LEDGER
ledgerjournal.org

ISSN 2379-5980 (online)
associated article DOI 10.5915/LEDGER.2020.148

Barter Machine: An Autonomous, Distributed Barter Exchange on the Ethereum Blockchain: Open Review

Author: Can Özturan*†

Reviewers: Reviewer A, Reviewer B

Abstract. The final version of the paper "Barter Machine: An Autonomous, Distributed Barter Exchange on the Ethereum Blockchain" can be found in Ledger Vol. 5 (2020) 20-35, DOI 10.5915/LEDGER.2020.148. There were two reviewers involved in the review process, neither of whom have requested to waive their anonymity at present, and are thus listed as A and B. After initial review by Reviewer A, the submission was returned to the authors with feedback for revision (1A). The author responded (1B) and resubmitted their work. It was then sent again to Reviewer A and also to Reviewer B (2A), who both provided further feedback for review. The author responded (2B) and again resubmitted their work, after which it was determined that the revisions made were sufficient to address reviewer concerns, thus ending the peer review process. Author responses are bulleted for clarity.

1A. Review

Reviewer A

This paper proposes an odd notion: that the advent of blockchain enables a global trustless barter economy which is somehow more desirable (albeit computationally more complex) than conducting trade via conventional monetary means.

The paper has a certain intellectual elegance and appeal but leaves the reader feeling uncomfortable that there are obvious issues of practical importance which have been ignored or side-stepped:

* 19HiB4AvutzjWU6VbkDNTqWTK2x6hxMrM3

† Can Özturan (ozturaca@boun.edu.tr) is a faculty member in the Department of Computer Engineering at Bogazici University, Istanbul, Turkey.

1. It is claimed that "We now have blockchain infrastructure to allow us to keep records of ownership of items and transfer them in trustless manner across the globe." Examples of items that could be transferred include houses, car and organs (kidneys etc.) Several issues immediately arise that are not dealt with in the paper: (a) we can transfer tokens around on blockchains all we like, but this does not correspond to the transfer of *legal* title in the relevant jurisdictions (land registries, vehicle licencing agencies etc. not generally using blockchains yet). (b) how can we be sure that the token being transferred actually represents a unique and real physical asset that isn't already claimed in ownership by another party? (c) how do we ensure the quality of the traded assets, timeliness of the delivery and compliance with local regulations (e.g. ethical approval related to the transport of organs).

2. The underlying problem being addressed is NP-complete, which is generally a disaster for the prospects of operating the system at full scale. This problem of finding these solutions may be discharged to a crowd of "Feasible Solution Finders" in the proposed architecture but this does nothing to improve the prospects of those solutions finders actually being able to find a solution to a very large problem. Indeed it is admitted that "The worldwide population and the number of items being traded are in the billions range" while a test case of just 10000 users and 10000 tokens cannot be solved in reasonable time according to the paper's own evaluation.

3. It is claimed "The likelihood of finding multiple coincidence of wants in smaller windows of time is higher by using AI powered search engines". No evidence whatsoever is provided to support this assertion.

In its current form I do not think the paper is acceptable for publication. If the paper were to be completely overhauled to be much less ambitious in terms of claimed scope e.g. why not "A prototype implementation of a smart-contract-based system for the bartering of ERC20 tokens", then I think it would retain most of its intellectual appeal without the feeling of having vastly overreached itself in terms of claimed and potential impact.

1B. Author Responses

Reviewer A

This paper proposes an odd notion: that the advent of blockchain enables a global trustless barter economy which is somehow more desirable (albeit computationally more complex) than conducting trade via conventional monetary means.

The paper has a certain intellectual elegance and appeal but leaves the reader feeling uncomfortable that there are obvious issues of practical importance which have been ignored or side-stepped:

1. It is claimed that "We now have blockchain infrastructure to allow us to keep records of ownership of items and transfer them in trustless manner across the globe." Examples of items that could be transferred include houses, car and organs (kidneys etc.) Several issues immediately arise that are not dealt with in the paper: (a) we can transfer tokens around on

ISSN 2379-5980 (online)
associated article DOI
10.5915/LEDGER.2020.148

blockchains all we like, but this does not correspond to the transfer of *legal* title in the relevant jurisdictions (land registries, vehicle licencing agencies etc. not generally using blockchains yet). (b) how can we be sure that the token being transferred actually represents a unique and real physical asset that isn't already claimed in ownership by another party? (c) how do we ensure the quality of the traded assets, timeliness of the delivery and compliance with local regulations (e.g. ethical approval related to the transport of organs).

