chaincode

History and Philosophy of Bitcoin Development

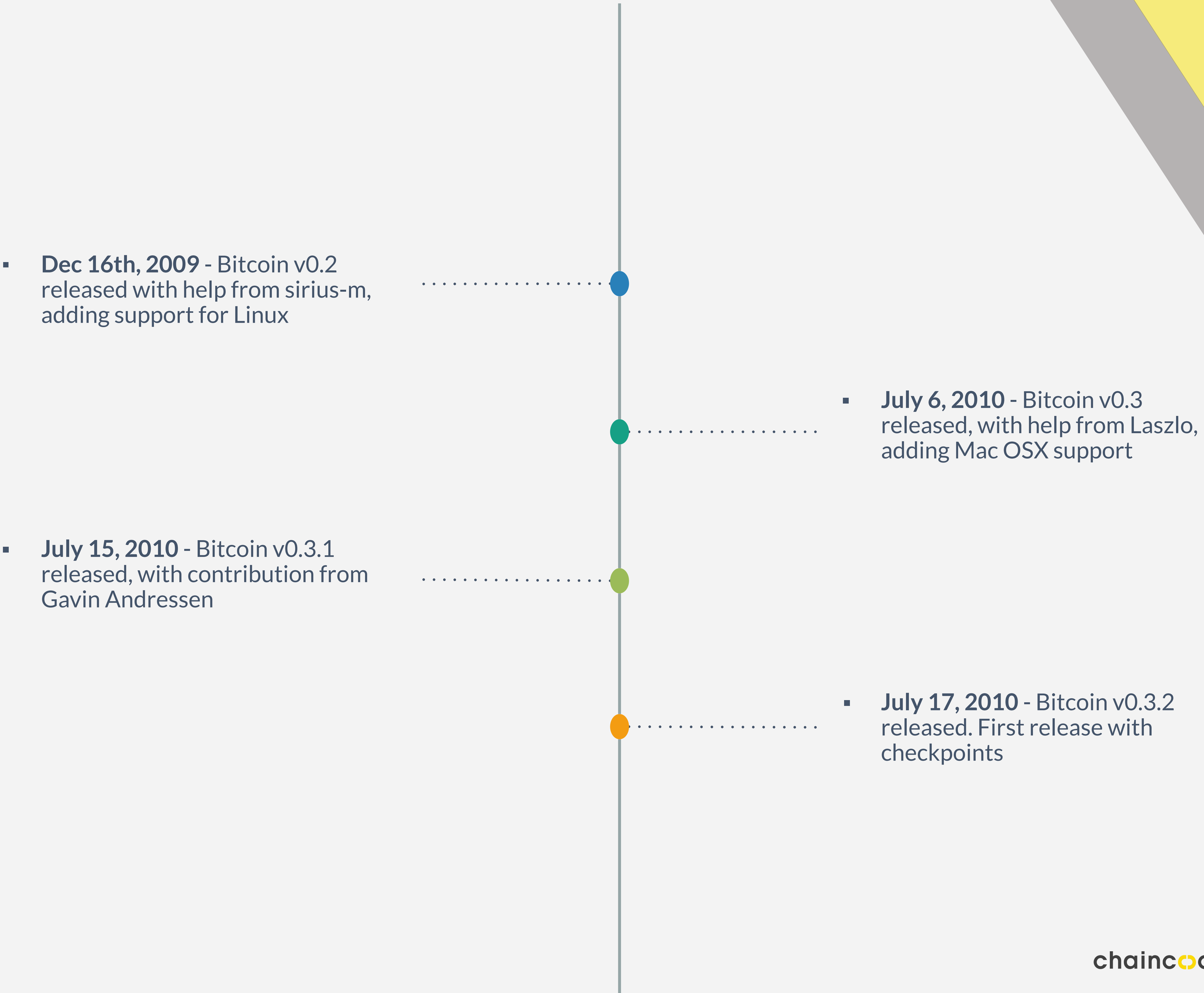
bitdevs summer series, June 19th 2019

History

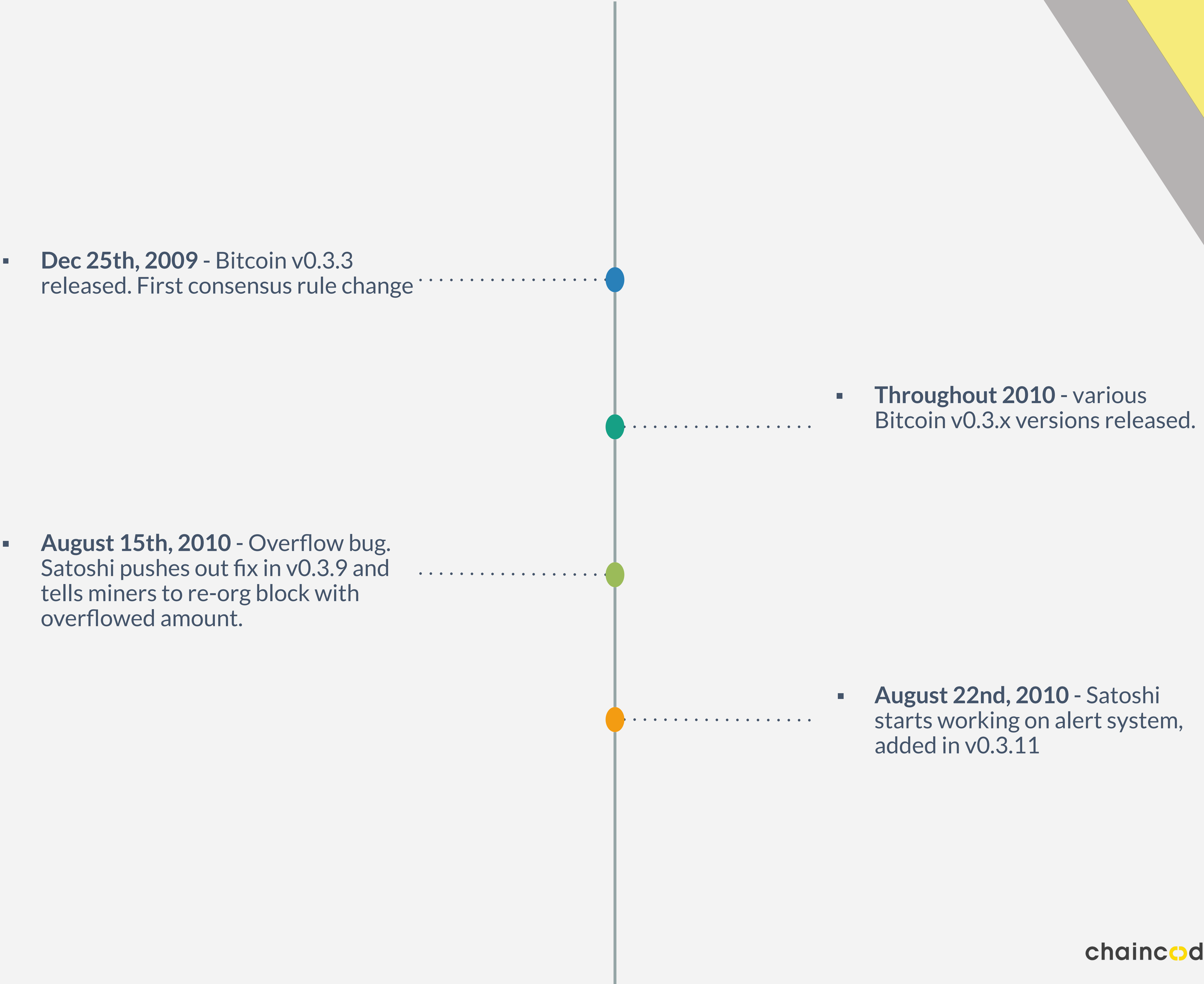
- **Early 2007** - Satoshi Nakamoto starts writing code for Bitcoin.
- **Nov 1st, 2008** - Bitcoin announced by ‘Satoshi Nakamoto’ on the Cryptography mailing list.
- **Somewhere between Jan 3rd and Jan 9th, 2008** - Genesis block is mined.
- **Jan 9th, 2008** - Bitcoin v0.1 is announced on cryptography mailing list.

“I've been working on a new electronic cash system that's fully peer-to-peer, with no trusted third party.”

