



# iDaemon as a Full Node

Business Model  
February 2017



# The Current Problem

The Bitcoin network currently experiences a bottleneck in capacity and transaction throughput (~7tps) which is constraining and hindering growth. Multiple solutions are available but, as code maintainers of the protocol reference implementation, the BitcoinCore development group effectively controls which direction gets adopted.

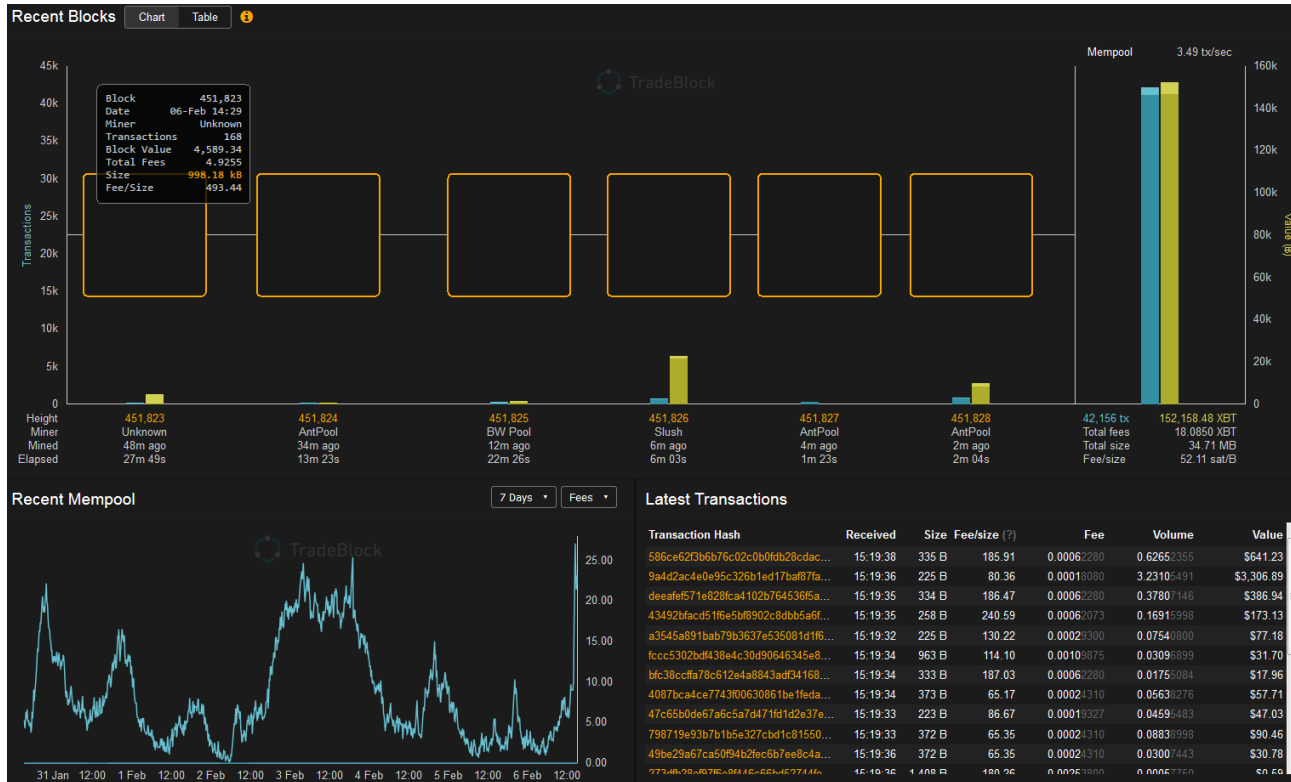
Furthermore, the BitcoinCore development group has significant overlap with the Blockstream engineering team. This talent crossover tends to create a situation that retards outside innovation for the Bitcoin protocol as Blockstream's corporate vision for the Bitcoin protocol is favoured and advanced.

In addition to a decided preference against on-chain scaling, BitcoinCore have disabled or removed many of the original Bitcoin scripting features and OP\_CODES.