- The topic of my paper is about how to implement an autonomous distributed barter exchange (a DEX) on Ethereum Blockchain (multiple quantity, multi-token bid solution verification and transfer of ownership algorithm and the associated smart contract design and implementation). My paper is more about computer science issues involved in developing a direct barter based DEX. The reviewer's above question, however, is more about social/legal issues in blockchain adoption, enforcement, owned product delivery and regulations which are topics outside the scope of my submitted paper. I will, however, try to answer the question. Blockchain is basically a ledger – an accounting book in which transactions are recorded. Blockchains such as Ethereum also provide smart contract feature. Within the context of a ledger, we are concerned about keeping accurate, verified records of things rather than things like physical transport or delivery of things or physical enforcement of ownerships. Just like a paper deed or a record on government computers can represent ownership of a car or a house, a record on the blockchain can also represent ownership of a car/house. Just like law enforcement officers can look at the government database and conclude that someone actually owns a car/house, law enforcement officers can also check/read blockchain records and perform enforcement actions. The concerns written in your question (a-c) (physical asset connection, timeliness of delivery, quality of traded assets etc.) also arise in current non-blockchain systems. In current non-blockchain systems, we can also have low quality assets like junk bonds/shares etc.
- Crypto/blockchain related regulations are evolving in different countries (see: https://complyadvantage.com/knowledgebase/crypto-regulations/) and there is now a more positive atmosphere toward crypto token type assets from countries/companies. Here are a few examples that involve regulated businesses:
    - Gemini USD stable coin (GUSD) (https://gemini.com/dollar/) is deployed as an Ethereum ERC20 compliant token contract and supported by a large custodian bank State Street Bank and Trust Company
    - Bitwala Blockchain Banking (https://www.bitwala.com/) in Germany.
    - Malta Security Token regulation: https://www.nasdaq.com/article/understanding-maltasleadership-on-security-token-regulation-cm1051452
    - UK HM Land Registry to explore the benefits of blockchain https://www.gov.uk/government/news/hm-land-registry-to-explore-the-benefits-of-blockchain
    - EU Blockchain Partnership Initiative https://ec.europa.eu/digital-singlemarket/events/cf/digital-day-2018/item-display.cfm?id=21244
- Once regulations mature and ownership records on blockchain are officially recognized by states/companies, then the enforcement of ownership can proceed as before or by the use of new technologies. For example:

ISSN 2379-5980 (online)
associated article DOI
10.5915/LEDGER.2020.148

  - For things like houses, enforcement can be done as before by law enforcement officials.
  - For things like tickets, enforcement can be done by the company that issues the ticket and provides the service associated with the ticket. Ticket ownership can be checked on the blockchain by the company before delivering the service.
  - Ownership of manufactured devices can be kept on blockchain and the device can include hardware/software that let the device to simply not operate if the current user is not the same as the owner recorded on the blockchain.
- One can argue that the above can be done by the current non-blockchain systems – this maybe true, but only within silos (within a specific company or a state etc.). This in turn may introduce serious problems such as centralization, conflicts of interests, non-standardization, high costs and transferability etc. Blockchains allow this to be done in a distributed, standardized, secure and low cost manner. In particular, ability to facilitate easy, low cost, fast, conditional, collective and atomic transferability of ownership records of things is one feature that blockchains can provide and current silo (nonblockchain based) systems cannot provide. In fact, arbitrary patterns of transferability (that reflects multi-unit, multi items , collective users) is something that blockchains can easily provide to masses all over the world through smart contracts whereas the current silo based non-blockchain systems simply cannot. For example, transfer involving operations, simple matching swaps, or more complex cyclic, hypercyclic swaps are proposed in this paper that can be facilitated by blockchains very easily (this paper's, i.e. BarterMachine's aim is to actually demonstrate that this can actually be done with the existing blockchain technology). Current non-blockchain systems do not offer such advantages. These direct general bartering patterns can save users a lot of money when compared with simple buy/sellwith-money type operations. For example, buying a house may involve a lot of time consuming bureaucratic processes and high fees and commissions. Blockchains can help by saving on these costs. Also, blockchains can facilitate multiple house owners to engage in direct multi-way trading of their houses using only small differential money amounts and enable the settlement and transfer ownerships to be carried out fast and in a low cost manner.

