

From Traditional to Decentralized Cloud



Svetlin Nakov
Inspiration Manager
Software University
<http://softuni.bg>



About Svetlin Nakov

- Software engineer, trainer, entrepreneur, PhD, author of 15 books, blockchain expert



- 3 successful tech educational initiatives (100,000+ students):



Telerik Academy



Book "Practical Cryptography for Developers"



SoftUni
Foundation

Welcome - Practical Cryptography for Developers

← → ↺ <https://cryptobook.nakov.com>

Type to search

Practical Cryptography for Developers

[Welcome](#)

[Preface](#)

[Cryptography - Overview](#)

› [Hash Functions](#)

› [MAC and Key Derivation](#)

› [Secure Random Generators](#)

› [Key Exchange](#)

Encryption: Symmetric and Asymmetric

› [Symmetric Key Ciphers](#)

› [Asymmetric Key Ciphers](#)

› [Digital Signatures](#)

› [Quantum-Safe Cryptography](#)

› [More Cryptographic Concepts](#)

› [Crypto Libraries for Developers](#)

[Conclusion](#)

Practical Cryptography for Developers Book

A modern **practical book about cryptography for developers** with code examples, covering core concepts like: **hashes** (like SHA-3 and BLAKE2), **MAC codes** (like HMAC and GMAC), **key derivation functions** (like Scrypt, Argon2), **key agreement protocols** (like DHKE, ECDH), **symmetric ciphers** (like AES and ChaCha20, cipher block modes, authenticated encryption, AEAD, AES-GCM, ChaCha20-Poly1305), **asymmetric ciphers and public-key cryptosystems** (RSA, ECC, ECIES), **elliptic curve cryptography** (ECC, secp256k1, curve25519), **digital signatures** (ECDSA and EdDSA), **secure random numbers** (PRNG, CSRRNG) and **quantum-safe cryptography**, along with **crypto libraries** and developer tools, with a lots of **code examples** in Python and other languages.

Summary

- [Welcome](#)
- [Preface](#)
- [Cryptography - Overview](#)
- [Hash Functions](#)
 - [Crypto Hashes and Collisions](#)
 - [Hash Functions: Applications](#)
 - [Secure Hash Algorithms](#)
 - [Hash Functions - Examples](#)
 - [Exercises: Calculate Hashes](#)
 - [Proof-of-Work Hash Functions](#)
- [MAC and Key Derivation](#)
 - [HMAC and Key Derivation](#)



Official site:

<https://cryptobook.nakov.com>

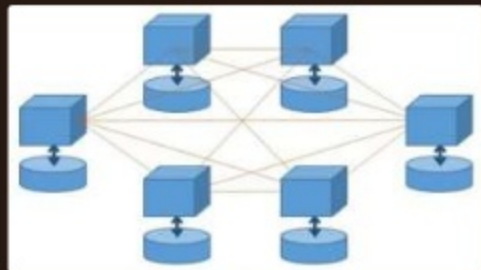
GitHub:

<https://github.com/nakov/practical-cryptography-for-developers-book>

- Technical advisor @ **LockChain / LockTrip**: <https://locktrip.com>
 - Raised ~ **10.000 ETH** in token sale (Sep-Nov 2017)
 - Currently **LOC** token holders book hotels @ 20-30% better price
- Head of blockchain education (Jan-June 2018) @ **Academy School of Blockchain**: <https://academytoken.com>
 - Raised ~ **48M USD** in token sale (Jan-Apr 2018)
- Tech advisor for blockchain crypto startups:
 - **Tokenize Exchange, Bountie, Weidex, IRIS Payments Solutions, Aeternity Ventures, FFQuest**

What is Blockchain?

