID hosted legal centers. Facilitators will communicate with the disputants and enable them to verbally record their cases. Both sides to the dispute will be able to hear and respond to the statements from the other side. Once both parties are satisfied with the case they have put together, a panel of elders will then be convened by phone. The elders will hear the statements from both sides and then be able to weigh in with their decision, and to record their rationale. The final decision will then be shared with the disputants, and each disputant will be able to review the recorded statements of the elders.[84]

The system was designed to be flexible and match elders with disputants according to the dialect or language spoken.[85] Rule and Nagarajan emphasized that feedback from participants would be crucial to tailor the system to reflect on-the-ground realities and cultural norms.[86]

While ultimately never fully implemented, the M-Jirga program nonetheless offers an excellent example of meeting communities where they are with dispute system designs. Technology was to be used to facilitate the traditional local, community-based courts, not supplant them with state-run systems, which were largely corrupt and ineffectual (or at least, perceived as such).

3. **Benoam – Self-Enforcing ODR System for Israel's Insurance Industry.**

An extraordinary example of an entire industry within a country creating and running its own private ODR system outside of state-run courts is Israel's "Benoam"

---

[84] Rule & Nagarajan at 11–12.

[85] Id. at 12.

[86] Id.

system. Benoam "handles the vast majority of property damages claims between insurance companies in Israel ('fender-bender' claims)."[87] These claims are referred to Benoam through an ODR system and database, which all insurance companies have contractually agreed to participate in.[88] "Benoam has, therefore, in effect displaced the court system in this particular domain of disputes."[89]

The Benoam agreement contains detailed Articles of Arbitration that set forth the rules of the system.[90] There are almost never any in-person hearings. Most claims are decided "on written pleadings and evidence submitted and stored digitally," which is possible due to the "generally uncomplicated nature of the claims and the fact that there is a limited set of recurring typical cases."[91] Data is transferred automatically from the insurance companies' internal databases onto forms for greater efficiency, and information on "decisions flow[s] from Benoam to the Insurance Association for the execution of rulings."[92]

Benoam does not use jurors or crowdsourcing, but professional, expert third-party neutrals as arbitrators, who "include retired judges, attorneys, appraisers, traffic

---

[87] Rabinovich-Einy & Katsh (2011) at 67.

[88] Id. *See also* Orna Rabinovich-Einy & Roee Tsur, *The Case For Greater Formality In Adr: Drawing On The Lessons Of Benoam's Private Arbitration System [Benoam, Orna Rabinovich-Einy,* 34 Vt. L. Rev. 529, 544 (2009) ("The vast majority of Israeli insurance companies, which controlled more than 95% of the auto insurance market, accepted the solution offered by the Benoam system and signed an arbitration agreement under which they were obligated to file all their subrogation 'fender bender' claims through Benoam (Agreement or Arbitration Agreement).").

[89] Rabinovich-Einy & Katsh (2011) at 67.

[90] Rabinovich-Einy & Tsur at 544.

[91] Rabinovich-Einy & Tsur at 545.

[92] Rabinovich-Einy & Katsh (2012) at 187–88.

examiners, and Certified Public Accountants (CPAs)."[93] Arbitrators are incentivized to render consistent and well-reasoned decisions by "being singled out as a 'leading' arbitrator, whose decisions are not reversed on appeal and whose rulings set important precedents."[94] And the risk of arbitrators seeking to curry favor with particular disputants by rendering favorable decisions is partly minimized "by the fact that users are repeat players who typically alternate between the plaintiff and defendant positions."[95]

These and other factors confer a perception of fairness to the Benoam system, thereby reinforcing its use. For example, "the availability of an internal appeals mechanism before another arbitrator or a panel of arbitrators proved an effective ex post mechanism for strengthening fairness."[96] The appeals process also allows Benoam to resolve fundamental questions that may arise.[97] In so doing, Benoam creates a form of res judicata and is able to set "precedents" within the system, including publishing "landmark decisions" to its site, without identifying the parties to the claim.[98] Such precedents create consistency among decisions, thereby further reinforcing perceptions of fairness.

---

[93] Rabinovich-Einy & Tsur at 545.

[94] Rabinovich-Einy & Katsh (2012) at 185.

[95] Id.

[96] Id. at 184.

[97] Rabinovich-Einy & Tsur at 546.

[98] Rabinovich-Einy & Katsh (2012) at 184.

Finally, arguably the most important feature of Benoam is its private enforcement mechanism:

> The system operates a clearinghouse and is therefore able to effortlessly execute the arbitration awards. The execution stage is conducted automatically, based on the parties' agreement to grant Benoam authorization to transfer funds directly to and from each party in accordance with Benoam rulings, making any additional action by the parties unnecessary. More specifically, the clearinghouse mechanism runs a monthly scan over the Benoam database and sums up all awards and expenses, crediting or debiting each party accordingly. In addition, the system can generate a number of comprehensive reports that allow insurance companies to effectively monitor the transfer of their funds through and by the system.[99]

As the leading experts on the system describe it: "The ability to execute arbitration awards swiftly and *independently of courts* allows Benoam to substitute power and authority for *consent*."[100] And this ability of Benoam to execute decisions independently from the courts is considered "a central factor in its success and legitimacy."[101]

4. Prospera Arbitration Center: Private Courts for Private Cities

The Free Cities movement aims to place individual liberty and voluntary choice at the center of governance through the creation of semi-autonomous territories within nation-states.[102] As the Free Cities Foundation explains, a private company would assume the duties of traditional government to furnish security and services, as directed by an actual, enforceable social contract signed with each individual resident:

---

[99] Rabinovich-Einy & Tsur at 546.

[100] Rabinovich-Einy & Tsur at 548 (emphasis added).

[101] Rabinovich-Einy & Katsh (2012) at 189.

[102] See https://free-cities.org/.

