LEDGER
ledgerjournal.org

ISSN 2379-5980 (online)
associated article DOI
10.5915/LEDGER.2016.37

Autonocoin: A Proof-of-Belief Cryptocurrency: Open Review

Authors: Michael Abramowicz*†

Reviewers: Reviewer A, Reviewer B, Reviewer C

Abstract. The final version of the paper "Autonocoin: A Proof-of-Belief Cryptocurrency" can be found in Ledger Vol. 1 (2016) 119-133, DOI 10.5915/LEDGER.2016.37. There were three reviewers, none of whom have requested to waive their anonymity at present, and are thus listed as A, B, and C. After initial review (1A), the author submitted a revised submission and response (1B). The assigned Ledger editor determined that the author had adequately addressed the reviewer concerns and asked the author for minor revisions which were carried out by the author, completing the peer- review process. Author's responses are in bullet form.

1A. Review, Initial Round

Reviewer A:

Overall assessment:

The paper presents the concept of Proof-of-Belief (i.e. a distributed consensus mechanism based on a tacit coordination game that let cryptocurrency owners determine which blockchain they "believe" is the most authorative one) as an alternative mechanism to Proof-of-Work and Proof-of-Stake, which is based on normative judgement instead of algorithmically quantifiable and verifiable actions (e.g. mining).

The paper is well written, clear and well structured and the author shows a good mastery of the subject. The paper provides a thorough description of Tacit coordination games and how they apply in the field of cryptocurrencies, and then explain how Proof-of-Belief could enable the emergence of a completely autonomous and self-governing cryptocurrency (Autonocoin) that relies on tacit coordination games in order to identify authoritative blocks and blockchains, as well as to make more sophisticated decisions such as whether to upgrade the protocol, and to how to reward arbitrary actions that ultimately benefit Autonocoin.

The article is timely and relevant, especially considering the recent governance issues raised

†Michael Abramowicz (abramowicz@law.gwu.edu) is Professor of Law at George Washington University, USA.
*1MioFQjewAb69Kw9rgtCDEQVscbFNLQ8DN

with the Bitcoin scaling problem. The article sets out to explore ways in which a decentralized cryptocurrency can incorporates also a mechanism to update its own protocol, according to what the community considers to be the most relevant. The ability for blockchain-based applications to incorporate an internal mechanism to update or upgrade themselves is really important, and the approach suggested by Abramowicz is an interesting solution in this respect.

Suggestions for improvement:

Part II on "Tacit coordination", though important and interesting, is a bit long and sometimes seems to go out of the scope of the paper. The part could be shortened, especially part II.B which could perhaps be dealt with together in part II.C as only one part. This would leave more space to develop the core of the article, which is about specific implementation of the Proof-of-Belief system as a particular implementation of a tacit coordination game.

Reviewer B:

Summary: I support publication of the article but suggest some clarifications and edits. It may also be helpful to have someone with an expertise in game theory review some parts given how dependent the arguments are on the ability of a formal tacit game coordination game to create a robust and self-governing decisionmaking mechanism.

The article proposes a new cryptocurrency (Autonocoin or the "CC") with a unique governance mechanism that determines what the authoritative code (client software) and version of the blockchain is, as well as how to reward users that have taken actions to benefit the CC. The article uses game theory to justify its conclusions. The consensus mechanism is called proof of belief (POB): "the central idea is that if a controversy develops as to which block chain is authoritative, this can be resolved through a tacit coordination game. Thus, the blockchain that cryptocurrency owners believe is authoritative will be recognized as such...." Emphasis in original.

The intro begins by noting that CCs don't have mechanisms to decide how their software is updated--it is decided by an open source process. The author's CC proposal seeks to make software update decisions autonomous and based on the CC's blockchain transactions. The CC also proposes a new way to distribute coins; that is, by community consensus as to the value of a user's contribution, and not by mining or pre-mining. It is argued that this process operates by means of a formal tacit coordination game that gives users an economic incentive to consider the preferences of others regarding a particular decision. The overall benefit of the CC is that it is completely self-governing.

