NYC Bitcoin Exchange

The First NYDFS Regulated Bitcoin Exchange

Problem

Bitcoin is innovative but exchanges have had problems

- **A brief history of Bitcoin**
  - Bitcoin: open source technology invented in 2009
  - Widely hailed as technological breakthrough
  - Like the early Internet, bumpy patches and security problems
  - Most prominent: Mt. Gox meltdown and funds loss
  - Also potential issues around KYC, AML, compliance

- **Where we are today**
  - Pressing need for a stable, regulated Bitcoin exchange
  - NYDFS is leading the way with a regulatory framework
  - Regulated exchange should have provisions for auditing of customer balances, KYC/AML compliance, strong security

Solution

A safe, regulated Bitcoin exchange under NYDFS

- **Compliance Goals**
  - <u>Compliance</u>: Provide full audit trails of every dollar and BTC that passes through the system, along with identities of large buyers
  - <u>Liquidity</u>: Ensure liquidity for the Bitcoin ecosystem, and have large enough reserve ratios to prevent Gox-like situation
  - <u>Trust</u>: Create trust in Bitcoin ecosystem, allow institutional investors to establish positions in digital currencies
  - <u>Reputation</u>: Build in partnership with established/reputable investors and venture capital firms

- **Technological Goals**
  - Easy to use front-end comparable to large consumer websites
  - Top-to-bottom emphasis on information security

Executive Team

Have built and scaled $1B+ in tech/finance companies

- Matt Pauker (CEO)
  - Founder, Voltage Security (>$40m rev)
  - Author of 15+ cryptography patents; commercialized IBE
  - BS Computer Science, Stanford

- Andrew Farkas (Board of Directors)
  - CEO of Island Capital
  - BA Economics, Harvard

- Balaji S. Srinivasan (Chairman)
  - Newest General Partner at Andreessen Horowitz (1, 2)
  - Founder/CTO, Counsyl (~5% US births, ~$1B+ val)
  - BS/MS/PhD EE, MS ChemE Stanford

- Terence Spies (CTO)
  - CTO of Voltage Security
  - Designed SSL server/client for Microsoft Internet Explorer
  - Chairs ANSI X9F1 bank cryptography committee

Technology

What technological considerations are involved?

Technical Challenges
Building a Bitcoin exchange is computer science

- **Security**
  - Exchange will be under constant attack by hackers around the globe; both Denial of Service and active threats (e.g., APTs)
  - Bitcoin relies on advanced cryptography; getting it wrong can result in loss of funds (see Mt. Gox)

- **Ecosystem integration**
  - Exchange is one of several core Bitcoin infrastructure services
  - Must provide tight API integration with wallets, merchant processors, miners

- **Compliance**
  - Technology must be designed to support (often conflicting) compliance goals
  - Leverage best practices from PCI, FFIEC, NIST

Technical Challenges

Our number one concern technologically is security

- **Threats**
  - Distributed denial of service (DDoS)
  - 0-day exploits in open source software
  - Spear-phishing
  - Advanced persistent threats (e.g. China)
  - Source code compromise
  - Social engineering attacks
 - Physical compromise of vaulting facility or datacenter

- **Mitigation**
  - FireEye/Mandiant (malware), Cloudflare (DDoS), Sift Science (fraud), Voltage (encryption), Skipfish/Ratproxy (headless)
  - Open bids for zero days in any software utilized
  - Constant penetration testing, automatic/manual (Detectify)
 - Static and dynamic checking of codebase (Coverity)

