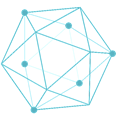
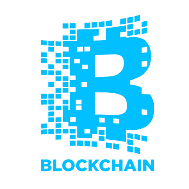
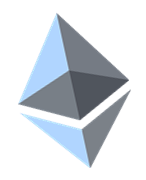
Practical Blockchain Cryptography for Developers

Hashes, HMAC, Key Derivation, Scrypt, AES, Elliptic Curve Cryptography (ECC), ECDSA, Digital Signatures, Blockchain Cryptography, Ethereum, Blockchain Addresses, Keys, Wallets, BIP39, BIP44, Ethereum Signatures, Ethereum Wallets

Svetlin Nakov, PhD

SoftUni – https://softuni.org



|  |
| --- |
| Practical Blockchain Cryptography for Developers  Hashes, HMAC, Key Derivation, Scrypt, AES, Elliptic Curve Cryptography (ECC), ECDSA, Digital Signatures, Blockchain Cryptography, Ethereum, Blockchain Addresses, Keys, Wallets, BIP39, BIP44, Ethereum Signatures, Ethereum Wallets  **Author:** D-r **Svetlin Nakov**, PhD  Cryptography - Overview, What is Cryptography?, Hash Functions, Cryptographic Hash Functions, Crypto Hashes and Collisions, Hash Functions: Applications, Secure Hash Algorithms, Hash Functions - Examples, Proof-of-Work Hash Functions, HMAC and Key Derivation, Message Authentication Code (MAC), HMAC and Key Derivation, HMAC Calculation - Examples, Deriving Key from Password, PBKDF2, Modern Key Derivation Functions, Scrypt, Bcrypt, Argon2, Diffie-Hellman Key Exchange, Diffie–Hellman - Concepts, Key Exchange by Mixing Colors, The DHKE Protocol, Symmetric and Asymmetric Encryption, Symmetric Encryption, Public Key Cryptography, Asymmetric Encryption, Symmetric Key Ciphers, AES Cipher - Concepts, AES Encrypt / Decrypt - Examples, Ethereum Wallet Encryption, Asymmetric Key Ciphers, RSA Cryptosystem - Concepts, RSA Encrypt / Decrypt - Examples, Secure Random Number Generators, Random Numbers - Examples, Entropy and HD Wallets, Exercises: Cryptography, Calculate Hashes, Calculate HMAC, Scrypt Key Derivation, AES Encrypt / Decrypt, Blockchain Cryptography, Elliptic Curve Cryptography, Elliptic Curves - Concepts, Public Key Compression, ECC Parameters and secp256k1, Digital Signatures and ECDSA, Ethereum Cryptography, Ethereum Key to Address – Examples, Ethereum Signatures, Sign Message in Ethereum – Examples, Verify Message in Ethereum – Examples, EdDSA and Ed25519, Sign / Verify Message with Ed25519, Wallets, Keys, Signatures, From Wallet to Ethereum Address, From Wallet to Bitcoin Address, Generate Bitcoin Address - Examples, Merkle Trees, Quantum-Safe Cryptography, Exercises: Blockchain Cryptography, Create Ethereum Signature, Ethereum Signature to Address, Ethereum Signature Verifier, Bitcoin Address Generator in C#, Bitcoin Address Generator in JS, Implement a Merkle Tree, RSA Encrypt / Decrypt, ECIES Encrypt / Decrypt, Popular Crypto Libraries, JavaScript Crypto Libraries, Python Crypto Libraries, C# Crypto Libraries, Java Crypto Libraries, Exercises: Sign / Verify Ethereum Messages, Sign Messages in Ethereum Style, Verify Messages in Ethereum Style, Exercises: Private Key To Blockchain Address, Generate Private Key and Address, Existing Private Key to Address, Exercises: Sign / Verify Transactions, Sign / Verify Transactions in JavaScript, Sign / Verify Transactions in Python, Sign / Verify Transactions in C#, Sign / Verify Transactions in Java  **License**: Copyrighted material. Cannot be used without the explicit written consent of Svetlin Nakov. Copyrighted materials include (but are not limited to) texts, presentation slides, graphics and images, exercise descriptions, tutorial guidelines, project descriptions and other written content. Except as otherwise expressly noted, Svetlin Nakov retains full copyrights, intellectual property and other proprietary rights to all content published in this book. If you would like to use any of this book’s content for any reason (including but not limited to teaching courses, creating video lessons, reproduction on other websites or digital media), you will need to contact Svetlin Nakov.  © Svetlin Nakov, 2018 – <http://www.nakov.com>  **Tags**: blockchain, cryptography, ECDSA, secp256k1, elliptic curves, digital signatures  GitHub: <https://github.com/nakov/blockchain-for-devs-book>  Site: <http://blockchain-dev-book.softuni.org>  **Practical Blockchain Cryptogtaphy for Developers**  Publisher: XXXXXXXXXXXXX  ISBN: XXX-XXX-XX-XXXX-X  San Francisco, 2018 |

Svetlin Nakov

SoftUni  – https://softuni.org

Practical Blockchain Cryptography for Developers

Hashes, HMAC, Key Derivation, Scrypt, AES, Elliptic Curve Cryptography (ECC), ECDSA, Digital Signatures, Blockchain Cryptography, Ethereum, Blockchain Addresses, Keys, Wallets, BIP39, BIP44, Ethereum Signatures, Ethereum Wallets

The **“Practical Blockchain Cryptography for Developers” book** introduces the most important concepts of the elliptic curve cryptography (ECC), key derivation and encryption (SCrypt, AES and HMAC), digital signatures (ECDSA, sign / verify) and crypto-wallets (HD wallets, mnemonics and BIP39, BIP44 and key derivation) with live examples in Python, JavaScript, C# and Java.

In book the author explains the key cryptographic concepts used in the blockchain systems and demonstrates them with code examples:

* Elliptic curve cryptography (ECC), ECC concepts, curves, secp256k1, ed25519
* From private key to public key to blockchain address
* Generating Ethereum addresses / signing / verifying signed messages
* Cryptographic hash functions like SHA256, SHA3, RIPEMD160, …
* HMAC and key derivation, key-derivation functions like HMAC-SHA256, PBKDF2, Scrypt
* Blockchain wallets: simple keystores and HD wallets (BIP39 and BIP44), wallet formats (like JSON / UTC), wallet encryption (AES + padding + CBC/CTR, Scrypt, HMAC)
* Ethereum signatures, Ethereum addresses, keys, wallets, APIs

Svetlin Nakov, PhD

*Co-Founder @ SoftUni,*

*Blockchain Developer and Trainer*