Imagine a system in which a private company as a "government service provider" offers you protection of life, liberty and property. This service would include internal and external security, a legal and regulatory framework, and independent dispute resolution. You would pay a contractually fixed amount per year for these services. Besides that, you would take care of everything yourself. You would be able to do as you please, limited only by the rights of others and the contractually agreed rules of coexistence.

The government service provider as the operator of the community cannot unilaterally change this "Citizen Contract" with you at a later date. Disputes between you and the government service provider would be heard before independent arbitration tribunals, as is customary in international commercial law. If the operator ignores arbitral awards or abuses their power, their customers would leave and they would go bankrupt. The operator therefore has to face the economic consequences of their actions, giving them an incentive to treat their customers well in accordance with their contract.

As conventional political systems reach their limits, Free Private Cities represent a peaceful and voluntary alternative for governance.[103]

A somewhat utopian vision, to be sure. But one implementation of this vision, called Próspera, is being attempted in a semi-autonomous "Zone for Economic Development and Employment" (ZEDE) on the island of Roatán in Hondurous.[104] The Próspera ZEDE was created by the Honduran National Congress through a constitutional amendment, and its existence is further stabilized through bilateral international agreements.[105]

Próspera residents sign an "Agreement of Coexistence" with the operating entity that sets forth the parties' obligations and rights, and specifies how disputes will be

---

[103] https://free-cities.org/free-private-cities/#freeprivatecities.

[104] https://prospera.hn/platform

[105] https://prospera.hn/platform. *See also* https://pzgps.hn/; https://pzgps.hn/all-publications/.

resolved.[106] Rules and regulations are published in a Charter & Bylaws, which includes a Resident Bill of Rights, as well as the Roatan Common Law Code.[107] The Agreement specifies arbitration as the exclusive mode of dispute resolution between residents or the residents and operating entities. The Agreement specifies arbitration by the default "Arbitration Service Provider," with arbitration governed by the Provider's rules in force at the time of the demand for arbitration.[108]

Próspera's default "Arbitration Service Provider" is a separate entity known as the Próspera Arbitration Center (PAC), with which the Próspera operator contracts with to provide dispute resolution services pursuant to the Agreement of Coexistence.[109] As a separate company, the PAC is also available to provide arbitration services to other special economic zones or even as contracted for between private individuals.[110] The PAC employs professional, expert arbitrators with experience as former judges, constitutional law professors, and practicing lawyers.[111] The PAC issues both binding and non/binding decisions. While not a full ODR system, the PAC claims to leverage technological solutions to drive efficiencies in decision-making (indeed, it does not currently have a physical forum).[112]

---

[106] *See* PRÓSPERA ZEDE e-RESIDENT AGREEMENT OF COEXISTENCE, available upon request at https://eprospera.hn/residency.

[107] https://pzgps.hn/all-publications/; https://pzgps.hn/charter-bylaws-carta-constitutiva-y-reglamentos/.

[108] PRÓSPERA ZEDE e-RESIDENT AGREEMENT OF COEXISTENCE, available upon request at https://eprospera.hn/residency.

[109] https://pac.hn/

[110] Id.

[111] Id.

[112]*See* https://pac.hn/services/.

Although striving to be a private dispute resolution system for private cities, the road to enforcement nonetheless leads back to the courthouse door. The PAC's website explains that "[a]wards of the PAC are enforceable internationally pursuant to the New York and Panama Conventions," thus requiring a court subject to those conventions to confirm and enforce awards whenever there is noncompliance.[113] Próspera has not designed a method to directly enforce judgments concerning its residents without the state's monopoly on violence, short of terminating the Agreement with noncompliant residents and, as a last resort, ejectment (which, of course, would require private violence).

Próspera PAC nonetheless offers a real-world model of an independent dispute resolution entity, whose jurisdiction and use can be consented to ex ante on a **community-wide scale**. And, being an independent business, the PAC is able to offer its services to **many different communities**, broadening its sources of funding, thereby increasing its likelihood of longevity as a stable forum. And, with increased funding comes the ability to attract skilled and high-quality expert arbitrators, whose employment further confers legitimacy to the dispute resolution program.

But without a peaceful automatic enforcement mechanism, the PAC and free private cities such as Próspera will continue to be tethered to the state's monopoly on violence, or be forced to privatize violence – a situation that is at odds with the movement's ethos of peaceful governance through consent. The thought leaders of the Free Private Cities movement are aware of the enforcement issue and have even

---

[113] https://pac.hn/.

suggested some form of smart-contracting[114] may be the answer. The founder of the

Free Cities Foundation, Titus Gebel, writes:

> Another option is to have every citizen provide a security deposit at the start of the contract from which enforceable titles can be satisfied. Of course, this is an additional burden that not everyone will be able to afford. The use of so-called smart contracts may make court and enforcement proceedings often superfluous, particularly in simple Cases.[115]

As explained in detail in the next part, developments in Bitcoin scaling

technologies can be harnessed to realize this suggestion (without the need for costly

security deposits) and untether community-wide dispute resolutions from violent

enforcement (both public and private).

IV. Designing a ₿DR System.

A.   Conceptual Framework.

The forgoing examples of existing cryptocurrency-based and community ODR

systems demonstrate both the potential and limitations of such systems in achieving

enforceable judgments not backed by the state's monopoly on violence. By

incorporating the best attributes of those existing systems into an ODR system

deployed through Bitcoin scaling technologies, it is possible to construct a viable

template for ODR that exists truly apart from the state and is able to scale to community

levels to resolve off-line and on-line disputes.

This section will establish the conceptual underpinnings of the ₿DR system by

synthesizing those attributes most conducive to peaceful, private enforcement of

---

[114] *See* Stabile, Prior, Hinkes at 26.