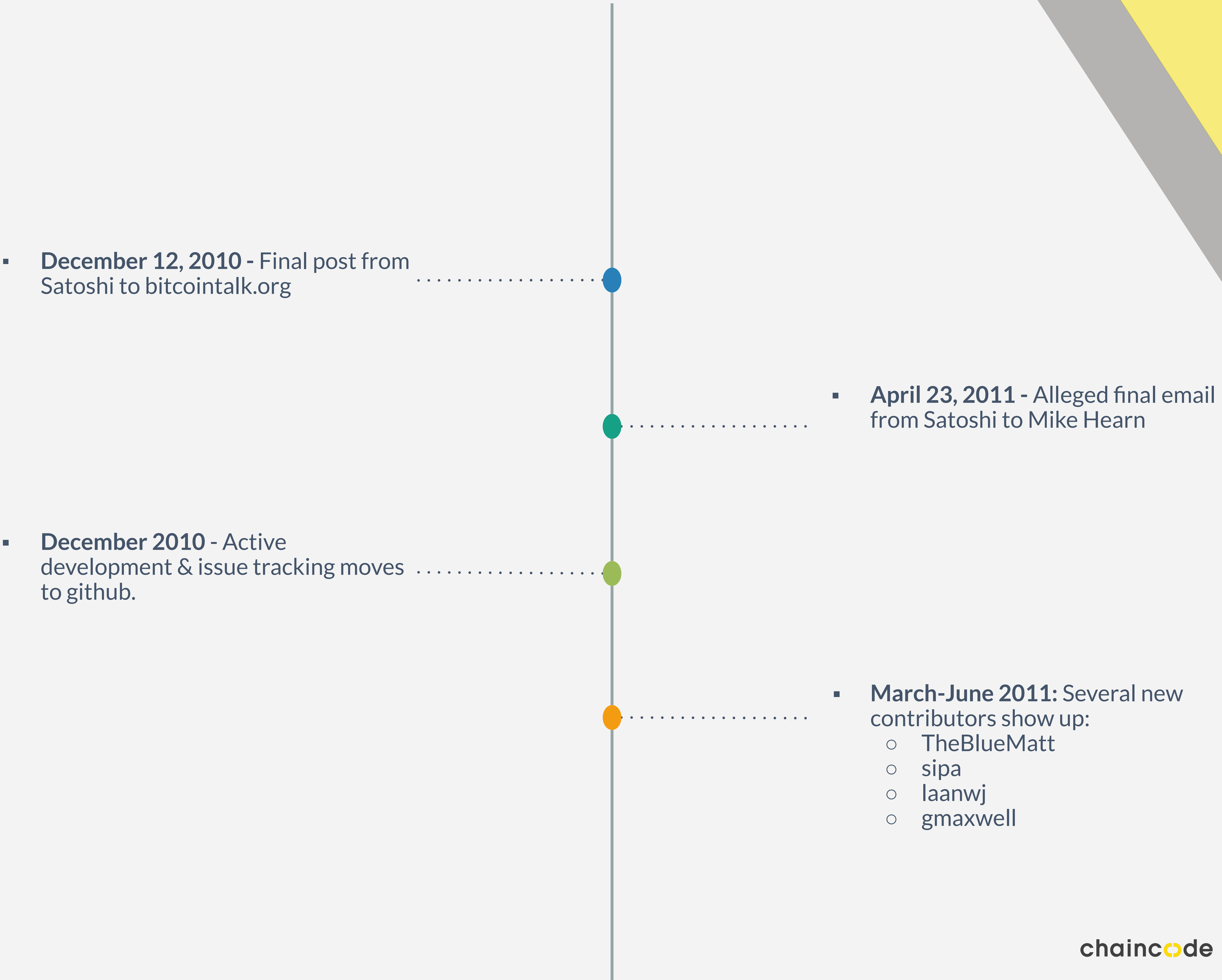
– Satoshi Nakamoto



- **Dec 16th, 2009** - Bitcoin v0.2 released with help from sirius-m, adding support for Linux
- **July 6, 2010** - Bitcoin v0.3 released, with help from Laszlo, adding Mac OSX support
- **July 15, 2010** - Bitcoin v0.3.1 released, with contribution from Gavin Andressen
- **July 17, 2010** - Bitcoin v0.3.2 released. First release with checkpoints



- **Dec 25th, 2009** - Bitcoin v0.3.3 released. First consensus rule change
- **Throughout 2010** - various Bitcoin v0.3.x versions released.
- **August 15th, 2010** - Overflow bug. Satoshi pushes out fix in v0.3.9 and tells miners to re-org block with overflowed amount.
- **August 22nd, 2010** - Satoshi starts working on alert system, added in v0.3.11



