Markus Oermann and Nils Tollner

NOC INTERNET GOVERNANCE CASE STUDIES SERIES: THE EVOLUTION OF GOVERNANCE STRUCTURE IN CRYPTOCURRENCIES AND THE EMERGENCE OF CODE-BASED ARBITRATION IN BITCOIN

January 15, 2014
Hans-Bredow Institute for Media Research

WITHIN THE

GLOBAL NETWORK OF **INTERNET AND SOCIETY** RESEARCH CENTERS

NoC Internet Governance Case Studies Series: The Evolution of Governance Structure in Cryptocurrencies and the Emergence of Code-Based Arbitration in Bitcoin

Markus Oermann and Nils Töllner
Hans-Bredow Institute for Media Research

Editorial Note: Context, Character, and Purpose of the Case Study

This case study is part of a globally coordinated, independent academic research pilot project by the Global Network of Interdisciplinary Internet & Society Research Centers (NoC). Facilitated by the Berkman Center for Internet & Society at Harvard University, this study examines existing multistakeholder governance groups with the goal of informing the future evolution of the Internet governance ecosystem. Building upon the NETmundial Principles and Roadmap, it contributes to current policy debates at the international level, including the Internet Governance Forum, the NETmundial Initiative, and other organizations and efforts.

Internet governance is an increasingly complex concept that operates at multiple levels and in different dimensions, making it necessary to have a better understanding of both how multistakeholder governance groups operate and how they best achieve their goals. With this need in mind, at a point where the future of Internet governance is being re-envisioned, colleagues from several NoC institutions around the world have written twelve case studies examining a geographically and topically diverse set of local, national, and international governance models, components, and mechanisms from within and outside of the sphere of Internet governance. Key findings from these cases are summarized in a synthesis paper, which aims to deepen our understanding of the formation, operation, and critical success factors of governance groups and even challenge conventional thinking.

The research, based on twelve case studies, suggests that there is no single best-fit model for multistakeholder governance groups that can be applied in all situations. Rather, it reveals a range of approaches, mechanisms, and tools available for both the formation and operation of such groups. The analysis demonstrates that the success of governance groups depends to a large degree on the careful selection, deployment, and management of suitable instruments from this "toolbox." As governance groups pass through different phases of operation, conveners and facilitators must remain alert to changes in circumstances that necessitate adjustments to the approaches, mechanisms, and tools that they deploy in order to address evolving challenges from inside and outside. This case study provides insights into how those instruments can be deployed and adjusted over time within such groups, and highlights how their interactions with important contextual factors may be successfully managed within given resource restraints.

The research effort is grounded in a diversity of global perspectives and collaborative research techniques. Adhering to objective and independent academic standards, it aspires to be useful, actionable, and timely for policymakers and stakeholders. More broadly, the Network of Centers seeks to contribute to a more generalized vision and longer-term strategy for academia regarding its roles in research, facilitation and convening, and education in and communication about the Internet age.

For additional information on the initiative, please contact Urs Gasser, Berkman Center for Internet & Society, at ugasser@cyber.law.harvard.edu.

Abstract: This case study describes the process by which Bitcoin revised its core code to accommodate a new feature called "multi-signature transactions." Bitcoin is a cryptocurrency, which was introduced in 2009 and has spread rapidly since then. It is based on open-source peer-to-peer software that establishes a network of user accounts (wallets) in which the units of account (bitcoins) are produced and transmitted. It is a goal of cryptocurrencies in general to operate without a central agent, which makes it complicated to resolve disputes. To address this, Bitcoin added multi-signature transactions. This case study examines how that change was made. In particular the case study explores how an open source community is able to maintain a stable codebase that can serve as a basis for an entire form of currency, while still making necessary changes. The case shows that the decision-making processes regarding transformations of Bitcoin's governance structure are not as transparent as one might expect given the cryptocurrency's commitment to open source. However, major changes to the code are publicly discussed in the Bitcoin developers' community and the authors could not identify a single case of a decision in which the core development team deviated from the consensus of the community.

Table of Contents

I. Values and Functions

A. Mission and Function

1. The Case: Emergence of Code-Based Arbitration in Bitcoin

When talking about the future of e-business, discussions often touch on the rapid spread of e-currencies or cryptocurrencies over the last five years. In that short period of time, Bitcoin quickly gained prominence as the most well known example of this new means of payment. No longer just a niche technical proof-of-concept, these new payment systems can be used to buy a Dell computer or donate to the Wikimedia Foundation, among other things.[1] For that reason, it is not unreasonable to say that they have become a real alternative to traditional "offline" currencies like the U.S. dollar, yen, or euro.

The rise of these cryptocurrencies has lent new urgency to the classic question of how to handle business conflicts. Due to some of the special conceptual and technological features that set them apart from traditional currencies, managing conflict can be a tricky matter when deals utilize cryptocurrencies instead of traditional currencies.