# Prepare to Transition from Hobbyist Phase

Number Active Users	Memory Pool Size	Transaction fees per day
5 million	100Tb	5 BTC
50 million	1,000Tb	15 BTC
100 million	2,000Tb	30 BTC
500 million	10,000Tb	150 BTC
1,000 million	20,000Tb	300 BTC
5,000 million	100,000Tb	1500 BTC

# Network Congestion Continues to Increase



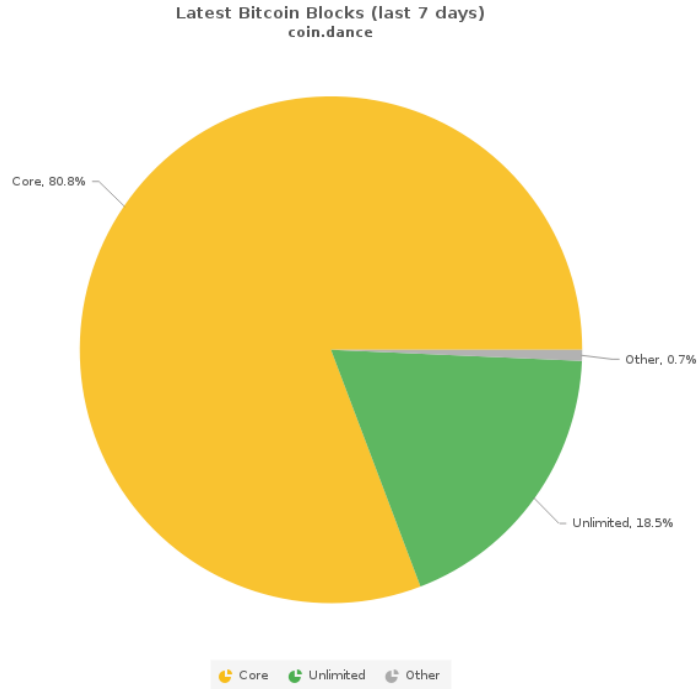
# The Current Problem

Essentially, this leaves two different routes to influence the direction of the Bitcoin protocol:

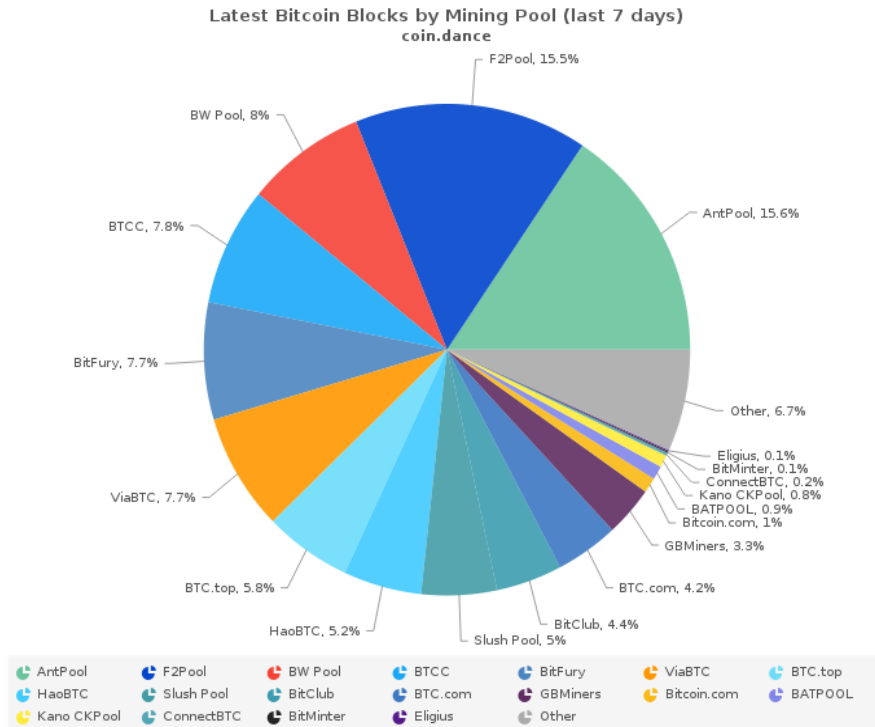
- (1) persuade the current development team to adopt change requests (via BIP process); or
- (2) propagate a credible and reliable alternative to BitcoinCore full node software using iDaemon.