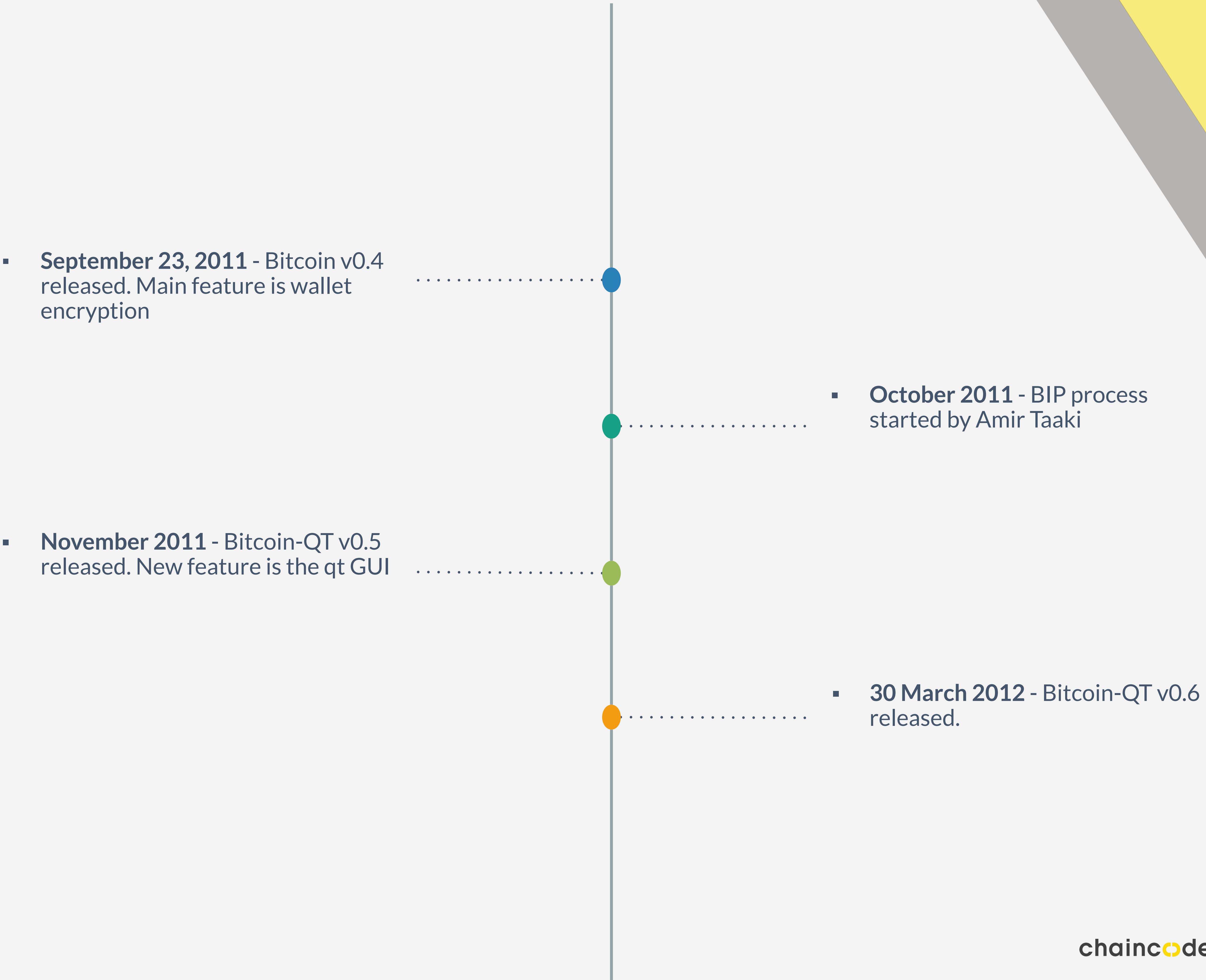
- **December 12, 2010 -** Final post from Satoshi to bitcointalk.org

