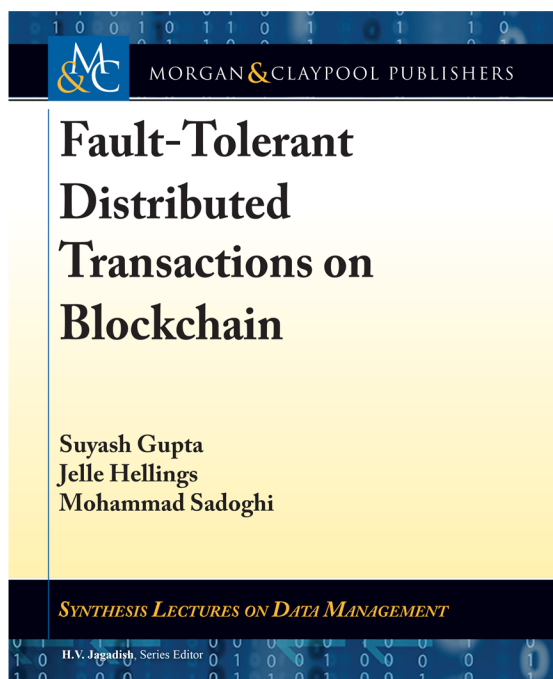▶ An in-depth study of blockchain, unraveling its revolutionary promise to instill computational trust in society, all carefully tailored to a broad audience including students, researchers, and practitioners.

Fault-Tolerant Distributed Transactions on Blockchain

Suyash Gupta, *University of California, Davis*
Jelle Hellings, *University of California, Davis*
Mohammad Sadoghi, *University of California, Davis*

Since the introduction of Bitcoin—the first widespread application driven by blockchain—the interest of the public and private sectors in blockchain has skyrocketed. In recent years, blockchain-based fabrics have been used to address challenges in diverse fields such as trade, food production, property rights, identity-management, aid delivery, health care, and fraud prevention. This widespread interest follows from fundamental concepts on which blockchains are built that together embed the notion of trust, upon which blockchains are built.

1. Blockchains provide data transparency. Data in a blockchain is stored in the form of a ledger, which contains an ordered history of all the transactions. This facilitates oversight and auditing.

2. Blockchains ensure data integrity by using strong cryptographic primitives. This guarantees that transactions accepted by the blockchain are authenticated by its issuer, are immutable, and cannot be repudiated by the issuer. This ensures accountability.

3. Blockchains are decentralized, democratic, and resilient. They use consensus-based replication to decentralize the ledger among many independent participants. Thus, it can operate completely decentralized and does not require trust in a single authority. Additions to the chain are performed by consensus, in which all participants have a democratic voice in maintaining the integrity of the blockchain. Due to the usage of replication and consensus, blockchains are also highly resilient to malicious attacks even when a significant portion of the participants are malicious. It further increases the opportunity for fairness and equity through democratization.

These fundamental concepts and the technologies behind them—a generic ledger-based data model, cryptographically ensured data integrity, and consensus-based replication—prove to be a powerful and inspiring combination, a catalyst to promote computational trust. In this book, we present an in-depth study of blockchain, unraveling its revolutionary promise to instill computational trust in society, all carefully tailored to a broad audience including students, researchers, and practitioners. We offer a comprehensive overview of theoretical limitations and practical usability of consensus protocols while examining the diverse landscape of how blockchains are manifested in their permissioned and permissionless forms.

CONTENTS

Print & eBooks at http://store.morganclaypool.com