I think the introduction should also explain POB more and how it relates to the over points of the article

Part II begins with a review of basic game theory; explaining tacit coordination games. This discussion is clear; the examples are helpful including with respect to normative games. It

ISSN 2379-5980 (online)
associated article DOI
10.5915/LEDGER.2016.37

then states that Bitcoin miners agree to accept changes in the code made by those who control the official code's repository and accordingly that this creates a status quo bias and that the process is not truly peer-to-peer. The subsequent argument and explanation supports these points.

Part II also explains how other aspects of Bitcoin operate by tacit coordination on page 3. I think this discussion jumps around a bit and could be more clear. Similarly, the following discussion on pages 3-4 about the normative aspects of Bitcoin's coordination game, the discussion of a CC's design, and other issues seem to be a bit of a digression. They are relevant to the overall paper, but they should be made and proceed in a more deliberate manner. They seem too stream of consciousness.

The remainder of Part II explains formal tacit coordination games and how the CC is built on them. It makes at least a plausible case that the formal game of Autonocoin will produce the type of outcomes the author argues for such as approving changes to code and awarding a quantity of coins.

Part II should link the points being made clearly to POB. Despite being implied in the Intro, I think there are room for links that make the argument more clear, even without first fully explain in POB.

In particular, the two paragraphs beginning with "Autonocoin is built on formal tacit coordination games" on page 5 left column are essential for the argument. They should be summarized more in the Introduction, and probably belongs in some form in Section III because it is discussing the POB consensus mechanism without calling it POB.

Part III is the core of the author's argument--the point being that if a CC can implement or use a formal tacit coordination game to update its software, distribute coins, etc., those aspects become self-managing and robust. III.A discuss POB which attempts to solve "the question of how to determine which "block chain is authoritative among multiple competing block chains" by "allowing decisions on the block chain as to whether any particular block is a valid block that should be on the block chain." This process is a formal tacit coordination game, according to the author. He further explains that the "measure of proof of belief in a particular block is the difference between payments made in support of a block's authenticity and payments made in opposition to a block's authenticity. The measure of proof of belief in a valid block chain (that is, one in which the hash for each block refers to the previous block) is the sum of the proofs of belief for each block." The valid block is that block that has the highest proof of belief measure. This section seems like it could use clarification how the process is different than proof of work in practice, as it seems to have many of the same attributes. Some examples could help as well.

It's great that the author makes clarifications and discusses potential weaknesses. But It should be more clear why any client would indicate the validity of a particular block without the problem-solving mechanism that Bitcoin uses. I know the answer is based upon game theory, but I think III.A would be a good place to clarify this. This is also why I think the author should work in a discussion of POB into Section II (subsection C, most likely).

ISSN 2379-5980 (online)
associated article DOI
10.5915/LEDGER.2016.37

Part III.A.2 discusses some limitations on proof of belief and other consensus mechanisms. This section is helpful but it would be good to specify the specific implications for the CC. For example, what is the role of the use of to the functioning of the CC (and the time stamping issue). The discussion of XRP relative to the CC is good.

This section could also clarify and explain with the context of POB exactly why deciding what block is valid is a normative question.

The Conclusion is good but some of the discussion make new or clarifying points that should be included elsewhere in the paper, including the Intro.

Finally, it would be great for the author to explain how Autonocoin is or is not susceptible to a blocksize update coordination problem, which presumably he thinks it would not be and is in that sense superior to Bitcoin. I have added specific reference to this coordination problem.

Reviewer C:

Does this paper represent a novel contribution to cryptocurrency or blockchain scholarship?:
No

If you answered "yes" to the previous question, in one sentence, describe in your own words the novel contribution made by this paper:

Is the research framed within its scholarly context and does the paper cite appropriate prior works?:
Important references are missing

Please assess the article's level of academic rigor.:
Unsatisfactory (better than poor but a long way from excellent)

Please assess the article's quality of presentation.:
Good (not excellent but a long way from poor)

How does the quality of this paper compare to other papers in this field?:
Bottom 50%

Please provide your free-form review for the author in this section.:
The author presents an analysis of a hypothetical crypto-currency based on a social protocol called "tacit coordination", which is essentially guessing what other people will do.