2. The underlying problem being addressed is NP-complete, which is generally a disaster for the prospects of operating the system at full scale. This problem of finding these solutions may be discharged to a crowd of "Feasible Solution Finders" in the proposed architecture but this does nothing to improve the prospects of those solutions finders actually being able to find a solution to a very large problem. Indeed it is admitted that "The worldwide population and the number of items being traded are in the billions range" while a test case of just 10000 users and 10000 tokens cannot be solved in reasonable time according to the paper's own evaluation.

- Please note the context in which I used the phrase "in the billions range". Here it is from the Introduction section of my paper:
- "…in his book Jevon stated "The first difficulty in barter is to find two persons whose disposable possessions mutually suit each other's wants. There may be many people wanting, and many possessing those things wanted; but to allow of an act of barter there must be a double coincidence, which will rarely happen." In the modern world, however, the difficulties mentioned by Jevons are easier to handle: (1) ... (2) ….(3)

ISSN 2379-5980 (online)
associated article DOI
10.5915/LEDGER.2020.148

The worldwide population and the number of items being traded are in the billions range. Hence, the likelihood of finding multiple coincidence of wants in smaller windows of time is higher by using AI powered search engines."

- Here, I am not implying that there is a single and connected NP-hard problem involving billions of variables specified for a small window of time to be solved. For example, how many times in his life time does someone sell/buy a house or a car or a ticket ? Within a small time frame (let's say two weeks), the number of bids may not be in the billions range. For example, consider cities London and Istanbul:
    - In 2019, London has a population of 8.7 million and Istanbul has a population of 15 million in 2019.
    - In 1600, London has a population of around 600 thousand and Istanbul has a population of 400-700 thousand.
- Within a small time frame, the likelihood of someone from London moving to Istanbul and someone from Istanbul to London is higher in the year 2019 than in the year 1600 simply because populations are in the millions range in the year 2019. And also with Internet and search engines like Google, Elastic Search etc. in the year 2019, it is easier for these two persons to locate house-for-sale or for barter notices. Just because London and Istanbul has combined population of 23.7 million, does not mean, there will be a single NP-hard bartering problem with 23.7 million variables in it all coupled together to be solved in a small time frame. Also please note that the resulting bid graph will not be a dense graph. It will be sparse and most probably geographically localized, and disconnected. Even if it is connected, one can run linear time strongly connected component algorithm (in the case of directed bid graphs) and in the more general case of directed hypergraphs, linear time barter-candidate components algorithm (see p. 160 of my paper [6] "Resource Bartering in Data Grids," Scientific Programming, vol. 12, no. 3, pp. 155-168, 2004. available as open access) to decompose the problems into smaller subproblems (smaller bid subgraphs) and solve each smaller subproblem separately. Each cycle or hypercyle or circulation (i.e. solution) obtained in the smaller subproblem can be submitted to the BarterMachine system.
- Even if strongly connected components algorithm or the barter candidate algorithms finds one or a few very giant components, heuristics can be designed to partition the giant bid graphs further by removing bids in order to have many smaller sized subgraphs. Feasible solutions can be searched on smaller subgraphs on parallel computers.
- One final note, multi item, multi unit version is the most general form. The simpler version in which the bid graphs forms a directed graph (network) has polynomial solution (provided there is no limitation of cycle lengths which artificially arises only because of the current public Ethereum gas limitation). The polynomial solution is given by minimum cost network flow algorithms (please see Sect. 2 on page. of 157-158 of my paper [6]) .

3. It is claimed "The likelihood of finding multiple coincidence of wants in smaller windows of time is higher by using AI powered search engines". No evidence whatsoever is provided to support this assertion.

ISSN 2379-5980 (online)
associated article DOI
10.5915/LEDGER.2020.148

- Please note that here I am referring to searching and location of products. Before bidding, a user has to locate the products/items that he wants to bid for. Before the age of Internet, search engines like Google or Bing and Elastic Search software etc. such a task would be extremely difficult. Yet, such search engines are essential for bartering to be realized on a large scale, because before bidding, people first have to locate the items they will bid for. The evidences for this are already around us. We can use Google and/or Bing search engines which have AI powered features in them. Once, a bid graph is formed, then bartering solvers can then run network flow algorithms or integer programming solvers to find solutions which represent “multiple coincidence of wants” in Economist Jevon’s words.

