

TALK

---

# Forkonomy: Blockchains, Time Travel & Possible Futures for ETC

Wassim Alsindi PhD

DIRECTOR OF RESEARCH

PARALLEL INDUSTRIES

WWW.PLLEL.COM // @PARALLELIND





# SPEAKER



Wassim  
**ALSINDI**  
DIRECTOR OF RESEARCH  
PARALLEL INDUSTRIES



## WHAT IS THIS ALL ABOUT?

---

- > Forkonomy 101
- > Forks as Parallel Timelines
- > What Maketh a Fork?
- > Fork-Merge: 2 Chains into 1
- > ETC Past, Present & Future
- > Blockchains as Time Machines?



# LITTLE BIT ABOUT ME

## SCIENCE KID

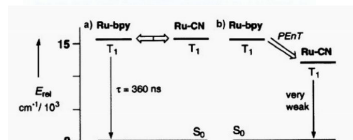
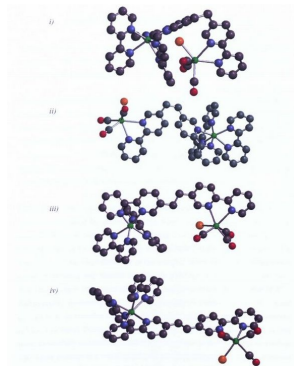


Figure 3.1.4: A schematic of the photophysics of RuCN-BI-Ruby in a)  $H_2O$  and b) DMSO. Reproduced from Ref. 1

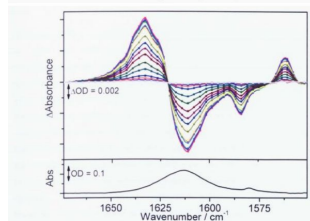


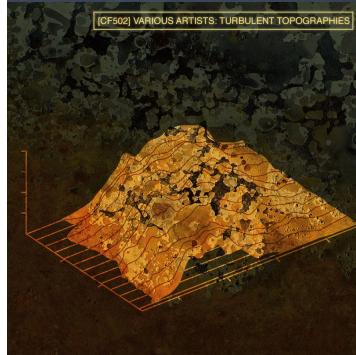
Figure 4.4.3.3: The FTIR (bottom) and ex-IR spectra between 1 and 750 ns (top) of RubyamideRPM in  $D_2O$  solution.

## EXPERIMENTAL ARTS

THE CENTRIFUGE PRESENTS  
OPEN SOURCE ACID



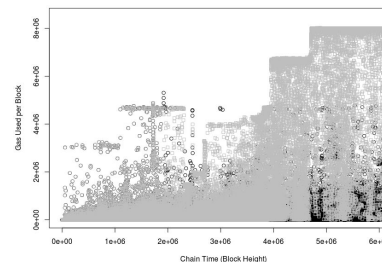
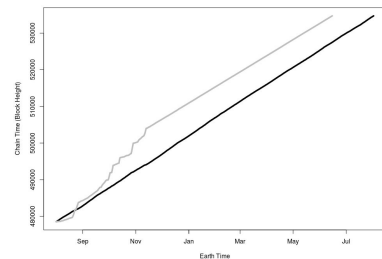
[CF502] VARIOUS ARTISTS: TURBULENT TOPOGRAPHIES



## D-TECH RESEARCH

### #ReachingEveryone

### #Forkonomy



Matt @MattoshN - Aug 6

Our first iteration of transaction-delaying software. Can be used to set a timer on a transaction (ideal for carrying, say, an empty @OPENDIME across borders). Ideally run on low-footprint, always-on Pi Zero.

CC: @paralleld  
#ReachingEveryone







# WTF IS FORKONOMY?

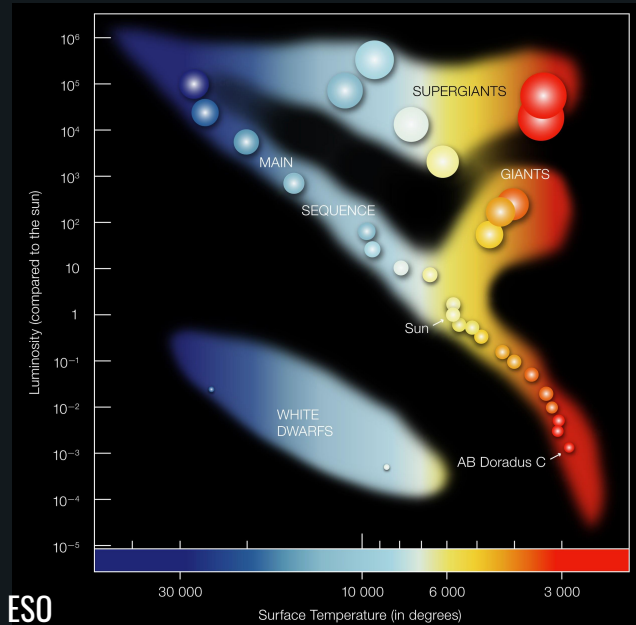


Credit: NASA, ESA, and S. Beckwith (STScI) and the HUDF Team  
<http://spacetelescope.org/images/heic0406a/>



Credit: ESO/[Y. Beletsky](#)

[https://www.eso.org/public/images/uhd\\_beletsky\\_alma\\_15/](https://www.eso.org/public/images/uhd_beletsky_alma_15/)



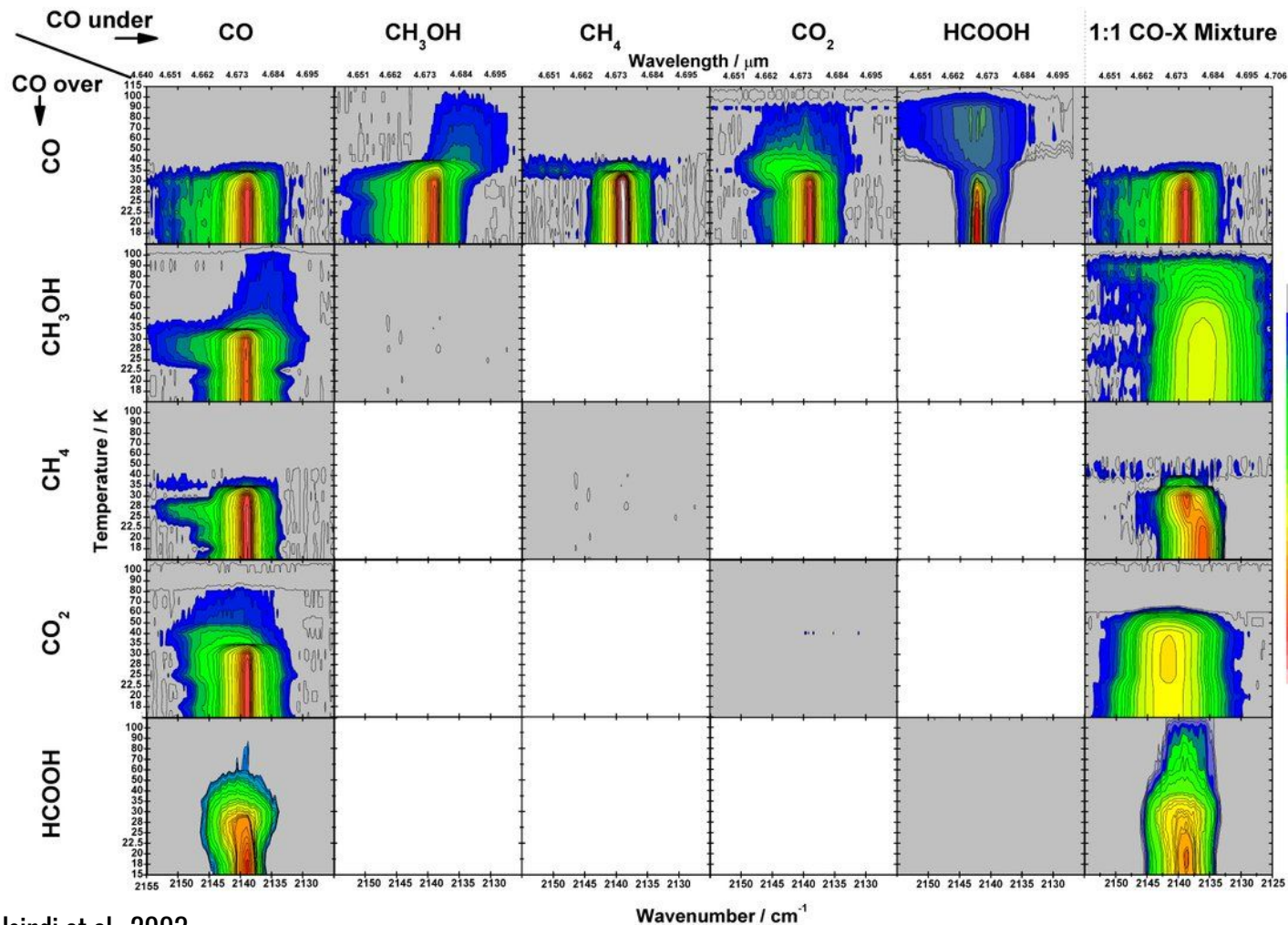
Credit: ESO

<https://www.eso.org/public/images/eso0728c/>





Credit: @LaurentMT  
<https://blog.goodaudience.com/gravity-10e1a25d2ab2>



Credit: W. Z. Alsindi et al., 2003.





*Testimonial Review: "Just a bunch of jargon"*



# Forks and Forkability

*WTF is forkonomy?*

O RLY?

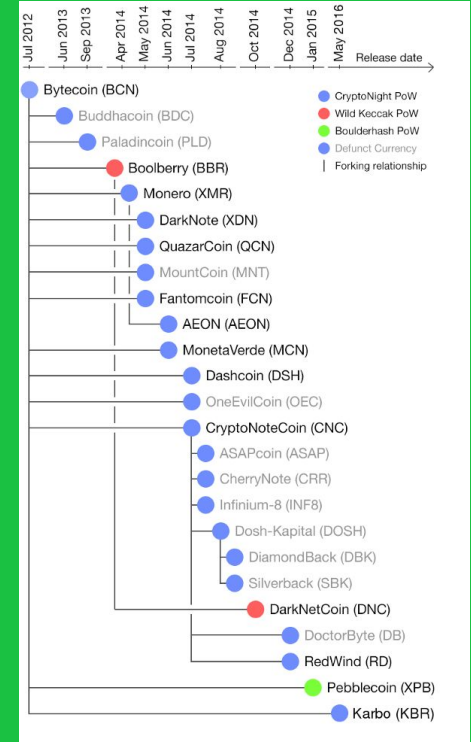
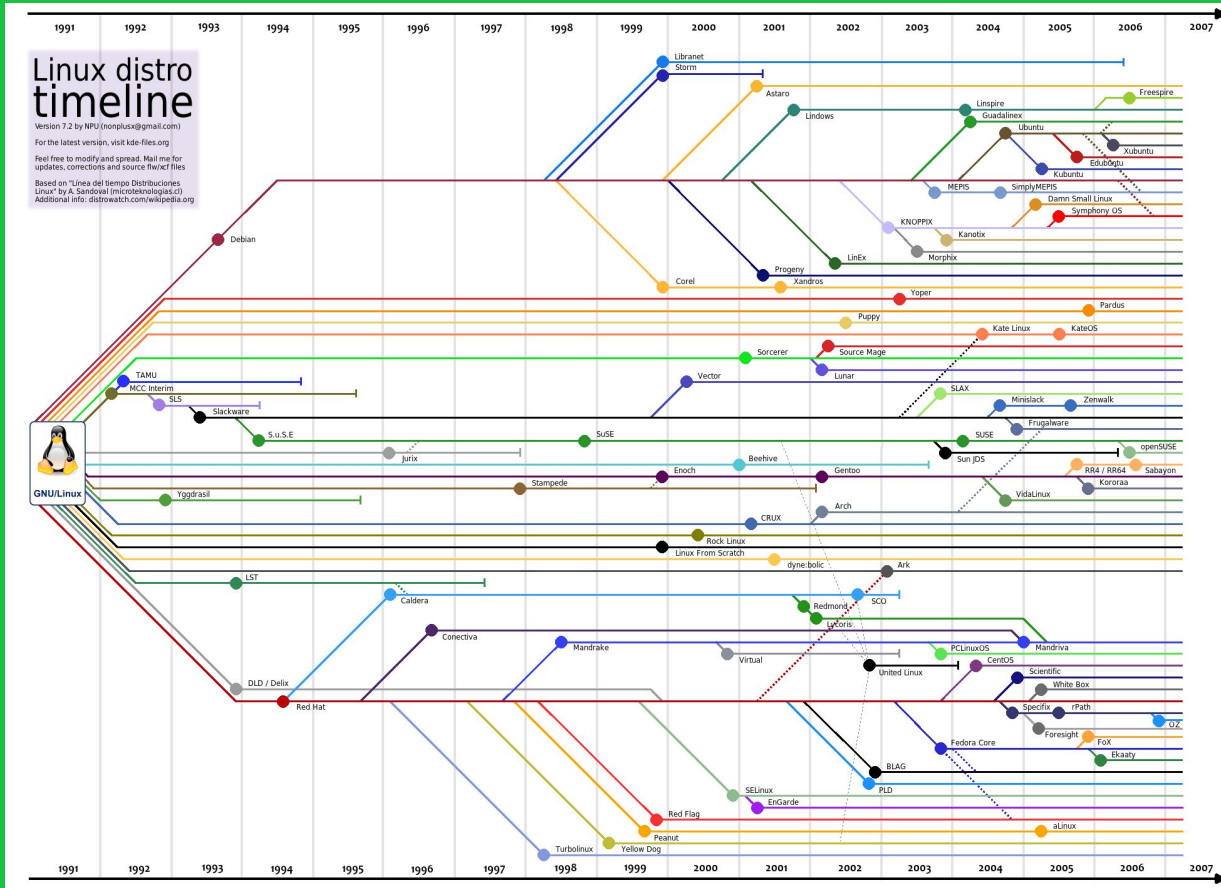
@parallelind