- **April 23, 2011 -** Alleged final email from Satoshi to Mike Hearn

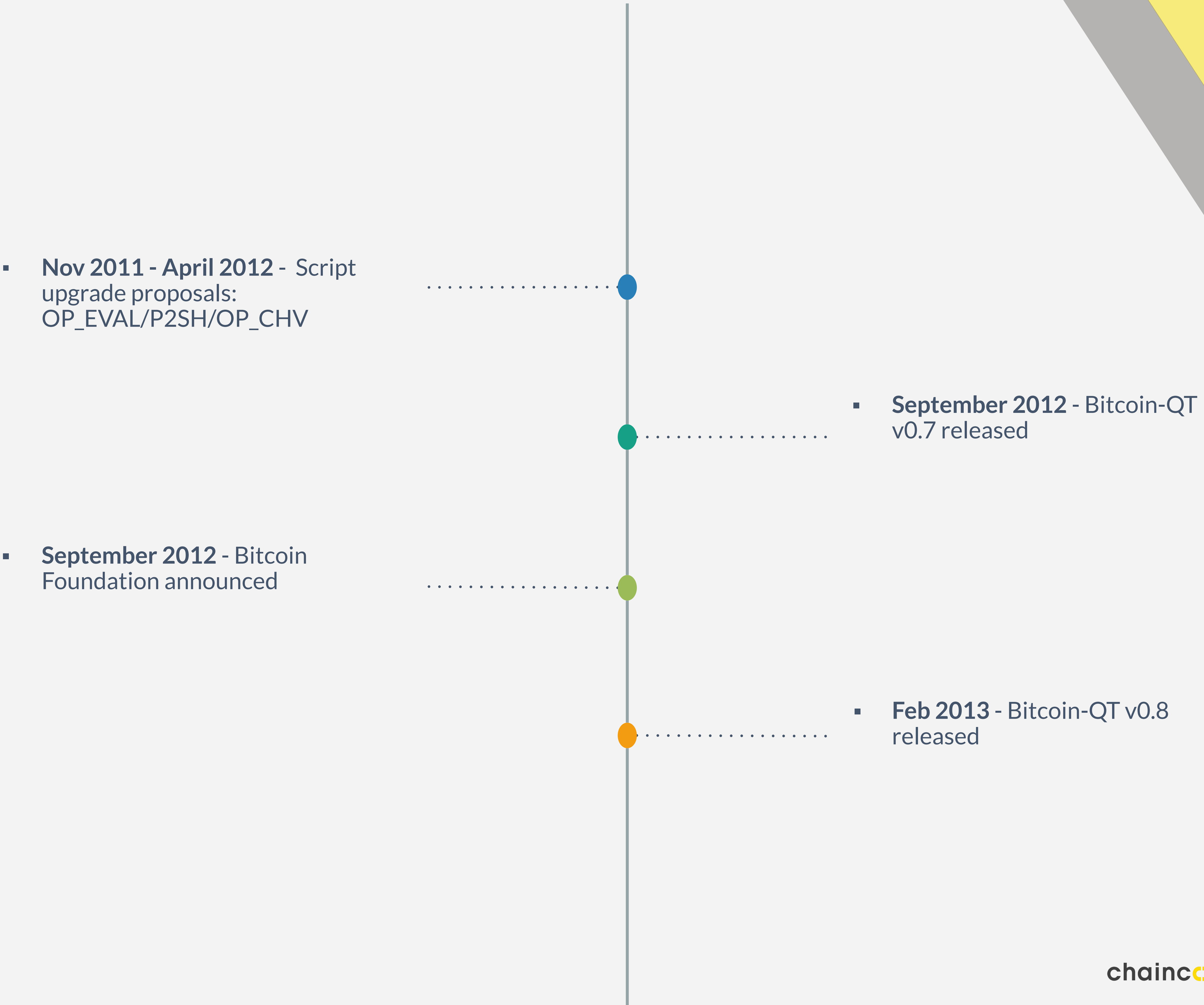
- **December 2010** - Active development & issue tracking moves to github.

- **March-June 2011:** Several new contributors show up:
  - TheBlueMatt
  - sipa
  - laanwj
  - gmaxwell

“I've moved on to other things. It's in good hands with Gavin and everyone.”

