



All



ADVANCED SEARCH

Conferences > 2016 IEEE Symposium on Security

Hawk: The Blockchain Model of Cryptography and Privacy-Preserving Smart Contracts

Publisher: IEEE

Cite This

PDF

Ahmed Kosba ; Andrew Miller ; Elaine Shi ; Zikai Wen ; Charalampos Papam... All Authors

1036 Paper Citations

44 Patent Citations

65355 Full Text Views



Alerts

- Manage Content Alerts
- Add to Citation Alerts

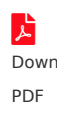
Free

Need Full-Text
access to IEEE Xplore for your organization?
CONTACT IEEE TO SUBSCRIBE >

IEEE CLIMATE CHANGE COLLECTION

Learn More

Abstract



Authors

Figures

References

Citations

Keywords

Metrics

More Like This

Abstract:Emerging smart contract systems over decentralized cryptocurrencies allow mutually distrustful parties to transact safely without trusted third parties. In the event of c... **View more**

Metadata

Abstract: Emerging smart contract systems over decentralized cryptocurrencies allow mutually distrustful parties to transact safely without trusted third parties. In the event of contractual breaches or aborts, the decentralized blockchain ensures that honest parties obtain commensurate compensation. Existing systems, however, lack transactional privacy. All transactions, including flow of money between pseudonyms and amount transacted, are exposed on the blockchain. We present Hawk, a decentralized smart contract system that does not store financial transactions in the clear on the blockchain, thus retaining transactional privacy from the public's view. A Hawk programmer can write a private smart contract in an intuitive manner without having to implement cryptography, and our compiler automatically generates an efficient cryptographic protocol where contractual parties interact with the blockchain, using

Accept & Close

adopt such a formal model when designing applications atop decentralized blockchains.

Published in: 2016 IEEE Symposium on Security and Privacy (SP)

Date of Conference: 22-26 May 2016 **INSPEC Accession Number:** 16232874

Date Added to IEEE Xplore: 18 August 2016 **DOI:** 10.1109/SP.2016.55

Publisher: IEEE

► **ISBN Information:**

Conference Location: San Jose, CA, USA

Electronic ISSN: 2375-1207

Contents



Authors



Figures



References



Citations



Keywords



Metrics



[CHANGE USERNAME/PASSWORD](#)

[PAYMENT OPTIONS](#)

[COMMUNICATIONS PREFERENCES](#)

[US & CANADA: +1 800 678 4333](#)



[VIEW PURCHASED DOCUMENTS](#)

[PROFESSION AND EDUCATION](#)

[WORLDWIDE: +1 732 981 0060](#)

[TECHNICAL INTERESTS](#)

[CONTACT & SUPPORT](#)

[About IEEE Xplore](#) [Contact Us](#) [Help](#) [Accessibility](#) [Terms of Use](#) [Nondiscrimination Policy](#) [IEEE Ethics Reporting](#) [Sitemap](#)
[IEEE Privacy Policy](#)

IEEE Account

- » [Change Username/Password](#)
- » [Update Address](#)

Purchase Details

- » [Payment Options](#)
- » [Order History](#)
- » [View Purchased Documents](#)

Profile Information

- » [Communications Preferences](#)
- » [Profession and Education](#)
- » [Technical Interests](#)

Need Help?

- » **US & Canada:** +1 800 678 4333
- » **Worldwide:** +1 732 981 0060
- » [Contact & Support](#)

A not-for-profit organization, IEEE is the world's largest technical professional organization dedicated to advancing technology for the benefit of humanity.

© Copyright 2022 IEEE - All rights reserved. Use of this web site signifies your agreement to the terms and conditions.