

## #203066: Legally binding anonymous multiparty commitments on a blockchain

Authors:  233657 [Debasish Ray Chawdhuri](#) (Talentica Software Pvt. Ltd.)

Send a message to these authors using your personal email client: [debasish.chawdhuri@talentica.com](mailto:debasish.chawdhuri@talentica.com)

**Abstract:** In recent times, many blockchain solutions have been proposed for automatic electronic contracts on a blockchain. The most prominent example of it is Ethereum smart contracts. However, smart contracts are only restricted to crypto-assets as the objects of the contracts. In many cases, it is necessary to be able to sign contracts involving things in the physical world that are not represented in the form of crypto-assets. Such contracts can be legally enforced after all the parties have signed them in case any party backs out after signing the contracts. We propose a solution to advertise and sign anonymous multi-party contracts that are designed to be acceptable and enforceable in a court of law once they are signed. To enable this, we also provide a novel demonstrable ring signature that allows a designated beneficiary to be able to break the anonymity of the signer.

**Topics:** Blockchain-Based Applications and Services  
Smart Contracts  
Security, Privacy, Attacks, and Forensics

**Conference and track:** ICBC 2020 / Poster Papers

**Category:** Full Paper

IEEE  
Copyright  
System  
Status  
Copyright  
type


**Paper identifier:** 331133748

**Notes:**



**Printing problems:**



**Status:** 

Uploaded files:	Description	Upload deadline	Allowed file types	Max size	Upload	Show	Size	Bibtex	Created	Delete
	Paper manuscript	Feb 08, 2020 - 03:10 PM (-03)	pdf				0.2 MB	<a href="#">[Bibtex]</a>	Dec 08, 2019 - 01:21 PM	

Type	Reviewer	Assigned (history)	Assigned by	Confirmed	Reminded	Due	Completed
review		2019-12-20 09:56:11	2019-12-20 09:56:11	2019-12-20 23:15:26	2020-01-22 23:21:40	2020-01-31	2020-01-25 23:14:50
2: Relevance:	3: Technical Content and Originality:	4: Organization and Presentation:	5: Reference to Related Work:	6: Overall Recommendation about accepting the contribution:	7: Poster acceptance: If this paper happens to be rejected, please express your opinion on accepting it as a poster.		
2: Somewhat Relevant	2: Fair	2: Poor	2: Poor	2: Weak Reject - I will not fight strongly against it	3: Weak Accept - I will not fight strongly in favor of accepting this work as a poster		

**8: What are the major strengths of this paper?**

This research is motivated not from smart-contract but from a kind of physically binding contract, which sounds a new: "In many cases, it is necessary to be able to sign contracts involving things in the physical world that are not represented in the form of crypto-assets. Such contracts can be legally enforced after all the parties have signed them in case any party backs out after signing the contracts."

The approach to resolve this issue is by cryptographic multiparty protocol, and the author propose a solution.

**9: What are the major shortcomings of this paper?**

The lack of the existing research survey:

The core technique of the proposal scheme is a RING signature with designated verifiers: "We propose a novel demonstrable ring signature that allows the anonymity of the signer but allowing the beneficiary of the signature to be able to know the true identity of the signer. The beneficiary is also able to demonstrate the true identity of the signer to anyone."

But, a very poor references on this topic.

**10: Comments for the authors (provide any detailed comments to improve the paper; also comment on any missing related work)**

The core technique of the proposal scheme is a RING signature with designated verifiers, and indeed some references: "A designated verifier signature [9], on the other hand, can be verified by only a chosen verifier that the signer intended to. A verifiable ring signature [10] is a ring signature that allows the signer to prove he/she indeed is the real signer to a verifier if he/she wants to."