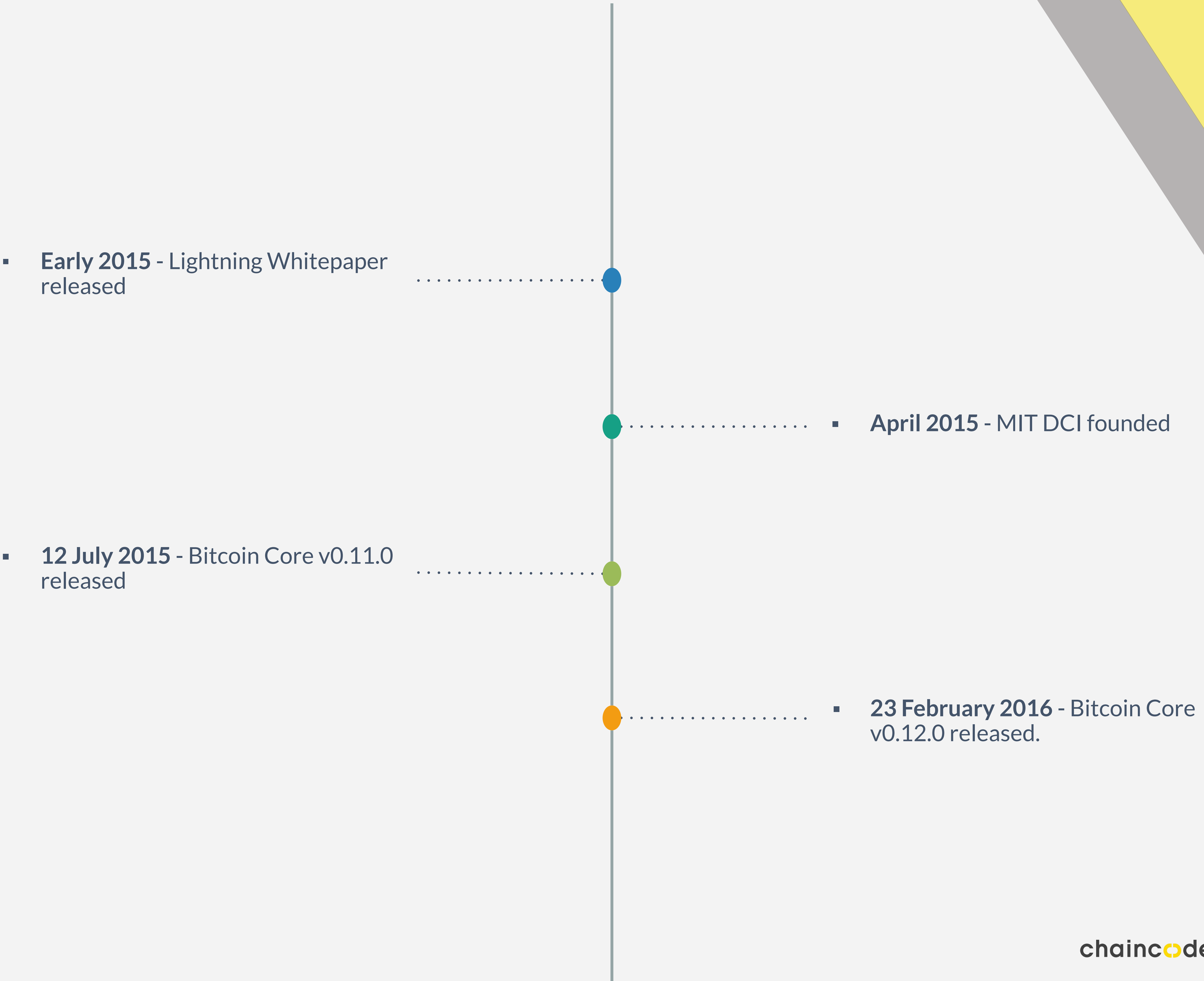


- **September 23, 2011** - Bitcoin v0.4 released. Main feature is wallet encryption
- **October 2011** - BIP process started by Amir Taaki
- **November 2011** - Bitcoin-QT v0.5 released. New feature is the qt GUI
- **30 March 2012** - Bitcoin-QT v0.6 released.