# **FORKS IN THE ROAD**

## **PARALLEL DIMENSIONS?**

# CODEBASE FORKS

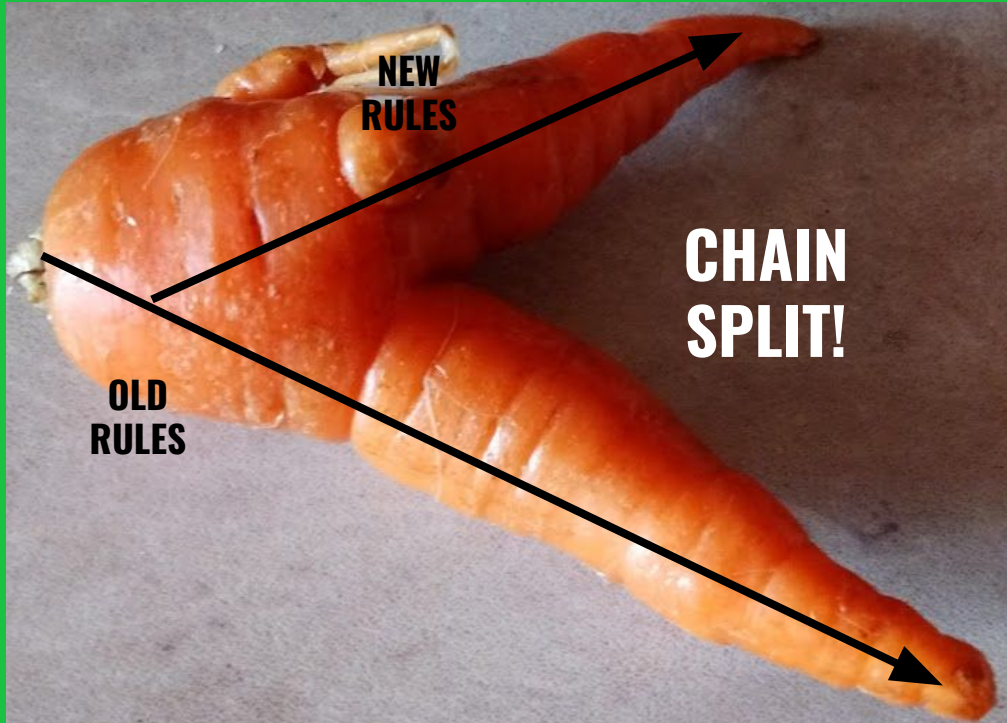


Credit: Kun Woo

<https://medium.com/@favakrypt/the-long-fork-story-of-monero-xmr-cryptonote-code-forks-chain-splits-and-network-upgrades-bc5250b4db>



# LEDGER FORKS



- > DYNAMIC PROCESS
  - > PARAMETER / CONSENSUS TWEAKS\*
  - > NETWORK FRAGMENTATION
  - > REPLAY ATTACKS\*
  - > CHAIN REORGs / WIPEOUTS\*
- 
- > **HARD** - RULE RELAXATION / IRREV.
  - > **SOFT** - RULE CONSTRICTION / OPT-IN
  - > **VELVET** - MIN. CONSENSUS-BREAKING

\*SOMETIMES / GENERALLY SPEAKING





Credit: <http://thecreativeadventurer.com/blog/exploring-glasgows-buchanan-street>



Credit: <https://pixabay.com/en/car-asphalt-delorean-parking-lot-3249993/>



Credit: <https://pixabay.com/en/car-asphalt-delorean-parking-lot-3249993/>



# WHAT MAKETH A FORK?

## INTENTION, SUPPORT, POLITICS





**Chandler Guo**

@ChandlerGuo

Follow

I am Chandler Guo, a 51% attack on Ethereum Classic (ETC) is coming with my 98G hashrate



powtopos

pow to pos

powtopos.com

1:33 PM - 24 Jul 2016



**Chandler Guo** @ChandlerGuo · 31 Jul 2016

Today i will turn on my 120GH for the ETC chain to protect ETC

ETC would definitely harm innocent people. Countless numbers of ETC holders would be harmed financially. Right now an attack on ETC by 51pool.org is the equivalent to the DAO hacker. Whoever does bad/evil, i'll attack. Today i will turn on my 120gh for the ETC chain to protect ETC

山西, 中华人民共和国



-269

发推

, 。 ? ! 、 .....

q

w

e

r

t

y

u

i

o

p

*And so I joined Ethereum Classic initially mostly as a protest. And I wanted to say, 'Listen, this is not ok. Not everybody agrees. You don't have 99% of the community behind you. There is certainly a subset of your population that thinks you have betrayed the social contract you raised the money for, and you have, in a way, damaged your community. And we're not going to take it. We're going to make sure that you understand that the decisions you have made are not free and they have some form of consequence.'*

*But then after interacting with the Classic community and having a lot of conversations and getting to know them, I've come to the conclusion that it is a self-sustaining ecosystem if it wants to be. Meaning that there is a tremendous amount of opportunity for Ethereum Classic to diverge from ETH and actually become its own coin and chart its own course and have a different philosophy and different roadmap. And that, in and of itself, is actually a really exciting thing. Whenever you find a good ecosystem, a good value, good developers, good community you don't just throw that away. That's something you keep, cherish, and grow and see where it goes."*



**Credit:** <https://www.ethnews.com/charles-hoskinson-tells-us-why-he-is-100-etc>  
<https://www.youtube.com/watch?v=f9YDXaVTXkg>  
<https://toshitimes.com/ouroboros-vs-casper-vitalik-buterin-and-charles-hoskinson-in-a-heated-debate/>



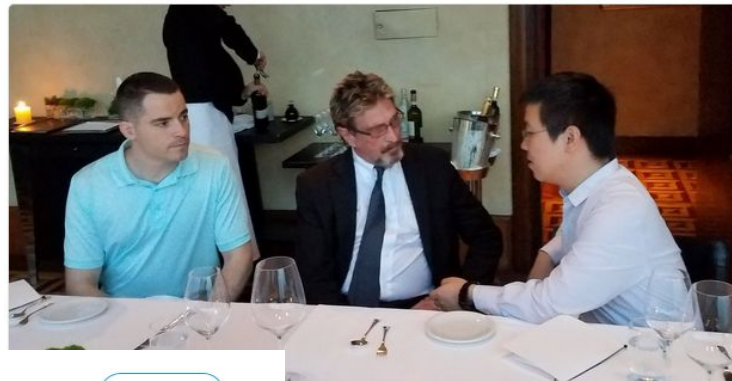
**John McAfee** ✓

@officialmcafee

Follow



Jihan Wu, Roger Ver and myself discussing how to put marriage and divorce on the blockchain.



**Dr Craig S Wright** ✓

@ProfFaustus

Follow



The fact, Bitcoin was never anti-banking. It was opposed to anti-free-market intervention.

The purpose of Bitcoin is to stop just the thing that Jihan, ABC and others are now calling for.

9:37 AM - 1 Sep 2018



# BTC & BCH

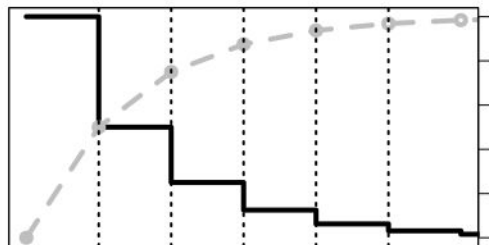
R: "Chain dynamics"

D1: Supply inflation &

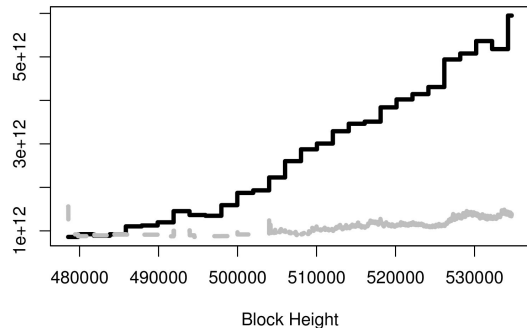
% issued over time,

D2: Mining Difficulty

Mining Subsidy Per Block



Mining Difficulty



BCH Difficulty Algorithm "Adjustments"

Data: <http://blockchair.com>, Image: Parallel Industries, <http://forkonomy.pllel.com>



# Bitcoin Cash double spends

Double spend is when a set of coins is spent in more than one transaction. This can happen for various reasons, but one of the reasons **is fraud attempts**.

If you are accepting 0-conf payments, it's in your interest to detect double spend attempts. If you want merchants to accept your 0-conf payments, it's in your interest to help detect double spend attempts.

**Bitcoin XT** detects double spends relayed to it. It allows you to react to double spends. It's also the only Bitcoin Cash node that forwards double spends to allow other nodes to detect them.

Help gathering double spends here and detecting them network wide by running Bitcoin XT and connecting to at least one other Bitcoin XT node, such as `respsnds.thinlink.com:8333`

Below are double spends detected with Bitcoin XT. Tags are applied to some as analysis for cause or motivation of the double spend.

Last updated 2018-08-29 17:57:56.354944

## Original 🏆

[Raw data](#)

Hash: 8a

First seen: 2018-08-29 17:47:10

Status: Confirmed!

Fee: 1.64444444 sat / bytes

Tags:

Inputs:

0.05765851 BCH from a6

Outputs:

0.00000700 BCH to qpzfq6ptdnnngmaz5jl9s3xe24rhj58xwv0unyud9

0.05764781 BCH to qrkzmsdyw6dzl7c5zv4c8lw58czfxtau5nv9pu3l6

## Double

[Raw data](#)

Hash: 71

First seen: 2018-08-29 17:47:10

Status: Lost!