However, more many exiting works on this topic, which should be surveyed well for distinguish the author's novelty: e.g. A STRONG DESIGNATED-VERIFIER RING SIGNATURE SCHEME PROVIDING ONE-OUT-OF-ALL SIGNER ANONYMITY

<https://jit.ndhu.edu.tw/article/view/688>

review	2019-12-20 09:56:11	2019-12-20 09:56:11	2020-01-13 06:24:26	2020-01-22 23:21:40	2020-01-31	2020-01-25 01:46:32
<b>2: Relevance:</b>	<b>3: Technical Content and Originality:</b>	<b>4: Organization and Presentation:</b>	<b>5: Reference to Related Work:</b>	<b>6: Overall Recommendation about accepting the contribution:</b>	<b>7: Poster acceptance:</b> If this paper happens to be rejected, please express your opinion on accepting it as a poster.	
3: Highly Relevant	3: Good	3: Good	3: Good	3: Weak Accept - I will not fight strongly in favour of acceptance	4: Strong Accept - I have strong arguments in favor of accepting this work as a poster	

**8: What are the major strengths of this paper?**

An interesting paper exploring an issue with real impact. The solution proposed seems adequate and sound.

The paper reads well overall and the flow is easy to follow. There are minor writing issues but they do not affect readability of the paper.

**9: What are the major shortcomings of this paper?**

The flow of the text at part needs to improve. Detailed comments are included in the following section.

The technical discussions at part need to improve. Specific recommendations are included in the following section.

**10: Comments for the authors (provide any detailed comments to improve the paper; also comment on any missing related work)**

Below are some specific comments that the author may find useful:

## \* Abstract:

Contributions well presented

- a. Advertise and sign legally enforceable contracts
- b. Novel demonstrable ring signature

## \* Introduction:

1. Good motivation analysis
2. A good description of the proposed solution
  - a. Anyone authorized can post anonymous advertisements for contracts
  - b. Anyone can communicate anonymously with advertiser
  - c. The system ensures all signatures made by validated users, but they still stay anonymous
  - d. The system ensures that identities know one another, but the contract stays anonymous. In case someone breaks the contract, the other must be able to prove the ID of the "breakers"
  - f. Two different kinds of contracts
  - g. The solution to the case of one party exiting the contract without signing, and knowing the identities of others who have already signed.

## Content issues

1. Reference to [6] lacks details, the description is not enough to get an idea of what

the referenced system does.

Writing issues

A. Typo: later is used instead of latter

B. "A system called Hawk [S], privacy is achieved [.]", it should be "In a system called [.]" instead

C. "Since the public keys [.] , a nd we assume [.]". If you start the sentence with "since" it is not correct to use "and" to introduce the corresponding countermeasure.

\* Contribution

The contributions are presented in a clear manner. However, the order in which the contributions are presented is different from the order in which each contribution is later elaborated in detail in their own dedicated sections.

\* Notations:

The authors give a very detailed explanation of the notations used.

\* Demonstrable Ring Signature

1. Instead of having a background section, the author briefly mentions the needed background for the contribution (demonstrable ring signature) presented in this section. These mentions are not detailed enough for someone who is not familiar with the topics. For example, the explanation of a ring signature is very short and, from this point on, it is given for granted, leaving the reader quite confused as the concept appears to have an important role in the rest of the section.
2. The first five paragraphs, which have the purpose to give a first simple explanation of what a demonstrable signature is in practice, are quite confusing and not really effective in their purpose.

\* Blockchain Model:

1. Due to the unclear explanation of the demonstrable signature in section IV, here it is difficult to understand what the function `verifyDemonstrableSignature()` does.