[115] Titus Gebel, FREE PRIVATE CITIES: MAKING GOVERNMENTS COMPETE FOR YOU, 186-87 (2018).

judgments introduced above, with those features that make the Bitcoin network peerless in its censorship-resistance.

<p align="center">DECENTRALIZATION.</p>

Bitcoin is the most decentralized, most widely distributed communications network for the transfer of value in existence. Bitcoin achieves this level of decentralization through its separation of roles (which anyone can assume, at any time): validating nodes, block miners, and developers. Miners can publish blocks to the blockchain only if the validating nodes determine that the transactions within the block, and the block itself, conform to the consensus rules of the Bitcoin network inscribed in the open-source code first devised by Satoshi Nakamoto, and which teams of pseudonymous developers now maintain and update according to the rough consensus of the entire Bitcoin network userbase.

The Bitcoin network has tens of thousands of validating nodes currently storing the entire Bitcoin chain (including every transaction and message) from the first, genesis block in 2009 through today.[116] This makes data published to Bitcoin's chain immutable, and thus uncensorable: deleting data simultaneously stored on tens of thousands of computers across the world is practically impossible.

Although it is theoretically possible for an entity with control of 51% of the mining network to force a reorganization of the most recently added blocks, this would require gargantuan levels of electricity and computer power, as the Bitcoin network is estimated

---

[116] One recent estimate of all nodes (visible and unreachable) was 44,280. *See* https://bitnodes.io/nodes/all/, last accessed (Jan. 30, 2023)

to use 115.62 TWh of electricity per year.[117] Indeed, the number of miners on the

Bitcoin network hit an all-time high in January of 2023, measured by computer hashing

power.[118] And after China's mining ban in the summer of 2021, the distribution of

mining hash-rate is more globally distributed than ever.[119] Thus, the high levels of

decentralization and participation in mining nodes makes Bitcoin the most secure

database in history.[120]

A final crucial factor in maintaining decentralization and trustlessness is the fact

that all updates to the Bitcoin network's code are (i) backwards compatible and

(ii) optional. This means that a Bitcoin wallet running code from 2009 will still

communicate and transact with the network and wallets running code from 2023.

Bitcoin achieves this through "soft-forks" to its code; whereas, networks like Ethereum

use mandatory, non-backwards compatible updates known as "hard-forks."[121] If Bitcoin

node runners do not agree with the updates to the code, they can simply maintain their

current version of the software and happily continue to participate in the network (albeit

with fewer features). Bitcoin, down to its code, enshrines an ethos of voluntary consent.

---

[117] *See* https://ccaf.io/cbeci/index

[118] *See* https://mempool.space/graphs/mining/hashrate-difficulty#1y.

[119] *See* https://ccaf.io/cbeci/mining_map.

[120] "Mining doesn't work to create bitcoin. That is not the purpose of mining; that is a side effect. The way I can prove it's a side effect is that one day, there will be no new bitcoin. But guess what? There will still be mining. Even after the last satoshi (the smallest unit of bitcoin) gets mined, mining continues. It must continue because its purpose is not to create bitcoin but to provide security, to provide validation of all of the transactions and blocks according to the consensus rules. Generating bitcoin is a side effect that currently serves as a mechanism of reward, creating game-theory incentives to make sure that the validation is done right. Once you understand that and you realize what we're paying for is security, it changes the perspective slightly." Andreas Antonopoulos, THE INTERNET OF MONEY, Vol 2.

[121] *See* Yan Pritzker, INVENTING BITCOIN 81–85.

Any ODR system that is intended to operate apart from the state's monopoly on violence will need to be anchored to a base layer that is immune from state capture or control. Bitcoin's immutable ledger distributed across tens of thousands of computers, secured by an equally distributed and massive mining network, run on code upgraded through an opt-in process that ensures perpetual backwards-compatibility, renders such state capture or control improbable. Certainly, there is no other network in the world that can boast Bitcoin's level of decentralization.

The Bisq network's dispute resolution system has used Bitcoin's decentralization and unstoppable nature to create largely self-enforcing decisions. Once a trade offer is accepted, the funds and security deposits are sent to the time-locked Bitcoin escrow address, which will transfer the funds to the DAO's donation address if no mutually agreed-upon resolution is adopted. The traders cannot stop this transaction, nor the DAO's mediators or arbitrators. To do so would require complete control over more mining power than existed even two years ago.

AN OPEN-SOURCE PROTOCOL.

A feature shared by Bisq and Kleros that will be necessary for the success of a private alternative to state-run legal systems is the open-source nature of the underlying code. Allowing anyone to view, audit, and propose changes to the system's code will increase perceptions transparency and legitimacy. Professors Rogers, Bordone, and Sander explain the problem of company "trade secrets" in dispute resolution software:

> Novel fairness issues emerge when software mediates or resolves disputes. Participants using a private online negotiation service to resolve buyer-seller disputes cannot tell whether the software operates neutrally. That ignorance may lead buyers to suspect that the provider designs the

software to favor sellers who typically pay the provider for the service and to certify them as compliant with dispute resolution results. Transparency might help, but private providers protect the trade secrets in their software. Even if the invisible software rarely contributes to unfairness, people may refuse to put themselves in a situation of having to use the software if they do not trust it.[122]

Bitcoin is entirely open-source[123], as are its scaling protocols, the Lightning Network and FediMint. The mantra in the Bitcoin community, stemming from its cypherpunk roots, is "verify, don't trust."[124] Because every line of code is auditable, anyone and everyone can see exactly how the software works, eliminating the need to trust a centralized company's statements about their proprietary, closed-source code. This type of transparency will be crucial to encouraging adoption and use of private ₿DR systems. Users can know that the software code is not favoring the operators of a private city, or the more powerful party in a bilateral contract.[125]

A related, but no less important, feature of a ₿DR system is that designers should first prioritize establishing a **protocol** not a platform or single company. This will work in concert with decentralization, in that many different developers and designers can deploy different flavors of the ₿DR protocol, ensuring there is no centralized company that presents a single attack surface for regulation or capture. And by

---

[122] DESIGNING SYSTEMS at 249.