In its current form I do not think the paper is acceptable for publication. If the paper were to be completely overhauled to be much less ambitious in terms of claimed scope e.g. why not "A prototype implementation of a smart-contract-based system for the bartering of ERC20 tokens", then I think it would retain most of its intellectual appeal without the feeling of having vastly overreached itself in terms of claimed and potential impact.

- In my first version of the paper, I already had a smart contract implemented for ERC20 tokens. I understand, however, that doing low level function calls on the smart contract is not very user friendly. Therefore, I now have developed a full prototype (web interface + a new smart contract with more features like support for ERC721 and consumable dummy tokens, and ENS names) so that ordinary users can use the system easily. It runs on the Ethereum Ropsten network and is now available at the address https://bartermachine.github.io/bartermachine/ropsten/ . I have revised the paper and added Section 5 about the prototype. I have documented functions of the new smart contract in Table 1.
- As far as potential impact is concerned, it is difficult to predict the future. But below I provide some use cases which motivated me to carry out this work:
- Use case 1: Transferable tickets Suppose you bought a non-refundable airline ticket and you will not be able to use the ticket on the specified date/time. Ability to barter it with other tickets can be very appealing to people. If the airline issues the tickets as ERC721 token, the current BarterMachine prototype system will able to barter it with other tickets. In the current systems, this is what you have to do: https://traveltips.usatoday.com/transfer-airline-ticket-60915.html . BarterMachine will also be able to do transfers among different airlines if they all issue their tickets on the blockchain as ERC721 tokens.
- Use Case 2: Property bartering Consider the following cases:
    - Suppose Alice has a house in San-Francisco and wants to move to New York because of a new job offer. She thinks her house is worth 325,000 USD and wants to sell it to buy a new house in New York.
    - Suppose Bob has house in Atlanta and wants to move to San Francisco because of a new job offer. He thinks his house is worth 275,000 USD and wants to sell it to buy a new house in San Francisco.
    - Suppose John has house in New York and wants to move to Atlanta because of a new job offer. He thinks his house is worth 300,000 USD and wants to sell it to buy a new house in Atlanta.

ISSN 2379-5980 (online)
associated article DOI
10.5915/LEDGER.2020.148

- We now have USD as a stable coin (for example, as Gemini GUSD ERC20 token) on the Ethereum blockchain. If regulations are passed that recognize property titles to be recorded on the blockchain, for example as ERC721 tokens, the following bids could be placed on the BarterMachine.
    - Alice: SanFranciscoHouse(1) => NewYorkHouse(1) + GUSD(25,000)
    - John: NewYorkHouse(1) => Atlanta(1) + GUSD(25,000)
    - Bob: AtlantaHouse(1) + GUSD(50,000) => SanFranciscoHouse(1)
- As a result, these users would be able to just trade their houses with each paying/receiving only differential money amounts of $25,000 and $50,000 and extremely low blockchain bid/solution submission transaction fees of few dollars (see. Tables 4 and 5 in my paper) on the Ethereum Blockchain. I really do not know how much it would cost to do this trilateral trading arrangement with banks/property agents in the current non-blockchain environments ; One thing is certain though, it will be far more expensive than a few dollars.
- Use case 3: Circular Economy BarterMachine can contribute to the Circular Economy vision by providing a worldwide collaborative circularity pattern discovery and settlement engine. Here is a list of references and quotations relating bartering and circular economy:
    - European Commission delivers Circular Economy Plan, March 4, 2019 https://ec.europa.eu/commission/news/commission-delivers-circular-economy-action-plan2019-mar-04_en
    - Circular Economy expert (Alexandre Lemille) : https://www.huffpost.com/entry/circular-economy-20_b_9376488 is calling for "... finance-as-you-access, bartering-as-you-need or alternative means of exchange that will flourish away from a standardised monetary format..."
    - EASAC's Circular Economy commentary: https://easac.eu/fileadmin/Reports/Easac_15_CE_web_corrected.pdf "One of the main stumbling blocks for achieving circularity is the lack of product take-back schemes and industrial infrastructure…" " ...significant opportunities: ... * In the consumption phase. Collaborative consumption models based on lending, swapping, bartering and renting products; and product service systems to get more value out of underutilised assets or resources (for example cars, tools, lodging)."

2A. Second Round Review

Reviewer A

Does this paper represent a novel contribution to cryptocurrency or blockchain scholarship?

