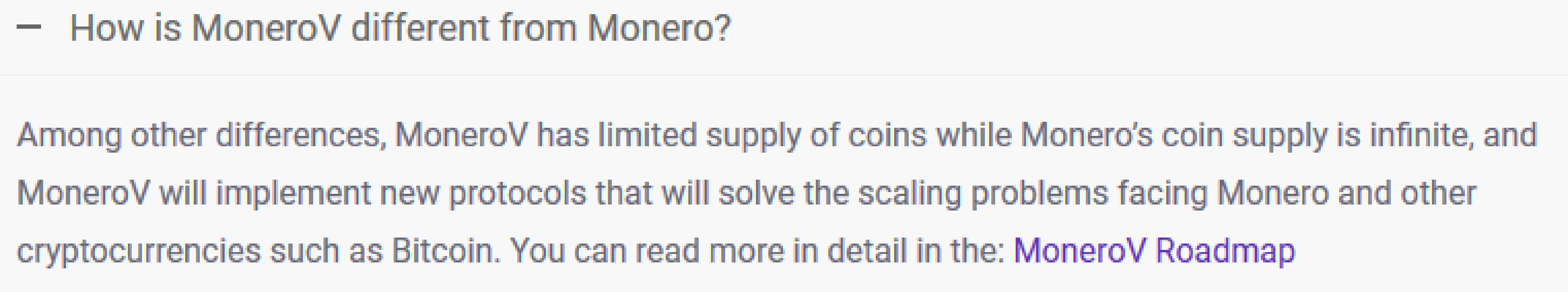
Why MoneroV is Indistinguishable from a Scam

By xmrscott

2018/03/05

Topics Covered

- MoneroV vs Monero
  - Inflation
  - Scalability
  - Privacy
- Red flag hunt
- Mythbusting



— How is MoneroV different from Monero?

Among other differences, MoneroV has limited supply of coins while Monero's coin supply is infinite, and MoneroV will implement new protocols that will solve the scaling problems facing Monero and other cryptocurrencies such as Bitcoin. You can read more in detail in the: MoneroV Roadmap

What is inflation?

“Inflation is the rate at which the general level of prices for goods and services is rising and, consequently, the purchasing power of currency is falling.” – Investopedia

Or put another way, if supply increases faster than demand, and all other things remaining equal, it takes more units to buy a good

What does MoneroV have to say?

“Bitcoin’s 21 million maximum coin supply was introduced specifically to avoid having a body that controls the money supply, completely **restricting future inflation and devaluation of Bitcoin coins**.

Based on this merit alone, Monero would never be able to compete with Bitcoin as the world’s best digital currency, since the idea of infinite coin supply is the incorrect intuition.

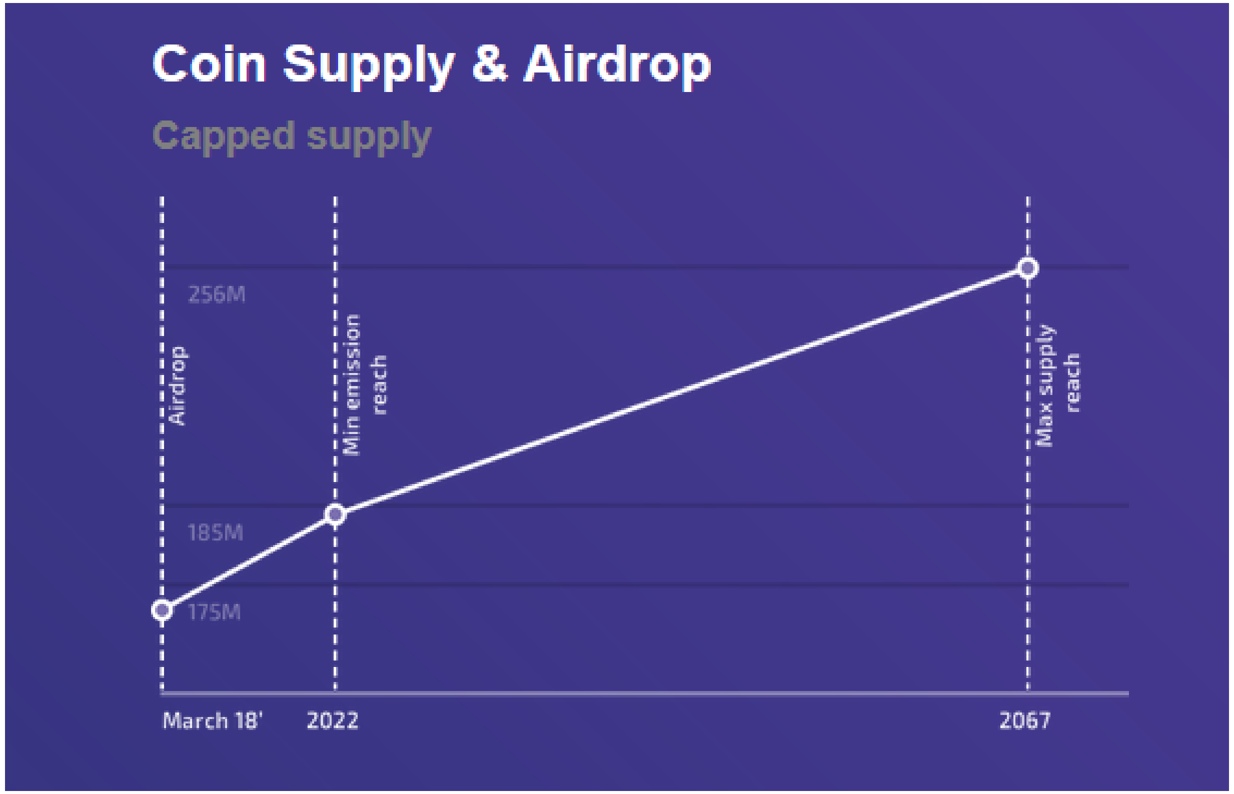
MoneroV adheres to core Austrian school of economics principles and caps the total amount of XMV coins that can be created to 256 million. The initial coin amount in circulation at the time of the hardfork would be 10 times the amount of XMR coins (~158 Million). XMR holders prior to the hard fork will receive 10 times the amount of XMV coins.”

