Dear authors,  
  
Your reviewers agreed upon some acceptance criteria for your paper's revision. We listed some clarification questions and corrections below. Please first read ALL THE REVIEWS carefully and address the revision list accordingly.  
  
Timeline: You are expected to finalize the revised version within 4 weeks.  
  
Working style: Please expect to have an interactive discussion to make sure that we are not missing any important point. That means that the requirement list could be updated with some additions and clarifications.  
  
Changelog: Please make sure you use latexdiff or similar tools when making the updates so that we make faster progress.  
  
Thanks for your collaboration and looking forward to working with you.  
  
  
Revision List:  
- Please detail further how PwDR is different than other Merkle Tree+block chain-based approaches.--> done-- page 2, 2nd column  
  
- Please indicate which party runs the algorithms defined in the Interface (Section 6).--> done  
  
- There are unclear parts in the security definitions. The definitions enumerate a set of conditions to pass for an attack to happen by a malicious client such as convincing the auditors that the bank did not issue a warning even though it did and two more. In the Definition 3, however, the conditions in the Pr, it is confusing that \sum\_j w\_{1,i} < e and v\_1 = 1 can conjugate with an AND. The description of v\_1 = 1 is that it satisfies that \sum\_j w\_{1,j} >= e. (Same for w\_{2, j} and v\_2). So, the condition in Pr is satisfied only if the algorithms verComplaint and resDispute does not run correctly. However, the protocols look like deterministic. How would that work?- Please clarify if the correctness of the protocol is randomized or deterministic.--> Now we have added a new appendix, Appendix A, to address the comment.

- Please discuss which part of the security definitions correspond the informal description.--> done—now we tag each event in Definitions 3 and 4 with the same label (e.g., (i)), used before the definition to describe the event informally. For instance, before Definition 3, we say: “…(i) make at least the threshold of the auditors, D𝑗 s, conclude that B should have provided a warning, although B has done so…” then in Definition 3 (in Pr) we say:

Diagram

Description automatically generated

- Please clarify: how would it be possible to include a smart contract in the middle of a communication between customer and bank server while still maintaining the end-to-end security of the communication? 🡪 In PwDR a smart contract is mainly used to securely log messages exchanged between the bank and the customer; other tamper-evident logging mechanisms can also be used. Also, in the case where new regulations oppose using a public blockchain, a permissioned and/or private blockchain can be used.

Moreover, PwDR itself offers three main features that a secure channel (such as TLP) would offer; namely, it offers (i) user authentication: because (i.1) the bank’s and customer’s identity, their public key, and their (Ethereum) account address are known to each other, (i.2) both parties know the smart contract’s fixed address so they can send messages directly to it, and (i.3) the bank and customer sign the messages that they send to a smart contract (as it is required by blockchain network), (ii) data integrity: due to use of digital signature and immutability of blockchain, and (iii) data privacy: as each party encrypt each outgoing messages, so the parties messages on the smart contract remains confidential from unauthorised parties.

Furthermore, in PwDR, a client still needs to log into its online banking account using standard mechanisms (e.g., using the bank’s website and multi-factor authentication mechanisms).   
  
- Please clarify: how does the proposed voting protocol compare to existing voting protocols? More specifically, in Section 7.4, the auditors need to agree on a shared secret key in order to participate in voting protocols. Why pis such a costly approach chosen in the protocol?-->   
  
- Please add an analysis about the auditors impact on the performance of the system.  
  
- Please revise: Section 4.1 is a taxonomy and not a threat model. Section 4.3 the definition of Smart contract needs to be revised.  
  
- It would be good to have the security analysis in the main body. Can the introduction be shortened?  
  
- Theorem 1 refers to several encryption schemes. The specification doesn't make clear that different encryption schemes are used. Please clarify.