Bitcoin, which was introduced in 2009 and has spread rapidly since then, is based on open-source peer-to-peer software that leverages a network of user accounts (wallets) set up on peripheral sites in which the units of account (Bitcoins) may be stored after they are produced and transmitted. A public ledger (the blockchain) plays a central role in this system, tracking every transaction in which Bitcoins are exchanged while maintaining the anonymity of the users behind the exchange through public key cryptography. Because it is very hard to connect the public keys used to announce exchanges to the associated private keys used to verify them, the parties of a transaction are essentially anonymous.[2] As the ledger is distributed among all the users in the network,[3] no central administrator or repository is needed to run the system.

There are two ways to obtain Bitcoins. First, users can gain Bitcoins through "mining." Due to the cryptographic nature of the system and the complex algorithms underlying it, verifying a Bitcoin payment and recording it in the ledger requires massive amounts of processing power. Users can provide computing power to the network to verify payment transactions, and in exchange they awarded a proportionate amount of new Bitcoins, a process called mining. In other words, new Bitcoins are produced as a by-product of payment processing and given to the users who helped process that transaction. Given that the number of possible Bitcoins has been limited to 21 million by the software protocol, the stock of potential new Bitcoins gets smaller with every Bitcoin created and released into the system. The algorithm is designed so that the processing power required to mine a new Bitcoin increases with every new user entering the network, making new Bitcoins harder to create. Accordingly, the second way to get Bitcoins is

[1] *Cf.* http://en.community.dell.com/dell-blogs/direct2dell/b/direct2dell/archive/2014/07/18/we-re-now-accepting-bitcoin-on-dell-com.aspx (retrieved from September 10, 2014); http://blog.wikimedia.org/2014/07/30/wikimedia-foundation-now-accepts-bitcoin/ (retrieved September 10, 2014).

[2] Problems of this privacy concept by pseudonymity are addressed by actual research, cf. e.g. Biryukov/Khovratovich/Pustogarov (2014): Deanonymisation of clients in Bitcoin P2P network, http://arxiv.org/pdf/1405.7418.pdf.

[3] As long as using the original client, every user stores a copy of it on her device, within her wallet.

through trade. The typical way a new user obtains her first Bitcoins is by changing an offline currency into Bitcoins via a dedicated trading platform.[4]

Bitcoin has been widely criticized for its technological implementation, its potential for abuse in illegal online platforms like the anonymous black market site the Silk Road, and for the volatility of the Bitcoin market.[5] This paper will not further discuss these criticisms nor develop its own line of reasoning regarding those arguments. This paper instead aims to examine the governance structures supporting the technical development of Bitcoin.

Before considering Bitcoin's governance structure, it is important to understand a goal central to cryptocurrencies in general, and Bitcoin in particular: these systems should work without a central agent in charge of enabling the payments and upon whose integrity and responsibility the system relies. Or, as Satoshi Nakamoto, the person who first proposed the concept of Bitcoin in a whitepaper in 2008, so aptly put it:

> "The root problem with conventional currency is all the trust that's required to make it work. The central bank must be trusted not to debase the currency, but the history of fiat currencies is full of breaches of that trust. Banks must be trusted to hold our money and transfer it electronically, but they lend it out in waves of credit bubbles with barely a fraction in reserve. We have to trust them with our privacy, trust them not to let identity thieves drain our accounts. Their massive overhead costs make micropayments impossible. (...) With e-currency based on cryptographic proof, without the need to trust a third party middleman, money can be secure and transactions effortless."[6]

Eliminating the middleman, however, creates some challenges for Bitcoin and other cryptocurrencies. Without trusting a middleman, traditional avenues for business dispute resolution no longer work because the common enforcement "infrastructures" (e.g., state courts or private courts of arbitration) cannot direct an intermediary, like banks or credit card companies, to reverse the payment. Instead of relying on intermediaries, Bitcoin's design transfers all the control over a transaction to the network itself. When a user wants to make a payment, she uses the recipient's public key as a substitute for a bank account number and then initiates the transaction by signing off on it with her own private key. The recipient then accepts the transaction by signing using his private key.[7] Undoing a transaction works similarly, making it impossible for an institution outside the system to revert a payment without the participation of the parties to the transaction.

Business transactions based on cryptocurrencies can result in conflict, just like business deals using any other currency. Imagine the purchase of a certain good, where the seller and buyer

---

[4] *Cf.* https://en.wikipedia.org/wiki/Bitcoin (retrieved September 10, 2014).

[5] *Cf.* Simonite, Tom (2013): Silk Road Bust Could Slow Bitcoin Economy, http://www.technologyreview.com/view/519846/silk-road-bust-could-slow-bitcoin-economy/ (retrieved from September 10, 2014); Quiggin, John (2013): The Bitcoin Bubble and a Bad Hypothesis, http://nationalinterest.org/commentary/the-bitcoin-bubble-bad-hypothesis-8353 (retrieved from September 10, 2014); Matthew Sparkes, "Software activist calls for 'truly anonymous' Bitcoins to 'protect democracy'," *The Telegraph (UK)*, December 2, 2013, http://www.telegraph.co.uk/technology/news/10488201/Software-activist-calls-for-truly-anonymous-Bitcoins-to-protect-democracy.html.

[6] Satoshi Nakamoto: *Bitcoin open source implementation of P2P currency*. 02-11-2009. http://p2pfoundation.ning.com/forum/topics/bitcoin-open-source (retrieved September 10, 2014).