Fee: 1.63716814 sat / bytes

Tags:

Inputs:

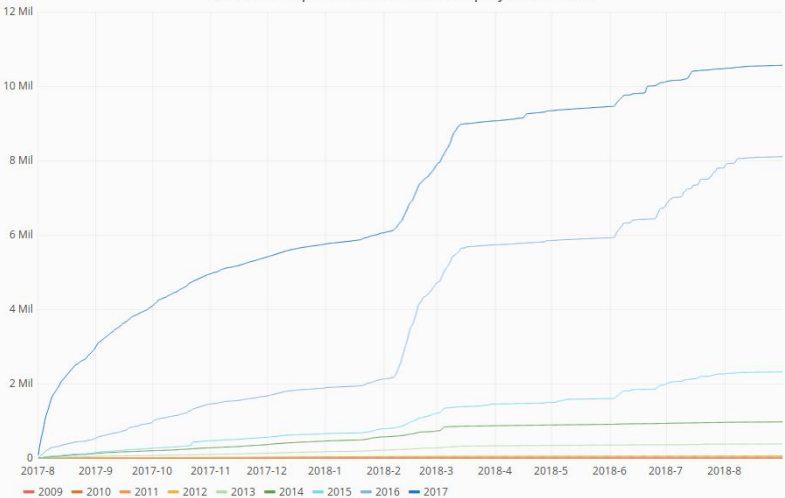
0.05765851 BCH from a6

Outputs:

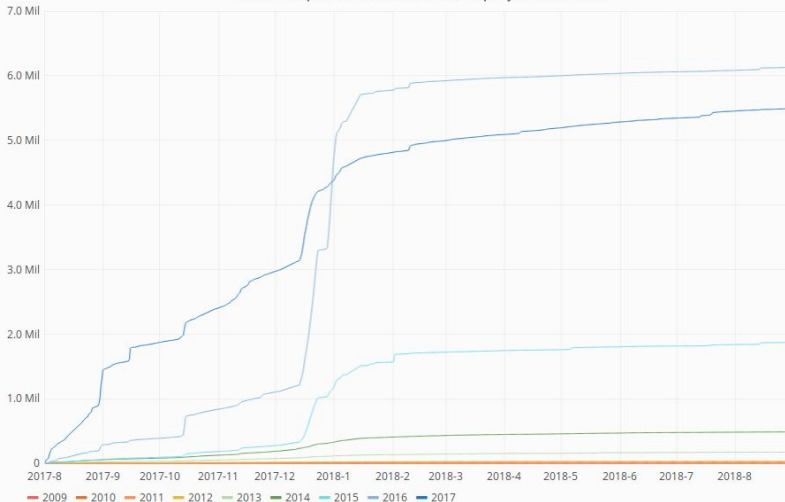
0.05764781 BCH to qrkzmsdyw6dzl7c5zv4c8lw58czfxtau5nv9pu3l6

0.00000700 BCH to qpzfq6ptdnnngmaz5jl9s3xe24rhj58xwv0unyud9

Number of outputs moved on the BTC side per year of creation



Number of outputs moved on the BCH side per year of creation



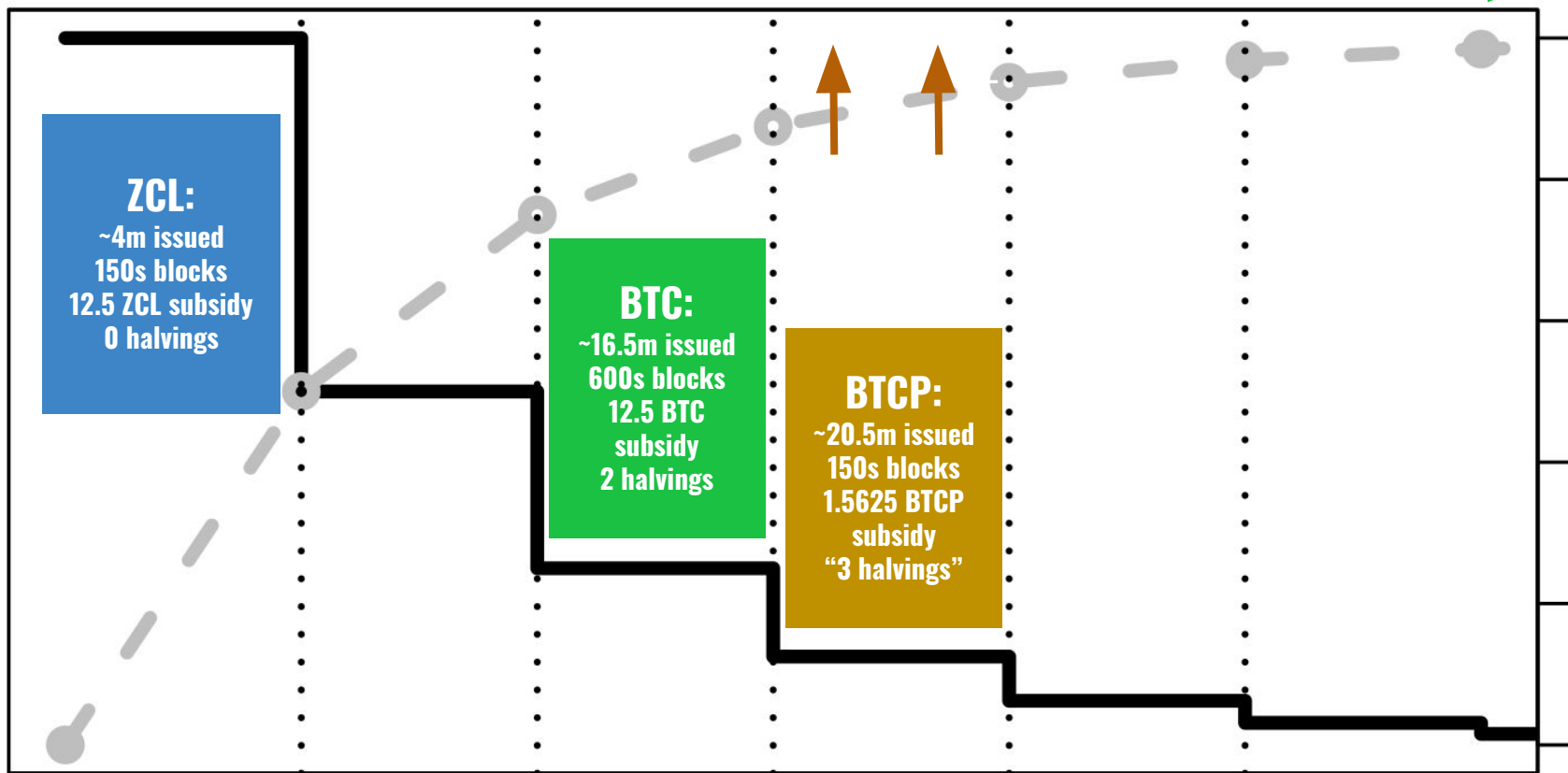


# **FORK-MERGE**

## **HOW TO BREED CHAINS TOGETHER (BADLY)**

# BTC, ZCL & BTCP Supply inflation / % issued over time

Increasing "Network Maturity" (Young / Mature / Elderly) →



(all three networks have 21m supply cap)

Credit: Parallel Industries, <http://forkonomy.pllel.com>

2018-08-31 16:30:50

# Bittrex - ZCL/BTC (D)

O: 0.00104892 H: 0.00120000 L: 0.00102416 C: 0.00109540

BTCP/BTC, HITB



charts by TradingView

2018-08-31 16:32:48

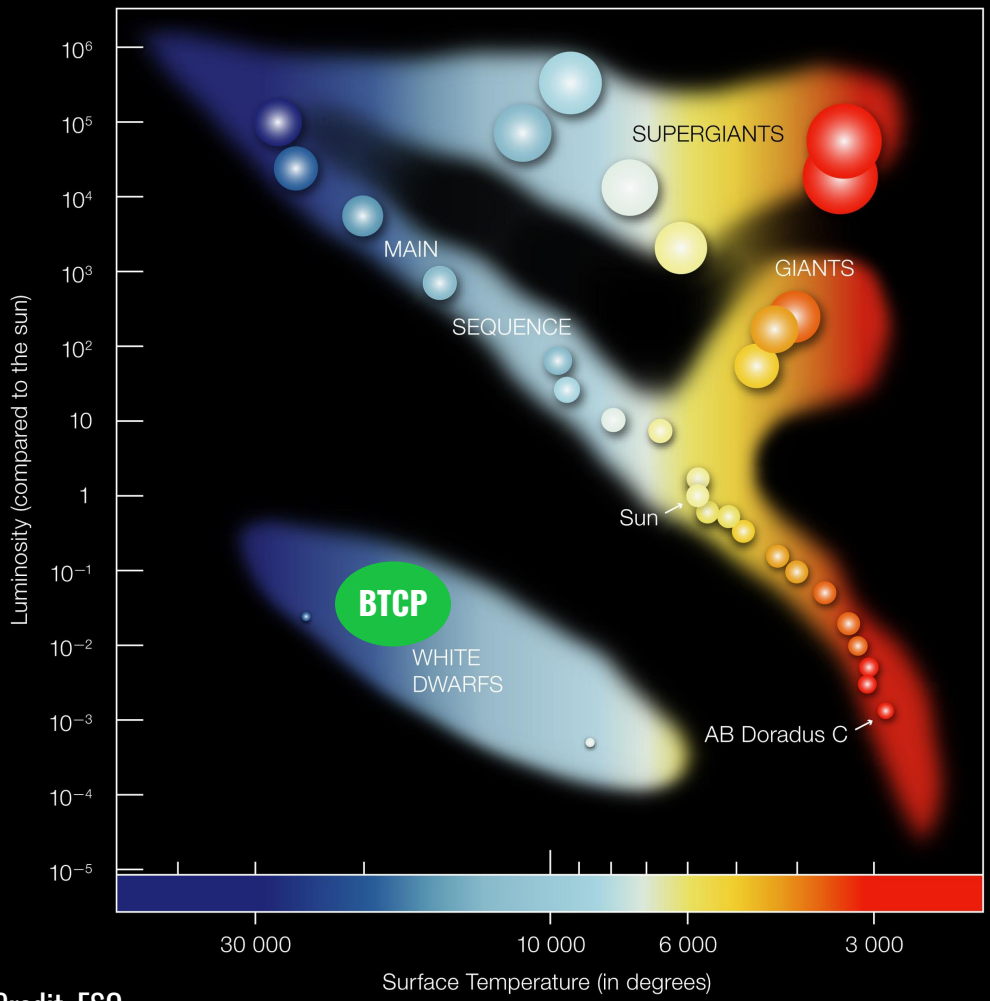
# Bittrex - ZCL/BTC (D)

O: 0.00104892 H: 0.00120000 L: 0.00102416 C: 0.00109540

BTCP/BTC, HITB



charts by TradingView



# WHITE DWARF CHAIN?

- > UTXO MERGE = “FULL LEDGER”
- > INSUFFICIENT MINING SUBSIDY
- > NO TX FEE MARKET
- > TINY HASHRATE (EQUIHASH = ASICs)
- > 51% ATTACKS TRIVIAL (<\$200/HR)
- > NO SoV / MoE PROPOSITION
- > NO “ECONOMIC GRAVITY”

TLDR: MATING CHAINS  
REKT BTCP



# **FOCUS ON ETC**

## **FIRSTLY, A LESSON FROM HISTORY**



# THE DAO IS REVOLUTIONARY.



## Hacking, Distributed

### A Call for a Temporary Moratorium on The DAO

Dino Mark, Vlad Zamfir, and Emin Gün Sirer

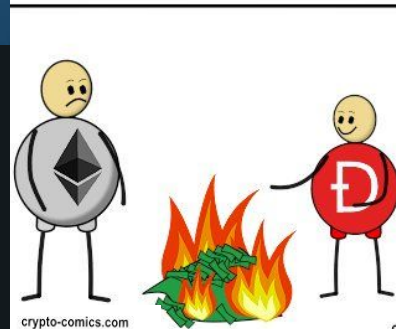
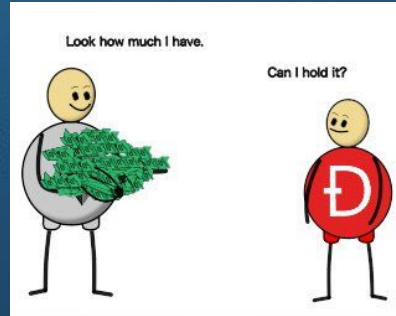
*ethereum dao smart contracts*