The author claims to be presenting a computer/networking protocol ("crypto-currency") however he does not include a sample implementation and one does not appear to be forthcoming, nor formal proofs of correctness, nor a set of security assumptions for this protocol. He also seems to be unaware of the relevant research in computer science regarding distributed consensus. (Specifically, the PAXOS and Raft algorithms, and their

ISSN 2379-5980 (online)
associated article DOI
10.5915/LEDGER.2016.37

descendants) Finally the title of the paper "proof-of-belief" seems to misunderstand the notion of a cryptographic proof. It is not clear how a mathematical/cryptographic proof has any bearing on the fuzzy and malleable subject of "belief".

Therefore I do not recommend this paper for publication in Ledger. I do think the author makes some interesting observations that would be valuable if recast in a different form.

In particular, I think the author's observations would be valuable if divorced from the notion of a "coin" or voting on blocks, and focused on an analysis of the game theory of evolving codebases and protocols. Social, human-based protocols for deciding how to evolve Bitcoin's code are an interesting question with many opposing opinions, and it's certainly possible to record opinions in a DAO-like manner. (Though to be clear, this is not "proof" -- it's simply a voting mechanism, and votes can be tracked by "coins" if desired)

I seriously question whether the notion of "tacit coordination" can be applied to a computer protocol in the manner the author desires. While humans may be able to guess as to the thoughts or actions of another, such "guesses" are not available to computers, which deterministically process inputs and create outputs. Any computer can predict with absolute certainty what every other computer will decide with regard to a given input (block).

The relevant literature in computer science are the PAXOS and Raft protocols for distributed consensus. If the consensus is to be fully automated (as would be required for "tacit coordination" to decide on blocks) the author would need to present a computer code that demonstrates his idea, and compare it to these two relevant protocols, which essentially do the same thing.

The "proof of belief" discussed on p.7 seems to amount to "has validated the transactions in the block". It is not necessary or desirable for nodes to signal that they accept a block. This would result in a tremendous amount of communications overhead of nodes signaling to each other that they have accepted the block. But any node already knows this by performing the validation himself. Therefore this communication has no value. It's not necessary to communicate "belief" regarding absolute, deterministic facts. By analogy, it would also be worthless for nodes to communicate that they believe $2 > 1$.

The question at hand is then not whether the block is valid, but consensus regarding the *validation*rules*. A change in these rules are the only reason two nodes would disagree about a block. But these rules are decided by human consensus, not protocol. This is why I think the author should recast his arguments and aim them at the humans who desire to improve or change the protocol rules. All our (non-faulty) computers will reach exactly the same answer regarding whether a given blocks is valid according to a given set of rules.

The author does not present any security model. There certainly exist actors who seek to subvert consensus for their own gain. As he points out, "costs of a coordination failure are high" and therefore active undermining of the "tacit coordination" game is in the interest of the status quo, and is a strategy that can be successfully applied. (See "false flag" operations)

I think the authors arguments are better directed at the human activity of open source software

ISSN 2379-5980 (online)
associated article DOI
10.5915/LEDGER.2016.37

development, and the consensus about it.

1B. Author's Response

Reviewer A:

Overall assessment:

The paper presents the concept of Proof-of-Belief (i.e. a distributed consensus mechanism based on a tacit coordination game that let cryptocurrency owners determine which blockchain they "believe" is the most authorative one) as an alternative mechanism to Proof-of-Work and Proof-of-Stake, which is based on normative judgement instead of algorithmically quantifiable and verifiable actions (e.g. mining).

The paper is well written, clear and well structured and the author shows a good mastery of the subject. The paper provides a thorough description of Tacit coordination games and how they apply in the field of cryptocurrencies, and then explain how Proof-of-Belief could enable the emergence of a completely autonomous and self-governing cryptocurrency (Autonocoin) that relies on tacit coordination games in order to identify authoritative blocks and blockchains, as well as to make more sophisticated decisions such as whether to upgrade the protocol, and to how to reward arbitrary actions that ultimately benefitAutonocoin.

The article is timely and relevant, especially considering the recent governance issues raised with the Bitcoin scaling problem. The article sets out to explore ways in which a decentralized cryptocurrency can incorporates also a mechanism to update its own protocol, according to what the community considers to be the most relevant. The ability for blockchain-based applications to incorporate an internal mechanism to update or upgrade themselves is really important, and the approach suggested by Abramowicz is an interesting solution in this respect.