[7] *Cf.* https://bitcoin.org/en/how-it-works (retrieved September 10, 2014).

disagree on its quality. The buyer is claiming deficiency, and the two sides seek to resolve the dispute, but neither party may want to involve official public institutions.[8] How could this conflict be dealt with and resolved if the parties are unable to find a solution through negotiation alone?

Beginning in late 2013, a feature of the Bitcoin protocol offered a solution to this challenge: "multi-signature" transactions. Every Bitcoin transaction is defined in a script, which sets conditions on how a subsequent user can access the coins. Because these rules are defined in code, they can be adjusted. One adjustment is setting a minimum number of parties required to sign off on any given transaction. In a standard two-party deal, for instance, the script can define that the signatures of two out of three users are needed to complete the transaction. This enables the two primary parties to a deal (a buyer and seller) to name a third user as an arbitrator in case of conflict. Where there is no disagreement, the parties can process the payment on their own, and the arbitrator cannot hinder it. But in case of a conflict, one side can refuse to sign the payment and invoke the arbitrator. The arbitrator can resolve the conflict and enforce her ruling by signing off of the transaction or not.[9] The feature of multi-signature transactions was actually included in the software protocol as a standard option in 2011-2012, but users largely ignored it because there was no representation in the graphical user interface until late 2013.[10] Once the feature gained prominence, sites such as https://www.bitrated.com emerged as platforms for parties to find independent arbitrators. A wide variety of people offer themselves on these platforms to be commissioned to act as arbitrators.[11]

This paper takes a deeper look at this change in Bitcoin's architecture. In our view, this is an interesting example of a structural evolution of a cryptocurrency system that we will analyze from a governance perspective.

When thinking about governance, we can examine phenomena of emergence, application and effects of collective norms and rules from at least three different angles. Which individual and collective actors form the governance group?[12] Based on the answer to this question we can take a look at how the power of influencing the normative content of the rules and their social realization is distributed among these actors. With an emphasis on processes, we can analyze if and how the production and stabilization of certain rule sets form new institutions and how these rule sets influence social reality by coordinating behavior. And third, we can focus on the norms and rule sets and analyze, across the factors of governance, which normative meanings they contain, and how the governance structure formed by them is configured.

---

[8] In fact, the Bitcoin Foundation recently published a primer for Bitcoin users on the basic legal requirements that cause a Bitcoin deal to activate a certain jurisdiction—and how to avoid this, *cf.* McFarlan, Robert A. (2014): *A Bitcoin Primer on Jurisdiction*. https://bitcoinfoundation.org/wp-content/uploads/2014/08/Bitcoin-Jurisdiction-Primer.pdf (retrieved from September 10, 2014).

[9] Dourado, Eli (2014): Stop Saying Bitcoin Transactions Aren't Reversible. http://elidourado.com/blog/bitcoin-arbitration/ (retrieved from September 10, 2014).

[10] *Cf.* https://github.com/bitcoin/bips/blob/master/bip-0011.mediawiki (retrieved September 10, 2014); https://github.com/bitcoin/bips/blob/master/bip-0019.mediawiki (retrieved September 10, 2014).

[11] More than 240 organizations or private persons offered to serve as arbitrators on bitrated.com in late September 2014.

[12] "Governance group" refers to the social formation that produces, establishes, and applies the norms and rules in this context.

This structural perspective supplies us with basic insights that lay the groundwork for the analysis from the other perspectives. We will start by clarifying the values and functions related to the change in Bitcoin's governance structure (**A.1.2**). Based on these reflections, we will shift our analytical focus to the governance group itself: what is its organizational model and structure? (**B.**). Then we will discuss from a procedural angle how actors could participate as members of this group (**C.**) and consider how decisions of and in the group are made (**D.**). In section **E.** we sum up the outcomes of our analysis and present the key lessons and takeaways from this case study.

2. A Heuristic Model of Governance Factors in Online Services

It is useful to consider the governance of Bitcoin using a heuristic model of governance factors impacting user behavior in online services in general. This model differentiates between the components of code, state law, contracts and social norms.[13]

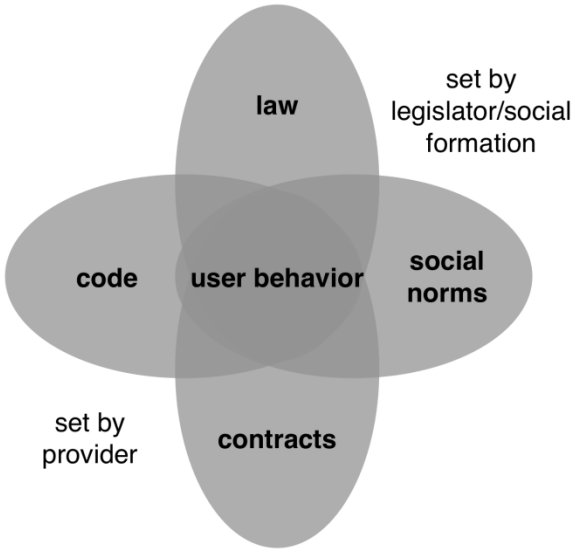

Figure 1. *Oermann/Lose/Schmidt/Johnsen (2014), note 12: fig. 1, p. 18.*

"Social norms" in this heuristic refer to all of those rules emerging from general tacit conventions in a society or norm sets developed by and applied in a specific social formation, such as the community of users of a certain online service. We sometimes find these norms codified as codes of conduct or (n)etiquette. These social norms are both established and executed by the social formation, which reacts to violations with social sanctions. In contrast, "state law" contains provisions for user behavior in online services stipulated by the state in