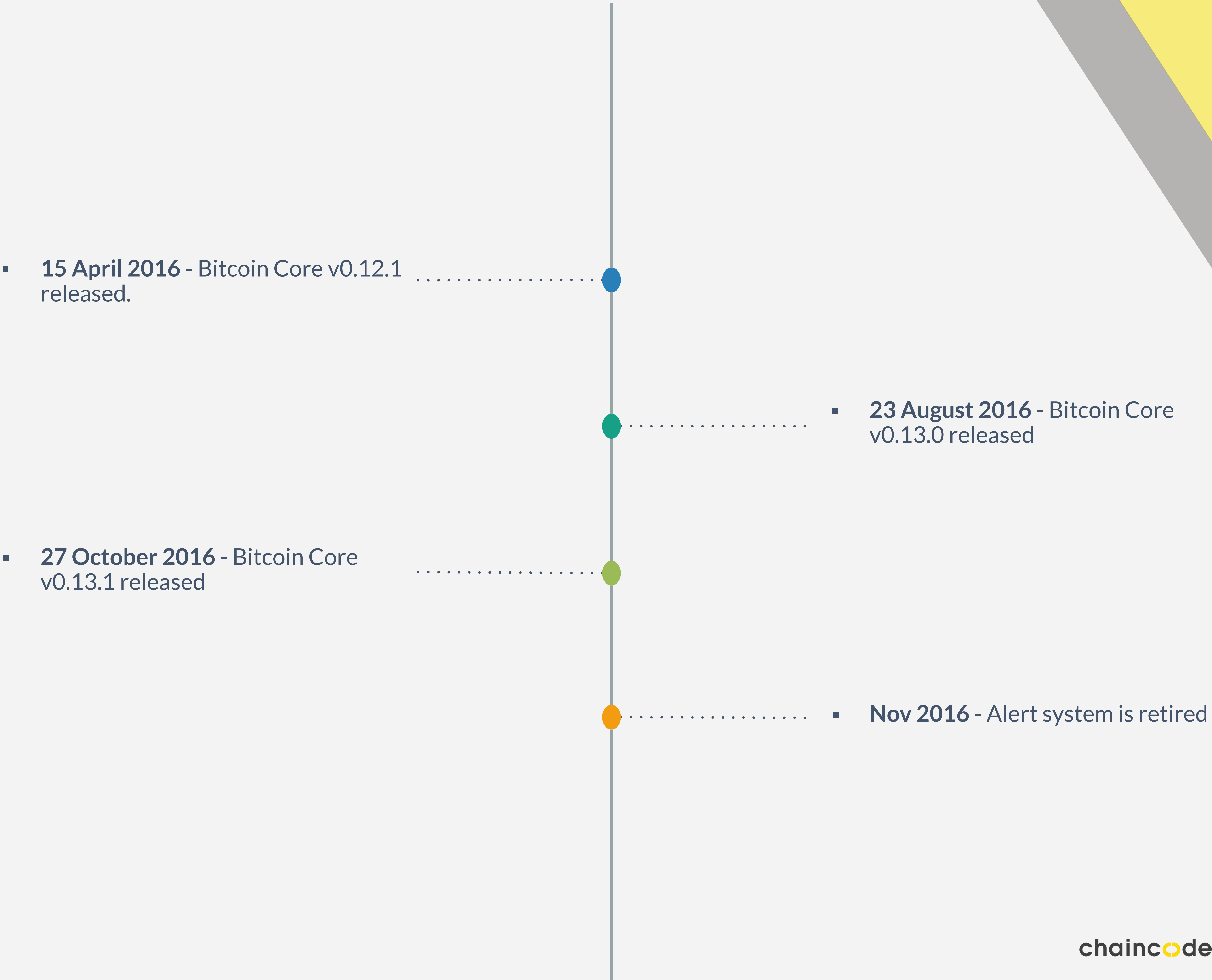


- **Nov 2011 - April 2012 -** Script upgrade proposals: OP_EVAL/P2SH/OP_CHV
- **September 2012 -** Bitcoin-QT v0.7 released
- **September 2012 -** Bitcoin Foundation announced
- **Feb 2013 -** Bitcoin-QT v0.8 released

- **November 2013** - Bitcoin software rebranded to Bitcoin Core
- **March 2014** - Bitcoin Core v0.9 released