Suggestions for improvement:

Part II on "Tacit coordination", though important and interesting, is a bit long and sometimes seems to go out of the scope of the paper. The part could be shortened, especially part II.B which could perhaps be dealt with together in part II.C as only one part. This would leave more space to develop the core of the article, which is about specific implementation of the Proof-of-Belief system as a particular implementation of a tacit coordination game.

- I have deleted a great deal of material in Part II. I have also reduced the number of subsections.

Reviewer B:

Summary: I support publication of the article but suggest some clarifications and edits. It may

ISSN 2379-5980 (online)
associated article DOI
10.5915/LEDGER.2016.37

also be helpful to have someone with an expertise in game theory review some parts given how dependent the arguments are on the ability of a formal tacit game coordination game to create a robust and self-governing decisionmaking mechanism.

- I would, of course, welcome game theorists' responses. I would add, however, that focal point coordination games are quite different from other games studied in game theory, because they inherently have multiple equilibria and equilibrium is achieved not by solving for a Nash equilibrium but by identifying a focal point.

The article proposes a new cryptocurrency (Autonocoin or the "CC") with a unique governance mechanism that determines what the authoritative code (client software) and version of the blockchain is, as well as how to reward users that have taken actions to benefit the CC. The article uses game theory to justify its conclusions. The consensus mechanism is called proof of belief (POB): "the central idea is that if a controversy develops as to which block chain is authoritative, this can be resolved through a tacit coordination game. Thus, the blockchain that cryptocurrency owners believe is authoritative will be recognized as such...." Emphasis in original.

The intro begins by noting that CCs don't have mechanisms to decide how their software is updated--it is decided by an open source process. The author's CC proposal seeks to make software update decisions autonomous and based on the CC's blockchain transactions. The CC also proposes a new way to distribute coins; that is, by community consensus as to the value of a user's contribution, and not by mining or pre-mining. It is argued that this process operates by means of a formal tacit coordination game that gives users an economic incentive to consider the preferences of others regarding a particular decision. The overall benefit of the CC is that it is completely self-governing.

I think the introduction should also explain POB more and how it relates to the over points of the article.

- I have added some further discussion of proof-of-belief and how it relates to formal tacit coordination games to the beginning of the article.

Part II begins with a review of basic game theory; explaining tacit coordination games. This discussion is clear; the examples are helpful including with respect to normative games. It then states that Bitcoin miners agree to accept changes in the code made by those who control the official code's repository and accordingly that this creates a status quo bias and that the process is not truly peer-to-peer. The subsequent argument and explanation supports these points.

Part II also explains how other aspects of Bitcoin operate by tacit coordination on page 3. I think this discussion jumps around a bit and could be more clear. Similarly, the following discussion on pages 3-4 about the normative aspects of Bitcoin's coordination game, the discussion of a CC's design, and other issues seem to be a bit of a digression. They are relevant to the overall paper, but they should be made and proceed in a more deliberate manner. They seem too stream of consciousness.

ISSN 2379-5980 (online)
associated article DOI
10.5915/LEDGER.2016.37

- I have reorganized and shortened this discussion.

The remainder of Part II explains formal tacit coordination games and how the CC is built on them. It makes at least a plausible case that the formal game ofAutonocoin will produce the type of outcomes the author argues for such as approving changes to code and awarding a quantity of coins.

Part II should link the points being made clearly to POB. Despite being implied in the Intro, I think there are room for links that make the argument more clear, even without first fully explain in POB.

In particular, the two paragraphs beginning with "Autonocoin is built on formal tacit coordination games" on page 5 left column are essential for the argument. They should be summarized more in the Introduction, and probably belongs in some form in Section III because it is discussing the POB consensus mechanism without calling it POB.

- I have amended the first of these paragraphs by referring to later discussion of proof-of-belief and have tried to briefly incorporate the basic idea into the introduction.