***The nChain team recommends the second route.***

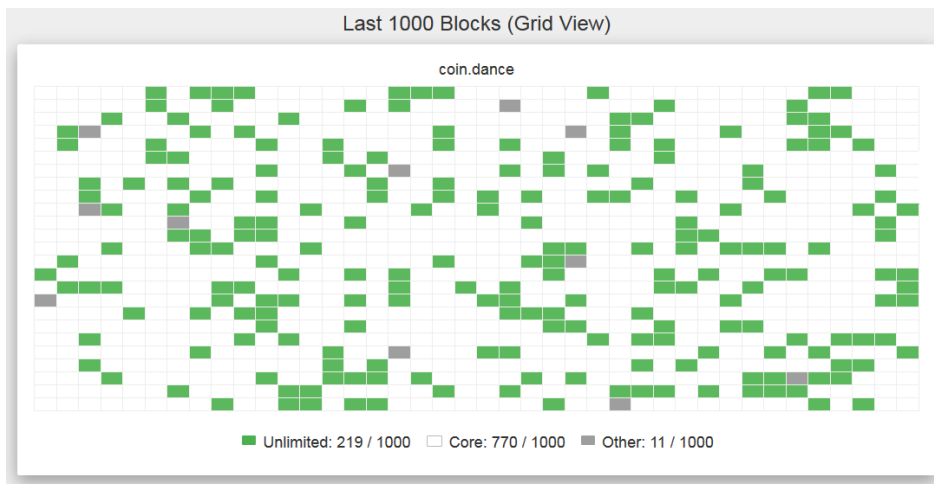
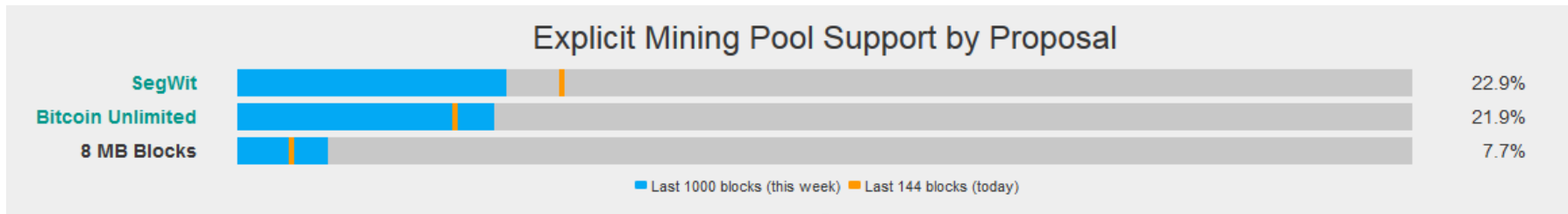
# Since Over 75% of Blocks Are Mined by BitcoinCore...



# ...nChain Must Incentivise Miners to Switch to iDaemon



# Challenger Nodes Locked in an Off-Chain vs. On-Chain Scaling Battle





# How Does nChain Phase Its Propagation?

We need to design a spark (or a hook) to convince some of the early mining resources to switch over to iDaemon. That incentive will be a combination of faster block propagation and efficient header data to achieve more successful blocks with reduced orphan rates.

**From 0% to 25%:** seed w/faster more profitable miners (launch/acquire mining pool)

From 25% to 50%: use abilities to stall software measures from others

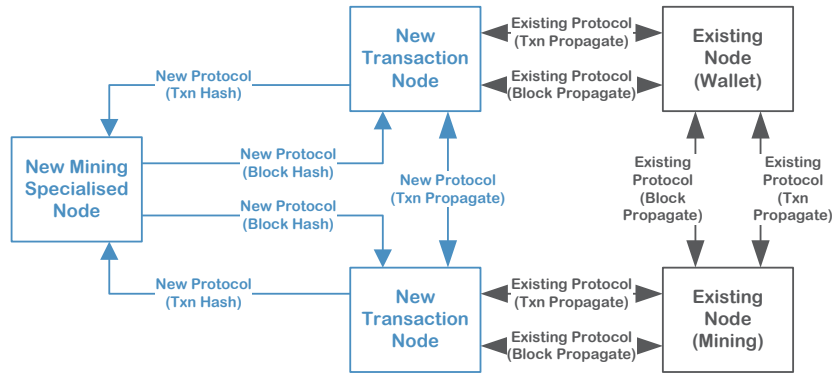
From 50% to 75%: with even consensus, introduce advanced techniques

From over 75%: with majority consensus, fork achieved (launch killer app)

# Details on Phase I Propagation [0-25%]

- With a distributed mempool, increase transaction propagation speeds by transmitting hashes only (current centralisation criticisms ignore massive mempool size)
- Optimised network bandwidth creates a hashing head start advantage of approximately 93.75% (15/16 milliseconds)
- There is enough SegWit resistance among the mining operators to switch
- Schedule London-based meetings with important mining groups for design input (ViaBTC, GBMiners, BTC.top, Bitcoin.com, Slush Pool)

# Phase 1 iDaemon Node Specialisation



New protocols massively limit the data traffic between nodes

Allow new mining node to start block mining faster than existing due to less data and processing

New transaction node handles both new and existing protocol to allow inter-connectivity with wider network

