LEDGER
ledgerjournal.org

ISSN 2379-5980 (online)
associated article DOI
10.5915/LEDGER.2016.15

Game Channels for Trustless Off-Chain Interactions in Decentralized Virtual Worlds: Open Review

Authors: Daniel Kraft*[†]

Reviewers: Reviewer A, Reviewer B, Reviewer C, Reviewer D, Reviewer E, Reviewer F

Abstract. The final version of the paper "Game Channels for Trustless Off-Chain Interactions in Decentralized Virtual Worlds" can be found in Ledger Vol. 1 (2016) 84-98, DOI 10.5915/LEDGER.2016.15. There were six reviewers who submitted responses, none of whom have requested to waive their anonymity at present, and are thus listed as A, B, C, D, E, and F. After initial review by Reviewers A, B, and C (1A), the author submitted a revised submission and responses (1B). The submission was sent to Reviewers D and E whose comments (2A) were addressed by the author with another revised submission and responses (2B). This second resubmission was evaluated by Reviewer F (2C), which aided the assigned Ledger editor in determining that the author had adequately addressed the pervious reviewers' concerns. This completed the peer- review process.

1A. Review, Initial Round

Reviewer A:

Overall, I thought this paper was interesting, clear and well written. The only real issue I had with it was fairly minor; The terms "price" and "price money" was used several times in the paper, where from context, it appears that "prize" and "prize money" were intended. This should be corrected, or if it was intentional, explained.

Reviewer B:

The paper presents an interesting idea on how two players can play games fairly off-chain (using 'game channels'), while resorting to the blockchain only for dispute-resolution. The strongest point of the paper is that it is clearly written and easy to follow.

That said, my main issue concerns the overall lack of rigor and comparison to previous

[†]D. Kraft (d@domob.eu) is a mathematician and the current Huntercoin main developer.
* 1domobKsPZ5cWk2kXssD8p8ES1qffGUCm

academic work, which one would expect in an academic publication. For example, most of the references cite Bitcoin forum posts and news articles. The authors should explore how similar ideas/frameworks were developed before (e.g.,work on authenticated Byzantine agreement similar to the off-chain one we see between players, fairness, and game theory) and clearly explain the novelty of their model or how it builds upon those ideas. This is not to say the paper is not novel, just that it feels detached.

On a related note, the protocols in the paper need some more detail/formalism. It is hard to assess the security of the presented protocols when only a high-level overview is given. Specifically, there was ambiguity regarding:

1. How is the ‘private blockchain’ actually constructed, and how are blocks chained together. For example, has this been implemented and pegged to Bitcoin, and is Script expressive enough to do dispute-resolution over arbitrary states? An example or an actual implementation of the script is quite necessary.

2. Similarly, what data is actually sent to the blockchain. How is the game state represented in a transaction to the blockchain?

3. What is the network model/communication model. Is every player connected to every other player in a private channel (O(n^2) channels), or is there some other topology? If it’s the latter, more details are required on how we ensure game channels aren’t disrupted by a potential adversary controlling some of the network.

4. There seems to be a potential adverse effect when one player ‘double-spends’ their turn (i.e., sends more than one move). It is rightfully mentioned that it’s the other player’s choice to decide which turn to take, but this is different than how games are played in reality. In some cases, a valid strategy might be to send many possible moves for a single turn, forcing the other player to think about all of them. This could be a form of ‘human’ denial of service, lengthening the time it takes for the honest player to respond, potentially forcing him to forfeit the game if he doesn’t respond in time, or more realistically - to force him into making less than optimal moves given the large space of options.

5. The paper mentions that it’s straight-forward to extend this to more than two players. This is a very strong assumption that is not backed in the paper. If we have n players and n is sufficiently large, this solution might not scale. Without a more formal definition, it is also not clear if collusion could prove to be a better strategy for adversarial players.

6. Is the hash commitment implemented using SHA-256 or is it simply SHA-256? If it’s the latter, then for simple discrete game states it would be easy to guess the move by enumerating all possibilities (in other words, this commitment scheme is not hiding).