[13] Deviating from Lessig's model we do take the "market" into account as a factor of governance because a "market" lacks in itself a normative dimension from our point of view. Saying that "markets" are comparable to law and code analytically could lead to misunderstandings because it could invite comparisons between the "natural laws" of markets of macroeconomic theory and the "designed" norms of law and code. We think that it is more fruitful, therefore, to look at social norms, which function as a transmitter of normative predictions which have been associated with "markets" when approaching governance in online services on a structural level. For a more detailed explanation of this argument, *cf.* Oermann, Markus/Lose, Martin/Schmidt, Jan/Johnsen, Katharina (2014): Approaching Social Media Governance. Berlin, HIIG Discussion Paper Series, (May 2014), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2498552 (retrieved September 10, 2014).

codified legal norms, which are enforced by state institutions like courts and public authorities. "Contracts" in the case of online services are found mostly in the form of Terms of Service (TOS) and are for the most part laid down unilaterally by the service providers and executed through mechanisms like content removal.

While the above three forces on user behavior are fairly self-explanatory, the concept of "code" in this model is less clear. Harvard Professor Lawrence Lessig applied this concept to online user behavior in 1999 with his famous analogy "code is law."[14] However, there still is no widely shared understanding of what is meant when we talk about "code" in the normative context of governance. Surely it is not just software source code, because software requires hardware in order to shape user experience. So we have to take the aspect of hardware into account, too. Furthermore, the source code alone does not help us understand how certain technology is used, nor does it explain the effect that technology will have on user behavior on a structural level. But we can look at the interfaces of technology and human behavior in order to analyze the affordances that the code (hardware and software) offers the user and the constraints it sets to them.[15] For our purposes, therefore, we refer to code as all the normative aspects of a certain technology, which encompasses more than simply source code.

So far we have established that all four concepts introduced above share a common quality: they constrain and shape user behavior. These predictions differ in their normative strength. If social norms, law, contracts or code provide the addressee with several possibilities for action ("If x is the case, you can do a, b, or c…"), they can be said to have minor normative strength. On the other hand, if they prescribe just a single course of action ("If x is the case, you must do y."), they have maximum normative strength. Of course, all gradations of normative strength are also possible for each of the four factors. The four concepts also differ concerning the consequences in case of deviating behavior. If we look at phenomena of human interaction in online services, we will always find a complex structured normative background formed by these factors, on which the application potential of the services are realized by the users and on which their behavior is coordinated. This is what we call the governance structure.[16]

If we now consider Bitcoin in light of this model, we see that this cryptocurrency is conceptualized in a way that three of the above factors should and actually do just play a minor role in its governance structure—at least as far as this is possible without endangering the functionality of Bitcoin as a means of payment:

- There should be no influence of law: Control by the state on payments, transactions and the underlying business deals should be prevented;
- Social norms should be also prevented from having an influence on the behavior of Bitcoin users, at least as far as they concern trust in the institutions that act as the

[14] Lessig, L. (1999): Code and Other Laws of Cyberspace. New York, U.S; Lessig, L. (2006): Code: And Other Laws of Cyberspace, Version 2.0. New York, U.S.
[15] Oermann, Markus/Ziebarth, Lennart (2015): Use of Cultural Artifacts by Way of Interpretation and Application—or: Adapting the Methodology to Analyze the Normative Contents of Law for the Analysis of Technology. *Computer Law and Security Review*, vol. 32(1) (forthcoming).
[16] *Cf.* Oermann, Lose, Schmidt, and Johnsen (2014), supra note 12, at 8-17.

conduits for offline currencies. Bitcoin is designed to prevent any connection to the traditional, regulated financial system;[17]

- And, because there is no central administrator in the system or any TOS that users have to accept, contracts are also not essential to governing how people use Bitcoin as a means of payment.[18]

So we can conclude that, owing to conceptual reasons, the central factor in Bitcoin's governance structure is code. The primary way to govern user behavior and tackle practical challenges resulting from its conceptual shortcomings, therefore, is to adjust the code of Bitcoin.

The introduction of "multi-signature" transactions, through which an automated arbitration mechanism can be realized in the Bitcoin architecture, represents a prominent and interesting case of such an adjustment by a change of code. Bitcoin is a complex, decentralized technological system offering advanced network-based services that was able to adapt to a conceptual challenge through activating its own governance structure, and in the process creating a structure for resolving conflicts with deals and transactions.

With these reflections on the mission and function of the change of Bitcoin's architecture in mind, we will now change our perspective to focus on the governance structure of Bitcoin, which enabled this change to take place.

II. Organizational Model and Structure

A. Overarching Structure

In order to grasp how this architectural change was implemented, we must take a closer look at how adjustments in the Bitcoin ecosystem can be accomplished in general. We have seen that Bitcoin's primary mode of influencing behavior is through code, so the leading questions are: Which actors make up the governance group that decides on changes of the code? And what is the internal structure of the group?