[123] *See* https://bitcointalk.org/index.php?topic=13.msg46#msg46 (Satoshi Nakamoto explaining, "[b]eing open source means anyone can independently review the code. If it was closed source, nobody could verify the security. I think it's essential for a program of this nature to be open source.").

[124] *See* https://mailing-list-archive.cryptoanarchy.wiki/.

[125] Colin Rule & Mark James Wilson, "Online Resolution and Citizen Empowerment: Tax Appeals and Court Resolutions in North America," DIGITAL TRANSFORMATION AND ITS ROLE IN PROGRESSING THE RELATIONSHIP BETWEEN STATES AND THEIR CITIZENS 116 (2020) (discussing how "transparency can build trust and work to ensure fairer outcomes across the board" when employing dispute resolution technology).

standardizing the major facets of the ₿DR system into a common protocol,

interoperability is increased across communities (as explained further in the proposed

₿DR design below). This is not to say that ₿DR companies will not exist and compete

to provide the best adjudicatory services, but standardization will allow for a larger

market to form, providing communities and individuals the greatest freedom of choice to

meet their specific needs. And, with greater optionality, the ability for any one company

to become the de facto legal system, and exploit that monopolistic power, will be greatly

diminished. Disputants and communities can simply choose a new provider if their

current ₿DR system compromises on fairness, consistency, or access.

<div align="center">

BITCOIN IS THE ONLY TOKEN NEEDED.

</div>

₿DR systems should not introduce their own tokens like Bisq's BSQ or Kleros's

PNK (if they did, they wouldn't be *Bitcoin* Dispute Resolution systems). As discussed

above, contrived tokenomics introduce unnecessary regulatory risk. Issuing bespoke

tokens can misalign incentives between the system's designer and developers,

disputants, and neutral decision-makers. And forcing users to obtain niche tokens to

access the dispute resolution system creates friction to adoption.

Because Bitcoin is truly decentralized, with its issuance controlled by no

individuals or group, ₿DR developers and designers do not risk running afoul of

securities laws for integrating their services within the Bitcoin ecosystem.[126] Indeed, as

detailed further below, ₿DR systems will not use bitcoin as a utility token to facilitate

---

[126] Of course, some attention must be paid by designers to the regulatory requirements of their chosen jurisdiction. But ₿DR systems can and should be designed to minimize the need to custody user funds or become classified as money transmitters.

decision-making, but rather will direct the flow of bitcoin between disputants to enforce judgments.

And by plugging into the most widely used digital cash in existence, with the largest market capitalization and strongest network effects, ฿DR systems gain the benefits of interoperability, reducing friction to adoption and use of the dispute resolution solution. Bitcoin allows for dispute resolution systems to extend across the world's population.

DIRECTING THE FLOW OF VALUE ALLOWS FOR PRIVATE ENFORCEMENT.

eBay's control over the flow of funds between disputants through PayPal is has been recognized as integral to its ability to privately enforce its dispute system's decisions.[127] Benoam achieves control over the flow of disputants' funds through its clearinghouse, access to disputants' accounts, and transparent record-keeping.[128] In both examples, the private enforcement mechanism "hinges on the availability of digital databases that allow for effortless connections between financial data and resources on the one hand, and resolution outcomes on the other."[129] At no point is a court order necessary to coerce compliance with decisions. The monetary judgments are simply executed by the digital systems.

---

[127] See Koulu at 76 ("In addition to providing an e-commerce platform for sellers and buyers, eBay has access to the world's largest Internet payment company, PayPal, which has been a subsidiary of eBay since 2002. The combination of access to the payment method and internal dispute resolution procedure is necessary for producing an effective private enforcement mechanism."); DESIGNING SYSTEMS at 118 ("eBay also developed its own enforcement processes. This was possible both because eBay managed the flow of money between the parties via its PayPal subsidiary and because eBay could restrict or remove users from the platform at any time.").

[128] See Rabinovich-Einy & Tsur at 546-48.

[129] Rabinovich-Einy & Katsh (2012) at 189.

As explained more fully below, a ฿DR system will interface with both the base layer database of the Bitcoin network, stored across tens of thousands of validating nodes globally, and the database of the communities or entities deploying the ฿DR system. Decision data will be relayed instantly from the ฿DR system to trigger transactions between disputants. Recent advances in Bitcoin scaling technology now allow for this type of smart-contracting or flexible scripting.

EMBEDDING ฿DR INTO COMMUNITIES.

Embedding ฿DR systems directly into communities, both online and offline, will be essential to success. All of the dispute systems explored in this paper, but for Kleros, were integrated in some way to a community or multiple communities. This allows the system to be tailored to its users, reflect cultural norms, and better address the needs of disputants.[130] As demonstrated with the Jirgas and M-Jirga design in Afghanistan, users are more likely to engage with and trust dispute resolution systems that incorporate familiar design elements.

Moreover, eBay's Community Court shows that placing a dispute resolution procedure within a community can drive juror participation without contrived incentive schemes.

And the Próspera PAC demonstrates the power of communities as a mechanism for furnishing access to justice to many people at scale, mostly separate from a nation-state.

---

[130] *E.g.*, Rule & Nagarajan at 12.

Indeed, Bitcoin-based communities are sprouting in towns across the world in areas marked by weak rule of law and immiserating economic conditions. The most well-known is Bitcoin Beach, in El Salvador, which inspired the country's President to make Bitcoin legal tender alongside the U.S. dollar. Bitcoin Ekasi, in Mossel Bay, South Africa, was, in turn, inspired by Bitcoin Beach.[131] There's also Bitcoin Lake in Guatamala[132], Bitcoin Mountain in Cameroon[133], Bitcoin Island in the Philippines[134], Praia Bitcoin in Brazil[135], and Bitcoin Jungle in Costa Rica.[136] These communities are already participating in the Bitcoin economy of the future and will drive Bitcoin adoption. BDR systems could easily complement the economic transformations occurring in any one of these localities and provide a vehicle for achieving rule of law that might otherwise be lacking under the respective state-run justice systems.