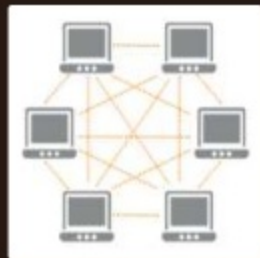
Distributed ledger



Secure

Transactions are
verified by the
entire network

Peer-to-Peer network



Nodes hold
ledger of facts +
history of updates

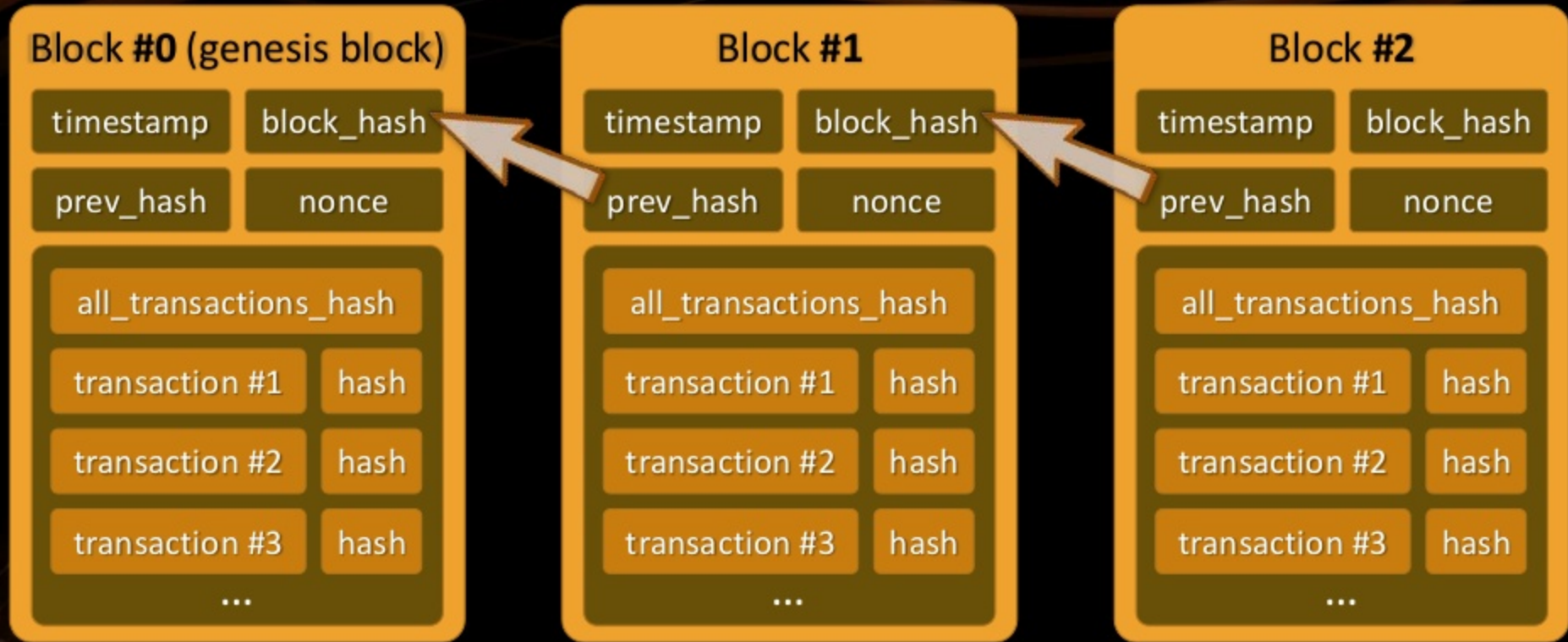
Decentralized (no owner)



Immutable



Blockchain == Chain of Data Blocks



Demo: <https://etherscan.io>

Smart Contracts: On-Chain Logic

Smart Contracts

Code (custom logic) running
in the blockchain network



Solidity

Blockchain programming
language for the Ethereum
network, running on EVM



Example: <https://etherscan.io/address/0xcale1a77e84698c83ca8931f54a755176ef75f2c>

Blockchain Applications

Cryptocurrencies



Digital money with
no central bank

Decentralized applications



Removing the
middlemen

Digital investments



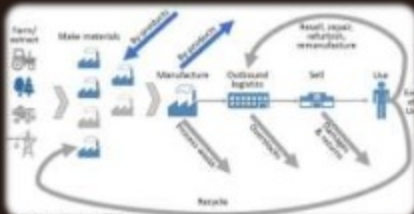
Fund raising /
ICO / token sales

Blockchain Transforms Many Industries

Finances



Supply Chain



Healthcare



Government



Forecasting



Insurance



Mobility



Voting



Why Blockchain & Decentralization?

Transparency



Security



Traceability



Reduced Costs



Cut-Out the Middleman



Decentralized Computing

Traditional Model



CPU + DB + storage:
local or in a data center
Payments: fiat money
Monetization: ads?

Cloud Model



Cloud servers + cloud
DB + cloud storage
Payments: fiat money
Monetization: ads

DApp Model



Decentralized logic
+ DB + storage + ...
Payments: crypto
Monetization: token
mechanics

Decentralized Organizations (DAO)

Decentralized Processes



Processes in the organization have no central point of control

Decentralized Data



All data is public, transparent, and accessible to everyone

Decentralized Governance



Stakeholders solve disputes, distribute incomes, drive the organization's future

DAO Example: Decentralized Uber

- Taxi rides DApp on the blockchain (or at other DApp platform)
- Passengers request rides
 - See the drivers around and get matched with a driver
 - Each ride ends with a payment (through a smart contract)
- Drivers join and publish their location
 - See, take and serve rides
 - Collect payments (tokens) and feedback (rating)
- The DApp have no owner and it is unstoppable

The Upcoming "Decentralized Cloud"



