Record Nr. UNINA9910974077103321 Autore Judmayer Aljosha Titolo Blocks and Chains: Introduction to Bitcoin, Cryptocurrencies, and Their Consensus Mechanisms / / by Aljosha Judmayer, Nicholas Stifter, Katharina Krombholz, Edgar Weippl Cham:,: Springer International Publishing:,: Imprint: Springer,, Pubbl/distr/stampa 2017 9783031023521 **ISBN** 3031023528 [1st ed. 2017.] Edizione 1 online resource (XIII, 109 p.) Descrizione fisica Synthesis Lectures on Information Security, Privacy, and Trust, , 1945-Collana 9750 005.8 Disciplina Soggetti Blockchains (Databases) Data protection Data protection—Law and legislation Cryptography Data encryption (Computer science) Blockchain Data and Information Security Privacy Cryptology Lingua di pubblicazione Inglese **Formato** Materiale a stampa Livello bibliografico Monografia Nota di contenuto Acknowledgments -- Introduction -- Background -- History of Cryptographic Currencies -- Bitcoin -- Coin Management Tools --Nakamoto Consensus -- Conclusion and Open Challenges --Bibliography -- Authors' Biographies. Sommario/riassunto The new field of cryptographic currencies and consensus ledgers,

> commonly referred to as blockchains, is receiving increasing interest from various different communities. These communities are very diverse and amongst others include: technical enthusiasts, activist groups, researchers from various disciplines, start ups, large

> enterprises, public authorities, banks, financial regulators, business men, investors, and also criminals. The scientific community adapted

relatively slowly to this emerging and fast-moving field of cryptographic currencies and consensus ledgers. This was one reason that, for quite a while, the only resources available have been the Bitcoin source code, blog and forum posts, mailing lists, and other online publications. Also the original Bitcoin paper which initiated the hype was published online without any prior peer review. Following the original publication spirit of the Bitcoin paper, a lot of innovation in this field has repeatedly come from the community itself in the form of online publications and online conversations instead of established peer-reviewed scientific publishing. On the one side, this spirit of fast free software development, combined with the business aspects of cryptographic currencies, as well as the interests of today's time-tomarket focused industry, produced a flood of publications, whitepapers, and prototypes. On the other side, this has led to deficits in systematization and a gap between practice and the theoretical understanding of this new field. This book aims to further close this gap and presents a well-structured overview of this broad field from a technical viewpoint. The archetype for modern cryptographic currencies and consensus ledgers is Bitcoin and its underlying Nakamoto consensus. Therefore we describe the inner workings of this protocol in great detail and discuss its relations to other derived systems.