\* Multi-party commitments

the author presents one of the two types of contracts: the seller-buyer commitments, which allows a "seller to get paid in cryptocurrency for something written in a legal contract, which is not a smart contract but preferably structured." This is a potentially important limitation of the proposed solution because the possibility of enforcing this "preferably structured" commitment is dependant on the structure itself. If this commitment is not written well from a "law point of view", then the technology proposed by this paper is not really useful, because the contract cannot be enforced for law reasons.

review	2019-12-20 09:56:11	2019-12-20 09:56:11	2020-01-23 00:35:17	2020-01-22 23:21:41	2020-01-31	2020-01-24 01:58:15
<b>2: Relevance:</b>	<b>3: Technical Content and Originality:</b>	<b>4: Organization and Presentation:</b>	<b>5: Reference to Related Work:</b>	<b>6: Overall Recommendation about accepting the contribution:</b>	<b>7: Poster acceptance:</b> <i>If this paper happens to be rejected, please express your opinion on accepting it as a poster.</i>	
2:Somewhat Relevant	2:Fair	2:Poor	2:Poor	2:Weak Reject - I will not fight strongly against it	3: Weak Accept - I will not fight strongly in favor of accepting this work as a poster	

**8: What are the major strengths of this paper?**

The main contribution of the paper seems to be the Zero-Knowledge Proof of Linear Member Tuple (ZKPLMT).

The paper also tries to bring binding of anonymous binding multiparty commitments to a blockchain.

The discussion and the theorems (and their proofs) on the ZKPLMT.

**9: What are the major shortcomings of this paper?**

The paper presents several problems related to the blockchain part. Some of them should be rewritten before the paper is accepted.

The paper seems to have two separate parts. Each part could be a separate paper, which would give more space for further discussion on each part.

There is a lack of related work discussion.

**10: Comments for the authors (provide any detailed comments to improve the paper; also comment on any missing related work)**

The paper presents an interesting section on the Zero-Knowledge Proof. It seems interesting but could have been in a different paper in itself, hence more discussion and samples or even an implementation of the system could have been presented.

The first part, which discusses the blockchain part, has several issues that should be corrected since it might bring some confusion to the reader.

In your abstract, you mention that "smart contracts are only restricted to crypto-assets", which is not the case. There are several samples where smart contracts are used, in healthcare, IoT, smart cities, supply chain, ..., in which not only crypto-assets are the used objects.

In your first paragraph, it seems that smart contracts are applications of the blockchain, which is not true. Smart contracts are more generic and have been used in blockchains. Smart contracts were defined before blockchains. There is a missing reference to that.

You present the proof-of-work consensus algorithm as an asset of the blockchain. What does that mean?

You have only one paragraph describing related work - the sixth paragraph of the introduction.

If you need an authority to legally enforce a signature, this authority might be a centralized system. If that the case, then one of the main ideas of blockchain, distributiveness, might be compromised.

You should include some references to the UTXO model at the beginning of Section V, and describe it briefly. Also, a reference to KYC.

You could explain when a transaction is valid and when it is invalid.

Why do you need a modified contract M'?

It is not clear what offline negotiation means and how the result is brought to the system.

If participants can abandon the protocol, couldn't that bring some security or privacy issues to the system, since someone can enter several signings in order to know who is participating in contracts after they abandon the contract?

How the participants negotiate a modified contract M' and how they decide the order of the signing?

review	2019-12-20 09:56:11	2019-12-20 09:56:11	2020-01-15 13:52:31	2020-01-09 13:20:54	2020-01-31	2020-01-16 19:58:08
<b>2: Relevance:</b>	<b>3: Technical Content and Originality:</b>	<b>4: Organization and Presentation:</b>	<b>5: Reference to Related Work:</b>	<b>6: Overall Recommendation about accepting the contribution:</b>	<b>7: Poster acceptance:</b> If this paper happens to be rejected, please express your opinion on accepting it as a poster.	
3:Highly Relevant	3:Good	2:Poor	3:Good	3:Weak Accept - I will not fight strongly in favour of acceptance	3: Weak Accept - I will not fight strongly in favor of accepting this work as a poster	

**8: What are the major strengths of this paper?**

The approach to determine approach for legally enforcing Smart Contracts applied to physical objects in the real world is very important. The technical support is provided by a new ring signature. Trades are formally defined by atomic swaps in case of cryptographic origins of tokens, however, non-native token swaps are based on cryptographic representations of physical assets. Thus, a third party may be required to ensure that the physical assets are correctly represented in the digital domain. Therefore, privacy-preserving contracts are key.

