Intermediate Go Developer → Beginner Blockchain Learner Syllabus

(Updated with Q-BIoT-DM Additions)

Phase 1: Blockchain Basics for Go Developers (2-3 weeks)

Week 1: What is Blockchain? The Big Picture

- Understand blockchain concepts: blocks, chains, decentralized ledger
- How transactions form blocks, how blocks link cryptographically
- Why decentralization matters (trustless systems, immutability)
- Differences: Public vs Private blockchain (Bitcoin vs Enterprise use cases)

Q-BIoT-DM Adds:

- Understanding permissioned blockchains like Ethereum PoA, which Q-BIoT-DM uses for scalable, controlled IoT device management.

Week 2: Blockchain Data Structures in Go

- Define block structs in Go (index, timestamp, data, prevHash, hash)
- Write Go code to create blocks and chain them
- Calculate SHA-256 hashes (`crypto/sha256`)
- Validate blockchain integrity (check hashes and chain continuity)

Q-BIoT-DM Adds:

- Integration of blockchain with relational databases (MySQL) for device data storage alongside blockchain audit logs.
- Blockchain-based device identity management.

Week 3: Transactions & Signatures

- What is a transaction in blockchain terms? (transfer of value/data)
- Basics of digital signatures: public/private keys, signing, verifying
- Implement ECDSA signing/verification with Go's `crypto/ecdsa`

- Create simple signed transaction struct in Go

Q-BIoT-DM Adds:

- Multi-layered authentication combining PQ signatures with JWT + TOTP for secure device and user authentication.
- Role-Based Access Control (RBAC) for different user roles (Admin, Developer, Device, Auditor).

Phase 2: Blockchain Consensus & Network (2 weeks)

Week 4: Consensus Mechanisms (Overview)

- Proof of Work (PoW) — what it is and why it matters
- Proof of Authority (PoA) and other consensus models (brief overview)
- Simple mining concept: finding nonce to satisfy difficulty

Q-BIoT-DM Adds:

- Deep dive into **Ethereum PoA consensus** mechanisms and how it supports enterprise-scale IoT blockchains.
- Concepts of validator nodes and signing blocks with PQ signatures.

Week 5: Implementing Proof of Work in Go

- Add nonce and difficulty fields to blocks
- Implement simple PoW mining function (hash must start with X zeros)
- Validate mined blocks

Q-BIoT-DM Adds:

- Implementing **smart contract integration** on Ethereum PoA for device lifecycle management and firmware update policies.

Phase 3: Post-Quantum Cryptography Basics (2 weeks)

Week 6: Why Quantum Computing Threatens Blockchain

- Understand quantum computing basics & threats to current crypto
- What makes ECDSA vulnerable

- Brief on Shor's algorithm and Grover's algorithm

Q-BIoT-DM Adds:

- Understanding PQ cryptography's role in **future-proofing IoT device identity and blockchain security**.

Week 7: Post-Quantum Cryptography Introduction

- What is Post-Quantum Cryptography (PQC)
- Intro to PQ signature algorithms (SPHINCS+, Dilithium)
- Overview of PQ hash functions (SHA3, BLAKE3)

Q-BIoT-DM Adds:

- Integration of PQ crypto with **JWT token generation and validation** for secure, quantum-safe API authentication.
- Working with real PQ libraries used in production-grade projects (`circl`, `liboqs-go`).

Phase 4: Building Quantum-Resistant Blockchain Components (3 weeks)

Week 8: Blockchain with PQ Signatures

- Modify your transaction struct to use PQ public keys & signatures
- Replace classical signatures with PQ signatures
- Adjust block validation accordingly

Q-BIoT-DM Adds:

- Applying PQ signatures for **device identity validation** in blockchain transactions.
- Handling PQ key management at scale.

Week 9: PQ Hashing & Block Validation

- Use SHA3 or BLAKE3 instead of SHA256 for hashing blocks
- Implement block validation with PQ-safe hashes

Q-BIoT-DM Adds:

- Using PQ-safe hashes for **firmware integrity verification** stored on blockchain.

Week 10: Simple PQ Consensus (Proof of Authority style)

- Implement validator signing of blocks with PQ keys
- Basic network message validation

Q-BIoT-DM Adds:

- Implementing PQ signature layers on Ethereum PoA validator nodes.
- Building blockchain-based **audit logs** with tamper-evident PQ signatures.

Phase 5: Wrap-up, Optimization & Next Steps (2 weeks)

Week 11: Performance & Signature Size Challenges

- Understand PQ signature size and performance trade-offs
- Explore signature aggregation and optimization techniques

Q-BIoT-DM Adds:

- Real-world strategies for **optimizing PQ crypto in resource-constrained IoT environments**.
- Handling large-scale device identity signatures efficiently.

Week 12: Deployment and Integration

- Dockerize your blockchain node
- Basic REST API for interacting with your blockchain (in Go)
- Prepare for real-world testing

Q-BIoT-DM Adds:

- Integration with **MQTT for real-time IoT telemetry**.
- WebSocket APIs for live dashboard telemetry.
- Multi-layer security: TLS, rate limiting, 2FA, and RBAC.
- Full CI/CD pipeline for production deployment.

Summary Table (with Q-BIoT-DM adds)

Phase	Goal	Focus	Time	Q-BIoT-DM Additional Focus Areas
1. Blockchain Basics	Understand blockchain & build simple chain	Blockchain + Go	2-3 wk	Permissioned blockchains, device identity, RBAC
2. Consensus	Learn consensus & mining, implement PoW	Consensus + Go	2 wk	Ethereum PoA, smart contracts, validator roles
3. PQ Crypto Basics	Understand quantum threats & PQ cryptography	Cryptography	2 wk	PQ JWT auth, real PQ libraries, IoT device identity
4. PQ Blockchain	Implement PQ signatures & hashing	PQ Crypto + Blockchain	3 wk	PQ signature device identity, PQ hash-based firmware validation
5. Optimization	Performance & deployment	Production ready	2 wk	MQTT/WebSocket, 2FA, RBAC, CI/CD, large-scale IoT device handling

---