-MoneroV Roadmap paper

Coin Supply – March 2018

MoneroV	158,000,000
Monero	15,800,000

Coin Supply – 2067



Coin Supply – 2067

MoneroV	256,000,000
Monero	25,500,460

.3*60(minutes)*24(hours)*365.25(days) = 157,788 coins/year from tail emission

18.4 mil + 157,788x, where x = number of years after 2022

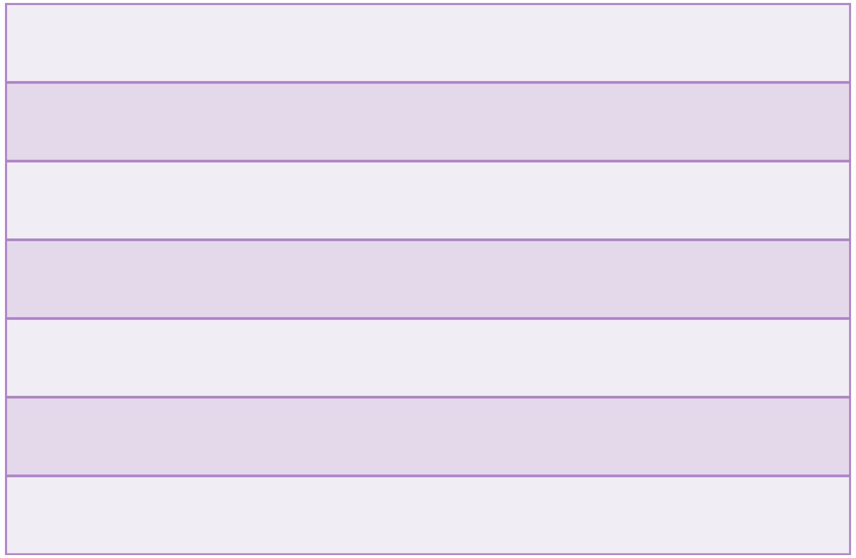
When Eclipse?

- 18.4 mil + 157,788x = 256mil
- Solving for x yields ~1,505.8 years
  - AKA ~3527 A.D.
- 0.06% inflation
  - Will continue to approach 0

But…why?

“to differentiate the two cryptocurrencies while making the two cryptocurrency wallets - MoneroV’s and Monero’s - to reject one another’s blockchain.”

Why Tail Emission?



Tx 1	.01 BTC
Tx 2	.01 BTC
Tx 3	.01 BTC
Tx 4	.01 BTC
Tx 5	.01 BTC
Tx 6	.01 BTC
Tx 7	.01 BTC
Tx 8	.001 BTC

Dynamic Blocksize

“We first consider a blocksize large enough (or effectively infinite). In this scenario competition among miners will drive fees towards zero since there is no scarcity. This will in turn cause the difficulty and consequently the security of the crypto currency to collapse. We must keep in mind that orphan block based arguments will also fail since these are based on the presence of a base emission. This is in fact the very legitimate fear of the small block proponents.

[...]