Yes

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

Prototype implementation of a smart contract for direct bartering

ISSN 2379-5980 (online)
associated article DOI
10.5915/LEDGER.2020.148

Is the research framed within its scholarly context and does the paper cite appropriate prior works?

Yes

Please assess the article's level of academic rigor:

Good (not excellent but a long way from poor)

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?

Top 50%

Please provide your free-form review for the author in this section:

The author has revised the paper and provided clarification that the contribution being claimed is not an economic or regulatory one but rather the technical achievement of realising a smart-contract-based prototype of an autonomous, distributed barter exchange on the Ethereum blockchain. That is fine in so far as it goes but:

1) The title of the paper should be changed to reflect the actual focus of the paper. Something like "BarterMachine: An autonomous, distributed barter exchange on the Ethereum Blockchain" would do the trick.

2) There is no escaping from the fact that solving the underlying optimisation problems optimally is NP-hard, and that the problem sizes could be very large indeed. Discharging the solution process to "solvers" does not change this fact. Unless Gurobi is capable of producing near-optimal solutions even for very large problems, and that is good enough?

3) I am still concerned that the author mentions organ trading etc. without consideration of the ethical, legal or regulatory implications. I would prefer it if the author would avoid such use cases and instead focus on those given by the author in the response to the reviewers.

4) It is not explicitly mentioned but it seems all quantities in the optimisation problem must be integers. Is that the case? Does that even apply to ETH tokens? (or would some subdivision of ETH be used in practice?)

5) One of the virtues of ordinary markets is that it is very easy for market participants to get an idea of the worth of their assets (by looking at the best offer price). They also receive the best available prices when placing market orders. In this way it is hard for them to be "ripped off". How do market participants get an idea of the worth of their assets in the barter exchange setting? And how do they ensure they aren't proposing something economically irrational in comparison to the best available market price for their assets (e.g. if I offer to swap 1 BTC for

ISSN 2379-5980 (online)
associated article DOI
10.5915/LEDGER.2020.148

1 ETH I am being very stupid and proposing something very far from the going rate; but how will I know this?)

6) How is the privacy of market participants preserved?

7) How can market participants trust the smart contract?

8) A race condition due to users withdrawing their funds is mentioned. Isn't there another sort of race condition when an "exclusive-or" type bid is resolved one way or the other? Or indeed when any sort of solution is published, rendering (possibly significant amounts of) in-progress computations redundant?

Reviewer B

Does this paper represent a novel contribution to cryptocurrency or blockchain scholarship?

Yes

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

This paper explains a full Barter smart contract to live on the Eth. blockchain for users to submit bids and solutions.

Is the research framed within its scholarly context and does the paper cite appropriate prior works?

Yes

Please assess the article's level of academic rigor:

Excellent (terms are well defined, proofs/derivations are included for theoretical work, statistical tests are included for empirical studies, etc.)

Please assess the article's quality of presentation:

Excellent (the motivation for the work is clear, the prose is fluid and correct grammar is used, the main ideas are communicated concisely, and highly-technical details are relegated to appendixes).

How does the quality of this paper compare to other papers in this field?

Top 5%

Please provide your free-form review for the author in this section:

ISSN 2379-5980 (online)
associated article DOI
10.5915/LEDGER.2020.148

This work is a very important contribution to the blockchain ecosystem. The paper explains concisely how the BarterMachine smart contract will operate, how users submit bids, and how feasible solution finders submit their solutions. My main concern was with gas prices for solution finders being prohibitively expensive, but table 3 assuages these fears by showing that solutions of bid size 40 can still be submitted and verified by the contract for very modest gas.

2A. Author Responses to Second Round

Reviewer A

Does this paper represent a novel contribution to cryptocurrency or blockchain scholarship?

Yes

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

Prototype implementation of a smart contract for direct bartering

Is the research framed within its scholarly context and does the paper cite appropriate prior works?

Yes

Please assess the article's level of academic rigor:

Good (not excellent but a long way from poor)

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?

Top 50%

Please provide your free-form review for the author in this section:

The author has revised the paper and provided clarification that the contribution being claimed is not an economic or regulatory one but rather the technical achievement of realising a smart-contract-based prototype of an autonomous, distributed barter exchange on the Ethereum blockchain. That is fine in so far as it goes but:

1) The title of the paper should be changed to reflect the actual focus of the paper. Something

ISSN 2379-5980 (online)
associated article DOI
10.5915/LEDGER.2020.148

like "BarterMachine: An autonomous, distributed barter exchange on the Ethereum Blockchain" would do the trick.