Finally, it is good that the authors address the issue of bloating the blockchain, but stating that this is unlikely to occur at scale is not well justified. First, for rational players who simply care about winning the game, it is pretty clear that there is an equilibrium in delaying the game and then filing a resolution, as this is no different from their perspective than making their move before a dispute arrises. For adversarial players who actually want to harm the blockchain, this might present a cheap way to do so.

Reviewer C:

This is a very interesting topic. But the paper reads at level of detail just a bit deeper than slideware. It's like a "white paper" to get VC investment, not a research article.
So I think that it needs to be expanded into a more careful and formal treatment of the subject. I am left with more questions than answers. But I am looking for answers. If someone says "bitcoin and gaming" a person familiar with bitcoin can basically figure out almost everything in the paper. But I feel like the author knows a lot more and likely has a lot more experience in real world implementation that is not being shared here.

Chapter 2

2.2

dispute proceeding:

1. What public network? The public blockchain?
How do you "send the sequence of moves to the public network"?

2. How can the "network" tell whether the moves are valid, if its a general blockchain like bitcoin? If its not a general blockchain, you need to describe it fully in another chapter. How does it confirm the dispute transaction? Can it run any game or does every game have its own public network?

3. "to and end state" -> "to an end state"

4. "Otherwise and if" is ackward, "full price money" -> priZe money (in several places)

Chapter 3:

Non-Stalling

This seems to stop users from aborting, but it doesn't seem to stop them from "stalling" (taking a long time to move, consider timed chess for example)

Fraud Proof

You cannot guarantee that the next block will have the dispute resolution.

And what if you file a dispute right before the timeout?

4.1 what happens if the move does not match the hash?

ISSN 2379-5980 (online)
associated article DOI
10.5915/LEDGER.2016.15

4.2 This works but stalling is a problem and the dispute resolution system (on bitcoin anyway) seems much too slow for this situation. You could make money by starting hundreds of sessions with different users and playing so slowly that they get bored and give up the 50 cents (or whatever). Its very little to them, they are unlikely to stick around. But its a lot to the attacker because the attack is repeated hundreds of times.

General comments:

Given a player who also has X% of the hash power, how do you stop him from ignoring dispute blocks, ignoring dispute resolution blocks, and other techniques. Given a player with hash power X, what is the minimum number of main-chain blocks required to ensure that the player can't cheat? What's the last dispute block that can be used before the player has Y% likelyhood of being able to time the game out?

Lightning and sidechains were mentionned but not really integrated in to the body of the work.

I think that a more detailed description of the money flow is needed. N players create an initial transaction with LOCKTIMEVERIFY... what is the content of that transaction? Where does that money go if all N players drop out at that moment? Where does it go if N-M players drop out? How is this achieved?

1B. Author’s Responses

In general, the main issue that both Reviewer B and Reviewer C seem to have with the paper is that it is, in their opinion, too vague and only describes a base idea without going into any details of a corresponding protocol or implementation (nor mathematical analysis of game theory, for instance). Having written mostly mathematics research papers in the past, I can fully understand their concern. That said, there are two reasons why I chose to submit the article in the form I did, without going into any more details or technical discussions:

First, the paper is mainly about communicating an idea. The idea is also somewhat easy to see once it is explained, but nevertheless novel and interesting to discuss. Describing an actual protocol or implementation in full glory would, in my opinion, be harmful with respect to communicating the basic concepts. It is also not what the paper is about, since I explicitly intend to not focus on any specific game or implementation. An actual implementation of gaming on a blockchain (including representation of game states and moves, but not yet incorporating game channels), Huntercoin, is referred to in [7], where interested people can dig into the code to find every detail if they wish. Second, I don't think that it would even be possible to give such a detailed description without breaking Ledger's 4,000 word limit.
Thus I came to the conclusion that the paper really fits much better in its current form (describing a core idea but not every detail or any specific implementation). If a particular, successful implementation of game channels becomes of interest on its own in the future, we can always submit a second paper describing its particular protocol and implementation.

