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

Publisher: IEEE

Ahmed Kosba ; Andrew Miller ; Elaine Shi ; Zikai Wen ; Charalampos Papamanthou **All Authors**

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 cryptographic primitives such as zero-knowledge proofs. To formally define and reason about the security of our protocols, we are the first to formalize the blockchain model of cryptography. The formal modeling is of independent interest. We advocate the community to 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 **DOI:** 10.1109/SP.2016.55

Date Added to IEEE *Xplore*: 18 August 2016

Publisher: IEEE

ISBN Information:

Conference Location: San Jose, CA, USA

Electronic ISSN: 2375-1207

Contents