May 27, 2016 at 01:35 PM

← Older

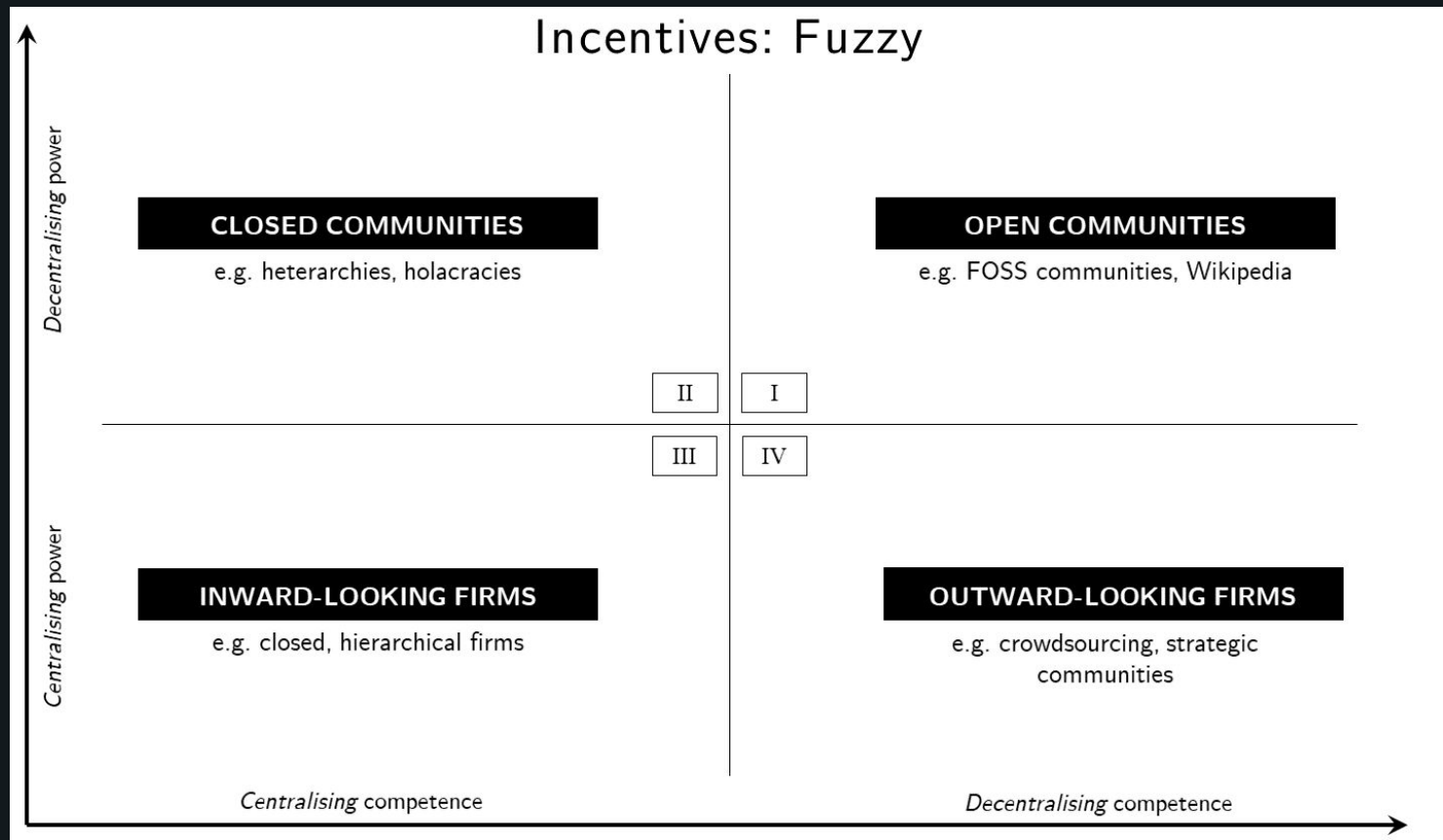
Newer →

The DAO is an exciting new construct: an investment vehicle governed by a program, directed by investors' votes, to seek out and fund proposals.

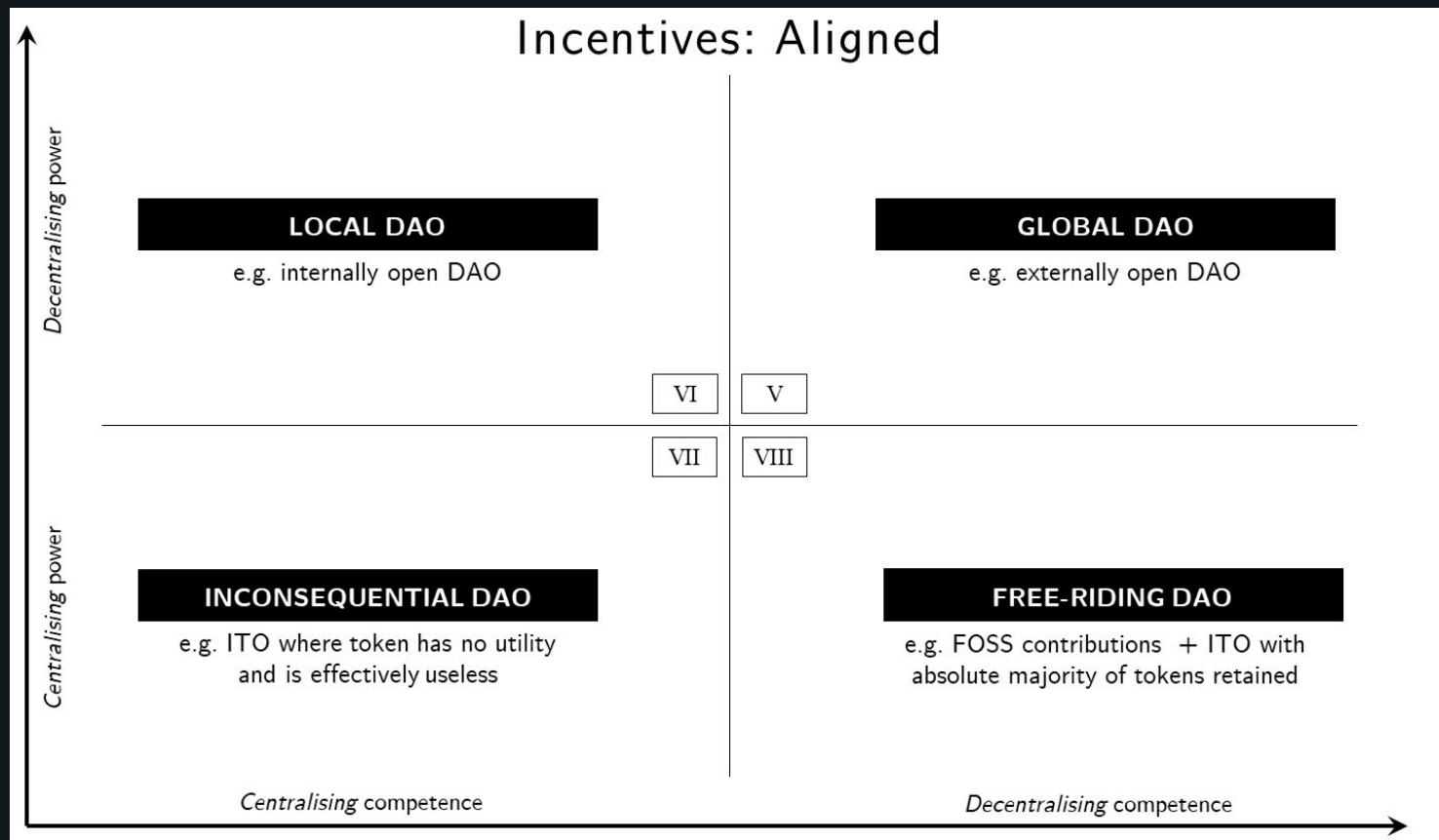


Credit: <https://daohub.org>, <http://crypto-comics.com>, <http://www.ethereum.org>, <http://hackingdistributed.com>

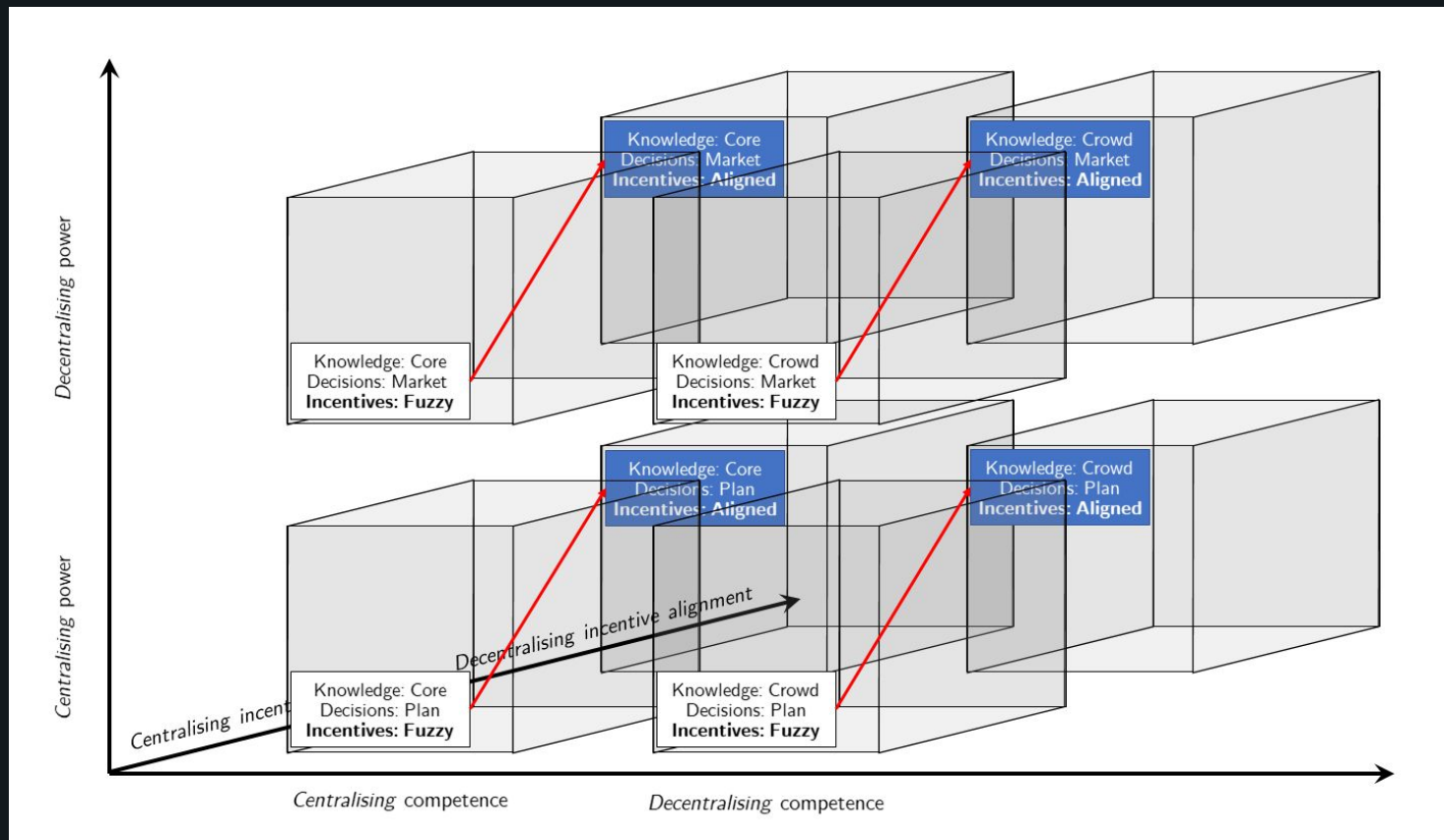
# DAOs STILL HAVE GREAT PROMISE, WHEN CAREFULLY DESIGNED & IMPLEMENTED



# DAOs STILL HAVE GREAT PROMISE, WHEN CAREFULLY DESIGNED & IMPLEMENTED



# DAOs STILL HAVE GREAT PROMISE, WHEN CAREFULLY DESIGNED & IMPLEMENTED



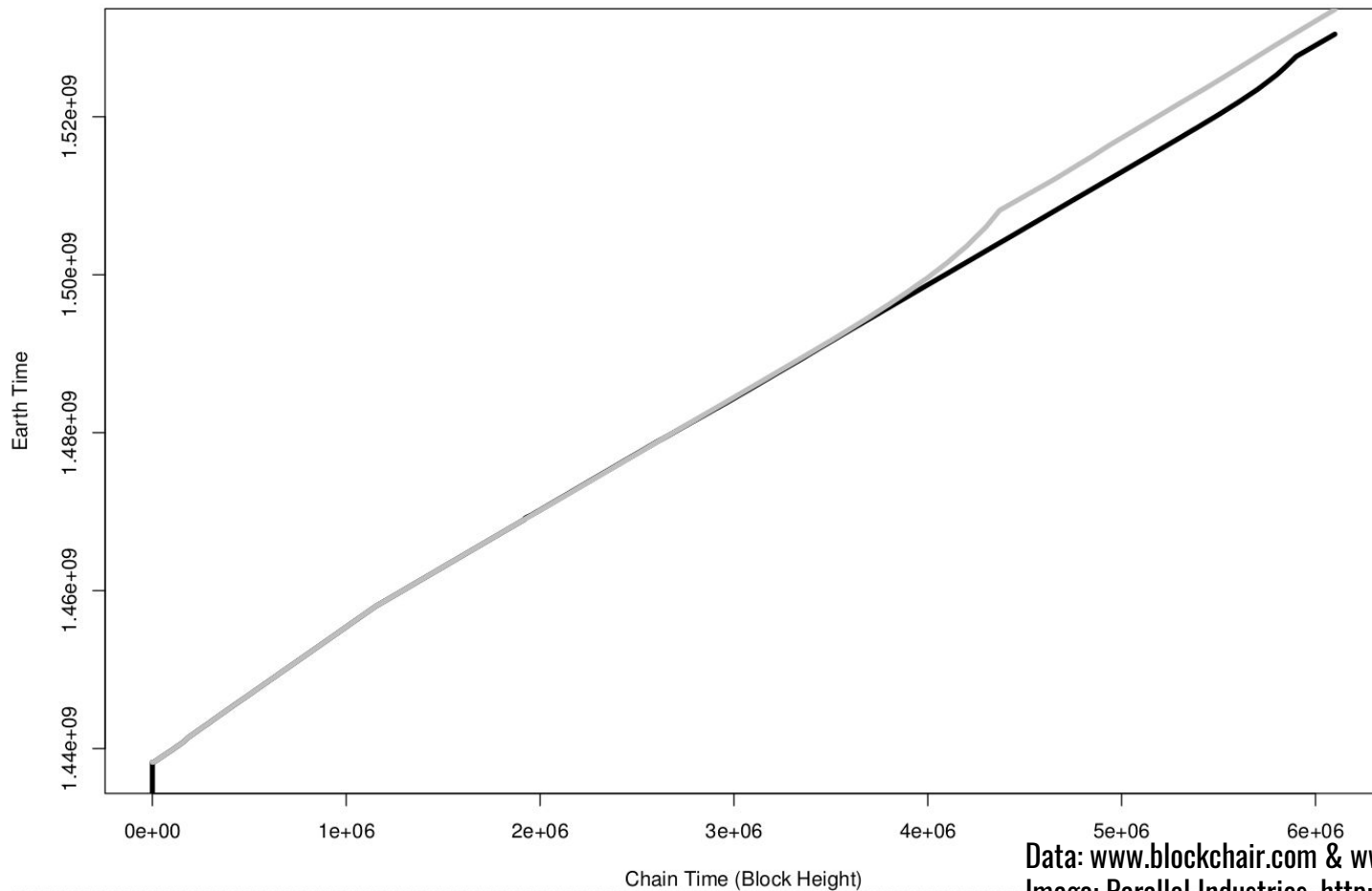
Credit: Theodor Beutel MSc Dissertation, University of Edinburgh, 2018.