So long as those communities and their residents consent to be bound by such services and their enforcement mechanisms expressly, not tacitly, through a conscious choice.

B.   Technological Framework.

With that conceptual framework established, the technical framework can now be explored for an effective private enforcement system built on Bitcoin. The first piece of

---

[131] https://bitcoinekasi.com/

[132] https://bitcoinmagazine.com/culture/dispatch-from-guatamala-bitcoin-lake

[133] https://twitter.com/_BitcoinMt

[134] https://pouch.ph/bitcoinisland

[135] https://praiabitcoin.org/en/

[136] https://www.bitcoinjungle.app/

the puzzle to understand is Bitcoin's scaling layers or protocols, the Lighting Network and FediMint.

The Lightning Network is known as a "Layer 2" technology in that it sits on top of the base layer, Bitcoin. The Lightning Network is akin to HTTP or SMTP, both of which are made possible by the base layer of the internet, TCP/IP.

The Lightning Network makes bitcoin payments fast (practically instantaneous) and nominally cheap (less than a cent, in most cases). It does this through a network of bilateral payment channels between nodes running the lighting software, which each contain a set amount of bitcoin.[137] These channels are like bar tabs.[138] Once you open the tab with a single, base-layer Bitcoin transaction, you can make an unlimited number of transactions until you close out. The act of "closing out" your tab is a second, base-layer Bitcoin transaction that settles all the lightning transactions made.[139] These payment channels are strung together throughout the Lighting Network such that parties to the payment do not need to have direct channels with each other, but merely one channel open to a "routing node" that will move the payment along to its final destination.[140] Many lighting wallets available for mobile phones abstract away the channels and automate the plumbing behind the scenes, making for a seamless

---

[137] *See* https://bitcoinmagazine.com/guides/how-lightning-network-scales-bitcoin-payment.

[138] *Id.*

[139] Id. *See also* MASTERING BITCOIN, https://github.com/bitcoinbook/bitcoinbook/blob/develop/glossary.asciidoc ("In a typical payment channel, only two transactions are added to the block chain but an unlimited or nearly unlimited number of payments can be made between the participants.").

[140] https://bitcoinmagazine.com/guides/how-lightning-network-scales-bitcoin-payment

payment experience.[141] By reducing the number of "on-chain", base-layer Bitcoin transactions to two per channel, the Lightning Network greatly scales the number of transactions possible, and further speeds up and reduces the costs of each transaction, in addition to allowing very tiny microtransactions. The Lighting Network is the glue that will bind subsequent community-based scaling layers, such as FediMint.

FediMint is another scaling layer for Bitcoin built on the well-established concept of "Chaumian e-cash,"[142] invented by cryptographer David Chaum and originally implemented through his company DigiCash in the 1990s.[143] E-cash was designed to be privacy-preserving using a cryptographic technic called "double-blind signatures" that obscures the e-cash holder's identity from the issuing entity or bank (called the "Mint"[144]), but allows that entity to know that the holder has not attempted to spend the same e-cash token multiple times.[145]

---

[141] Breez wallet, bluewallet, Phoenix wallet, and Muun are all excellent examples of simple and user-firendly UX.

[142] https://fedimint.org/docs/GettingStarted/TechCompontents.

[143] DigiCash partnered with Mark Twain Bank to offer "E-Cash" to account holders, backed by the bank's deposits. Steven Levy, CRYPTO: HOW THE CODE REBELS BEAT THE GOVERNMENT—SAVING PRIVACY IN THE PROCESS 293–94 (2001). *See also* https://en.wikipedia.org/wiki/DigiCash.

[144] https://fedimint.org/docs/GettingStarted/TechCompontents.

[145] https://fedimint.org/docs/CommonTerms/Blind%20Signatures. In 1996, Professor A. Michael Froomkin offered the following contemporaneous explanation of e-cash and double-blinded signatures:

> Using "blinded coins" Alice can acquire digital cash with a unique serial number from a bank without allowing the bank to create a record of the coin's serial number. Despite the bank's ignorance of the serial number, the number's uniqueness helps ensure that Alice cannot spend it twice. The techniques that achieve this, developed and patented by David Chaum and being marketed by a company he founded called DigiCash, are complex. Like a basic digital coin, a blinded coin begins with a large random serial number, but this time the serial number is generated by Alice, the customer who intends to acquire a coin from the bank. Alice multiplies this serial number by another random factor ("the blinding factor"), and sends the product (the "blinded" number) to the bank. As in the basic case, the bank signs the number with its secret key.

FediMint, a portmanteau of "federated Chaumian Mint," implements e-cash's mint

structure in a new way, through a federation, rather than a single centralized bank or

entity.[146] "This means that the mint is jointly owned and operated by multiple people,"

called "guardians."[147] According to the protocol's website:

> By federating the operation, Fedimint gains several advantages over single server deployment.
>
> 1. The bitcoin held in the mint is never subject to the control of a single individual making it harder for a corrupt guardian to steal funds.
>
> 2. Increases redundancy as guardians can go offline and transactions will still be processed where a quorum is reached.
>
> 3. Changes the regulatory space of the federation as no single individual controls coin issuance and redemption.[148]

In addition to e-cash and the federated mint, a third technological component to

FediMint is "Lightning Swaps," which will allow separate federations to link with one

another through the Lightning Network.[149] The interoperability of Lighting and Bitcoin

links federations to the broader world economy. Users can deposit bitcoin into the

---

Unlike the basic case, however, a bank issuing a blinded coin does not know the true serial number of the coin at the time the bank issues it by affixing its digital signature to the "blinded" number. All that the bank knows is that Alice has purchased a coin of a given denomination, and the "blinded" number Alice submitted.

