3:Chaieb, M., Yousfi, S., Lafourcade, P., & Robbana, R. (2019). Verify-your-vote: A verifiable blockchain-based online voting protocol. In *Information Systems: 15th European, Mediterranean, and Middle Eastern Conference, EMCIS 2018, Limassol, Cyprus, October 4-5, 2018, Proceedings 15* (pp. 16-30). Springer International Publishing.

**Verify Your Vote A Verifiable Blockchain based Onl-WT\_Summaries**

**Brief Description of the Topic:**

The paper presents "Verify-Your-Vote" (VYV), an innovative online voting system utilizing Blockchain technology. It aims to ensure secure and verifiable elections by leveraging robust cryptographic primitives and a transparent bulletin board system. VYV offers a comprehensive set of properties, including eligibility verification, voter authentication, vote privacy, receipt-freeness, fairness, and both individual and universal verifiability. The protocol’s design emphasizes security and trust in the voting process while maintaining voter privacy and integrity.

**Conclusions of the Paper:**

The research introduces the VYV protocol, showcasing its novel approach to online voting. By scrutinizing various existing systems like TIVI, Follow My Vote, Open Vote Network, and Agora, the paper demonstrates that VYV provides enhanced security and privacy features compared to its counterparts. The VYV protocol utilizes Blockchain technology, a public bulletin board, and cryptographic primitives to ensure a persistent view for voters, securing the election process from eligibility validation to result verification. The study substantiates the system's robustness through security analyses and formal verification using ProVerif, confirming its ability to maintain vote privacy, authentication, and coercion resistance while enabling scrutiny of the voting process.

**Critical Opinion of the Paper:**

While the paper offers an intricate analysis of the VYV protocol and its security measures, some aspects could be further elaborated. The paper occasionally assumes familiarity with advanced cryptographic concepts, potentially alienating readers not well-versed in this domain. A more detailed explanation or supplementary material on these concepts would enhance accessibility and understanding. Additionally, while the security analyses using ProVerif are informative, practical implementation challenges or real-world feasibility studies could add depth to the paper. Exploring the scalability and practical applicability of VYV in diverse election scenarios would augment its practical relevance.

The paper's comprehensive exploration of cryptographic primitives and formal verifications establishes the robustness of the VYV protocol. However, expanding on real-world use cases, potential challenges in deployment, and considerations for large-scale implementation would provide a more holistic view. Addressing these aspects would solidify the paper's contribution, making it more accessible and impactful for a broader audience interested in secure e-voting systems.