Technical Challenges

Security expertise must be baked into every layer

Example: Heartbleed: Security issues are subtle
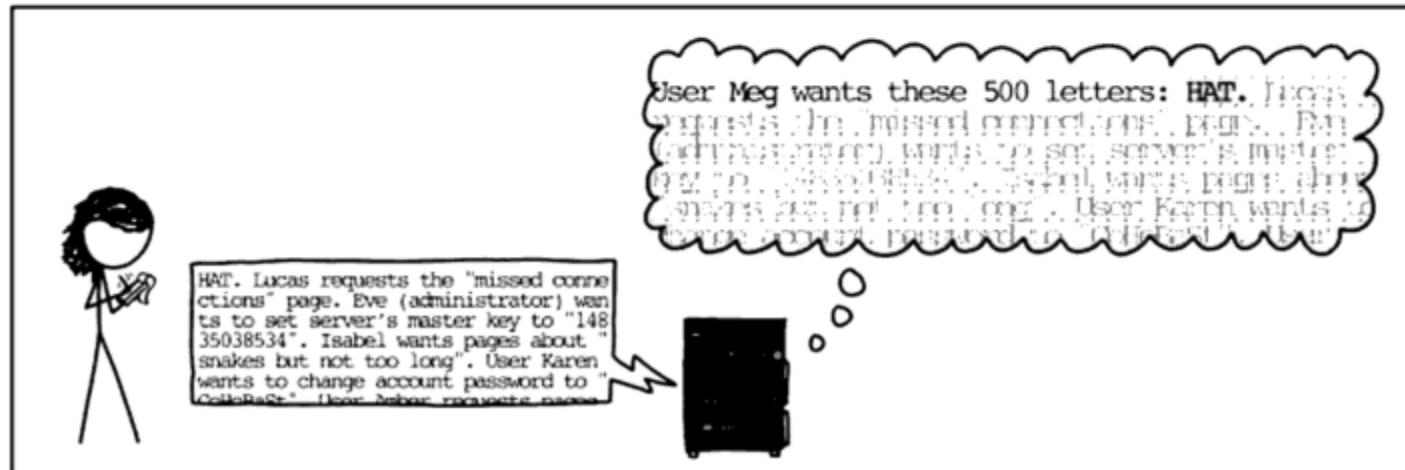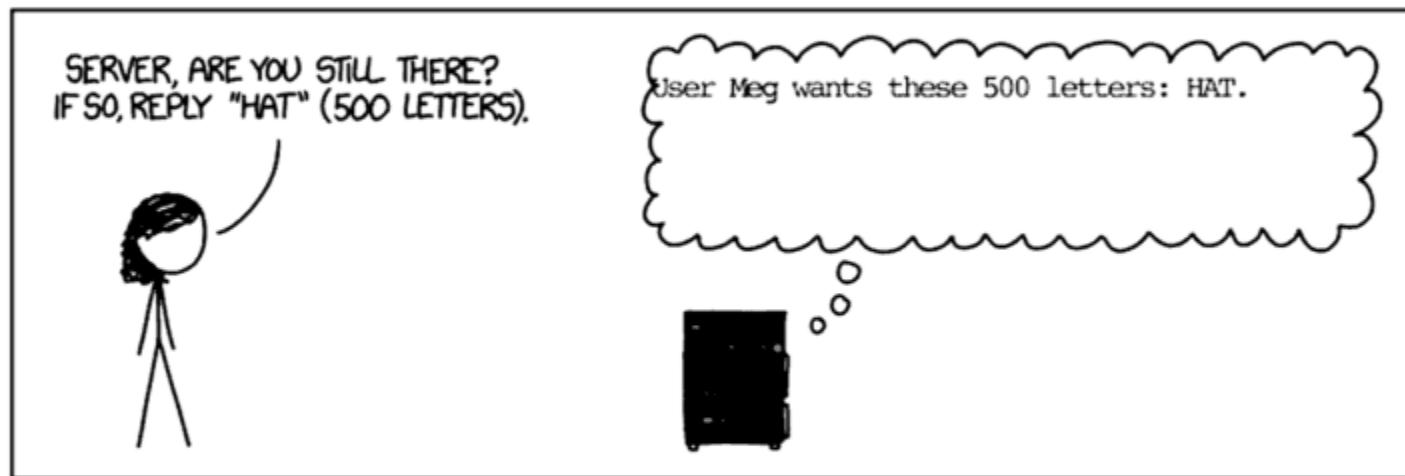
Technical Architecture

