BUILDING ON LIBBITCOIN

LISBON 2018

- Libbitcoin Developer (5 years)
- Entrepreneur (20 years)
- Investor/Advisor (12 years)
- Microsoft Architect (3 years)
- Traveler (76 countries)
- USN Fighter Pilot (10 years)
- Martial Artist (27 years)
- Anarcho-Capitalist (26 years)
- Computer Scientist (37 years)

ERIC VOSKUIL

eric@voskuil.org

https://github.com/evoskuil

https://twitter.com/evoskuil

https://linkedin.com/in/evoskuil

WHAT IS BUILDING ON BITCOIN?

- More than development of financial tools that use Bitcoin.
- Tools the increase individual power enhance Bitcoin.
- Tools that reduce individual power diminish Bitcoin.
- Power is expressed by:
  - Confirming Bitcoin transactions (miner)
  - Validating receipt of Bitcoin (merchant)
- Independent exercise of power implies covert operation.
- Power requires independent control over a Bitcoin node.

HOW DOES ONE OPERATE COVERTLY?

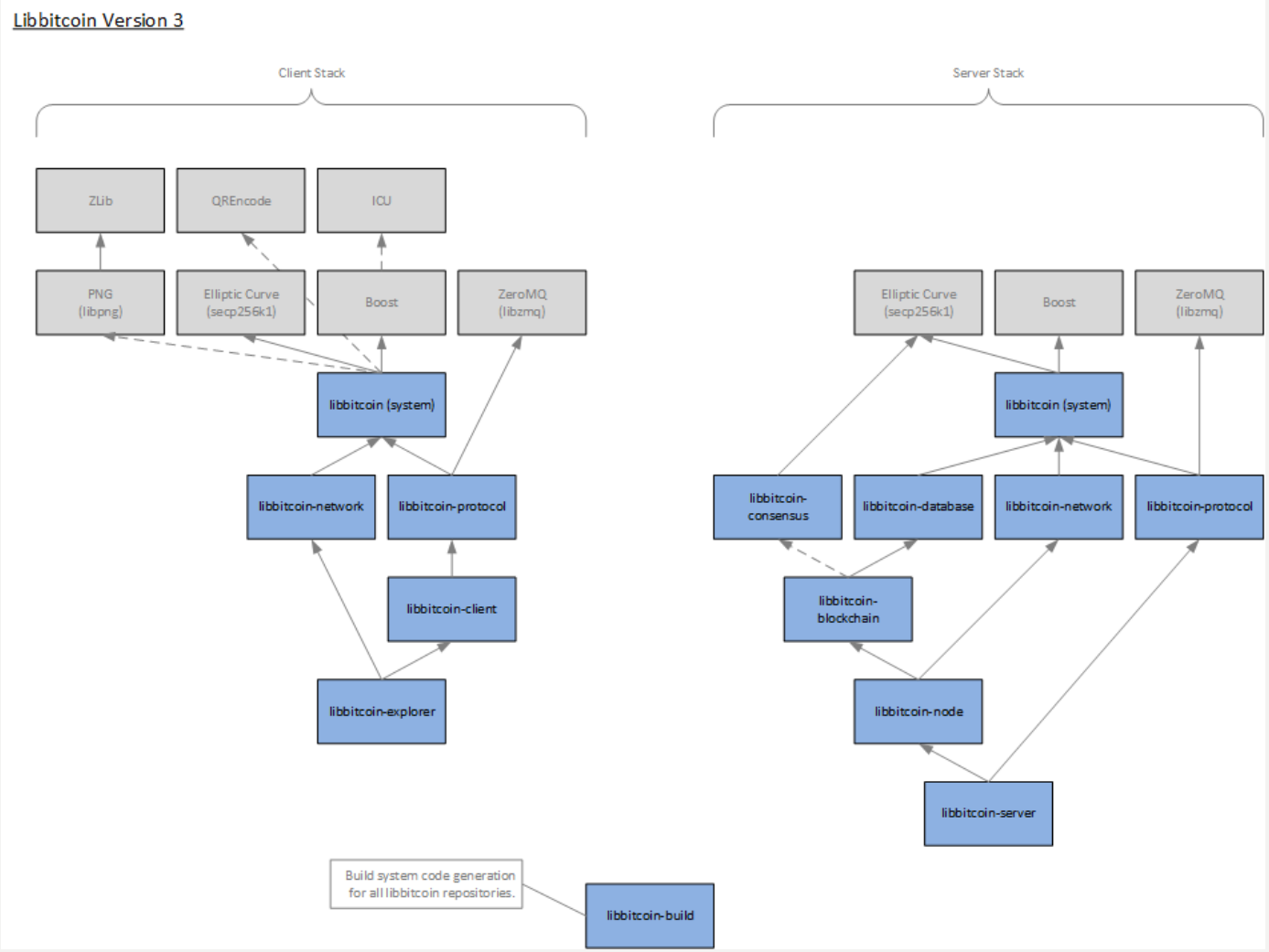
- Anonymity is the essential element of covert operation.
- Bitcoin relies on verifiable public data to achieve anonymity.
- Large operations are inconsistent with anonymity.
- Decentralizability is (independent) small operation performance.
- Bitcoin requires competitive performance for small operations.