- Done. The title has been changed to the more descriptive title suggested.

2) There is no escaping from the fact that solving the underlying optimisation problems optimally is NP-hard, and that the problem sizes could be very large indeed. Discharging the solution process to "solvers" does not change this fact. Unless Gurobi is capable of producing near-optimal solutions even for very large problems, and that is good enough?

- Gurobi can be given time limit and it can also report sub-optimal solutions (https://www.gurobi.com/documentation/9.0/refman/finding_multiple_solutions.html).
- I have added the following paragraph in the discussion section (Section 7). Note that I have mentioned these approaches in my 2nd revision answers-to-reviewers document.
- As the bids accumulate, very large sized instances of the most general NPhard bartering problem will be challenging to solve. However, there are few approaches that may be pursued to reduce the problem sizes and possibly get, not necessarily optimal, but feasible and profitable solutions:
- (1) Barter candidate components of the whole bid graph can be computed using linear time algorithm described in Ref. [6]. Optimization problem can then be solved on each smaller component in parallel. Also, due to geographical proximity of users bartering such things as tickets, houses and cars, we can expect localized components corresponding to towns and cities to be present. Even if the whole graph is connected, a heuristic that employs some graph partitioning software such as Metis can be used to break up the bid graph into multiple parts with small cut sizes and hence producing smaller sized components on which Gurobi solver can be applied in parallel.
- (2) The simpler versions of the problem, e.g., differential barter auction with unrestricted solution size described in Ref. [9,10] can be solved by polynomial time minimum cost network flow algorithms [2]. Even though the bid pattern is simpler in this case, (i.e. item1 + money => item2 or item1 => item2 + money, or item => money, or money => item), it may appeal to people when bartering their cars, tickets or houses with differential money amounts. Components involving only these bids can be extracted and solved fast. Also the users can be informed that if they submit bids in differential form, their bids are more likely to be picked up by solution finders employing fast polynomial time minimum cost solvers

3) I am still concerned that the author mentions organ trading etc. without consideration of the ethical, legal or regulatory implications. I would prefer it if the author would avoid such use cases and instead focus on those given by the author in the response to the reviewers.

- Done. I removed the use of such cases (from page 2, paragraph 2).

4) It is not explicitly mentioned but it seems all quantities in the optimisation problem must be integers. Is that the case? Does that even apply to ETH tokens? (or would some subdivision of ETH be used in practice?)

ISSN 2379-5980 (online)
associated article DOI
10.5915/LEDGER.2020.148

- Yes, the quantities are all integers. Note that in the Solidity smart contracts all ETH quantities are stored as integers in the smallest denomination which is Wei. My web user interface has been programmed so as to display quantities such as 0.5 ETH which is actually stored as integer Wei quantities in the smart contract. For ERC20 tokens, quantities are also stored as integers (ERC20 contracts also have a field called digits after decimal point but the quantities are stored as integers in terms of smallest denomination). In the world of finance where exact balances are kept, integer quantities are used to store quantities of valuable things since every cent counts and we do not want to loose cents due to round-off errors that occur in floating point calculations.

5) One of the virtues of ordinary markets is that it is very easy for market participants to get an idea of the worth of their assets (by looking at the best offer price). They also receive the best available prices when placing market orders. In this way it is hard for them to be "ripped off". How do market participants get an idea of the worth of their assets in the barter exchange setting? And how do they ensure they aren't proposing something economically irrational in comparison to the best available market price for their assets (e.g. if I offer to swap 1 BTC for 1 ETH I am being very stupid and proposing something very far from the going rate; but how will I know this?)