Increase security via subsystem isolation, cold storage

Accounting System	User Mgmt System	Exchange System	Wallet System
Customer Accounts	Enrollment (KYC)	Web UI / API	Cold Wallet
Txn History	Authentication	Transaction Validator	Warm Wallet
	Funds Transfer	Core Engine	Hot Wallet
			Bitcoin Network Interface
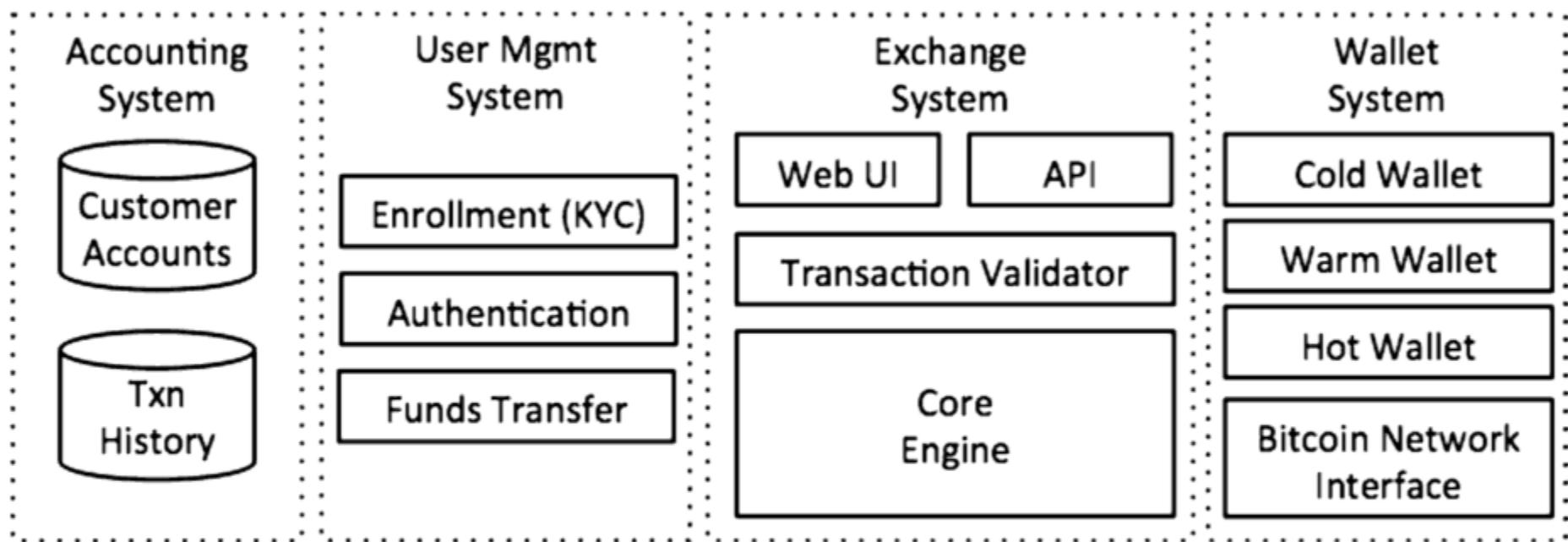
- **Services-Oriented Architecture improves security**
  - Discrete, well-defined subsystems reduce risk of spillover attacks
- **Full auditability for all functions**
  - User activity, funds, trades
- **Will work closely with NYSDFS on functionality & user interface**
  - Ensure regulatory compliance, proper disclosures, transparency