A. Michael Froomkin, *Flood Control on the Information Ocean Floor: Living with Anonymity, Digital Cash, and Distributed Databases*, 15 J.L. & Com. 395 460–61 (1996). Professor Froomkin's legal research on privacy, cryptography, and digital cash was far ahead of its time, and worth returning to for a clearer understanding of the legal implications of Bitcoin and other digital asset altcoins. *See* A. Michael Froomkin, *The Essential Role of Trusted Third Parties in Electronic Commerce*, 75 Or. L. Rev. 49 (1996); A. Michael Froomkin, *The Metaphor Is the Key: Cryptography, The Clipper Chip, and The Constitution*, 143 U. Penn. L. Rev. 709 (1995).

[146] https://fedimint.org/docs/GettingStarted/TechCompontents.

[147] Id.

[148] Id.

[149] Id.

federated mint through the lightning network in exchange for bitcoin-denominated e-cash. And then users can send their bitcoin-denominated e-cash outside the federation by, essentially, redeeming their e-cash instantly for bitcoin at the point of contact with the Lighting Network.[150]

The ultimate purpose of FediMint is to facilitate "community custody solutions" and simplify a bitcoin-owner's ability to secure their funds.[151] Federations are designed to scale from the family level to the friend, community, and private online levels.[152] Guardians who control the keys in a large multi-signature arrangement are intended to be those whom users trust and know, replacing faceless, unknown centralized third-party custodians with incentives that do not align with their customers.[153] Custodial risk is mitigated through the multi-party arrangement, which would require a supermajority of the guardians to collude to abscond with the bitcoin held by the mint.[154] In arrangements where all parties know and trust each other, collusion is less likely.

Besides improving custody relationships and enhancing the Bitcoin ecosystem's privacy through blinded signatures, FediMint also extends Bitcoin's capabilities through modules. FediMint's website explains that the core of the protocol is the "ability to agree on and process transactions," and that "[t]he possible input and output types of

---

[150] https://fedimint.org/docs/GettingStarted/How-FM-Transactions-Work.

[151] https://fedimint.org/docs/GettingStarted/Who-are-the-fms

[152] Id.

[153] Id.

[154] Id.

these transactions are defined by modules."[155] The two necessary modules run the logic for the wallet and e-cash mint, but other modules like "smart contracts or even a federated market place could be implemented."[156] FediMint's developers intend these "3rd party modules" to be "driven by the needs of the fedimint community."[157]

In other words, FediMint is a "general framework for federated financial applications," plugged into the Bitcoin network through lighting.[158]

A ḂDR system can be implemented as a FediMint module. Smart-contracts within the module will grant the ḂDR system the necessary control over federation funds to achieve enforcement without state-run court intervention. Further, by interfacing through FediMints, the ḂDR system will operate at the community level, widening access to its services. An outline of the system follows.

C.   An Initial Proposal: ḂDR Modules for FediMints.

The core of the ḂDR system will be the enforcement layer. This base ḂDR layer will reside in a FediMint module containing the "if, then" logic necessary to translate the outcome of the dispute resolution process into a self-executing judgment capable of transferring value from the liable party to the injured party. A suitable smart-contracting language for such logic is Simplicity[159], which has been in use on Blockstream's

---

[155] https://fedimint.org/docs/MiniMintDetails/Architecture

[156] Id.

[157] https://fedimint.org/docs/GettingStarted/Running-a-Fedimint

[158] https://fedimint.org/docs/MiniMintDetails/Architecture

[159] *See* Russell O'Conner, *Simplicity: A New Language for Blockchains*, available at https://blockstream.com/simplicity.pdf. *See also* https://github.com/ElementsProject/simplicity.

federated sidechain, Liquid Network (which shares some attributes with FediMints). The enforcement module will simply receive the "if" condition and execute the "then" function, transferring the funds within the federation between members. By keeping the FediMint module simple and limited to enforcement logic, it is easier to standardize into a protocol that can be adopted by all federations in a "plug and play" manner.

The next layer can be considered the "resolution" layer. This resolution layer will be housed on a separate platform and contain the complexity of the dispute resolution systems. Many flavors or BDR types can be offered on this layer by service providers or the communities themselves. Communities can choose which ḄDR type to integrate with their federation. Perhaps one community wants expert arbitrators, another wants a community court system with jurors pulled from the federation, still another federation wants to use anonymous crowdsourcing where jurors earn bitcoin fees for resolving disputes. All these different ḄDR court types will nonetheless share the common dispute logic necessary to transmit the "if" condition to the FediMint module. In this way, the ḄDR resolution layers act as oracles. In addition to receiving the "if" condition of the resolution layer's decision, the FediMint enforcement layer will also need to relay information back to the resolution layer about the disputants, even if only pseudonymously.

This architecture will leverage the benefits of embedding dispute resolution into communities discussed above, as well as enable the necessary flexibility to tailor dispute resolution procedures to the individual communities based on cultural norms or contractual agreement. And it allows any individual person to opt into the enforcement scheme consensually. If one does not agree with the dispute resolution process

employed by a federation, or wishes to simply remain "judgment proof," one can simply not join that federation.

But consider if a free private city like Prospera were to operate its own FediMint. The governing agreement between residents and the operator could specify the ฿DR resolution layer to be used, and require residents to join the federation by depositing a certain sum of bitcoin, which would be converted to e-cash and subject to enforcement through the FediMint enforcement layer module. Most residents would likely choose to keep some of their funds in the federation of their own volition, in order to transact with other residents and businesses within the community.