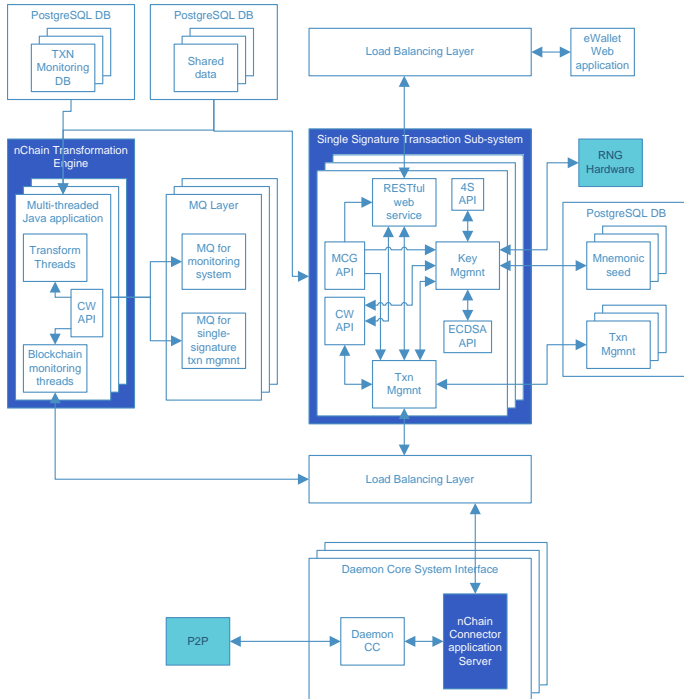
# Business Model and Vision

Governance of the Bitcoin protocol is asserted through the dominant propagation of its reference implementation. If nChain becomes the leading reference implementation adopted by the majority of network nodes, it will assume an influential leadership role in both practice and thought.

nChain intends to utilise its iDaemon full node as a wedge to achieve maximum propagation across the Bitcoin network. This allows the nChain team to lead, coordinate, and expand the protocol direction for maximum functionality thereby enabling a platform play.

Bitcoin is the killer app. Additionally, one or more viral “killer apps” (such as a viral wallet linked to SIM) will be selected in order to gain attention from users and to proactively demonstrate the scaling and capacity features of the iDaemon architecture.

# iDaemon Architecture Suited to the Task



iDaemon already supports component distribution and clustering

This was to improve resilience and availability

Further optimisation will be required to implement the full functional segregation of the fast transaction network

