

Abstract: Typically, a decentralized collaborative blockchain decision-making mechanism is realized by remote voting. To date, a number of blockchain voting schemes have been proposed; however, to the best of our knowledge, none of these schemes achieve coercion-resistance. In particular, for most blockchain voting schemes, the randomness used by the voting client can be viewed as a witness/proof of the actual vote, which enables improper behaviors such as coercion and vote-buying. Unfortunately, the existing coercion-resistant voting schemes cannot be directly adopted in the blockchain context. In this work, we design the first scalable coercion-resistant blockchain decision-making scheme that supports private differential voting power and 1-layer liquid democracy as introduced by Zhang et al. (NDSS'19). Its overall complexity is $\mathcal{O}(n)$, where n is the number of voters. Moreover, the ballot size is reduced from Zhang et al.'s $\mathcal{O}(n^2)$ to $\mathcal{O}(n)$, where n is the number of experts and/or candidates. Its incoercibility is formally proven under the UC incoercibility framework by Alwen et al. (Crypto'15). We implement a prototype of the scheme and the evaluation result shows that our scheme's tally procedure is more than 6x faster than VoteAgain (USENIX'20) in an election with over 10,000 voters and over 50% extra ballot rate.

@misc{cryptoeprint:2023/1578, author = {Zeyuan Yin and Bingsheng Zhang and Andrii Nastenko and Roman Oliynykov and Kui Ren}, title = {A Scalable Coercion-resistant Blockchain Decision-making Scheme}, howpublished = {Cryptology ePrint Archive, Paper 2023/1578}, year = {2023}, note = {\url{https://eprint.iacr.org/2023/1578}}, url = {https://eprint.iacr.org/2023/1578} }

<https://eprint.iacr.org/2023/1578>