Part III is the core of the author's argument--the point being that if a CC can implement or use a formal tacit coordination game to update its software, distribute coins, etc., those aspects become self-managing and robust. III.A discuss POB which attempts to solve "the question of how to determine which "block chain is authoritative among multiple competing block chains" by "allowing decisions on the block chain as to whether any particular block is a valid block that should be on the block chain." This process is a formal tacit coordination game, according to the author. He further explains that the "measure of proof of belief in a particular block is the difference between payments made in support of a block's authenticity and payments made in opposition to a block's authenticity. The measure of proof of belief in a valid block chain (that is, one in which the hash for each block refers to the previous block) is the sum of the proofs of belief for each block." The valid block is that block that has the highest proof of belief measure. This section seems like it could use clarification how the process is different than proof of work in practice, as it seems to have many of the same attributes. Some examples could help as well.

- I have greatly rewritten this section, and I have contrasted proof of belief more clearly with proof of work.

It's great that the author makes clarifications and discusses potential weaknesses. But It should be more clear why any client would indicate the validity of a particular block without the problem-solving mechanism that Bitcoin uses. I know the answer is based upon game theory, but I think III.A would be a good place to clarify this. This is also why I think the author should work in a discussion of POB into Section II (subsection C, most likely).

- I'm a bit hesitant to do much more than foreshadowing of proof-of-belief in Section II. Proof of work (Part III) builds on the formal tacit coordination games (Part II), so I

ISSN 2379-5980 (online)
associated article DOI
10.5915/LEDGER.2016.37

think it could be confusing if I delved too much into proof-of-belief in Part II before really introducing it (Part III). But I have tried to indicate a bit more clearly the problem that Bitcoin solves and how proof of work is an alternative.

Part III.A.2 discusses some limitations on proof of belief and other consensus mechanisms. This section is helpful but it would be good to specify the specific implications for the CC. For example, what is the role of the use of to the functioning of the CC (and the time stamping issue). The discussion of XRP relative to the CC is good.

- I have changed my discussion of the time-stamping. Time-stamping is not necessarily critical. The point was to show how any fraud in this area could lead to detection and the exercise of human judgment, even if ordinarily, everything were processed by computers.

This section could also clarify and explain with the context of POB exactly why deciding what block is valid is a normative question.

- I have clarified this. Ordinarily, it is a mechanical question, but there could be close cases, and in any event this is an alternative to proof of work.

The Conclusion is good but some of the discussion make new or clarifying points that should be included elsewhere in the paper, including the Intro.

- I have tried to integrate some key points earlier.

Finally, it would be great for the author to explain how Autonocoin is or is not susceptible to a blocksize update coordination problem, which presumably he thinks it would not be and is in that sense superior to Bitcoin.

- I have added specific reference to this coordination problem. I haven't gotten into details on block size per se, since this is a normative question beyond my scope, but I have clearly referenced the controversy and explained how Autonocoin could solve it. The more general point is that miners don't control Autonocoin. Arguably, they control Bitcoin.

Reviewer C:

Does this paper represent a novel contribution to cryptocurrency or blockchain scholarship?:
No

If you answered "yes" to the previous question, in one sentence, describe in your own words the novel contribution made by this paper:

Is the research framed within its scholarly context and does the paper cite appropriate prior works?:
Important references are missing

ISSN 2379-5980 (online)
associated article DOI
10.5915/LEDGER.2016.37

- I believe this is a reference to PAXOS and Raft, which I will respond to below.

Please assess the article's level of academic rigor.:
Unsatisfactory (better than poor but a long way from excellent)

Please assess the article's quality of presentation.:
Good (not excellent but a long way from poor)

How does the quality of this paper compare to other papers in this field?:
Bottom 50%

Please provide your free-form review for the author in this section.:
The author presents an analysis of a hypothetical crypto-currency based on a social protocol called "tacit coordination", which is essentially guessing what other people will do.

The author claims to be presenting a computer/networking protocol ("crypto-currency") however he does not include a sample implementation and one does not appear to be forthcoming, nor formal proofs of correctness, nor a set of security assumptions for this protocol. He also seems to be unaware of the relevant research in computer science regarding distributed consensus. (Specifically, the PAXOS and Raft algorithms, and their descendants) Finally the title of the paper "proof-of-belief" seems to misunderstand the notion of a cryptographic proof. It is not clear how a mathematical/cryptographic proof has any bearing on the fuzzy and malleable subject of "belief".