- **October 2014** - Adam Back, Matt Corallo, Greg Maxwell, Pieter Wuille et al form Blockstream and release the sidechains whitepaper.
- **16 Feb 2015** - Bitcoin Core v0.10.0 released



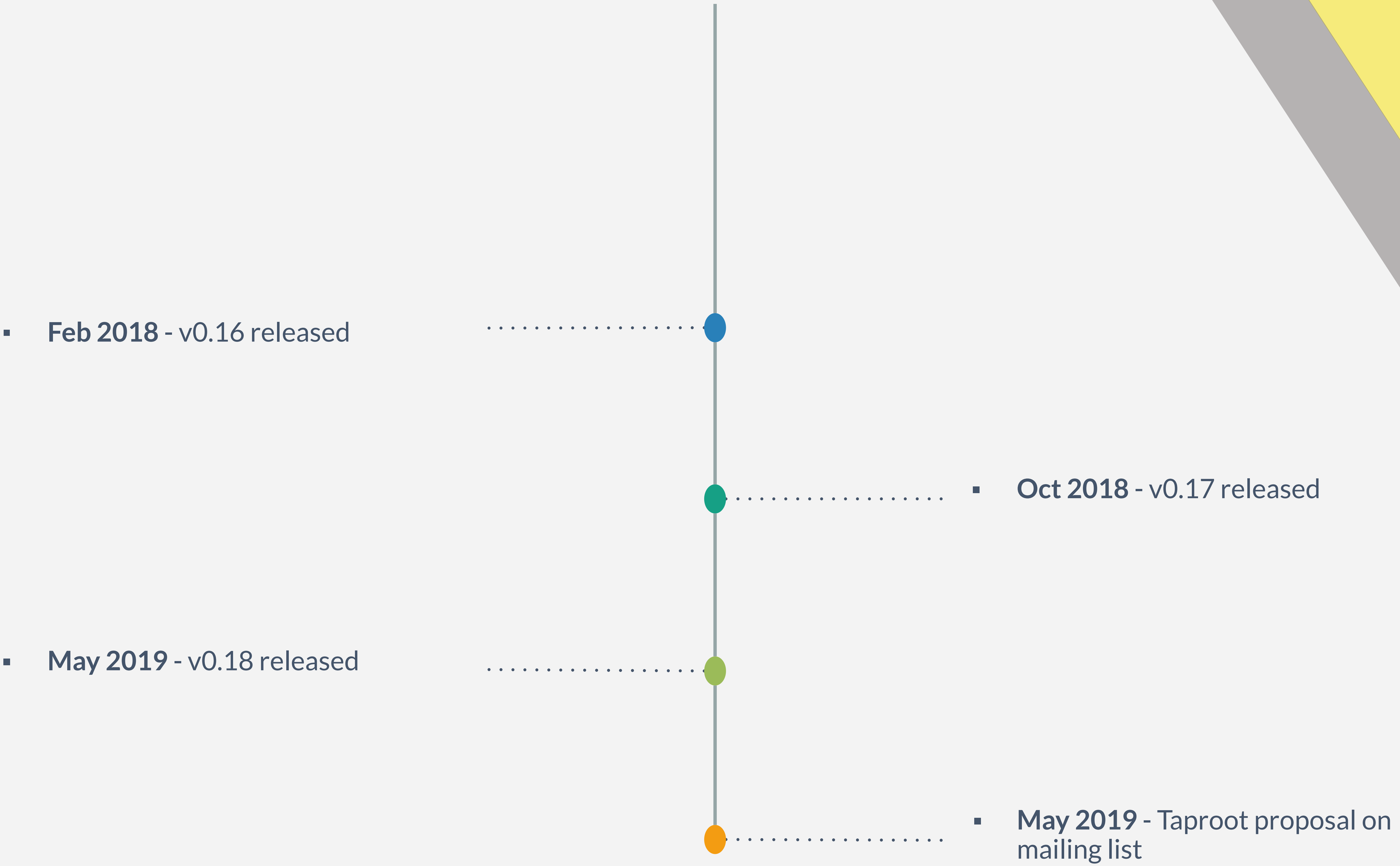
- **Early 2015** - Lightning Whitepaper released
- **April 2015** - MIT DCI founded
- **12 July 2015** - Bitcoin Core v0.11.0 released
- **23 February 2016** - Bitcoin Core v0.12.0 released.