ISSN 2379-5980 (online)
associated article DOI
10.5915/LEDGER.2016.15

I thus really suggest to keep the paper in its current spirit instead of overloading it with details unnecessary for understanding the fundamental concepts I want to communicate. (Clarity of description is very important to me, which also the reviewers acknowledged. I think this is particularly true for an interdisciplinary journal like Ledger.) I have nevertheless added a statement to the paper describing this decision and referring readers interested in a detailed example of blockchain-based gaming more explicitly to Huntercoin's code base.

Let me now comment in more detail on particular points raised by the reviewers. I tried to address them also by revising the paper accordingly, with my edits highlighted (most of the time) in blue in the revised manuscript:

Reviewer A:

- This is a very good catch. Indeed, "prize" and "prize money" is what I meant (I am not a native speaker). I have fixed it now.

Reviewer B:

1) 2) See general discussion above.

3) I have added a statement addressing this question. The communication takes place on a direct link between both players. We do (by far) not expect all pairs of players to have a game channel open at all times, so that the scaling concerns of the reviewer (O(n^2)) are not justified.

4) While the concern seems valid in theory, this is not a real problem. It is always possible for a player to resolve a situation where the counterparty tries to engage in the described strategy by simply acting on, say, the first move received. It is not necessary to consider all options in case this leads to issues. Since the reacting player is always at the advantage when it receives more than one move (as described in the paper), I do not see how it could be a valid strategy to post more than one move. (And even if a player does it nevertheless, this is no issue as discussed.)

5) I believe that this should indeed be easily possible for the situations I have currently in mind, but I agree that the statement is probably too strong. I changed it to state more neutrally that one can think about extending the situation to more than two players, but that this is outside of the scope of the current paper.

6) As stated above, I have no really concret protocol in mind, and want to just communicate the base idea. The concern about a potentially small number of states that can be enumerated to "break" the hash is a valid one, though. I have made it more explicit in the paper that this must be prevented by including a salt into the commitment.

Bloating the blockchain: The reviewer's remark is of course justified, we do not have any proof that bloating does not happen in the way discussed. We tried to clearly state in the paper that we do not have any experience in this at all yet, so that it remains to be seen

ISSN 2379-5980 (online)
associated article DOI
10.5915/LEDGER.2016.15

whether this becomes a practical problem or not. We believe that it may not be an issue and gave our reasons, but we understand that these are no proofs (and never tried to frame it as such). This is the best we can do at the moment before a practical system at scale is built and deployed in the wild.

Reviewer C:

For the initial comments, see my general comments above.

2.2.1) I tried to clarify "public network" and "public blockchain" at the end of the general part of section 2. I hope this clears things up.

2.2.2) We assume that the blockchain is built on purpose for the game being played, thus the miners can verify the moves. We are mainly thinking about a particular game, but as mentiond in the conclusion, it is also possible to define a "general gaming blockchain" where the individual game rules are programmed when creating a channel. I tried to make things clear with respect to this as much as possible.

2.2.3) Good catch, fixed.

2.2.4) I tried to rephrase the sentence to be clearer.

Non-stalling: This is true, and it is something I discuss at the end of section 3. It remains to be seen how this affects games in practice, which may also be different for various concrete games and implementations.

Fraud proof: This is true, but I never stated that Bob's resolution must be mined within one block. The timeout may well be longer than that, with the actual parameters tuned for the concrete game that is being built (and depending on the overall blocktime of the blockchain, for instance). I tried to make this clear as far as possible in the paper.

4.1) A move not matching the hash is simply invalid and thus ignored by the other player. This is stated in step 3.

4.2) This is a valid concern; it is true that players intentionally stalling can disrupt the "near real-time" interaction. It remains to be seen in practice how this plays out, and if it works most of the time or not. It is up to the actual game implemented to define a balanced set of rules (timeouts, fees, and so on) to handle these situations. This will definitely be challenging to implement and interesting to observe once there is an implementation deployed widely. This is not yet the focus of this initial paper, though, and I tried to make this clear.