SHORTCUTS?

- Non-economic nodes are irrelevant.
- Layering does not change the individual node requirement.
- Pruning does not remove the full chain validation requirement.
- Checkpointing reduces individual power by delegating validation.
- SPV reduces individual power by delegating validation.
- Bitcoin requires competitive performance for full nodes (in small operations).

LIBBITCOIN PRINCIPLES

- Privacy
  - Bitcoin should always remain as private as possible for its users.
- Scalability
  - Bitcoin built today with the future in mind.
- Integrity
  - No individual or group should have enough power over the network to compromise its original aims.



LIBBITCOIN

Cross Platform C++ Developer Toolkit

- libbitcoin (system)
- libbitcoin-blockchain
- libbitcoin-build
- libbitcoin-client
- libbitcoin-consensus
- libbitcoin-database
- libbitcoin-explorer
- libbitcoin-network
- libbitcoin-node
- libbitcoin-protocol
- libbitcoin-server

BITCOIN SERVER

- BS is an executable wrapper around the libbitcoin-server library.
  - Command line options and configuration settings
  - Single file deployable to Linux, macOS and Windows
- libbitcoin-server is an interface layer over libbitcoin-node and libbitcoin-protocol.
  - ZeroMQ (transport independent) with optional CurveCP
  - Web Sockets (v4) with optional TLS
  - Built on Bitcoin for others to Build on Bitcoin
- Interface
  - Query
  - Payment subscription
  - Block and Transaction broadcast

```
$ bs
```