Architectural framework already in place

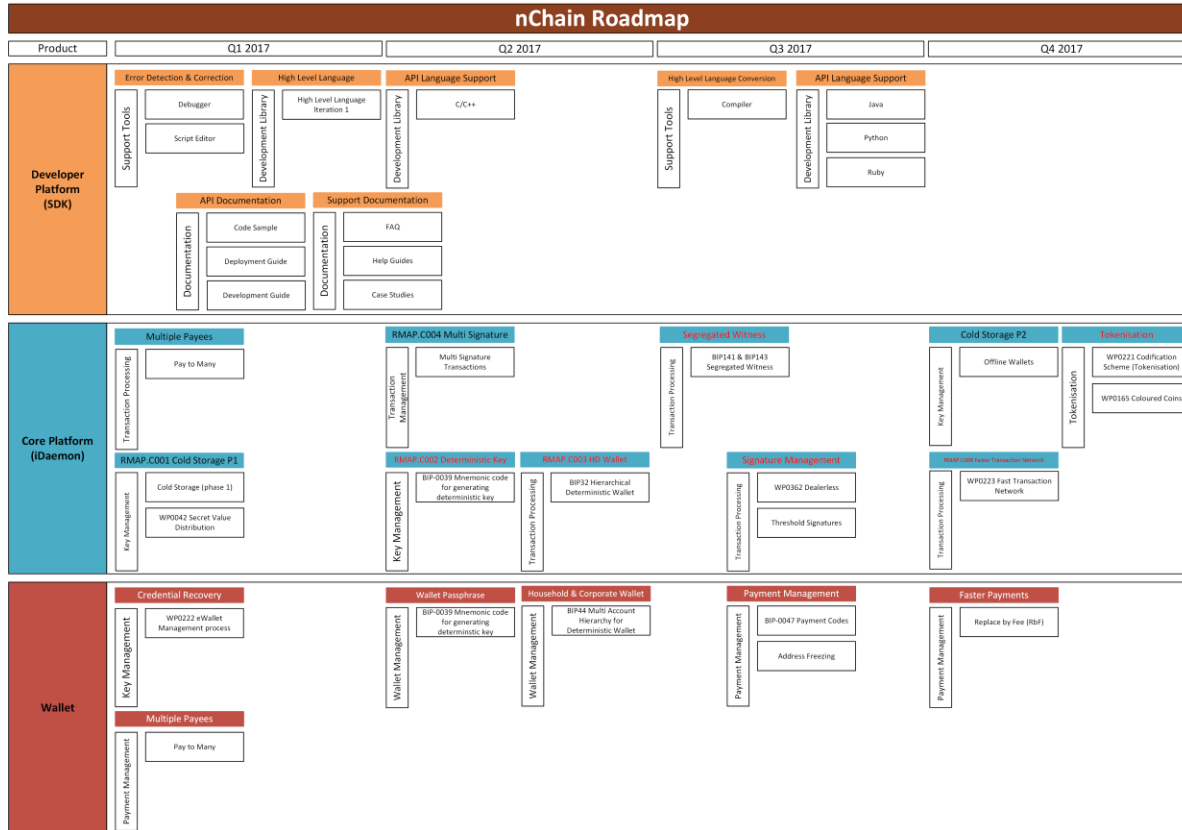
# Attributes of a Platform Strategy

- I. **Connection** – the platform allows others to easily interact for sharing and transacting
- II. **Gravity** – the platform attracts global participants, both producers and consumers
- III. **Flow** – the platform fosters the exchange and co-creation of value

# Building Blocks of Successful Platforms

- A. The Toolbox creates connection by making it easy for others to plug into the platform;
- B. The Magnet creates pull that attracts participants to the platform with a kind of social gravity and incentives;
- C. The Matchmaker fosters the flow of value by making connections between consumers and producers.

# Product Road Map





# Strategy

iDaemon as a Full Node



# Factors for Success

a) Gain first-mover advantage

b) Obtain as many users as possible

c) Innovate aggressively via advanced software features

d) Acquire complementary assets

e) Use commercialisation objectives to drive research

(platform network effect)

(revenue is deferred)

(sustained leadership)

(minimize competition)

(patents are defensive)



## 2-Year Strategy to Execute

- Target the network mining nodes as early adopters by appealing to their sense of profit
- Select a spark incentive and/or feature set to spur adoption of iDaemon under the current protocol conditions
- Establish credibility within the Bitcoin coding ecosystem by gradually expanding iDaemon functionality (i.e., node specialisation, increased OP\_CODES, threshold signatures, parallel processing, multi-threading, etc.)
- Focus on sophisticated network monitoring techniques to aid scalability
- Partner with (or acquire) select wallet providers for compatibility and functionality
- Identify premium services to justify various revenue streams with partner companies

# Revenue Overview

- Mining Operations
- iDaemon Joint Ventures
- SDK Licensing
- nTrust Operations



# Where is Non-Mining Revenue Coming From?

As Bitcoin node specialisation occurs, the revenue opportunities will most likely be available at the infrastructure layer, which involves either running a scalable data processing centre or joint venture partnering with large-scale data processing centres:

1. Cloud computing environments, such as Amazon Web Services, IBM, or Microsoft Cloud
2. Telecom and network communication providers, such as China Mobile, Verizon, AT&T, Vodafone, NT&T, Softbank, Deutsche Telekom, Telefonica, and Tata
3. Financial service institutions, such as banks and custodial exchanges
4. Mobile platform and wireless traffic leaders, such as Google and Apple

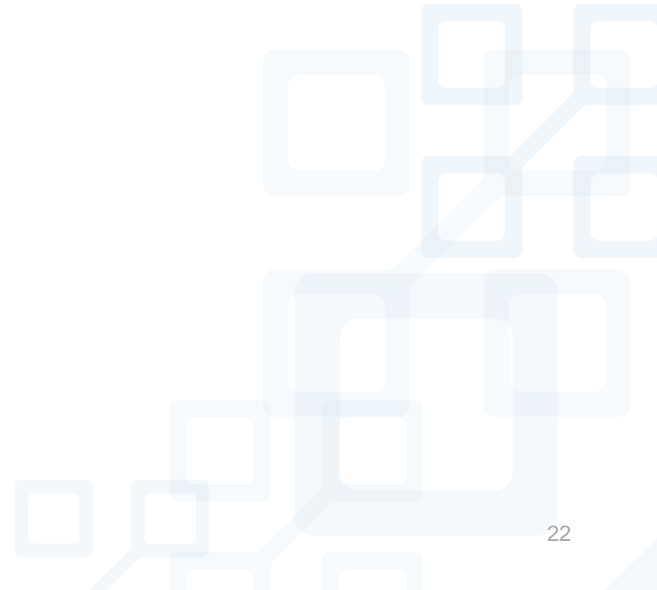
# Possible Types of Non-Mining Revenue Streams