- It is true that this paper is not about providing a cryptographic proof, and tacit coordination games do not seem to translate well into cryptographic proofs. Meanwhile, PAXOS and Raft are generally applied in a context in which it is assumed that the “voters” are non-hostile. Where hostility is a possibility, a simple voting protocol resolves this. The approach in my paper works with hostile adversaries and even if the number of hostile servers is greater than the number of non-hostile servers. The key is that the voting algorithm does not depend on how many voters there are, but on how committed they are to their position. I have now added a mention of PAXOS and Raft and distinguished them from the normative distributed consensus generated by formal tacit coordination games.

Therefore I do not recommend this paper for publication in Ledger. I do think the author makes some interesting observations that would be valuable if recast in a different form.

In particular, I think the author's observations would be valuable if divorced from the notion of a "coin" or voting on blocks, and focused on an analysis of the game theory of evolving codebases and protocols. Social, human-based protocols for deciding how to evolve Bitcoin's code are an interesting question with many opposing opinions, and it's certainly possible to record opinions in a DAO-like manner. (Though to be clear, this is not "proof" -- it's simply a voting mechanism, and votes can be tracked by "coins" if desired)

- Agreed that this is not a proof.

ISSN 2379-5980 (online)
associated article DOI
10.5915/LEDGER.2016.37

I seriously question whether the notion of "tacit coordination" can be applied to a computer protocol in the manner the author desires. While humans may be able to guess as to the thoughts or actions of another, such "guesses" are not available to computers, which deterministically process inputs and create outputs. Any computer can predict with absolute certainty what every other computer will decide with regard to a given input (block).

- I have clarified that this approach works in part because humans can intervene where oddities or attempts at manipulation are detected. I agree that absent AI, we cannot rely entirely on computers to make normative assessments. This is especially clear when it comes to questions such as how the cryptocurrency convention should be changed.

The relevant literature in computer science are the PAXOS and Raft protocols for distributed consensus. If the consensus is to be fully automated (as would be required for "tacit coordination" to decide on blocks) the author would need to present a computer code that demonstrates his idea, and compare it to these two relevant protocols, which essentially do the same thing.

- I do not believe that the consensus must be fully automated. It would generally be automated, but humans can intervene. Your comment helped me recognize that the prior draft was not clear on this point. This is now clarified and emphasized.

The "proof of belief" discussed on p.7 seems to amount to "has validated the transactions in the block". It is not necessary or desirable for nodes to signal that they accept a block. This would result in a tremendous amount of communications overhead of nodes signaling to each other that they have accepted the block. But any node already knows this by performing the validation himself. Therefore this communication has no value. It's not necessary to communicate "belief" regarding absolute, deterministic facts. By analogy, it would also be worthless for nodes to communicate that they believe 2 > 1.

The question at hand is then not whether the block is valid, but consensus regarding the *validation*rules*. A change in these rules are the only reason two nodes would disagree about a block. But these rules are decided by human consensus, not protocol. This is why I think the author should recast his arguments and aim them at the humans who desire to improve or change the protocol rules. All our (non-faulty) computers will reach exactly the same answer regarding whether a given blocks is valid according to a given set of rules.

- I do highlight the use of tacit coordination games to change the validation rules. But there are also situations in which a computer following the appropriate convention says that transaction X should be included in a block, and a manipulator computer says that transaction X should not be, because it was not received on time. In the absence of an objective means to determine which is the manipulator, we need a process for subjectively making any assessments. I have tried to clarify this in the draft.

The author does not present any security model. There certainly exist actors who seek to subvert consensus for their own gain. As he points out, "costs of a coordination failure are

ISSN 2379-5980 (online)
associated article DOI
10.5915/LEDGER.2016.37

high" and therefore active undermining of the "tacit coordination" game is in the interest of the status quo, and is a strategy that can be successfully applied. (See "false flag" operations)

- I have now highlighted the possibility of manipulative actors and emphasized that the tacit coordination game is designed to stimulate identification of such actors.

I think the authors arguments are better directed at the human activity of open source software development, and the consensus about it.

ISSN 2379-5980 (online)
associated article DOI
10.5915/LEDGER.2016.37