Technical Architecture

Limit amount of "hot" Bitcoin; most in cold wallet
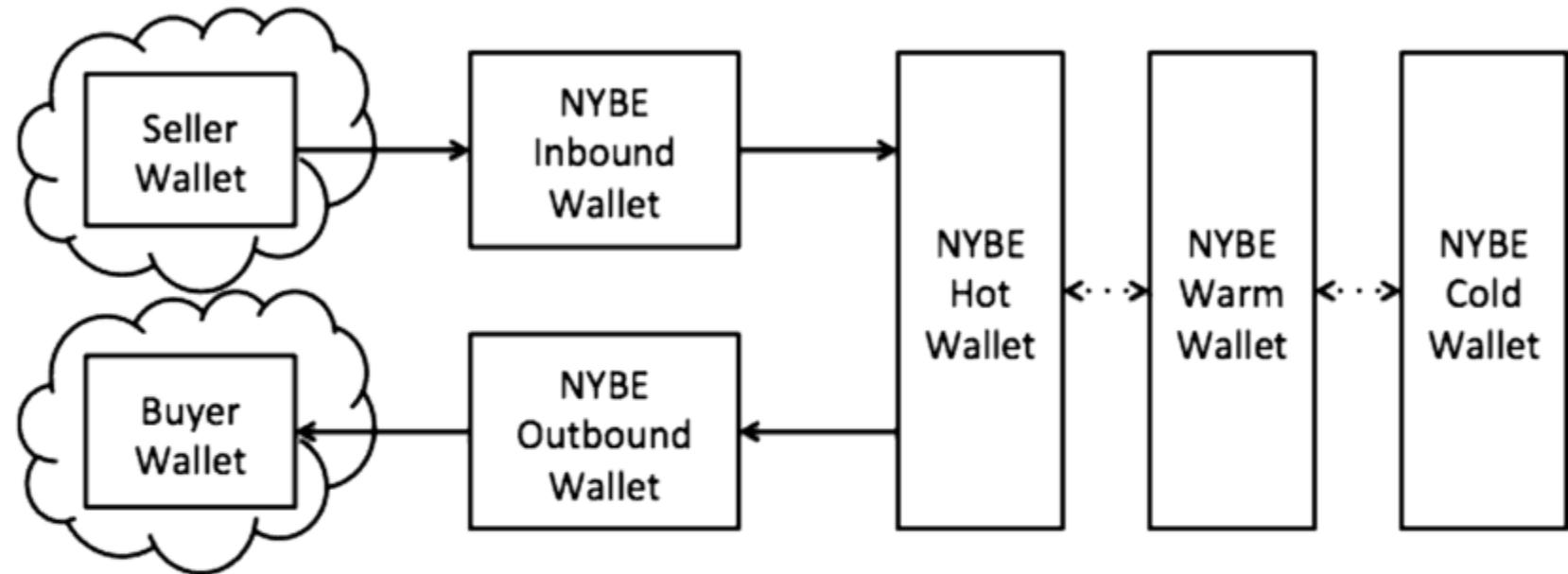
- **Typical transaction flow:**
  - Seller sends BTC into NYBE Inbound Wallet, then stored in Hot Wallet
  - After trade, BTC is moved to Outbound Wallet, then Buyer Wallet
  - Seller & Buyer Wallets reside at 3rd party (Coinbase, Xapo, etc.)
- **Occasionally: money moved out of Hot Wallet**
  - Maintain minimum required amount of BTC online

Technical Architecture

Security principles for wallets, passwords, pentesting

- **Bitcoin wallets**
  - Not a consumer wallet provider: only hold customer funds for trading
  - Three-tiered wallet hierarchy
    - Hot: online, available immediately (~25%)
    - Warm: offline, available within 24 hours (~25%)
    - Cold: offline & geo-dispersed, available within 72 hours (~50%)

- **Industry-standard best practices**
  - Least-privilege architecture
  - Two-factor user authentication
  - n-of-m key sharing
  - Bank-level network & data security design (256-bit encryption, anti-DDoS)

- **Continuous evaluation**
  - Regular internal security audits
  - External "red teams" to identify potential vulnerabilities

Technical Architecture
We build the exchange for extensibility beyond BTC

- **Exchange built to handle more digital currencies over time**
  - Compliance is key in all of this; start with BTC, generalize as we build confidence
  - Technology: simply requires additional wallet subsystems on top of existing architecture

- **Items we may trade over time**
  - Altcoins: Bitcoin "clones" (Litecoin, Namecoin) which primarily change some parameters
  - Appcoins: new proof-of-work systems with new functionality (Namecoin, Ethereum, Mastercoin)
  - Side-chains: support for side-chains & proof-of-burn
  - Smart property: can use the blockchain to exchange software licenses, stock certificates, digital keys to houses, etc.
  - And more: Colored Coins video gives sense of what Bitcoin can enable

Exchange Economics
Two possible models for an exchange

- **Model I: Pure facilitation of trades**
  - In this model, we bucket all buy/sell orders into (say) .1 BTC buckets
  - We then match buyers and sellers in the same bucket
  - Buyers and sellers exchange directly with each other and the exchange takes a commission

- **Model II: Serve as counterparty**
  - In this model, we are the buyer and seller of BTC traded on the exchange
  - We maintain BTC and USD reserves that are sufficient to handle large spikes in buy or sell orders
  - The exchange monetizes through the size of the bid/ask spread
  - Benefit: greater liquidity for exchange customers. Cost: larger reserve ratios.

Next Steps

We'd like to work with NYDFS on this.

Next Steps

What's the next step from NYDFS's perspective?

- **Areas we are seeking input**
  - What is the optimal corporate structure for this vehicle in NYDFS's view?
  - What existing legislation/regulatory framework is NYDFS thinking about using as a basis for this?
  - How does NYDFS think about annual Bitlicense/exchange fees and the like, if any?
  - What type of ongoing supervision does NYDFS envision?
  - These are the sorts of questions we'd like to figure out collaboratively; please tell us how we can help.