As described above, we adopt a broader definition of "code" than simply source code. That said, hardware is of no importance to the arbitration functionality in Bitcoin's system code; the new features are enabled purely by software. Thus, we can narrow our focus to the actors involved in the development of the software used by Bitcoin users.

While there are several Bitcoin clients that provide end users with "wallets" on different operating systems and devices,[19] the Bitcoin core client ("original client") is the central software in the currency's ecosystem. Since nearly all crucial functionalities of the network are provided

[17] Certainly there are general social norms on how to process business deals and there are also special social norms concerning the "right" ways of using Bitcoin evolving in its user community. Both of these affect user behavior, but the concept of Bitcoin does not rely on these elements to fulfill a central function in its system. *Cf.* https://bitcoin.org/en/developer-guide#contracts (retrieved September 10, 2014).

[18] We have to distinguish these from the contracts that are concluded between Bitcoin users to process the underlying business deals. These business contracts include reciprocal provisions for user behavior, e.g. that a user has to initiate the transaction of bitcoins when he received the good he purchased. But the original concept of Bitcoin did not cover these contracts, which meant that enforcement mechanisms in case of a breach have been missing.

[19] *Cf.* https://bitcoin.org/en/choose-your-wallet (retrieved September 10, 2014).

and processed by machines running the core client, other clients have to be designed in compliance with the core client's source code.[20] For that reason, the original client forms not only the software backbone of the network, but in a sense also the blueprint for other implementations: all other clients are descendants from that original client. Whoever wants to change Bitcoin's code must change the code of the original client. We can therefore focus on the governance group around the Bitcoin core client.

As mentioned above, the Bitcoin core client is open-source software.[21] Simply put, this means software whose source code is open and accessible to the public, mostly via special online platforms like GitHub, sourcefourge.org, or code.google.com. By providing the technological means to organize open-source software development, these platforms form a dominantly code-based governance structure for that process. They can be understood as a meta-structure influencing the governance group of the Bitcoin core client and its processes of participation.

B. Participation

1. Primary Categories of Participation

Open source software often comes with certain inherent expectations regarding participation.[22] Someone wishing to launch a software project on any open-source platform starts by uploading and publicly hosting the initial source code on a repository. Other developers can then subscribe to that repository and submit new source code as suggestions for improvement. The developer in charge of a project's code repository has full control over the changes to the source code because she can decide which suggestions are accepted as official modifications. Sometimes, a group of users manages the repository instead of an individual.

Additionally, these platforms provide revision control features, which track every change in the source code so that they can be reverted, if necessary. In fact, these version control systems are central tools in (collaborative) software development in general, in open- source and proprietary contexts alike. The technical interaction between these platforms and their users is strongly influenced by the use of revision control software. The platforms provide teams with a central storage for the source code while publishing it at the same time. Some platforms also offer social networking functions that enable users to stay up-to-date and discuss and review changes to the code. In this way, these platforms help manage projects and organize the collaborative workflow and, in a sense, determine the primary categories of participation.

Bitcoin's main client is hosted on GitHub,[23] a popular open-source platform. All changes to Bitcoin's source code are organized through GitHub. The (social) interaction on that platform is

[20] Alternative nodes must "follow the reference client 100% (bug for bug)," https://en.bitcoin.it/wiki/Category:Nodes (retrieved September 10, 2014).
[21] *Cf.* https://bitcoin.org/en/developer-documentation and http://opensource.org/licenses/mit-license.php (retrieved September 10, 2014).
[22] *Cf.* http://opensource.org/docs/osd (retrieved September 10, 2014). The approaches may differ among the several software projects more or less, but it is beyond the scope of this paper to discuss those similarities and slight variances within the open-source scene. Many statements in this section might be characteristic for open-source software and others not. Our goal is only to conceive an idea—how the distributed governance group behind Bitcoin is formed—while having in mind that it is a distinctive example of open-source programming.
[23] https://github.com/bitcoin/bitcoin (retrieved September 10, 2014). The source code of the website "bitcoin.org" is also stored and maintained via GitHub.

where the refinement of the code can best be observed and is therefore a good starting point to examine the governance group behind Bitcoin.

On GitHub, registered users can work on the code repositories that belong to their accounts and make use of the described features like version control. Users can also work on the source code together with others by adding collaborators to a repository. Furthermore, GitHub offers its users the ability to start and join organizations, which are the "owners" of the project's code repositories. Members of an organization can be structured in teams and granted different levels of permission:

- Administrators can add new or remove members of the organization.
- Ordinary members may revise the code in the repositories.[24]
- Users who are not part of the organization can submit code proposals.[25]

Bitcoin is one organization on GitHub. The source code of the core client and several other repositories are managed through this organization structure. In this structure, we can observe three different categories of participation: administrators of Bitcoin's organization on GitHub; members of the organization on GitHub, who consider themselves part of the Bitcoin development team;[26] and non-members who submit their code proposals to members. This means, in essence, that anyone with the ability to program and the will to participate could be seen as an aspirant for membership of the governance group. Because any person could submit snippets of new source code to the organization, anyone could, in theory, influence the governance structure of Bitcoin.