# ETC & ETH

## DIVERGING PATHS

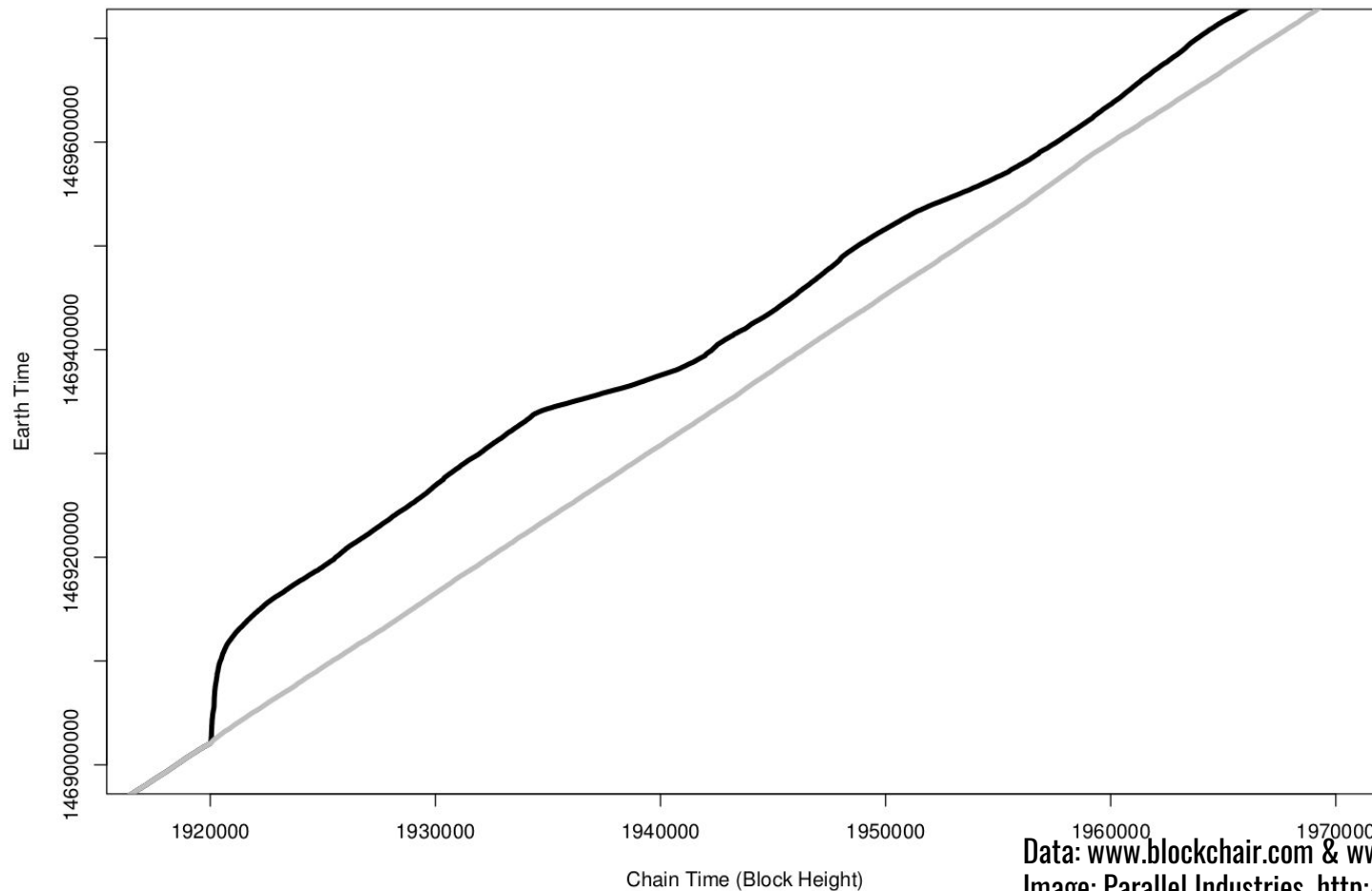
# ETC & ETH “Chain Dynamics” (all time)



Data: [www.blockchair.com](http://www.blockchair.com) & [www.etherhub.io](http://www.etherhub.io)

Image: Parallel Industries, <http://forkonomy.pllel.com>

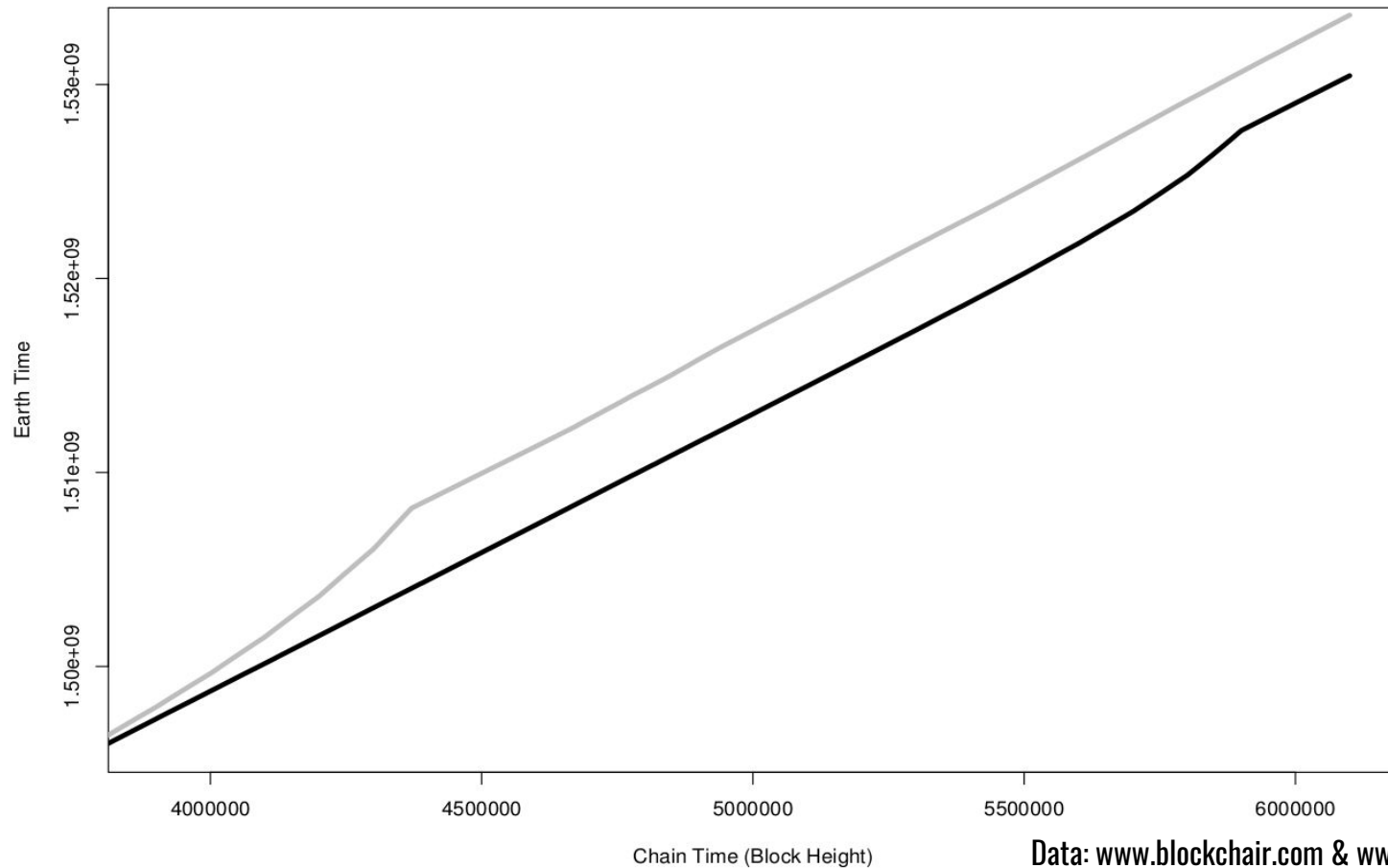
# ETC & ETH “Chain Dynamics” (~ETH DAO exploit)



Data: [www.blockchair.com](http://www.blockchair.com) & [www.etherhub.io](http://www.etherhub.io)  
Image: Parallel Industries, <http://forkonomy.pllel.com>