It is also conceivable that parties in complex and recurring business arrangements could create their own FediMints with ฿DR modules to resolve disputes, in essence replacing and simplifying Benoam's clearinghouse system.

In designing ฿DR resolution layers, some best practices from the dispute resolution design field should be followed. As a threshold matter, designers should refrain from over-automating the resolution and decision-making process. When code is law, and the code bugs out, unintended outcomes occur. Early scholarship on use of smart-contracts in dispute resolution was correct to note that "giving authority to human oracles who decide whether the factual basis for performance has been met, or employing arbitrators who resolve disputes through a multisig arrangements, may avoid some of the draconian implications of fully self-enforcing agreements."[160]

---

[160] Kevin Werbach & Nicolas Cornell, *Contracts Ex Machina*, 67 DUKE L.J. 101, 163 (2017).

Moreover, some mechanism for appeal or further review should be allowed before the decision is transmitted to the FediMint's enforcement module for execution. This will guard against arbitrary or patently incorrect outcomes increasing due process, and thereby adding to the sense of fairness that participants have. The process can allow for one free appeal, or raise the expense with each successive review (as Kleros does).

The resolution process should avoid live hearings where possible. In every example considered in Part III, asynchronous communication was the default. As Rule and Nagarajan observed, asynchronous communication is superior to synchronous communication in many ways:

> Over time ODR practitioners learned the benefit of asynchronous, text-based online exchanges. These types of communication urged participants to be reflective, and they enabled disputants to consider their comments before posting. They also opened up the possibility of research and consultation during a dispute resolution process. Both participants could engage with the process when it was convenient for them to do so, and that turned out to enable a more deliberate interaction that was conducive to conflict resolution. Asynchronous communication was impractical if not impossible to sustain in a face-to-face interaction; the very nature of online communication created the possibility for asynchronous conflict resolution to occur. If ODR experiments had hewed unwaveringly to the arc of innovation predicted at the inception of the field – namely, replicating face-to-face interactions – the new capabilities of online communications channels might have been overlooked."[161]

In the words of Richard Susskind, "[a] system whose foundations lie in a print-based world, dominated by paper and [face-to-face] meetings, will soon be out of step with the daily lives of citizens of a digital society."[162] Live hearings are a vestige of the

---

[161] Rule & Nagarajan at 4.

[162] Susskind at 84.

analog world and risk both the efficiencies of a dispute resolution design and its credibility. Justice should not have to wait for the courtroom to open.[163]

By unshackling itself from traditional civil justice systems, a ḄDR system can extend beyond mere dispute resolution services and approach justice more wholistically.[164] Dispute resolution should not be the first step in the process. The first step should be education. Disputants will not access justice unless they think their rights have been violated. The FediMint wallet used by the federation could incorporate a "know your rights" tab to educate on federation members' rights and responsibilities (as set forth by the relevant governing contracts or even local law and customs). The wallet could link federation members to a grievance assessment wizard furnished by the ḄDR service provider that could categorize the conflict through a series of basic questions and propose tailored solutions based on the type of conflict at hand.[165]

After the diagnosis stage, if the claimant determines they do, in fact, have a claim, the second tier of the ḄDR system can employ technologies and techniques to contain the dispute, instead of waiting for it to escalate and sides to become

---

[163] Pilot public ODR programs have shown "85% of resolutions through ODR are achieved during times when the court is not open for business." Rule & Wilson at 114.

[164] Susskind refers to this as the "extended court," which would include "tools to help users understand their rights, duties, and options open to them, facilities that assist litigants to marshal their evidence and formulate their arguments, and systems that advise on or bring about non-judicial settlement." Susskind at 61.

[165] A "grievance assessment process will seek, in the first instance, to settle some pretty basic questions, such as the following. Does your problem concern (a) an injury you have suffered, (b) some money you are owed, (c) a product or service with which you are unhappy, or (d) a problem arising from a contract? Is your problem with (a) an individual, (6) a business, (c) a public body? When did the problem occur? Where did the problem arise?" Susskind at 125. *See also Rule & Wilson* at 114 (summarizing a "common design" for dispute "diagnosis wizard" that can assess and propose resolutions to "small claims disputes," "landlord tenant disputes," and "family disputes").

entrenched. Bisq and eBay facilitated early communication between counterparties to

alleviate misunderstandings and empower disputants to reach a mutually agreeable

outcome before resorting to official resolution procedures. The traders and buyers and

sellers on those platforms were aware of their rights and obligations due to conspicuous

educational content, and thus were able to engage in more informed and constructive

discussions. Armed with the knowledge of their rights and obligations, disputants in the

 BDR process could communicate through asynchronous, end-to-end encrypted chats

that maintained their privacy.

Another containment tool short of human decision-making that produces a fully

self-executing judgment would be "automated negotiation."[166] Examples of automated

negotiation include "double-blind bidding" to narrow and reach agreement on dollar

settlement amounts[167], or "negotiation support systems … that assist[] negotiating

parties in determining their own interests as well as reaching a mutually accepted

resolution that maximizes joint gain for all parties."[168]

Notably absent from these design concepts is the lawyer. Truly efficient and

affordable dispute resolution systems should strive to eliminate the necessity of hiring

---

[166] *See* Rabinovich-Einy and Ethan Katsh, Lessons from Online Dispute Resolution for Dispute Systems Design, Online Dispute Resolution: Theory and Practice, 1-24 (Mohamed Abdel Wahab, Daniel Rainey & Ethan Katsh, eds.) (2011) at 53.

[167] More specifically, "a claimant and defendant each submit the lowest and highest settlement figures that are acceptable to them. They do not disclose the amounts but if the two ranges overlap, a settlement can be suggested by the system, the final figure often being split down the middle. This type of automated negotiation is used when liability between parties is agreed but there is dispute over the amount due." Susskind at 139.