## Transaction-Based Revenue

- Fast validation processing fees
- Coin mixing fungibility fees
- Block propagation relay fees

## Custodial-Based Revenue

- Foreign exchange conversion fees
- Tokenisation issuance and management fees
- Smart contract scripting fees
- Escrow and underwriting fees



# Competitive Analysis of Blockchain Efforts

## Primary (research; IP)

21.co (\$121m)

Blockstream (\$76m)

Digital Asset Holdings (\$67m)

SETL (\$39m)

## Secondary (applications; service)

R3 Corda (\$150m)

Ripple “Interledger” (\$93m)

Chain.com Core (\$30m)

Juzhen Financials (\$23m)

IBM Open Blockchain “Fabric”

Intel Ledger “Sawtooth Lake”

Microsoft Azure “BaaS”

Deloitte “Rubix”

# Tactics

iDaemon as a Full Node





”

“We are leaders not followers. Propagating the nChain vision as full node software will achieve over one billion users.”

– *Craig Wright*

# There Are Two Primary Tactical Approaches

- I. Operate proprietary mining operation in Iceland (influence nodes)
- II. Go global with nTrust mobile wallet (influence users)



# Enter the Bitcoin Mining Business

- Revenue model <insert here>
- Estimated breakeven point to recover initial investment <insert here>
- Cost to achieve 5% network computational power <insert here>
- Proprietary mining operation in Iceland; then open as a mining pool
- Barter nChain iDaemon software for ASIC hardware

# Tactics for Mining and iDaemon Propagation

1. iDaemon design at a minimum must support the current BIP functionality in BitcoinCore
2. Rename iDaemon to something that connotes 'speed' and 'reliability' and 'security'
3. Consider collaboration with other propagation efforts, although this is risky
4. Retain high-profile, experienced influencers that have contributed to BitcoinCore
5. Establish and maintain a GitHub/Mercurial presence with select commit access
6. Influence and steer public opinion through a comprehensive communications strategy

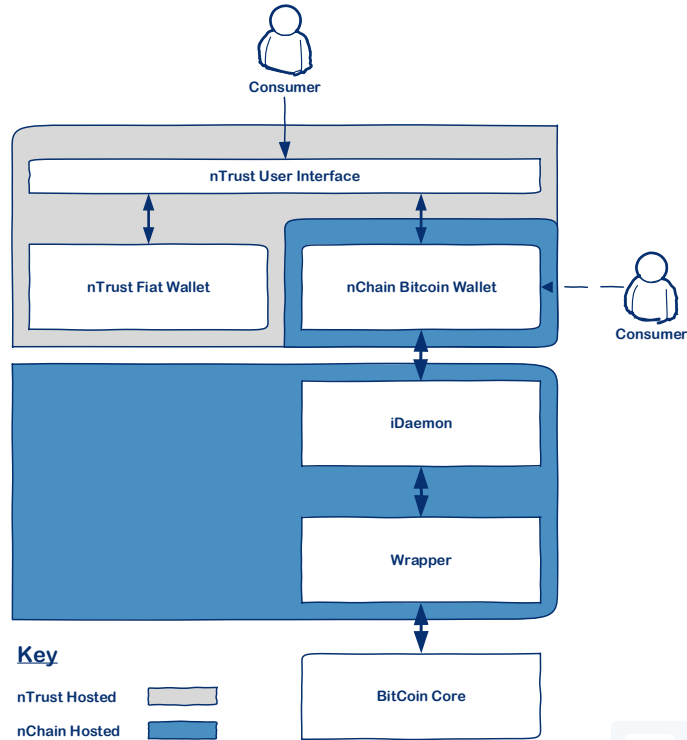
# Detailed Communications Strategy

- Retain public relations agency (respond to prior CSW media questions)
- Prepare coordinated web site in advance
- Target technical points of the Bitcoin protocol (not personalities)
- Publish academic papers in support of iDaemon's technical approach
- Engage multiple public speaking resources on the road
- nChain community manager engages social media forums

# Tactics for nTrust Wallet

1. Open nTrust London office for increased accountability and EU presence
2. Shift nTrust priorities to become aligned with nChain priorities
3. Launch Android/iOS wallet with mobile number bitcoin addressing (Mobi, Zebpay, KnC)
4. Design new scope and budget for software engineering resources
5. Consider acquisitions for speed to market (Samourai, Cubits, Epiphyte)