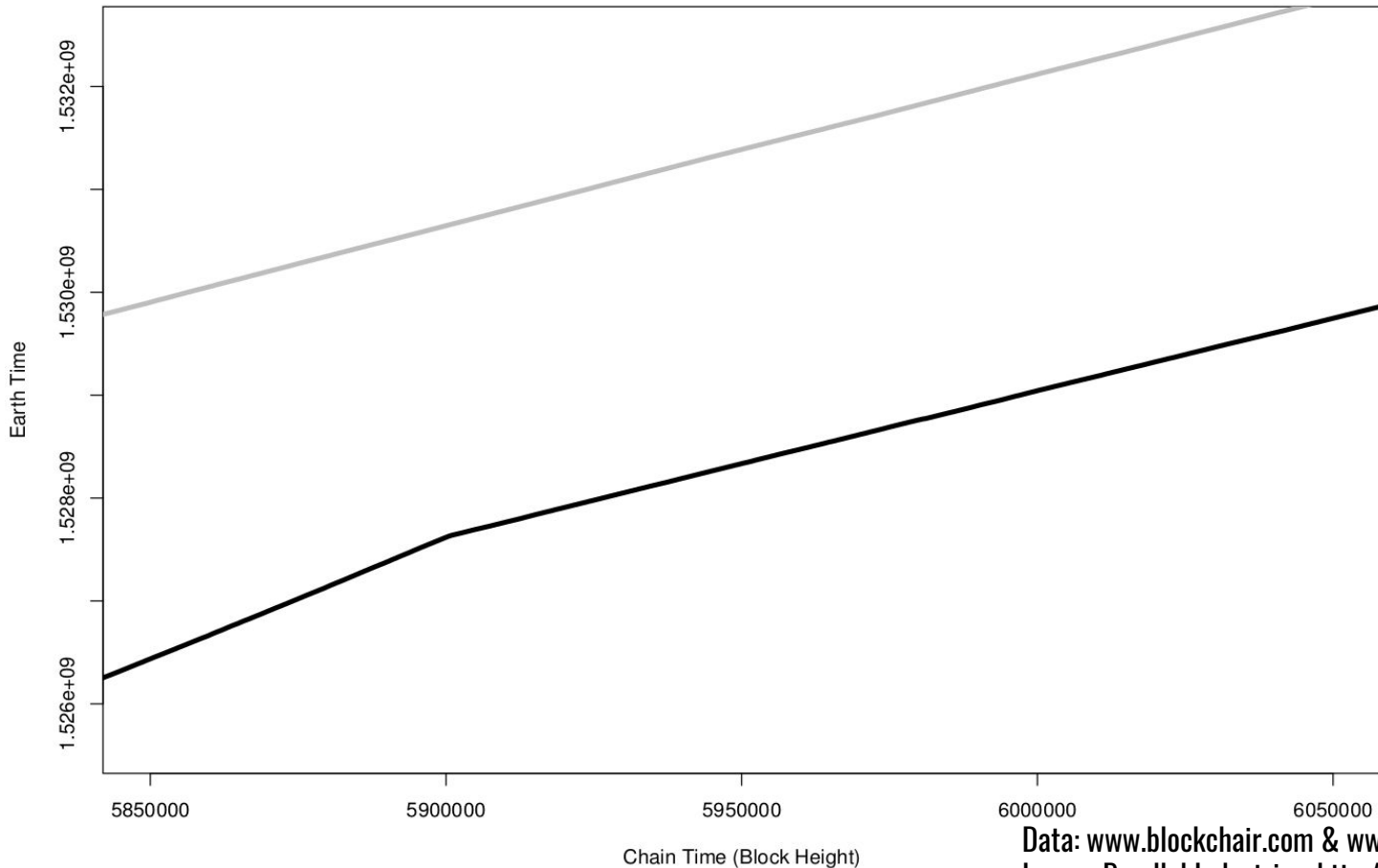


# ETC vs ETH “Chain Dynamics” (~ETH Parity bug)



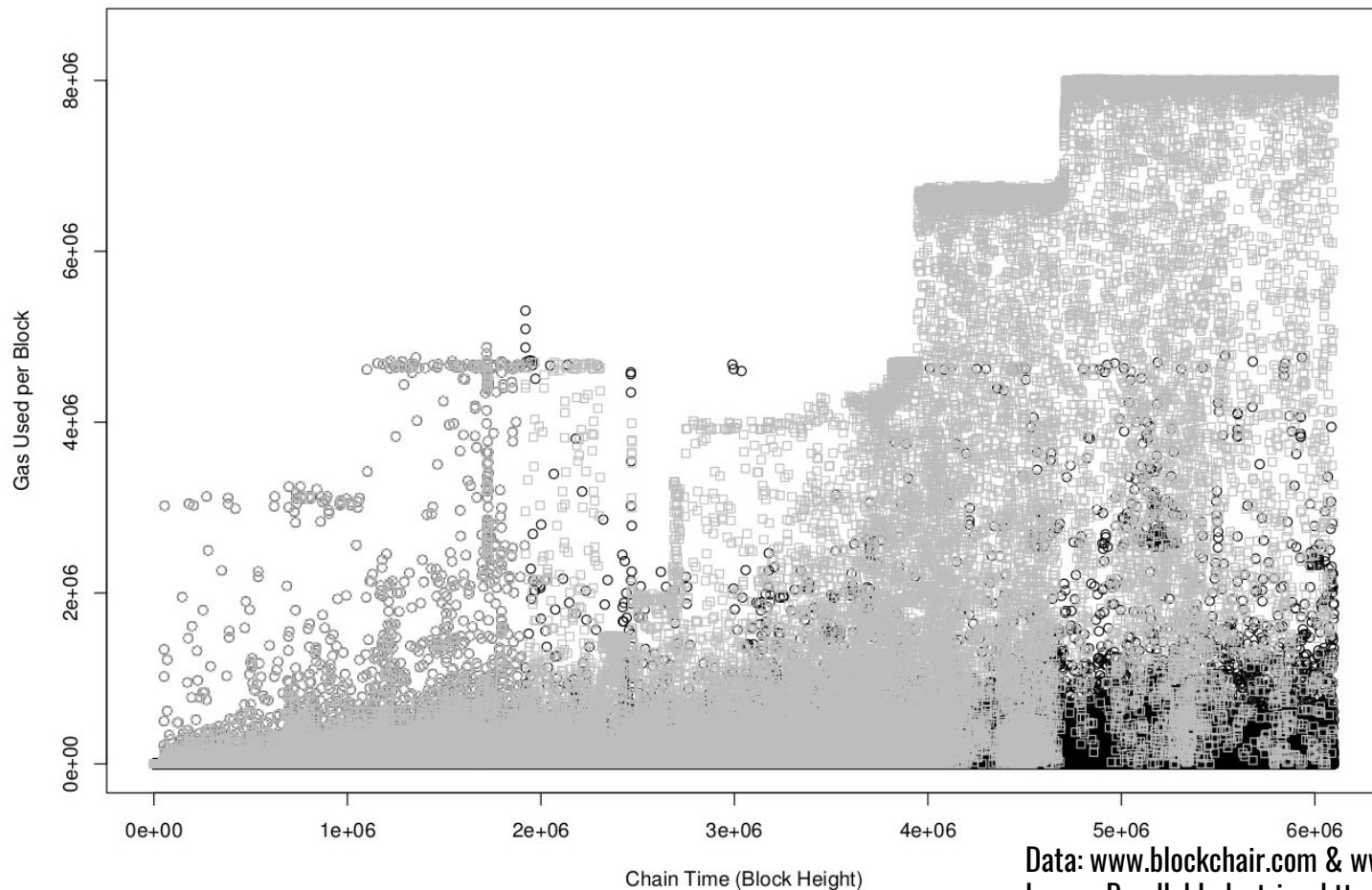
Data: [www.blockchair.com](http://www.blockchair.com) & [www.etherhub.io](http://www.etherhub.io)  
Image: Parallel Industries, <http://forkonomy.pllel.com>

# ETC vs ETH “Chain Dynamics” (~ETC Diff bomb HF)

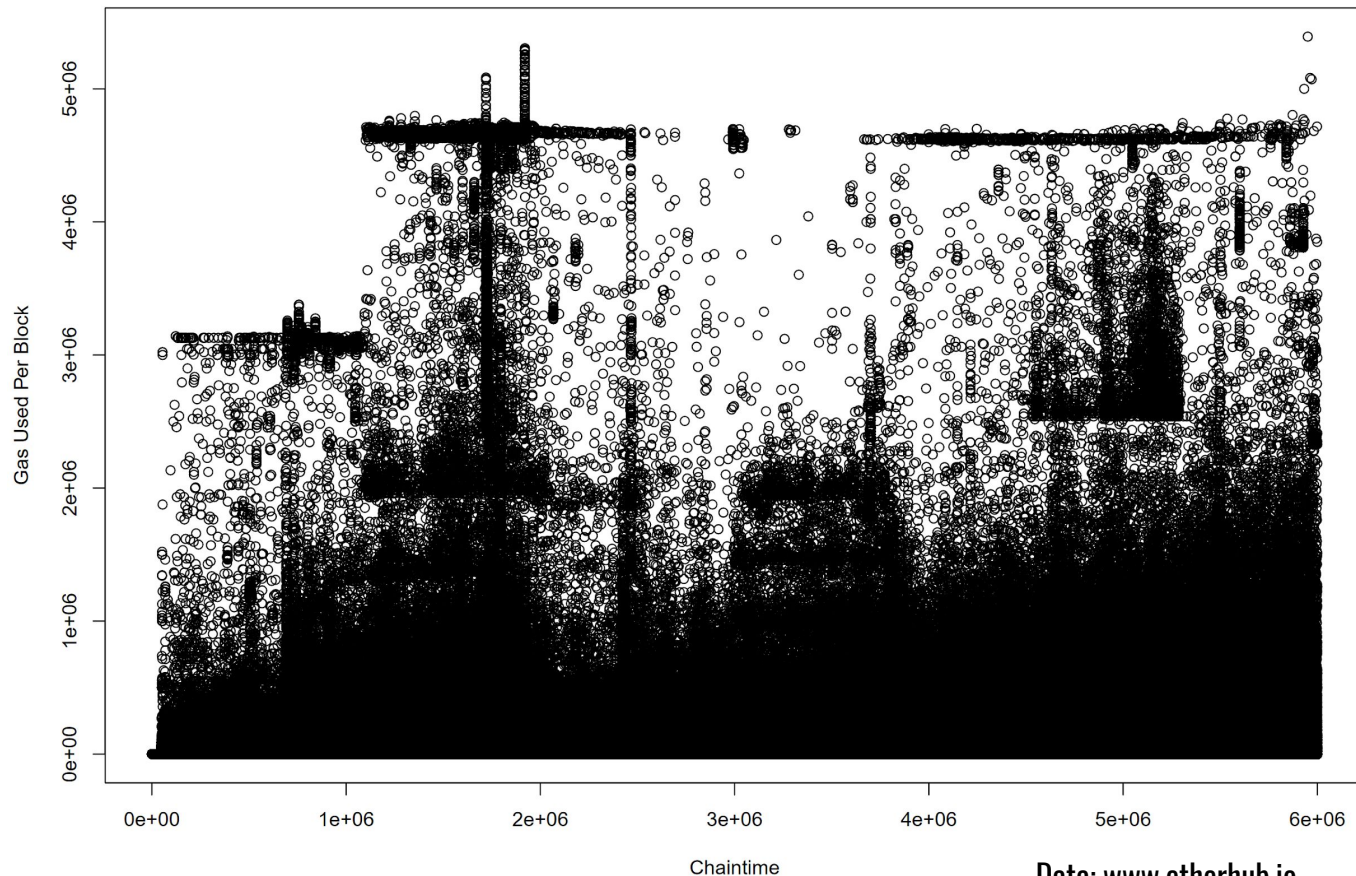


Data: [www.blockchair.com](http://www.blockchair.com) & [www.etherhub.io](http://www.etherhub.io)  
Image: Parallel Industries, <http://forkonomy.pllel.com>

# ETC vs ETH Gas Used vs Block Height



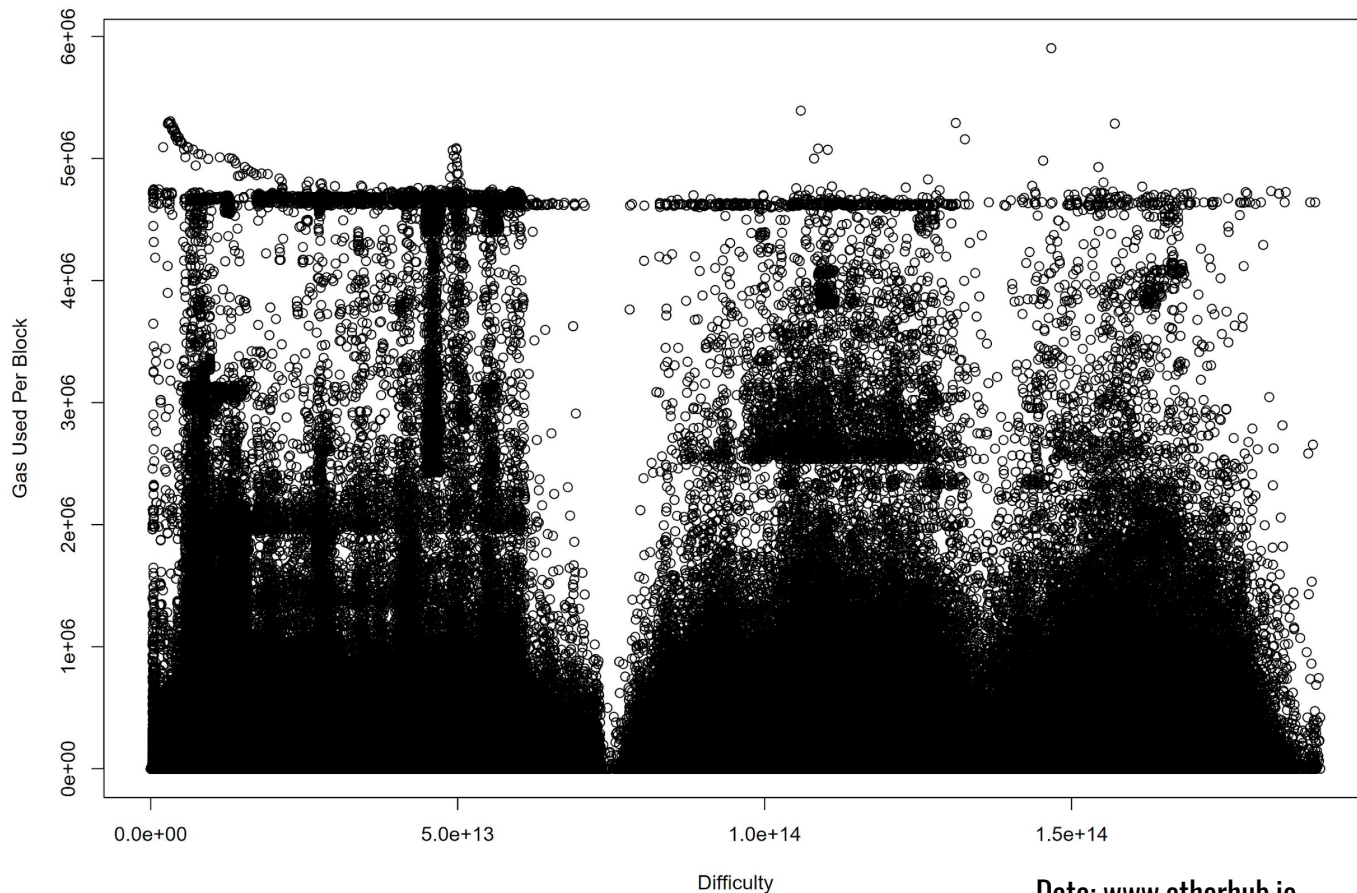
# ETC Gas Used vs Block Height



Data: [www.etherhub.io](http://www.etherhub.io)