- **15 April 2016** - Bitcoin Core v0.12.1 released.
- **23 August 2016** - Bitcoin Core v0.13.0 released
- **27 October 2016** - Bitcoin Core v0.13.1 released
- **Nov 2016** - Alert system is retired

chaincode

- **8 March 2017** - Bitcoin Core v0.14 released
- **14 September 2017** - v0.15 released
- **11 November 2017** - v0.15.1 released
- **24 August 2017** - segwit activated!



- **Feb 2018** - v0.16 released
- **Oct 2018** - v0.17 released
- **May 2019** - v0.18 released
- **May 2019** - Taproot proposal on mailing list

What do Bitcoin users care about?

What do Bitcoin Users Care about?

- Centralization
- Consensus
- Robustness/security
- Incentive alignment
- Privacy
- Fungibility
- Scalability
- Conservatism
- Monetary Policy

Centralization

“A lot of people automatically dismiss e-currency as a lost cause because of all the companies that failed since the 1990's. I hope it's obvious it was only the centrally controlled nature of those systems that doomed them. I think this is the first time we're trying a decentralized, non-trust-based system.”

– Satoshi Nakamoto

Centralization

- Why? Because a system like Bitcoin can’t survive if it becomes centralized.
- Trusted third parties defeat the whole point
- We’re already too centralized - need to make sure we don’t do anything to make that worse

Aspects of Centralization

- Node/ledger
- Mining
- Mining hardware
- Exchange and economy
- Developer

Consensus

Consensus

- BTC is a consensus system
- Consensus failures can destroy the whole system
- Consensus code should be ringfenced
- Limit user choice
- Are alternative implementations desirable?

Robustness/security

Robustness/security

- Consensus failures
- P2P code
- Logic bugs
- Incentive alignment

Incentive alignment

“The incentive may help encourage nodes to stay honest. If a greedy attacker is able to assemble more CPU power than all the honest nodes, he would have to choose between using it to defraud people by stealing back his payments, or using it to generate new coins. He ought to find it more profitable to play by the rules”

– Satoshi Nakamoto

Incentive alignment

- Behaviour of node should be for benefit of users, and benefit of users should be aligned with benefit of system
- Examples:
    - RBF
    - default blockmaxsize for miners
    - coin selection in wallet
    - P2P ‘altruism’
    - Block/tx propagation

Privacy

“I can't seem to find the link to your bank account records, mind posting them for us?”

– Greg Maxwell

Privacy

- Financial privacy is essential for fungibility in Bitcoin
- Financial privacy is essential for the efficient operation of a free market
- Financial privacy is essential for personal safety
- Financial privacy is essential for human dignity
- Financial privacy isn't incompatible with law enforcement or transparency

Fungibility

Fungibility

- An asset cannot function as a currency without fungibility.
- If all users needed to do coin analysis on all the funds they received, then the utility of the system drops to zero.
- Money that is not fungible is at risk of censorship.

Usability

Usability

- System must be easy for users
- Defaults are important!
- Remove footguns
- Don’t create/expose shortcuts that people will misuse
- Move complexity off-chain

Scalability

“Use the blockchain for what the blockchain is good for”

– Andrew Poesltra

Scalability

- Keep the base layer simple
- Incentives should be to minimize validation cost

Conservatism

“I think we should remember that we're not just writing code for ourselves, but for hopefully a much larger set of future engineers. If we are going to burden people with complicated reasoning about a consensus topic, it should be because it's really important.”

– Suhas Daftuar

Conservatism

- Bitcoin is a money, so should be stable in the long run
- We should be conservative about making changes
    - to minimize risk to the system
    - allow people to continue using the system in the way they see fit

Monetary Policy

“Escape the arbitrary inflation risk of centrally managed currencies!”

– Satoshi Nakamoto

Monetary policy

- Bitcoin monetary supply is:
  - predictable
  - approaches zero inflation
  - allocated to miners in exchange for securing the system
- Is this ‘optimal’? What does that mean? Would users ever want to change it?

Questions?
Comments?