**9: What are the major shortcomings of this paper?**

The paper lacks the full-fledged set of arguments, why certain assumptions made hold and in which way the specifics of an fine design, as well as an implementation, may look like the next comments exemplify this statement made. Furthermore, while the theoretical approach seems to be sound, the technical dimension on how to specify such extensions determined remains basically unanswered. The approach reads quite well on the theoretical side, however, the practical prototyping dimensions and related problems or lacking clarity are not addressed at all and all high-level assumptions made (which are very true and relevant) are never being returned to in any suitable explanation with respect to the newly developed mechanisms.

**10: Comments for the authors (provide any detailed comments to improve the paper; also comment on any missing related work)**

Why are SC restricted to crypto assets?

Sec 1 is well written and the required properties are clearly listed.

Sec 2 is a bit short and it may makes sense to integrate it into Sec 1

Sec 3 may be added as an appendix or integrated into Sec 3, because it does not deliver digestable information, due to the lack of reasons even notations may see arguments on why they are needed the way they are defined. Sec 4 starts a bit with related work, thus the separation of material and methods form your own work is lost. Reconsider a new Section on background and/or related work, which clearly presents knowledge you base your proposal on. And Sec 3 as well Sec XXX introduce the ring signature unnecessarily twice.

Sec 5 extends the UTXO model with a new functionality, which is not clearly described: How can a UTXO models functions being called, while they do not cause the use of a UTXO model? Furthermore, it is not clear, in which way the system methods can be implemented in a secure and reliable manner. Unfortunately, the description is less detailed as needed, since the protocol requires some broadcast of messages remains very vague, some is highly unspecific!

Sec 6 defines two types of contracts, which do not seem to be new, since a similar distinction had been made in [A]. Unfortunately, Sec 6 ends as well without a clear information on how these types of contracts are being specified within a concrete use case and deployed in a suitable application.

Sec 7 addresses the Zero-Knowledge Proofs, in which it was hard, even impossible to determine which updates, changes, or additions e.g., compared to [7] had been made. A statement like we are faster lacks the justification.

Sec 8 starts of the with the details of the obviously, however, not made explicit new ring signature: what is new or different here? It starts off with a problematic statement: .. has three parties and the list of (a) signer, (b) several beneficiaries, and (c) a verifier results in at least four parties involved Thus, it is better to term the first sentence as has three roles etc.

Sec 9 drops out of the blue with the term ZkPLMT what is that? And this section is not bound in an explicit manner to the sections before, thus, the fine design is incomplete. Although this Sec and the one before provide theoretical proofs, their relation and clear binding to the statements made in Sec 1 are not clear at all, since only implicitly being hidden in your flow of arguments. This is, very unfortunately, the key problem of the paper it states and outlines highly relevant goals and properties and starts to dive into theoretical details, which are never mapped onto those initial statements made, thus, the readability of the paper is basically fully lost, since the reader needs to redo the thinking and work the author already did, which is improper.

Finally, Sec 10 is basically decoupled from Sec 2 to Sec 9, as these sections read like pieces of a very nice mosaic, which is never glued together, thus, lacking to deliver the message which would be a very important one if it could work not only in theory but in practice, too.

Generally, the paper is way too modularized in terms separate sections, which are too small and floating. Thus, unnecessary connecting sentences exist, such as the last before Sec V, which hampers the harmonized readability.

[A] Sina Rafati Niya, Florian Schüpfer, Thomas Bocek, Burkhard Stiller: A Peer-to-peer Purchase and Rental Smart Contract-based Application (PuRSCA); De Gruyter, it-Information Technology, Vol. 60, No. 5, October 2018, ISSN 2196-7032, pp 307320.

**Withdraw this paper** 



[\[Conference chair\]](#)

A service of [Maintained by](#) [Cooperation with](#)