SoftUni
Foundation

Classical Public Cloud



Cloud computing & PaaS

Cloud databases

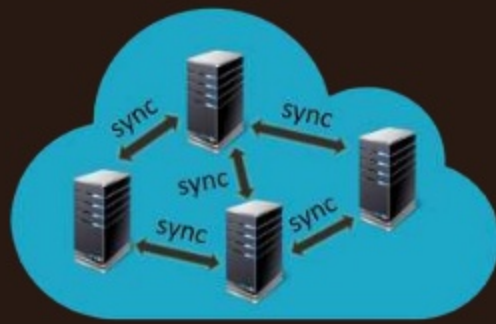
Cloud storage

Other cloud services

Platforms: AWS, Azure, Google



Decentralized Cloud



Decentralized computing

Decentralized databases

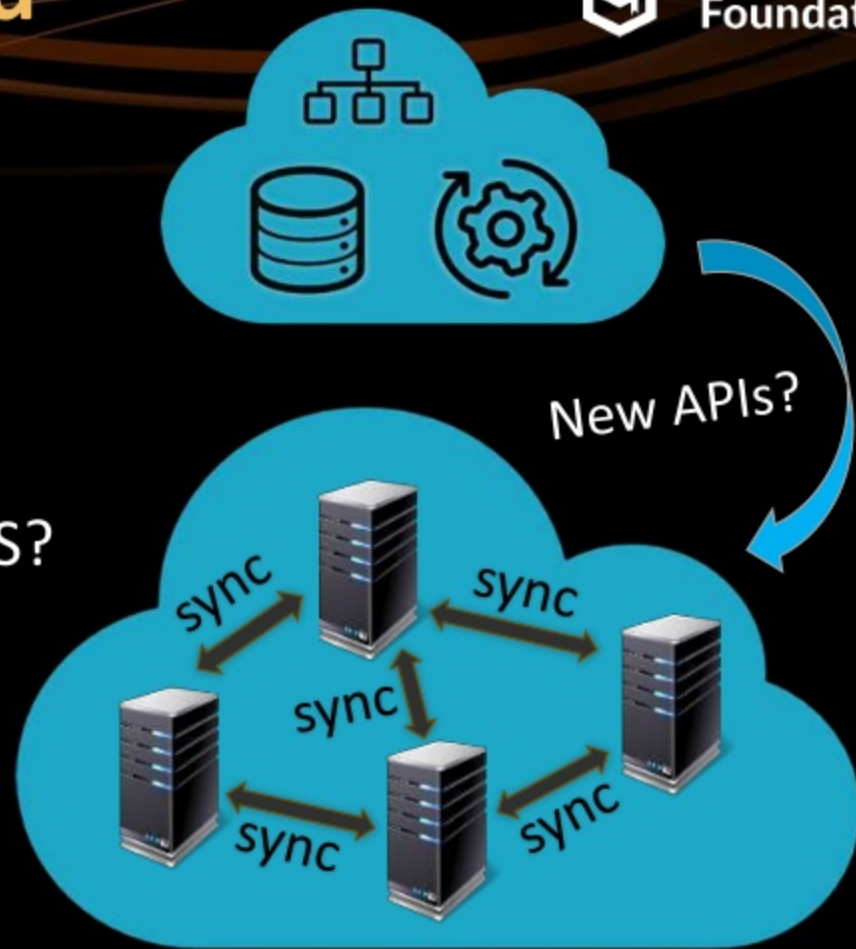
Decentralized storage

Other decentralized services

Platforms: EOS, TRON, Ethereum

The "Decentralized Cloud"

- **Miners** and mining companies
 - Provide **decentralized services**
 - App hosting, DB, storage, etc.
 - **Incentivized** by token economy
 - Big players like Microsoft and AWS?
- **Developers** and **businesses**
 - Use **decentralized services** to write and run DApps
 - Pay by **tokens** or by **staking**



Decentralized Infrastructure & Web 3.0

- Smart contract platforms (programmable blockchains)
 - Ethereum, EOS, Aeternity, LockTripChain, POA Network
- Decentralized storage
 - IPFS, Storj, Filecoin
- Decentralized databases
 - BigChainDB, Bluzelle, Orbit DB, BlockStack, Fluence
- Decentralized messaging & append-only logs
 - IPFS Log, Matrix

The Web 3.0 Abstracted Stack

Diagram v.1.0 by @stephantual - 26 May 2017

Dapps Browsers

(Parity, status.im, Mist, LETH, Metamask, etc.)

Decentralized Applications

(slock.it, Gnosis, Melonport, Zonafide, Etherisc, jaak.io, etc.)

Messaging

(whisper, telehash, etc.)

Storage

(IPFS, SWARM, StorJ, maidsafe, etc.)

State Machines

(EVM, MSC/qtum-like, custom, etc.)

Consensus

(PoW, PoS, PoA, PoET, etc.)

Data Feeds

(Oracize.it, Town Crier, etc.)

Off-chain Computing

(Cloud, Ewasm VMs, etc.)

Governance

(DAOs, futarchy, hard/soft forks, etc.)

State Channels

(Raiden, Lightning Network, etc.)

Cryptographic Network & Transport Protocols

(RLPx, roll your own, etc.)

Optional Internet Routing Protocols

(none, Tor, i2P, etc.)

From Traditional to Decentralized Cloud



SoftUni
Foundation



Questions?