# Drive New Features/Apps Through nTrust

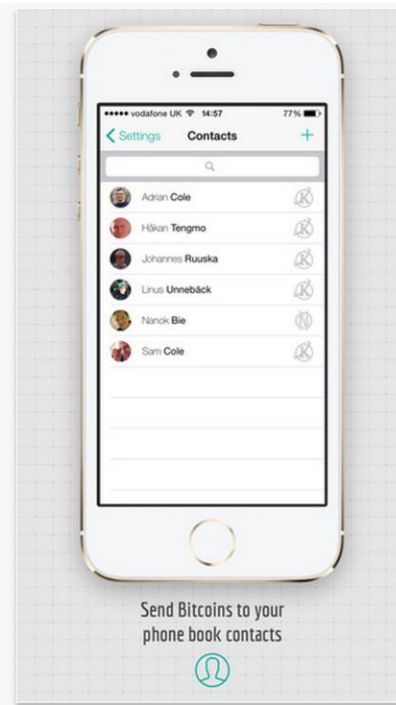
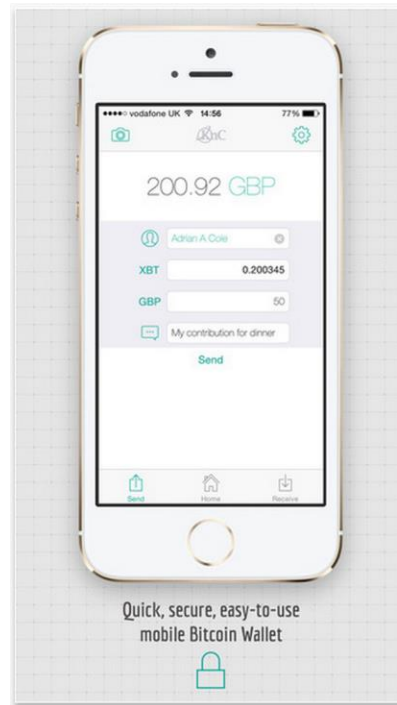
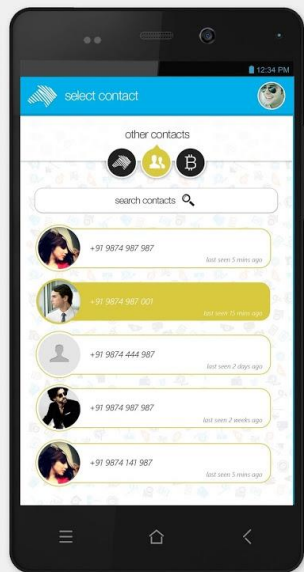


# Mobile Number Bitcoin Addressing

60+ CURRENCIES.  
RIGHT AT YOUR FINGERTIPS.



Send / Receive bitcoins to mobile numbers  
or bitcoin addresses





# Risks

iDaemon as a Full Node



# Risks (financial)

1. This strategy requires intensive ongoing development and rigorous testing, because ultimately it will be entrusted with a \$16 billion+ global network
2. Since this is a two-year platform infrastructure play, significant upfront investment must be made with a payoff pushed out into the future
3. Design specification for iDaemon as a Full Node will reorganise resources from ongoing patent and research programme to targeted problem solving
4. nTrust trading platform development will be suspended

# Risks (non-financial)

1. Dormant IP rights of nChain may be seen as a barrier to initial adoption
2. Alternative Bitcoin code implementations may complicate nChain deployments
3. nChain unable to innovate fast enough or to maintain upgrade releases
4. BitcoinCore deviates from their current plan and decides to incorporate rapid scalability improvements prior to iDaemon gaining network dominance (may be a win)
5. Perception of nChain as a centralised 'benevolent dictator'
6. No current backup strategy to CSW as Chief Scientist

# Charts

iDaemon as a Full Node



# Overview of Bitcoin Protocol Implementations

## Node Types

Bitcoin Core (v0.13.2)

Bitcoin Core (forked implementations)

Full Nodes (alternative implementations)

Overlay to Core (overlay protocols)

## Wallet Types (O/S)

Desktop (Windows, Apple, Linux)

Mobile (Android, iOS)

Web

# Alternative Bitcoin Implementations Today

## Full Node (not incl. forks to Core)

libbitcoin (C++) \*

Bitcoinj (Java)

Btcd (Go) \*

Picocoin (C++)

Bits of Proof (Java)

BCoin (Javascript) \*

Toshi (Ruby)

Caesure (Python)

NBitcoin (C#)

## Overlay Protocol (to Core)

Bitcore (Javascript) \*

Armory (Python)