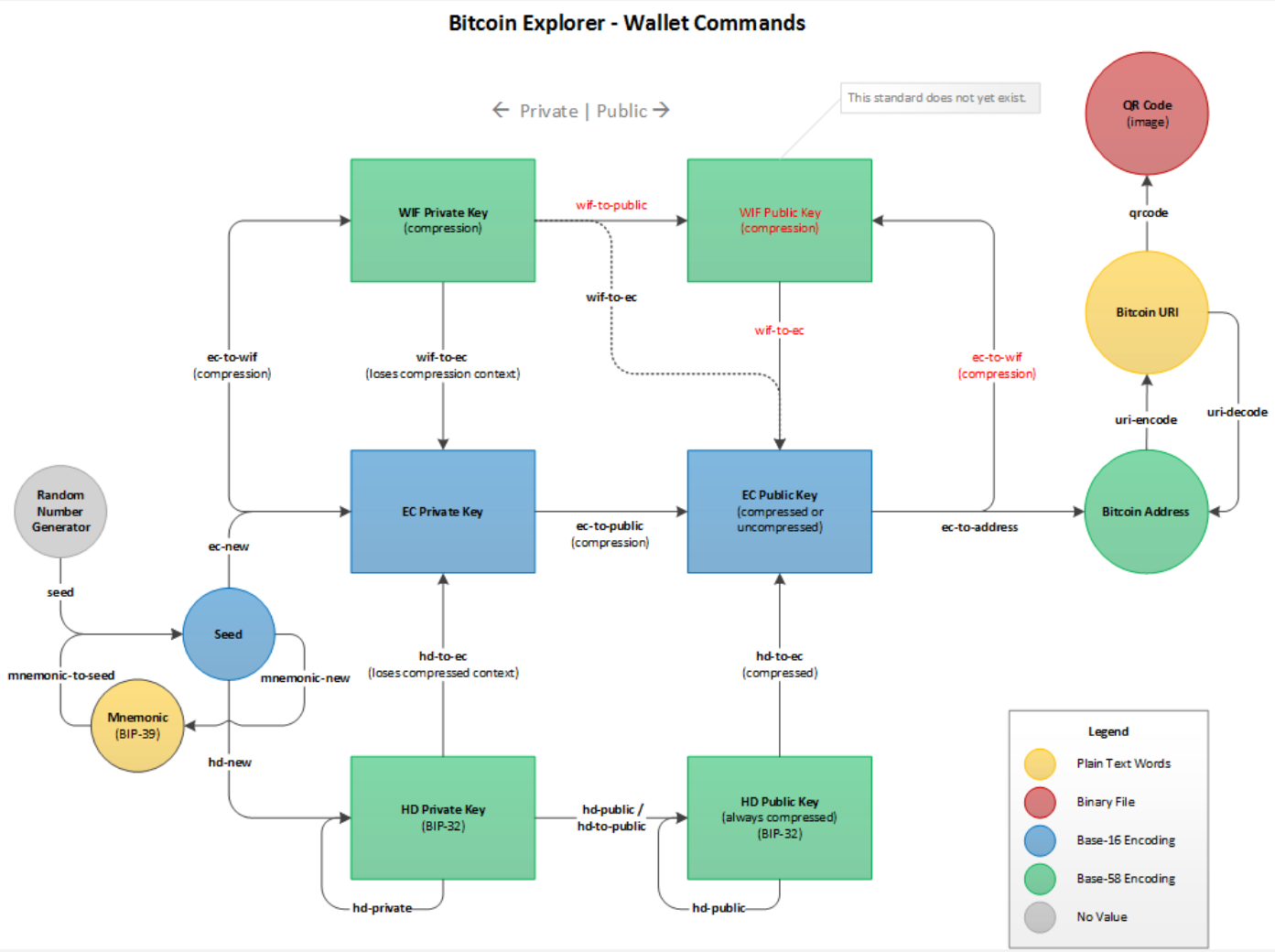
```
04:15:32.222545 INFO [server] ================ startup 03/08/17 20:15:32 ================
04:15:32.224009 WARNING [server] ================ startup 03/08/17 20:15:32 ================
04:15:32.224009 ERROR [server] ================ startup 03/08/17 20:15:32 ================
04:15:32.239812 FATAL [server] ================ startup 03/08/17 20:15:32 ================
04:15:32.255410 INFO [server] Using config file: "bs.cfg"
04:15:32.255410 INFO [server] Please wait while the server is starting...
04:15:32.321948 INFO [network] Starting manual session.
04:15:32.323923 INFO [server] Seeding is complete.
04:15:32.339683 INFO [node] Node start height is (430806).
04:15:32.339683 INFO [network] Starting inbound session on port (8333).
04:15:32.339683 INFO [network] Starting outbound session.
04:15:32.386530 INFO [server] Bound secure query service to tcp://*:9081
04:15:32.440000 INFO [server] Bound public query service to tcp://*:9091
04:15:32.486873 INFO [server] Bound secure heartbeat service to tcp://*:9082
04:15:32.486873 INFO [server] Bound public heartbeat service to tcp://*:9092
04:15:32.521662 INFO [server] Bound secure block service to tcp://*:9083
04:15:32.540320 INFO [server] Bound public block service to tcp://*:9093
04:15:32.555944 INFO [server] Bound secure transaction service to tcp://*:9084
04:15:32.571570 INFO [server] Bound public transaction service to tcp://*:9094
04:15:32.571570 INFO [server] Server is started.
04:15:33.523913 INFO [blockchain] Block [430807] 2570 txs 4673 ins    0 wms  456 vms   98 vμ
04:15:34.519618 INFO [blockchain] Block [430808] 2177 txs 4018 ins    0 wms  344 vms   86 vμ
04:15:35.572365 INFO [blockchain] Block [430809] 1665 txs 5119 ins    0 wms  394 vms   77 vμ
04:15:36.494041 INFO [blockchain] Block [430810] 1824 txs 4728 ins    0 wms  375 vms   79 vμ
04:15:37.673376 INFO [blockchain] Block [430811] 2829 txs 4404 ins    0 wms  388 vms   88 vμ
04:15:38.792796 INFO [blockchain] Block [430812]  952 txs 4594 ins    0 wms  314 vms   68 vμ
```

BITCOIN SERVER

Full Node and Query Server

BITCOIN EXPLORER

- BX is an executable wrapper around the libbitcoin-explorer library.
  - Command line options and configuration settings
  - Single file deployable to Linux, macOS and Windows
- libbitcoin-explorer is a command utility over libbitcoin-client and libbitcoin-network.
  - ZeroMQ (transport independent) with optional CurveCP and SOCKS5 (Tor)
  - P2P network (transaction submission and broadcast)
  - Built on Bitcoin for others to Build on Bitcoin
- Interface
  - Query
  - Payment subscription
  - Block and Transaction broadcast



BITCOIN EXPLORER

Command Line Tool

- Wallet (17)
- Key Encryption (9)
- Stealth (5)
- Messaging (2)
- Transaction (9)
- Online (16)
- Encoding (13)
- Hash (6)
- Math (8)

SCALING LIBBITCOIN

- Less is more
- Built for speed
- No compromises
- Catching up

LESS IS MORE

- No tx memory pool
- No block memory pool
- No signature or script cache
- No unspent output store
- No delete/reorder (append only)

BUILT FOR SPEED

- Memory mapped files
- Performance scales with RAM
- All files are array or hash table
- All queries constant time in chain size (including unconfirmed)

NO COMPROMISES

- Small number of files
- Always tx index
- Always spent-by index
- Node size as bitcoind w/o tx index
- Server ElectrumX index/size

CATCHING UP

- Persistent
  - Candidate and Confirmed arrays
  - Headers, Blocks, Transactions hash tables
- Ephemeral
  - Tx metadata DAG
  - Block metadata tree
- Continuously parallel
  - Initial or restart

QUESTIONS