Nevertheless, in the end, decisions are made—or executed at least—by a team of core developers because only they have the technical permissions to accept submissions. Those core developers form, at least at first sight, Bitcoin's governance group in a narrower sense. Every adjustment to Bitcoin's governance structure must pass through the bottleneck of this small group of people. So let us take a closer look at how this group is composed.

C. Membership Structure

According to the Bitcoin page on GitHub, 247 people have contributed to the original client,[27] but only seven members in the organization are currently listed as core developers.[28] As has been mentioned above, a contributor only has to create an account on the GitHub platform to be able to submit code proposals for the core client or to make use of social networking features like commenting on others' changes to the code. Becoming a member of an organization is not quite as simple: the owner or an administrator of the organization must add the user.

[24] https://help.github.com/articles/permission-levels-for-an-organization-repository (retrieved September 10, 2014). So the main task of an organization's members is to work on the development of the code in their repositories or to decide whether code proposals of other GitHub users become part of the project or not.

[25] This procedure is called "submitting a pull request," because the maintainer of the source code is supposed to "pull" the proposals into the current development line.

[26] https://github.com/bitcoin/bitcoin (retrieved September 10, 2014).

[27] https://github.com/bitcoin/bitcoin (retrieved September 10, 2014); https://bitcoin.org/en/development (retrieved September 10, 2014).

[28] https://github.com/orgs/bitcoin/people (retrieved September 10, 2014).

It is not clear who exactly has this central membership authority in the case of Bitcoin. Gavin Andresen, Chief Scientist at the Bitcoin Foundation, is listed as "Project Lead" on several Bitcoin-related Internet pages.[29] But we can only guess at the actual roles, teams, and competencies of the other Bitcoin core developers because we could not locate additional publicly accessible information.[30]

Nor we did find any evidence for institutionalized rules of entry or exit laid down for this governance group. One of the core developers was cited on a news page about Bitcoin calling the development team a "meritocracy."[31] This metaphor is an interesting self-description: it points to the fact that people are judged by their merits in the Bitcoin community. It seems fair to assume, then, that current core developers ask an ordinary member to join the core team if this user has made numerous valuable contributions over a certain period of time.

The metaphor of a meritocracy also helps us understand how the group determines what code submissions are approved. As noted above, members must approve code submissions. Generally, developers copy the whole code into their own personal accounts, work on it, and finally submit a request for the organization to add the code proposal into the repository. The request appears on Bitcoin's GitHub development page so that anyone can review and comment on it. Eventually, another core developer closes the request or pulls it into the development code line. Our analysis of recent code changes to the Bitcoin client shows that trivial code proposals (i.e., small bug-fixes) are pulled into the code without further discussion. In contrast, non-trivial changes must achieve consensus before they are adopted.[32] Core developers give themselves leeway regarding the question of what is trivial and what is not. Core developers submit their own code changes using the same processes of participation; in many cases the core developers open their own proposals to public debate before pulling them into the main development line.

D. Mechanisms for Participation

The most common avenue for participation is revising the source code, as described above. As we have seen, both ordinary and core contributors can propose new source code, which will either be accepted or rejected based on public discussion.

In addition, there is a mechanism of participation for proposals of new features on a conceptual level: the "Bitcoin Improvement Proposal" (BIP). BIPs are essentially concept papers on potential new functionalities in the Bitcoin software. In most cases these new functionalities require more sophisticated changes or additions to the source code than smaller features or bug fixes. Therefore, a BIP consists of technical details about the proposed feature and different kinds of meta-information like the author's name and the status of the document. All submitted BIPs are listed in a repository on GitHub as well as on the Bitcoin Foundation's wiki site.[33]

---

[29] *Cf.* https://bitcointalk.org/index.php?topic=7269.0 (retrieved September 10, 2014).
[30] To unveil the distribution of power in this Governance Group would need further research based on methods like discourse analysis or network analysis.
[31] http://www.coindesk.com/bitcoin-developer-jeff-garzik-on-satoshi-nakamoto-and-the-future-of-bitcoin/ (retrieved September 10, 2014).
[32] https://github.com/bitcoin/bitcoin/blob/master/README.md (retrieved September 10, 2014).
[33] https://github.com/bitcoin/bips/blob/master/README.mediawiki (retrieved September 10, 2014); https://en.bitcoin.it/wiki/Bitcoin_Improvement_Proposals (retrieved September 10, 2014).

If a developer wants to add a new feature to the Bitcoin software, she can author a specification draft. This document must then be sent to the developer mailing list, to which the development community subscribes. After discussion on the mailing list, the draft is added to the list of BIPs if a majority accepts the listing of the proposal. BIPs thus allow substantive debate on the changes in the protocol even before developers put any effort into programming source code. Furthermore, people without the will or the ability to program are able to take part in the discussion on the further evolution of Bitcoin.[34] If the BIP reaches consensus in the broader public debate on GitHub, a core developer will set its status to "active,"[35] and a code contributor can start to write an implementation. This implementation draft can then be submitted as an ordinary source code pull request using the participation process described above.