Image: Parallel Industries, <http://forkonomy.pllel.com>

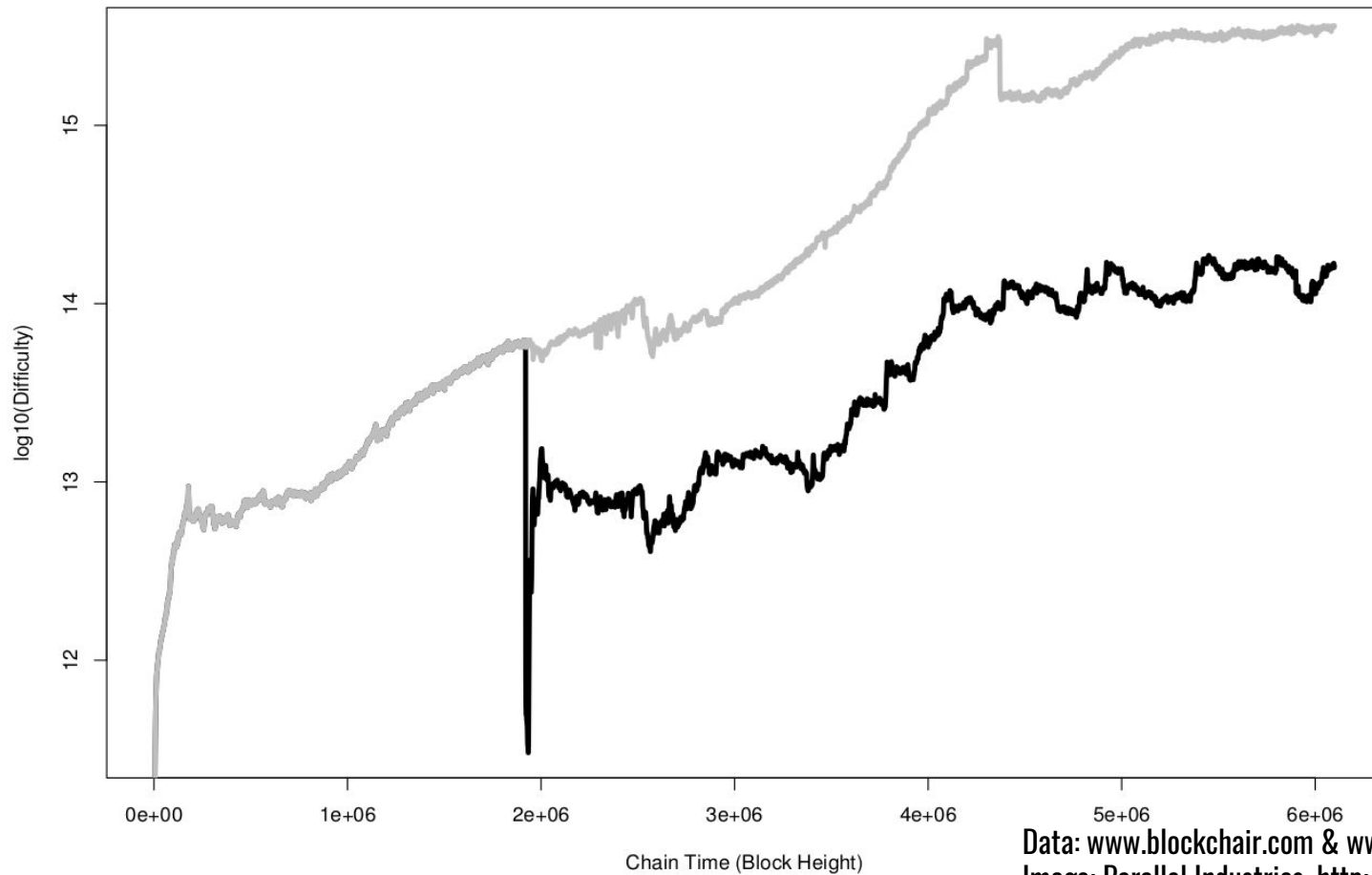
# ETC Gas Used vs Difficulty



Data: [www.etherhub.io](http://www.etherhub.io)

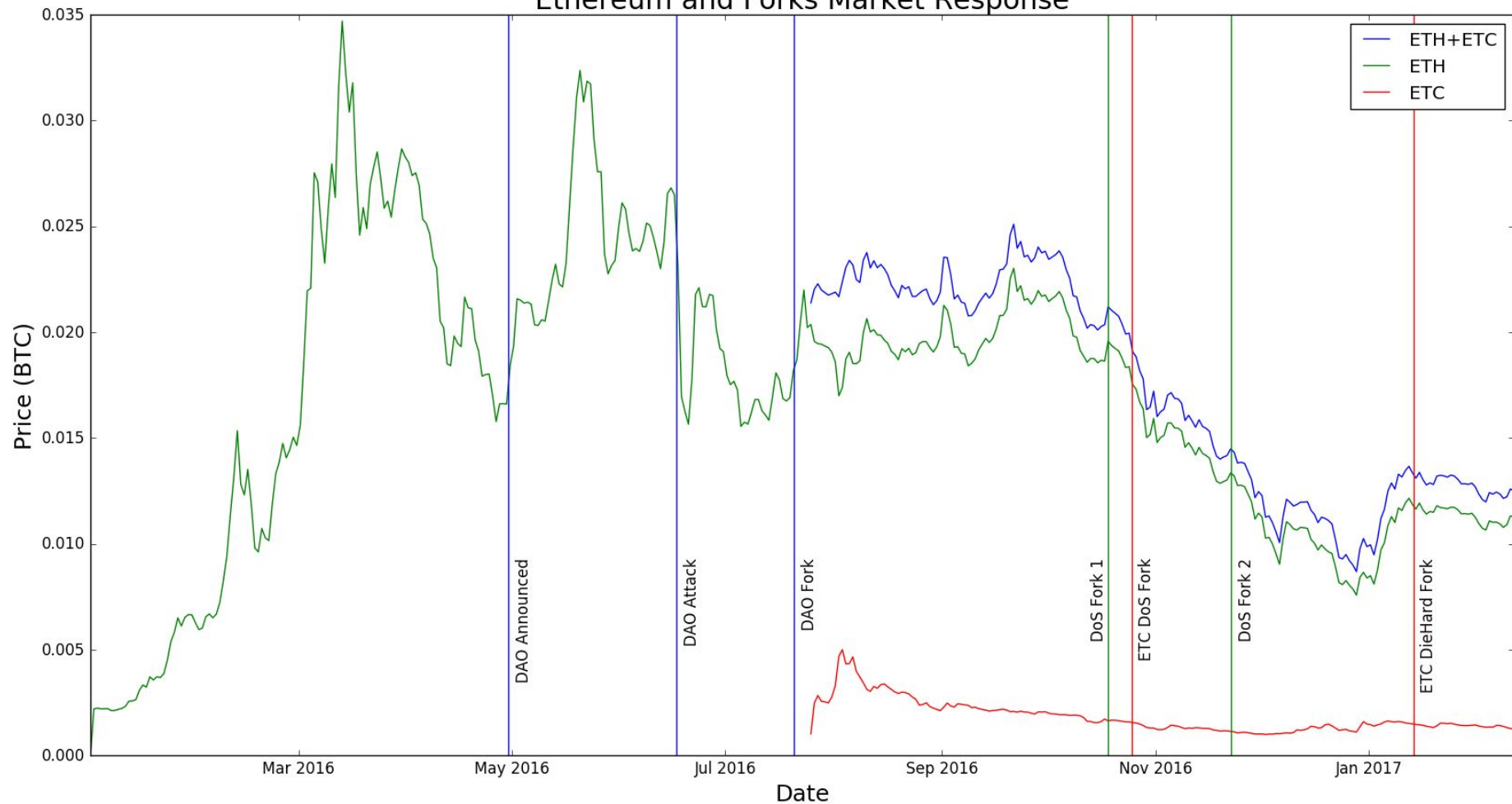
Image: Parallel Industries, <http://forkonomy.pllel.com>

# ETC vs ETH $\text{Log}_{10}$ -Difficulty vs Block Height



Data: [www.blockchair.com](http://www.blockchair.com) & [www.etherhub.io](http://www.etherhub.io)  
Image: Parallel Industries, <http://forkonomy.pllel.com>

