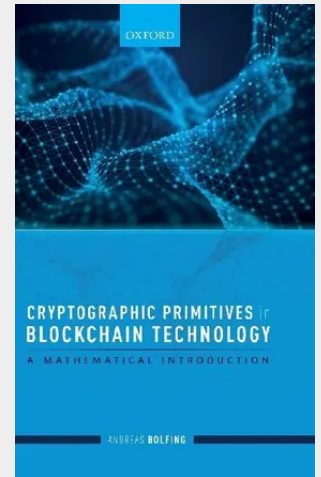


CRYPTOGRAPHIC PRIMITIVES IN BLOCKCHAIN TECHNOLOGY

Many online applications, especially in the financial industries, are running on blockchain technologies in a decentralized manner, without the use of an authoritative entity or a trusted third party. Such systems are only secured by cryptographic protocols and a consensus mechanism. As blockchain-based solutions will continue to revolutionize online applications in a growing digital market in the future, one needs to identify the principal opportunities and potential risks. Hence, it is unavoidable to learn the mathematical and cryptographic procedures behind blockchain technology in order to understand how such systems work and where the weak points are. Cryptographic Primitives in Blockchain Technology provides an introduction to the mathematical and cryptographic concepts behind blockchain technologies and shows how they are applied in blockchain-based systems. This includes an introduction to the general blockchain technology approaches that are used to build the so-called immutable ledgers, which are based on cryptographic signature schemes. As future quantum computers will break some of the current cryptographic primitive approaches, Andreas Bolfing considers their security and presents the current research results that estimate the impact on blockchain-based systems if some of the cryptographic primitive break. Based on the example of Bitcoin, he shows that weak cryptographic primitives pose a possible danger for the ledger, which can be overcome through the use of the so-called post-quantum cryptographic approaches.

Cryptographic Primitives in Blockchain Technology provides an introduction to the mathematical and cryptographic concepts behind blockchain technologies and shows how they are applied in blockchain-based systems.



130,30 €

130,30 € (zzgl. MwSt.)

Lieferfrist: bis zu 10 Tage

Artikelnummer: 9780198862840

Medium: Buch

ISBN: 978-0-19-886284-0

Verlag: ACADEMIC

Erscheinungstermin: 10.09.2020

Sprache(n): Englisch

Auflage: Erscheinungsjahr 2020

Produktform: Gebunden

Gewicht: 681 g

Seiten: 352

Format (B x H): 161 x 240 mm

