# Article information:

SCPKI | Proceedings of the ACM Workshop on Blockchain, Cryptocurrencies and Contracts
<https://dl.acm.org/doi/10.1145/3055518.3055530>

# Article summary:

1. The current Public Key Infrastructure (PKI) system has several drawbacks due to its centralised and non-transparent design.

2. SCPKI is an alternative PKI system based on a decentralised and transparent design using a web-of-trust model and a smart contract on the Ethereum blockchain.

3. This system makes it easier to detect rogue certificates when they are published, as well as allowing for fine-grained identity verification of entities in the system.

# Article rating:

May be slightly imbalanced: The article presents the information in a generally reliable way, but there are minor points of consideration that could be explored further or claims that are not fully backed by appropriate evidence. Some perspectives may also be omitted, and you are encouraged to use the research topics section to explore the topic further.

# Article analysis:

The article is generally trustworthy and reliable, providing an overview of the current Public Key Infrastructure (PKI) system and its drawbacks, as well as introducing an alternative solution in SCPKI which uses a web-of-trust model and a smart contract on the Ethereum blockchain. The article provides evidence for its claims, such as instances of certificate authorities publishing rogue certificates for targeted attacks, and explains how SCPKI can help to address these issues. It also provides information about the acceptance rates of the workshop where this paper was presented, which adds credibility to the article's claims.

The article does not appear to have any major biases or one-sided reporting; it presents both sides of the argument fairly by discussing both the drawbacks of the current PKI system and how SCPKI can be used to address them. It also does not appear to contain any promotional content or partiality towards either side of the argument. However, there are some points that could be explored further in order to provide more comprehensive coverage of this topic; for example, there is no discussion about possible risks associated with using SCPKI or potential challenges that may arise from its implementation. Additionally, while it does provide evidence for its claims, there is no exploration of counterarguments or other perspectives that could be taken into consideration when evaluating this proposed solution.

# Topics for further research:

* Risks associated with SCPKI
* Challenges of implementing SCPKI
* Counterarguments to SCPKI
* Alternatives to SCPKI
* Advantages of PKI system
* Security implications of web-of-trust model

# Report location:

<https://www.fullpicture.app/item/7f3b049172fbf7587a6501f1bd30e5a6>