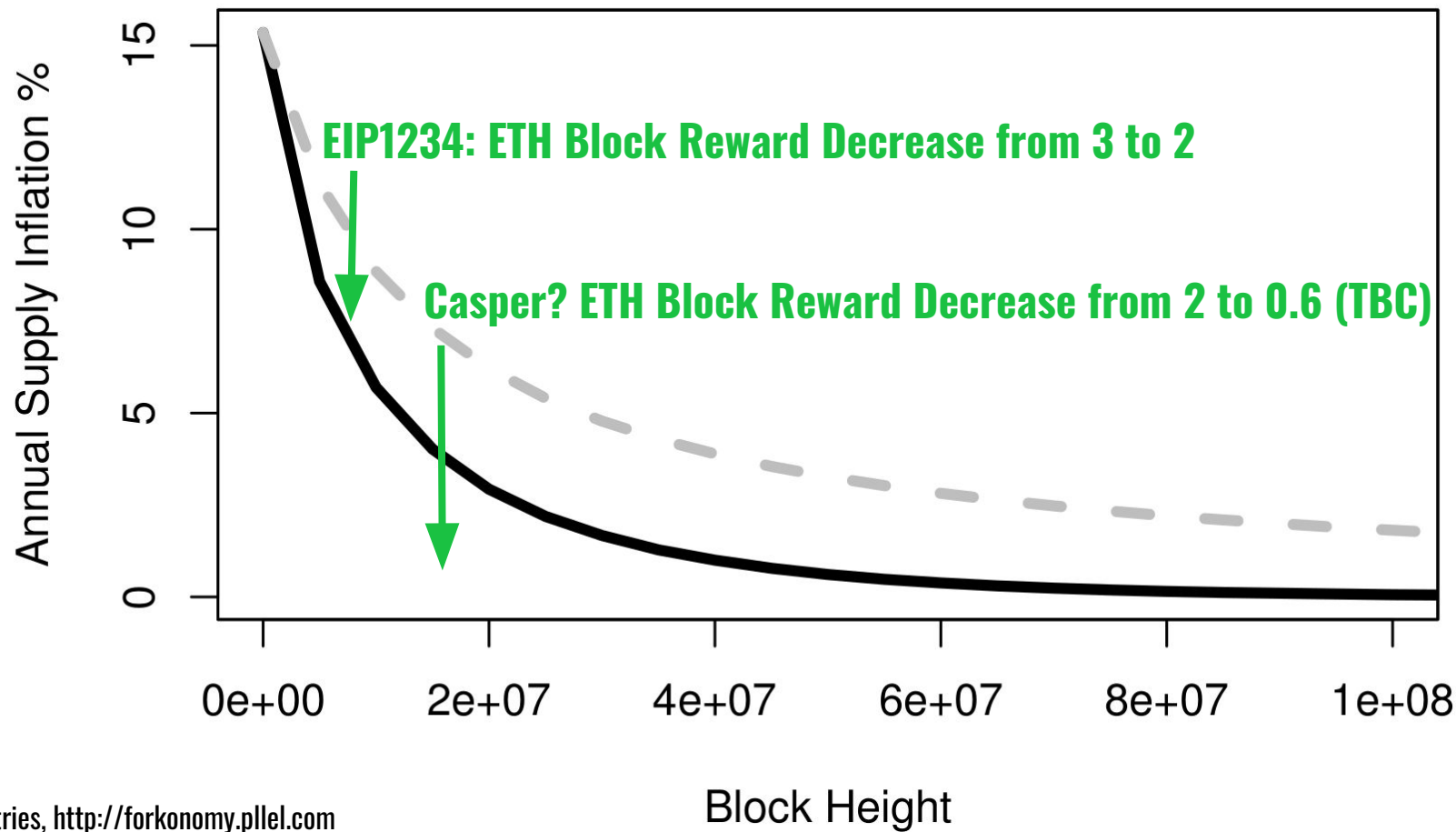
## Ethereum and Forks Market Response



Credit: Philip Daian, <https://pdaian.com/blog/stop-worrying-love-etc/>

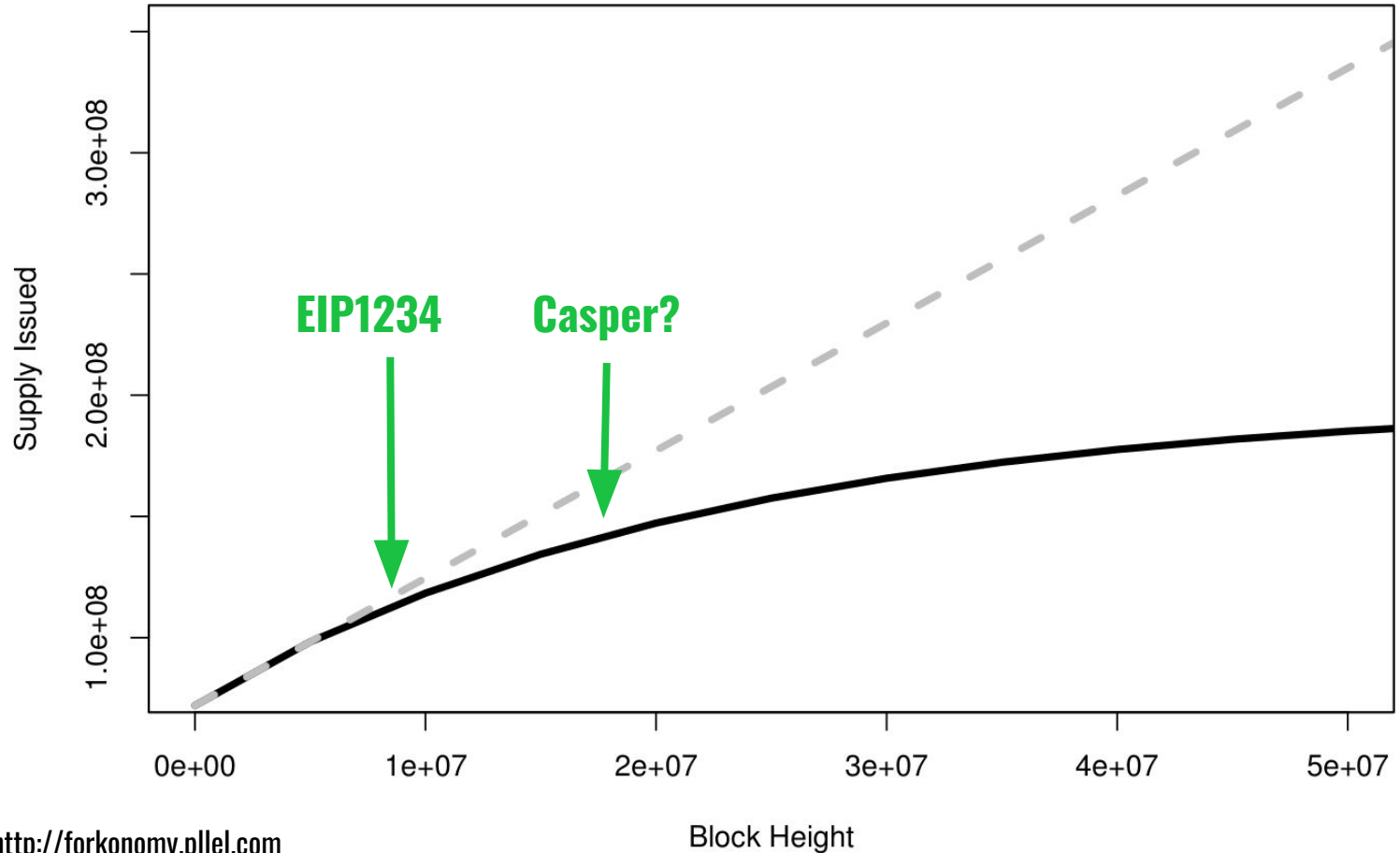


# ETC & ETH: Annual Supply Inflation %





# ETC & ETH: Supply Issuance



# WHERE TO NOW?

- > ETH to PoS?
- > ETHASH ASICS -> ?
- > FPGAs -> ?
- > REDUCING MINING DAG SIZE
- > SIDECHAINS
- > FORMAL METHODS
- > MULTIPLE DEV TEAMS
- > IMMUTABILITY
- > CENSORSHIP-RESISTANCE
- > **MOST SECURE S.C. NETWORK?**

- > MINING POOL CENTRALISATION
- > GAS ARBITRAGE\* / FRONTRUNNING\*  
(SEE PHIL DAIAN'S FRONTRUN.ME, FOMO3D)
- > DAO ATTACKER / RHG REMNANTS?
- > PoW CHANGE?
- > LEGACY ISSUES (??????)
- > GOVERNANCE/DECISION-MAKING
- > Y NO DAOs?



# **PEERING BEHIND THE VEIL**

# **BLOCKCHAINS AS TIME MACHINES**

# THANKS FOR YOUR ATTENTION!

## WANT TO HELP US DO MORE?

SPONSOR/COLLAB/DISCUSS:

[info@pllel.com](mailto:info@pllel.com), [www.pllel.com](http://www.pllel.com), [@parallelind](https://twitter.com/parallelind)



BTC

BTC: 1GgUDrQvdycsr473eMJQZq4GYTgGUdJQfn  
ETC: 0x9ec1e3aa7b7428dfa9d22685c33267d90afa2c80  
ETH: 0x3c260b1b53dbc122068b98da7a7c196df4dc1211  
DOGE: DKPYfbidZUqmcCa79rT5ZBh92RoqQNv4WR  
LTC: LTGS78HRTJbSEo7Y5PxYXj1XE2ZYPh3NM5  
ZEC: t1LktPAdT6bTuNTgQt97JZRRKXfq6cit3bt



ETC

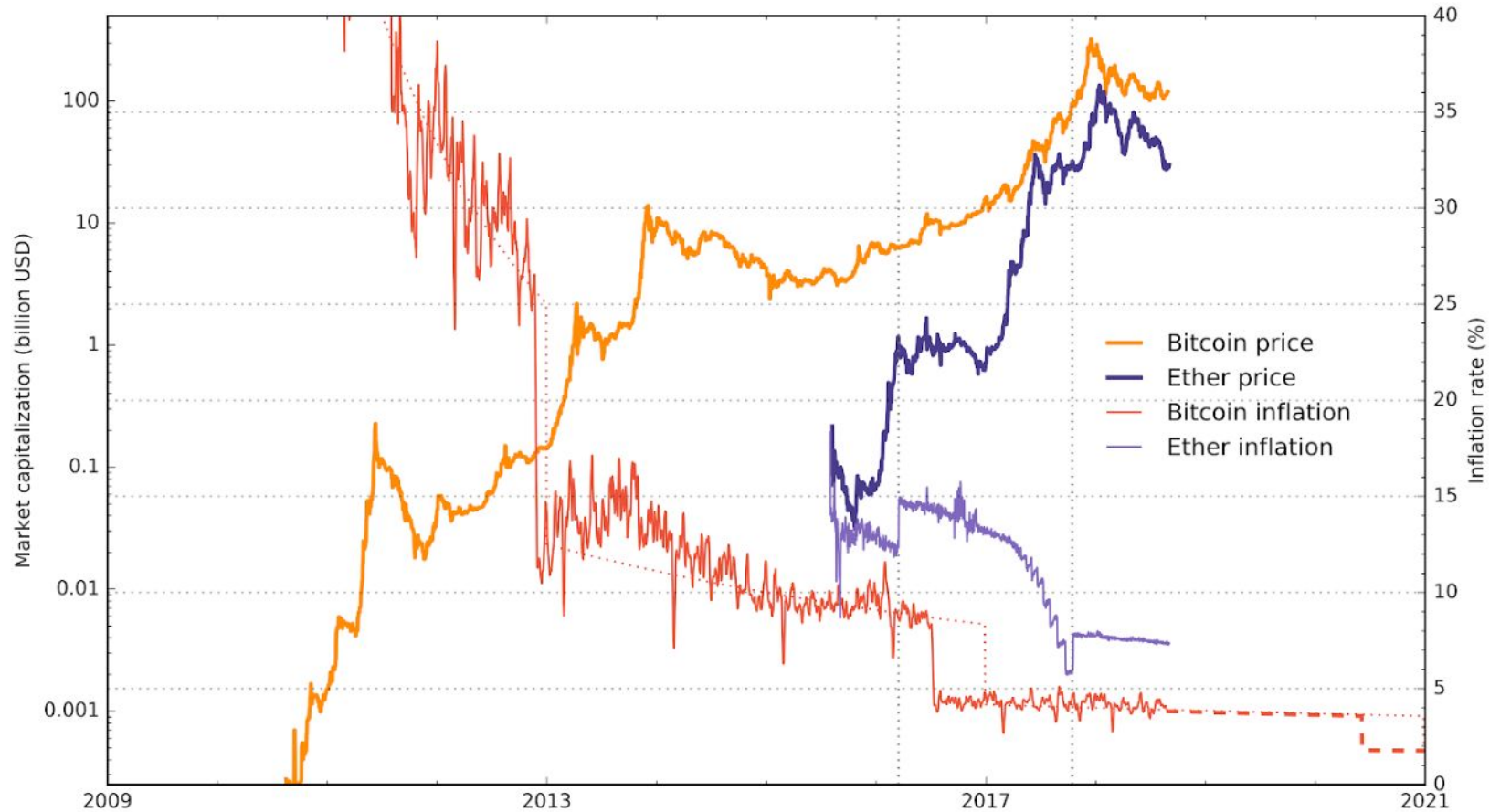
PAPER: [FORKONOMY.PLLEL.COM](http://FORKONOMY.PLLEL.COM) / SLIDES: [ETCSUMMIT.PLLEL.COM](http://ETCSUMMIT.PLLEL.COM)

## 2.2 Research Methods and Resources

This work has relied on numerous primary and secondary data sources as cited in the text. Blockchain analytics of BTC, BCH, ETH, ETC, XMR, MONA, ZCL and BTCP was achieved through the use of block explorers Blockchair.com, Blockchain.info, Etherscan.io, Etherhub.io, Bchain.info, Monerohash.com and Bitinfocharts.com with data exported in CSV or JSON formats. This was imported into the statistical computing suite RStudio (built upon R) for cleaning, treatment, analysis and visualisations. Network-wide observation and inference was conducted using publically available sources Coin.dance for node count and implementation versions for BTC and BCH, Crypto51.app for ZCL and BTCP network hashrates, Doublespend.cash for malleated transactions on BCH, Coinmetrics.io for high-level network heuristics and Onchainfx.com for networks' token price, supply issuance and monetary policy.



# Ethereum vs Bitcoin

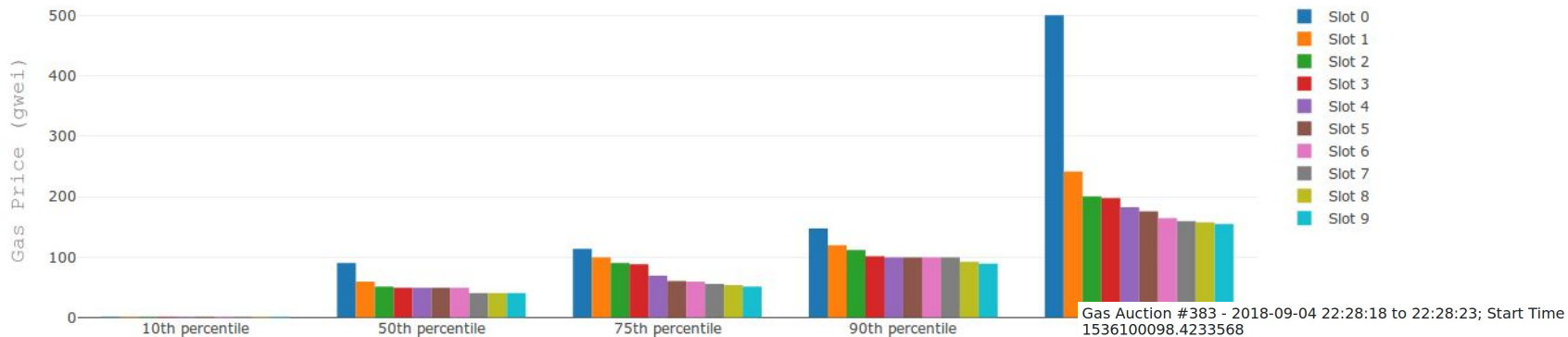




# FRONT RUN ME

## Global Market Overview

Priority Pricing Market for Gas Slots



Price percentile (since block ~5M)

Gas Price Bids over Time