Player with X% of the hashrate: This is also a valid concern, but one that is common to all kinds of blockchain systems. The statistics of answering the questions posed by the reviewer are also the same for all such systems, and not specific to game channels. Thus, for the sake of describing the actually novel difficulties related to gaming in as clear and brief a way as possible, we did not touch on this subject. (But it is mentioned that we assume no player to "control" mining on the network, for obvious reasons.)

Lightning and sidechains: They are not integrated into the work, since the work does not really "use" them. Both ideas are just somewhat related, which is the reason for giving credits and citing them as inspirations.

Money flow: This is, again, something that should be specified in a concrete procotol and implementation for a concrete game. While I agree that this may help to clarify the situation for a reader, it is nothing that can be specified in the general scope the paper adopted. See my initial discussion.

2A. Review, Second Round

Reviewer D:

I'm concerned about the novelty of the Game Channels paper, and that it doesn't cite any of the related academic work about optimistic off-chain contracts. I'll explain more below.

Although the reviewers have also raised these concerns, the average rating is "revisions required" (i.e., one "accept", one "revisions needed", one "resubmit for review"). However, I think we should either "reject" or "resubmit for review" with some additional instructions from the editors.

On novelty:

=====
Huntercoin (the subject of the present paper) is most likely the first system to implement these ideas in a cryptocurrency, but there's a separate burden to show that this is novel compared to the ideas in other published research papers.

In particular I'm worried this has very limited novelty compared to [A], which is a protocol for playing games like Poker off-chain, and using the blockchain to handle disputes. Other related works from the Computer Security community include [B] and [C].

Also even within the Bitcoin community, while the paper cites Lightning Network [13] and Sidechains [15] as "inspiration" and "a basis" for the present work, it doesn't explain what the novelty is compared to these.

In general there is a long line of work in crypto/security on "optimistic execution", such as fair exchange, fair contract signing, etc. [D] is one example. The main idea is that you have a trusted arbitrator, and you only invoke the arbitrator when the parties involved in the protocol have a dispute. Here, the "blockchain" itself serves as the arbitrator.

Most of the research effort has been about providing good privacy even during a dispute, or making it so that the arbitrator has to do very little work during the dispute, etc.

ISSN 2379-5980 (online)
associated article DOI
10.5915/LEDGER.2016.15

The present paper here takes a fairly trivial approach, since the “blockchain” has to replay all of the steps since the previous checkpoint (so no privacy, and worst-case efficiency).

[A] How to Use Bitcoin to Play Internet Poker
http://www.cs.technion.ac.il/~ranjit/papers/poker.pdf

[B] Hawk: The Blockchain Model of Cryptography and Privacy-Preserving Smart Contracts
https://eprint.iacr.org/2015/675.pdf

[C] A Fast and Scalable Payment Network with Bitcoin Duplex Micropayment Channels
http://link.springer.com/chapter/10.1007/978-3-319-21741-3_1#page-1

[D] Optimal Efficiency of Optimistic Contract Signing
http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.75.8114&rep=rep1&type=pdf

Reviewer E:

Although the contribution appears novel, I found I was desiring more detail of the actual (possible) implementation- especially when it came to understanding Huntercoin. In order to get the most of the article: I had to read it first, then perform significant research to understand Huntercoin, and then read the submission again. I do not feel this should be the case of most readers and thus the paper should provide more substance regarding how to reduce the contribution to practice and should be able to stand on its own without simply pointing readers to towards the implementation details of Huntercoin.

Moreover, these additional questions came up during my review. The quantity of questions (on its own) suggests that more work is needed. See below:

================

There should be more information about the rules of the game (Huntercoin) and how the concept of side chains relates to that.

Can bots be eliminated within disputes - it sounds like they are a big problem for Huntercoin. If you create a game channel to prove that both players are human, can the game channel then augment huntercoin game play?

How are the rules of the Game Channel codified and agreed upon?

Can you formalize the type of game and what game theoretic properties can be analyzed?

Can the rules of the side channel game be statically analyzed? What prevents bad rules?

ISSN 2379-5980 (online)
associated article DOI
10.5915/LEDGER.2016.15

What happens if you create absurd rules that only a bot would agree to, can you defraud if you rig the game successfully?