Jeff Garzik, a core developer of Bitcoin, made an insightful remark about the dynamics of the two mechanisms of participation. He told a news website that the Bitcoin community considered itself very conservative when it comes to new functionalities. The core developers generally did not accept completely new features if these were made as concrete source code proposals. Instead the core development team would always seek to reach a high level of consensus among the Bitcoin community about new functionality.[36] Additionally, the BIPs function as a mechanism for slowing down the process of change.

The development of multi-signature transactions began in the form of two different BIPs.[37] This is not surprising given that multi-signature transactions were a major update to Bitcoin's functionalities. Reviewing the discussions around those BIPs in the mailing list archives, we found several threads already discussing the details of these proposals.[38] Interestingly, a general debate on the pros and cons of this new functionality never came up, at least as far as we could see. A possible explanation for this is that the community had already recognized the necessity of such a feature. In the end, the BIP process helped to confirm consensus on the functionality and establish consensus on side issues of how to implement the arbitration mechanism in the Bitcoin system.

E. Decision-Making Structures

1. Decision Makers

[34] Aside from GitHub's communication features, a large online community interested in Bitcoin and its development utilizes various common online communication tools like wikis, forums, IRC-chats or mailing lists. Debates on new features could therefore also take place with the involvement of other stakeholders in the Bitcoin ecosystem like the miners, the users, etc.
[35] *Cf.* supra note 34.
[36] Bradbury, Danny (2013): Bitcoin developer Jeff Garzik on Satoshi Nakamoto and the future of Bitcoin, http://www.coindesk.com/bitcoin-developer-jeff-garzik-on-satoshi-nakamoto-and-the-future-of-bitcoin/ (retrieved September 10, 2014).
[37] https://github.com/bitcoin/bips/blob/master/bip-0010.mediawiki (retrieved September 10, 2014); https://github.com/bitcoin/bips/blob/master/bip-0011.mediawiki(retrieved September 10, 2014).
[38] *Cf.* http://sourceforge.net/p/bitcoin/mailman/message/28374763/ (retrieved September 10, 2014); http://sourceforge.net/p/bitcoin/mailman/message/32614927/ (retrieved September 10, 2014); http://sourceforge.net/p/bitcoin/mailman/message/27842517/ (retrieved September 10, 2014).

As we have seen in sections C and D, decisions of core developers are shaped by the social norms of the Bitcoin development community and by the tools that are used to enable community participation and collaborative development. Consensus in the community is a hard guideline for decisions because this benchmark is strictly enforced as a requirement for implementation of proposals.

It is important to note that the overarching goal among Bitcoin's core developers is to prevent a breakup of the system. Compared with other types of open software projects, this goal is even more fundamental because Bitcoin's success as an alternative means of payment depends on the ubiquity, integrity, and security of the technological infrastructure it provides. It is for this reason that the group is inherently suspicious of new features, and might even reject new features in the face of community support.[39]

To get the entire picture of Bitcoin's governance, we also have to take into account the Bitcoin Foundation. Seven founding members established the Bitcoin Foundation in September 2012.[40] According to its self-description on its website, the foundation serves three main goals: to foster standardization, to protect the integrity of Bitcoin protocol, and to publicly promote Bitcoin.[41] What should be noted regarding our case is that the Bitcoin Foundation now functions as an institutional framework for core developers. Lead Bitcoin developer Gavin Andresen is employed by the foundation as "Chief Scientist" and at least three other core developers are also on the foundation's payroll.[42] This raises the question of whether and how the Foundation might influence Bitcoin's code development.

The founding documents (the Foundation's bylaws) and legal grounding (legal provision by District of Columbia's law) of the Foundation delineate its governance structure. Understanding the interaction between the Foundation and the core developers is challenging to answer just by looking at the founding documents of the Bitcoin Foundation. The Foundation's central decision-making body is its Board of Directors.[43] It has seven seats, which are elected by the members of the foundation. There are three different categories of membership: founding members, industry members, and individual members. The founding members mentioned above elect one seat on the board. Companies offering services and products based on Bitcoin can apply to become industry members, and these members have the right to elect three directors. The last three board members are elected by individual members of the foundation. Individual members "shall be natural persons transacting in, promoting or otherwise contributing to the Bitcoin system or other similar distribute-digital currency system."[44] Individual membership thus is the way for the Bitcoin user community to be represented in the Foundation.

Since there is no public record of the Foundation's decisions, we did not find any evidence that the Board of Directors is influencing the strategic decisions of the core developer team. Yet we

[39] *Cf.* Bradbury (2013), supra note 37: "This notion of consensus doesn't necessarily make Bitcoin a push-button democracy, though; the core developers carry ultimate veto, and they're notoriously cautious."
[40] Bylaws of the Bitcoin Foundation, Sec. 3.2.
https://github.com/pmlaw/The-Bitcoin-Foundation-Legal-Repo/blob/master/Bylaws/Bylaws_of_The_Bitcoin_Foundation.md (retrieved September 10, 2014).
[41] https://bitcoinfoundation.org/about/overview/ (retrieved September 10, 2014).
[42] *Cf.* https://bitcoinfoundation.org/about/overview/ (retrieved September 10, 2014).
[43] *Cf.* Bylaws of the Bitcoin Foundation , Sec. 5.
[44] Bylaws of the Bitcoin Foundation, Sec. 3.2.

assume that there is at least some kind of coordination of decisions because the interests of the industry members are affected by strategic decisions on the technological evolution of Bitcoin.[45] As a core developer, as well as a member of the Foundation's Board of Directors, Gavin Andersen could act as link between them.

