LDK Roadmap - **DRAFT**

This is intended to communicate the direction of the project as viewed by the active contributors of the project. It is a working document that will continually be refined as we learn more from prospective developer users. It can also be impacted by new contributors helping take the project in new directions.

Value Proposition

LDK provides developers an easy-to-use and customizable development kit with a highly secure and privacy-preserving Lightning implementation.

2020

What we want to achieve:

- Host an LDK workshop
    - An LDK user in 2020 will be an early adopter type; someone comfortable working with the bleeding edge, eager to provide feedback and help shape the future of the LDK and API, and is willing to deal with rough edges.
- Run our own mainnet LN node based on LDK as a proof of concept
- Support at least 1 project to develop a testnet application based on LDK
- Create a culture that is welcoming and supportive of non-Square contributors

How we achieve it:

- Refactorings (router, ChannelMonitor, and other)
- Stay up to date with the spec
    - Anchor outputs
- Support at least 2 programming languages (eg Swift, JS/Node, Java/JVM, Python)
- Implement sample code LDK modules
    - Chain data via Core RPC/REST
    - On-chain wallet
    - On-chain transaction broadcasting
    - Fee estimator via Core RPC/REST
    - Data backups to local filesystem
    - Source of entropy

Related ecosystem coordination:

- Addressing security issues with fees and mempool congestion
- Nudge Schnorr/Taproot along for hopeful 2021 activation; this enables PTLCs and more efficient channel open and closing transactions

2021

What we want to achieve:

- Ship a production-level LDK
    - An LDK user in 2021 should have a decent out-of-box experience in terms of documentation and getting started. They should be confident to launch a service based on LDK to have it function at the highest levels of scalability and security that the LN protocol specification and ecosystem supports. They will likely still need to provide several modules to make LDK work, such as providing a key store (on-chain wallet).
- Support at least 3 projects to ship an application based on LDK
    - Support for funding and channel state in at least 1 hardware wallet (eg HTC Exodus, Trezor, Ledger, Crypto Advance)
    - Examples of customization (that didn't require knowledge of Rust or modification of LDK) should be evident (eg custom routing, custom pathfinding, failover capabilities, custom storage, single wallet for bitcoin/LN, web wallet, blockchain truth sourcing, custom channel scripts)
- There should be a noticeable shift in the amount of contribution from non-Square Crypto contributors so the project appears and is not as dependent upon Square Crypto.

How we achieve it:

- Stay up to date with the spec
    - Spontaneous payments
    - PTLCs
    - Schnorr scriptpubkeys
- Support 2 more programming languages (selected based on user needs)
- Implement sample LDK modules
    - Auto channel creation/peer selection
    - Chain data via compact block filters (AKA neutrino, BIP 157/158)
    - Support for Lightning Labs Loop, Loop Out submarine swaps
- Ship production versions of these modules
    - Chain data via highest-demand source (determined by user feedback)

    - Support for Talaia LN watchtower
    - Improved default router that
        - Downloads network graph
        - Supports retrying payments (can return more than just cheapest path)
        - Node Scoring + downloading node subset based on scoring

Related ecosystem coordination:

- ANYPREVOUT consensus change enabling “Eltoo” upgrades

2022 and beyond

Where we should be:

- Dozens of projects based on LDK
    - At least 1 major service with 1M+ users
- An LDK user should have an excellent out-of-box experience, with a basic wallet working out of the box, ready for customization and optimization by the user. The robustness and reputation of LDK should be the highest quality in the bitcoin ecosystem, approaching the trust level that Bitcoin Core and libsecp256k1 projects have.
- It should be evident that the amount of contribution from non-Square Crypto contributors is sufficient to sustain the project regardless of Square Crypto’s involvement (but, hopefully Square Crypto remains heavily involved :)