- As stated in Section 1, BarterMachine has been proposed for the trading of tokens representing houses,tickets (airline,bus,ship,concert tickets), company shares, services (worker hours), vehicles(new and used cars), electronic goods such as mobile phones, computers and tablets. It is the user’s responsibility to be aware of the value of the items whose tokens he is bartering.
- Please note that BarterMachine’s application domain is different from traditional centralized high speed exchanges which specialize in high volume and simple pair trading. BarterMachine supports more generalized bids having multiple items and multiple quantities. If the traditional centralized high speed exchanges start supporting generalized multiple item and multiple quantity bids, they will have difficulty estimating what the values of multiple items are from the perspective of users (how will the exchange know about the value of my bmw and ford, if for example I place a bid like bmw + ford => mercedes + 1 btc ?).
- Hence, BarterMachine just guarantees delivery of what the user requires on the right side of his bid if the bid is satisfied. This is the agreement protocol of the BarterMachine.
- Since BarterMachine matches collective bids, it is also not very clear someone placing BTC(1) => ETH(1) is acting in a stupid manner. It depends on the situation at that time. Suppose only the following bids are present:
    - 1. Alice: BTC(1) => ETH(56)
    - 2. John: cruiseholiday(1) + ETH(1) => BTC(1)
    - 3. Bob: BTC(1) => ETH(1)
- In the above scenario, if Bob urgently needs 1 ETH, a solution involving bids 2 and 3 is possible. Bids 1 and 2 does not form a solution. Therefore, Bob can be better off submitting BTC(1) => ETH(1) bid not out of stupidity but out of urgent need for 1 ETH.

ISSN 2379-5980 (online)
associated article DOI
10.5915/LEDGER.2020.148

- I should also note that weird trades may also happen in the traditional high speed high volume centralized exchanges as this news mentions (ethereum price crashing from $319 to 10 cents): https://www.cnbc.com/2017/06/22/ethereum-price-crash-10-cents-gdax-exchange-after-multimilliondollar-trade.html
- One final note, currently solution finding and submission is open to anyone. If solution finding privilege is granted to a single party (please read answer to reviewer's Question 8 further below), then it may be possible, perhaps through some legal agreement, to have the single party produce solutions that take into consideration the issue raised by the reviewer.

6) How is the privacy of market participants preserved?

- Ethereum (and Bitcoin) are public blockchains and contain transactions involving pseudo-anonymous addresses. BarterMachine runs on the public Ethereum blockchain and accepts transactions involving pseudo-anonymous addresses

7) How can market participants trust the smart contract?

- Please note that I have provided the Algorithm for settlement of the submitted solution in Section 4. I have also provided explanations for the correctness of the algorithm (which has also been endorsed by the second reviewer). Once correctness of an algorithm used by the smart contract is established, market participants can trust the smart contract.

8) A race condition due to users withdrawing their funds is mentioned. Isn't there another sort of race condition when an "exclusive-or" type bid is resolved one way or the other? Or indeed when any sort of solution is published, rendering (possibly significant amounts of) in-progress computations redundant?

- I have added the following paragraph at the end of Section 3:
- "We note that our BarterMachine prototype currently supports open solution submission policy meaning any user can support a solution ; whoever's solution transaction is first entered into a block, those solution bids will be satisfied.Hence, solution finders run the risk of wasting their computational efforts due to being late. This is the disadvantage you get in return for offering the advantage of being open to anyone. We have a similar situation in Bitcoin and Ethereum mining process where miners solve a hash puzzle. The networks are open and anyone can mine (i.e. try to solve the hash puzzle), but whoever solves the hash puzzle first gets the mining reward. In order to save on computational efforts, other policies can be considered in the future. For example, we can have ERC721 tokens representing time intervals. Then, only the person who buys the token representing an interval can submit solution in that time interval."

ISSN 2379-5980 (online)
associated article DOI
10.5915/LEDGER.2020.148

Reviewer B

Does this paper represent a novel contribution to cryptocurrency or blockchain scholarship?

Yes

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

This paper explains a full Barter smart contract to live on the Eth. blockchain for users to submit bids and solutions.

Is the research framed within its scholarly context and does the paper cite appropriate prior works?

Yes

Please assess the article's level of academic rigor:

Excellent (terms are well defined, proofs/derivations are included for theoretical work, statistical tests are included for empirical studies, etc.)

Please assess the article's quality of presentation:

Excellent (the motivation for the work is clear, the prose is fluid and correct grammar is used, the main ideas are communicated concisely, and highly-technical details are relegated to appendixes).

How does the quality of this paper compare to other papers in this field?

Top 5%

Please provide your free-form review for the author in this section:

This work is a very important contribution to the blockchain ecosystem. The paper explains concisely how the BarterMachine smart contract will operate, how users submit bids, and how feasible solution finders submit their solutions. My main concern was with gas prices for solution finders being prohibitively expensive, but table 3 assuages these fears by showing that solutions of bid size 40 can still be submitted and verified by the contract for very modest gas.

- Thanks for the feedback.

ISSN 2379-5980 (online)
associated article DOI
10.5915/LEDGER.2020.148