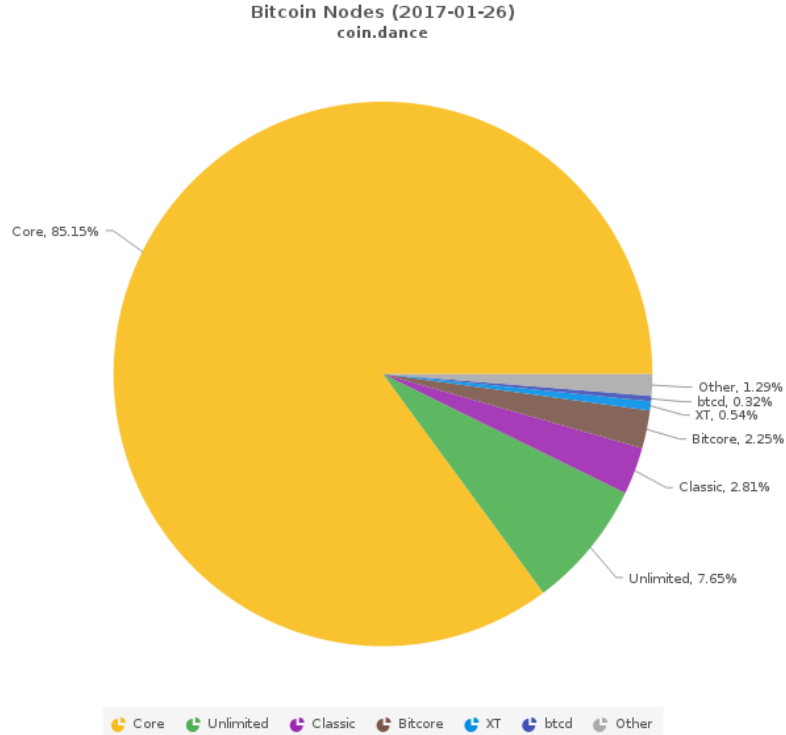
Electrum/Stratum (JSON-RPC 2.0)

Haskoin (Haskell)

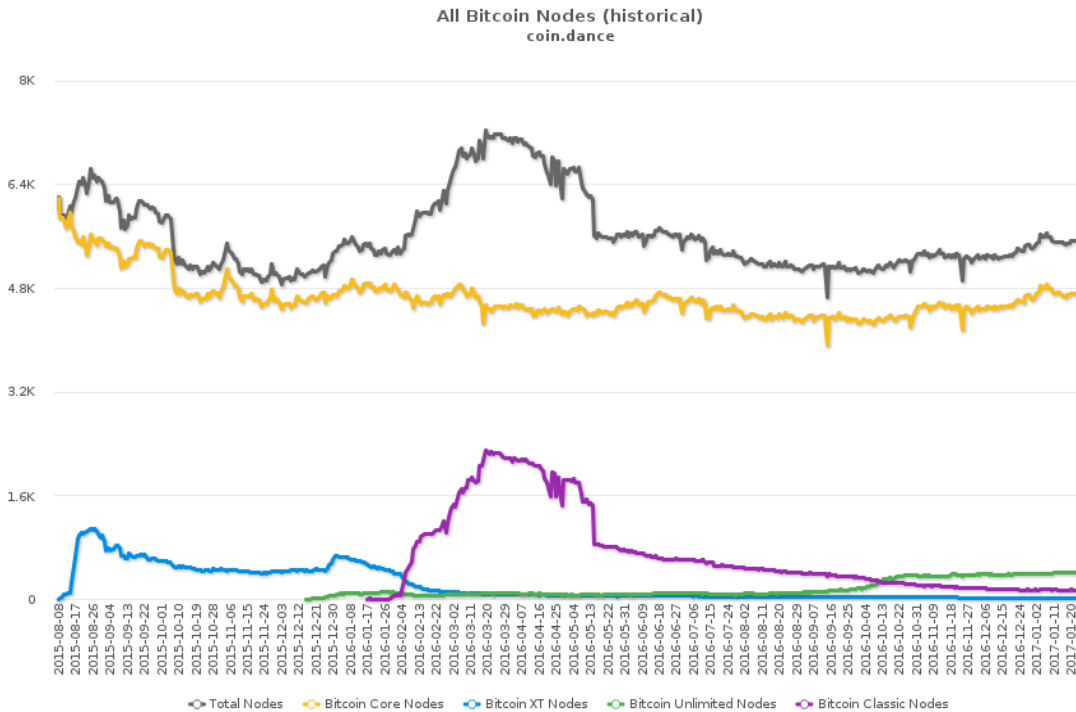
MultiBit (Java) \*\*

nChain iDaemon today (Java)

# Global Bitcoin Network Nodes



# All Bitcoin Nodes





# Growth of Bitcoin Unlimited