Another interesting observation is that the Bitcoin Foundation represents an institutionalized central administrator in a system originally designed as a decentralized network.[46] If additional research were to show that the Bitcoin Foundation is in fact powerful in shaping the evolution of the system, we would have a good reason to ask how the system handles the resulting frictions between conceptual expectations and factual reality.

III. Outcomes

A. Resolution of Problem

The introduction of multi-signature transactions demonstrates the application of Bitcoin's predominantly code-based governance structure. Our analysis of that case showed that the decision-making processes regarding transformations of Bitcoin's architecture are not as transparent as one might expect given the cryptocurrency's commitment to open source. Major changes to the code are publicly discussed in the Bitcoin developers' community and we could not find a single case of a decision in which the core development team deviated from the consensus of the community. But the true nature and extent of the direct and indirect influence of the Bitcoin Foundation and its bodies on current processes is largely unclear.

It is useful to distinguish between two levels of governance structures in online services. On the first level there is the normative background of user behavior and the second level is a meta-structure that frames the processes of structural evolution on the first level (see fig. 2 below).

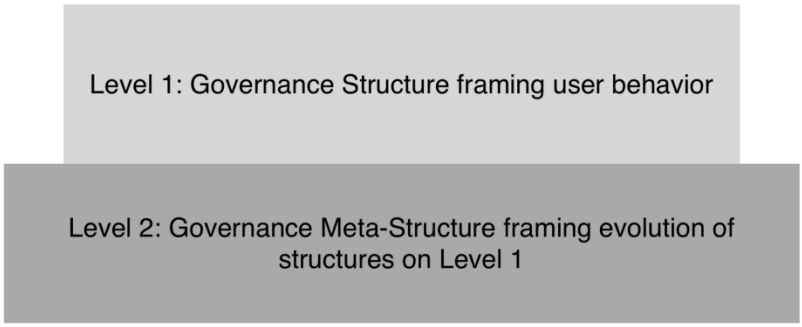

Figure 2.

On an abstract level, we can take the case of Bitcoin's arbitration mechanism as an example of the implementation of a governance (infra)structure that tackles a complex social challenge by offering a means for dispute resolution (level 1). As we have seen, that evolution is shaped by social norms and the code of the platforms on which Bitcoin's source code is maintained and further developed (level 2). Together, these factors form a complex multi-layer structure that

[45] To prove this assumption we would need to use additional methods like participating observation or expert interviews.
[46] *Cf.* Bylaws of the Bitcoin Foundation, Sec. 1.1 and Sec. 2.2.

defines and enables Bitcoin as a payment system. In this regard, Bitcoin might be comparable to other complex open-source technological systems like Linux or Wikipedia. An interesting follow up to this paper would be to analyze whether these projects also have an underlying multi-level governance structure.

B. Best Practices and Templates

The first lesson that we can take away from this case study is that the evolution of governance in open-source online services can be highly dynamic because its underlying code can be changed more easily than, for example, law.

Furthermore, we have seen a case of a decentralized, primarily code-based governance structure (level 2) that was invoked in order to create a code-based governance structure for addressing disputes between users (level 1). It is important to recognize the interactions between the two levels. A first hypothesis derived from this analysis is that an open, code-based governance structure serving such a highly complex social function as providing the normative foundation for a payment system is itself in need of meta-structures on a second level that frame the evolutionary processes of the structures on the first level.

At this point, it is important to clarify that we are not making the argument that political and normative questions are not of importance in such systems that at first glance might seem decentralized. On the contrary, they become even more relevant. In fact, if the normative structures become multi-layered, and more and more complex, questions about power and legitimacy only become more important.

Finally, this case evokes the question of whether code-based dispute resolution systems could be a model for dealing with conflicts in other systems. In terms of governance structures this is certainly possible. Further contemplation of this possibility leads us back to the question on how the meta-structures framing the development processes would have to be configured in these systems to achieve this aim in a transparent and legitimate way. The concept of open source could be a starting point but is not the last word on this question, as our case study has shown.[47] From our perspective, this aspect needs more research. Additionally, analysis of a second evolutionary process for Bitcoin's architecture would help corroborate our findings and assist in determining whether they are generalizable at least within Bitcoin's system.[48]

[47] As far as public interest would be affected by conflicts in this system, rationality of decisions would have to be guaranteed by procedural rules and sets of pertinent criteria.

[48] A promising second case is already in sight: the Bitcoin community is currently discussing whether a deep code change is needed in response to a certain mining cooperative providing for a short period of time over 50% of the system's overall computing power. During this time, the mining group was theoretically able to control all the transactions in Bitcoin. Because antitrust laws are not enforceable, this situation fundamentally challenges the system in a comparable manner to the case of the missing infrastructures for arbitration. *Cf.* http://hackingdistributed.com/p/2014/06/13/in-ghash-bitcoin-trusts/ (retrieved September 10, 2014).