How can others verify the rules were good and what affect does this have on dispute resolution?

What happens if a signed move is actually not valid given the rules or the state of the game?

What makes Huntercoin different that it allows the concept of Game Channel?

What can be improved in huntercoin or otherwise and what types of games does this work for and not work for?

How is the state of the huntercoin game represented and what constraints does this put on the Game Channels?

Describe in better detail (for the uninitiated reader) how/what state, actions and acceptance criteria for wins/awards/losses are represented

It seems like the paper is just about introducing side chains to huntercoin. Thus, a better review of the concept of side chains is needed and what is different about this implementation?

To what extend has this been implemented and what examples of side channel games exist (if any)?

2B. Author's Responses

In general, the main messages of the reviews so far seem to be two points:

1) A lot of reviewers asked for additional details about the virtual worlds and gaming ideas in general and Huntercoin in particular.

2) Concerns were raised about the novelty of the content, particularly as it is formulated very abstractly and in general terms. This also raised the issue of how game rules are specified and verified in a general setting.

After recourse with the editors, I was able to extend the paper beyond the initial 4,000 word limit, and thus address these two concerns with a major extension in the following way:

1) I've added an entirely new background section describing Huntercoin on a high-level, including how the gaming and virtual world is integrated with the blockchain layer. I also

discussed metrics of the Huntercoin blockchain to motivate why game channels are interesting in this context.

2) Another new section is added at the end, where I describe concretely how game channels can be applied to Huntercoin and allow virtual worlds to scale by sharding them. This is what I believe is completely new material and my own actual interest in game channels.

More specifically, the concerns raised by reviewers D and E in the second round of review have been addressed as follows:

Reviewer D:

I am very glad for the literature suggested by the reviewer, as I am not from this particular academic background. My own interest with the paper is mostly the application to Huntercoin-like game worlds and not the abstract protocol. Due to the extension, I was able to point this out more clearly. The paper now explicitly states that the discussed protocol should not be seen as state-of-the-art research about abstract contract signing, but more about one possibility (that may be refined with more complex abstract protocols) to allow the final application to game worlds. For this purpose, I have also cited some of the suggested literature.

Since the reviewer acknowledges that game worlds like Huntercoin are a novel concept (pioneered by Huntercoin), I think that this should alleviate most concerns the reviewer raised.

Reviewer E:

The main concerns should be addressed with the new background section, which gives exactly the information the reviewer asks for: It should give the information necessary to understand the paper without having to research Huntercoin, and the revised paper details much more how the side-chain concept relates specifically to Huntercoin.

I also briefly discuss the issue of bots, although I think that this is only slightly related to the paper---bots appear to not be a big issue any more in Huntercoin after changing the game rules, and handling them is more a game-mechanics issue than something requiring game channels.

All the questions about verifying game rules are not directly related (at least any more), since my situation is about a game where the rules are already prescribed. This should be more clear now that I refined the paper to be more directly about Huntercoin.

2C. Final Reviewer Appraisal

Reviewer F:

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

ISSN 2379-5980 (online)
associated article DOI
10.5915/LEDGER.2016.15

Yes

If you answered "yes" to the previous question, in one sentence, describe in your own words the novel contribution made by this paper:
Using blockchains to permit players to verify the game state, "human mining" and scaling via "geographic" sharding.

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 20%

Please provide your free-form review for the author in this section:
This paper is significantly improved from the initial submission. I recommend that it be accepted subject to the author meeting any requests the editor might have to meet Ledger's formatting requirements.

Note some awkward english on p. 1:
"allows to get rid of" -> "removes the need for"
"this allows to build" -> "this allows building"

Please provide your recommendation to the Editor.
Accept (this paper should be published subject only to minor corrections [described in my comments] that can be coordinated between the author and editor)

Ledger is published by the University Library System of the University of Pittsburgh as part of its D-Scribe Digital Publishing Program and is cosponsored by the University of Pittsburgh Press.

ISSN 2379-5980 (online)
associated article DOI
10.5915/LEDGER.2016.15