[168] Orna Rabinovich-Einy and Ethan Katsh, Lessons from Online Dispute Resolution for Dispute Systems Design, Online Dispute Resolution: Theory and Practice, 1-24 (Mohamed Abdel Wahab, Daniel Rainey & Ethan Katsh, eds.) (2011) at 53.

and paying for attorneys. ₿DR should seek to simplify and streamline conflict

resolution, empowering individuals to advocate for their own rights, thereby leveling the

playing field an providing greater access to justice for all, not just those who can afford

it. That's not to say that in some situations or complex matters attorneys won't be

needed, but they should be the exception, and not the rule.

The foregoing architecture and best practices provide a starting point for a fully

voluntary dispute resolution system anchored into the Bitcoin economy. In Part IV,

concerns and trade-offs will be discussed.

V.   PROBLEMS AND TRADE-OFFS.

CONFIDENTIALITY V. TRANSPARENCY

₿DR systems will need to determine the appropriate tradeoff between

confidentiality and privacy on the one hand, and transparency on the other. FediMint, in

particular, and Bitcoin, more generally, is designed to preserve as much privacy as

possible for individuals. Traditional ADR and ODR systems are likewise built from a

starting point of confidentiality. But critics of private ADR and ODR systems have rightly

pointed out that "public airing of disputes was crucial for ensuring norm development,

equality, accountability and quality control, and democracy."[169]

---

[169] Rabinovich-Einy at Tsur at 532 ("In addition, as described below, ADR processes are typically confidential and rarely made public. Therefore, it seems adverse to the essence of ADR to send signals through outcomes. In other words, the general understanding is that we cannot expect norm-generation in individualized processes applied ad hoc for the resolution of disputes. Additionally, we cannot expect other users of these processes to know about these outcomes and modify their behavior and expectations where resolutions are kept private.").

Indeed, the ODR design experts Orna Rabinovich-Einy and Ethan Katsch have

expressly identified this tension between confidentiality and transparency in the

"blockchain" dispute resolution context:

> [I]n dispute resolution, knowing the identity of the parties to the dispute is
> often important for establishing trust, for understanding the context of the
> dispute and its roots, for devising an appropriate resolution, and for ensuring
> effective execution. At the same time, blockchain is attractive to many
> because of the ability to remain anonymous while securing the transaction.
> While this is not an insurmountable challenge, it nonetheless presents a
> challenge for the design of effective systems of dispute resolution.[170]

Moreover, transparency in outcomes is necessary to establish common law

precedent and ensure consistency in decision-making, as demonstrated by Benoam's

reporting and landmark decision system. Providing a database of reported outcomes

allows the disputants to determine "whether the outcome is in line with outcomes

offered to other" disputants in similar situations.[171] Outcome transparency enables

users "to see inside the black box, which demystifies the process and makes them

While these concerns are real, and any BDR design will need to address them,

FediMint may be able to strike the appropriate balance between transparency and

confidentiality because it is built on cryptographic technology that allows some details

about federation users to be known without disclosing their full identity. Indeed, even

without such advanced technological solutions, Benoam was able to report decisions by

---

[170] Orna Rabinovich-Einy & Ethan Katsch, *Blockchain and the Inevitability of Disputes: The Role for Online Dispute Resolution*, 2019 J. Disp. Resol. 47, 73 (2019).

[171] Rule & Wilson at 116.

redacting sensitive or identifying information of the disputants. Similar reporting

systems could be established for ḄDR.

CHOOSING THE DECISION-MAKERS.

Great care must be given to choosing the ultimate decision-maker(s). This paper

explored various examples ranging from expert, professional arbitrators, to community-

member jurors, to random, anonymous jurors-for-hire.

Professional, expert arbitrators will increase the cost of any ḄDR system, as

arbitrator fees will necessarily need to be sufficient to attract capable and competent

neutrals. For resolution of complex matters, or matters of first impression in interpreting

a new type of agreement or governance structure, such legal acumen could be

necessary. For resolution of low-value, simple recurring disputes, which will make up

the majority of disputes[172], such expertise is not needed and may be cost prohibitive.

Indeed, studies have shown that "parties seem to settle as often whether or not their

mediator had expertise in the field of law at issue and have no different perceptions of

the fairness or benefit of the process depending on this expertise by the mediator."[173]

Crowdsourced juror systems, however, also have their drawbacks, as discussed

above, including misaligned incentives and lack of grounding on which to rule. These

flaws could be mitigated through appropriate juror educational materials (jury

---

[172] Susskind reports that "from 2008 to 2009," in the civil courts of England and Wales, "eighteen life events were identified as consuming the lion's share of the work of the civil courts." Susskind at 157.

[173] DESIGNING SYSTEMS at 154 (citing Pearson, Jessica, and Nancy Thoennes (1988) "Divorce Mediation Research Results;' in Jay Folberg and Ann L. Milne eds., DIVORCE MEDIATION: THEORY AND PRACTICE 429, 434–36, 450 New York: Guilford Press).

instructions) and decision-making tools (verdict forms) that are populated based on the diagnostic wizard results, and which incorporate the relevant communities' laws, contractual provisions, or norms. The ḄDR designers must ensure accurate statements of relevant contractual provisions or laws, however, and should always seek to include community members in the design process for this reason.

Ultimately, ḄDR systems could strike the balance between expertise and cost by providing a sliding scale of decision-makers, based on the amount in controversy or level of complexity, as determined by a diagnostic wizard or agreed upon by the parties.

V.   CONCLUSION.

The goal of this paper was to begin the discussion on ḄDR and introduce the framework. The work of realizing this idea lies ahead for the attorneys, judges, activists, freedom fighters, community organizers and leaders, software developers, and cypherpunks intent on separating justice from the state's monopoly on violence, and spreading the rule of law across the globe on the most decentralized and censorship resistant communications network ever created.