Either the mining revenue collapses first or the purchasing power of the mining revenue collapses first.” – ArticMine

MoneroV on Scalability

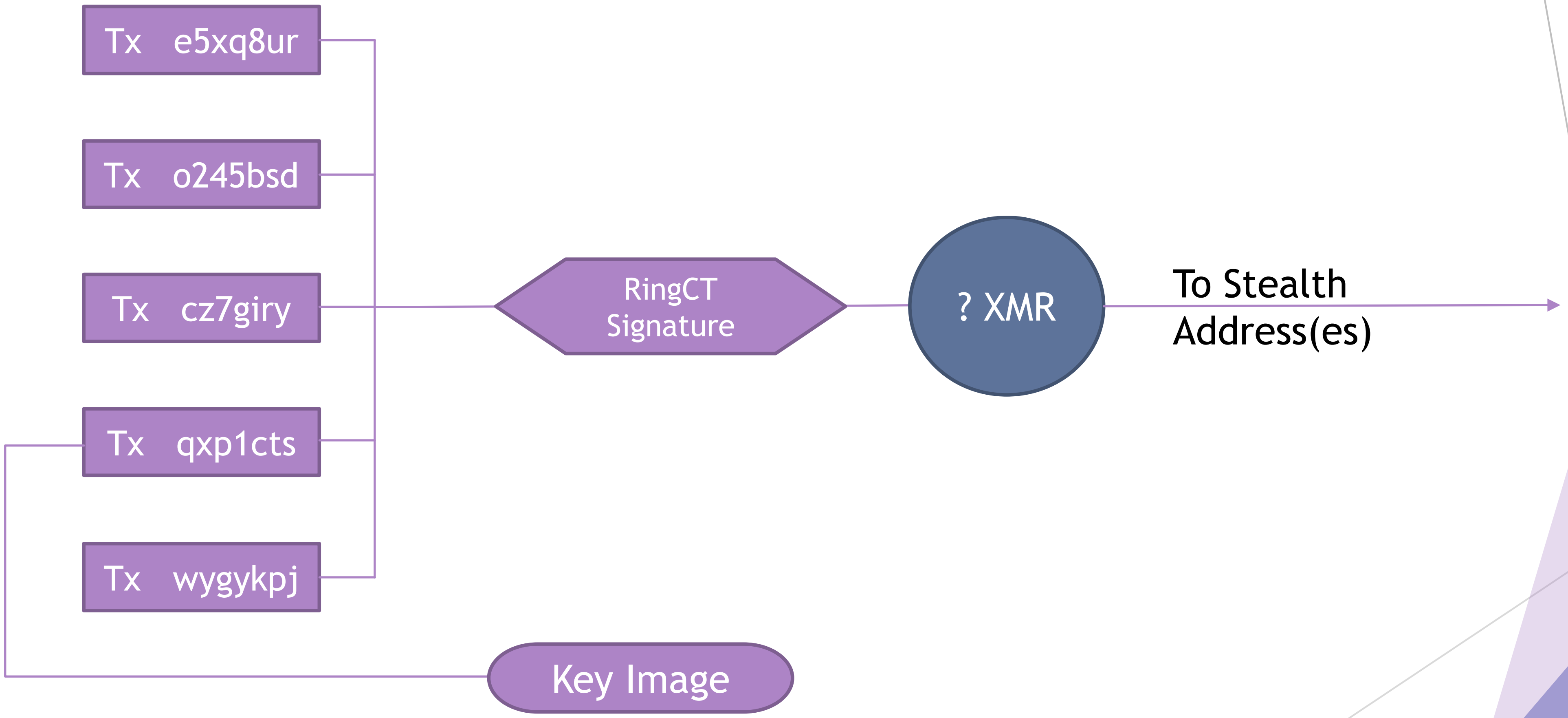
“Monero does not scale. As of the time of this writing, Monero’s median transaction size excluding coinbase transactions is 51.2 times larger than Bitcoin’s median transaction size (13.21 kb vs 258 bytes). If Monero was to handle the cumulative transactions amounts of Bitcoin, its blockchain size would be higher than 7.7 Terabytes (in comparison to Bitcoin’s 155 Gigabyte blockchain). In turn, the fear from an imminent bloated juggernaut blockchain comes with higher median transaction fees than Bitcoin.

MoneroV plans to tackle the scaling issues, which is the main source of problems in Monero, and in all cryptocurrency coins for that matter, and integrate the MimbleWimble protocol so that the blockchain size will be bound to the number of users using MoneroV (not the number of transactions being made in the network). This will significantly reduce both transaction costs and blockchain size, permanently solving the scaling problem.”

MoneroV’s Scalability Solution

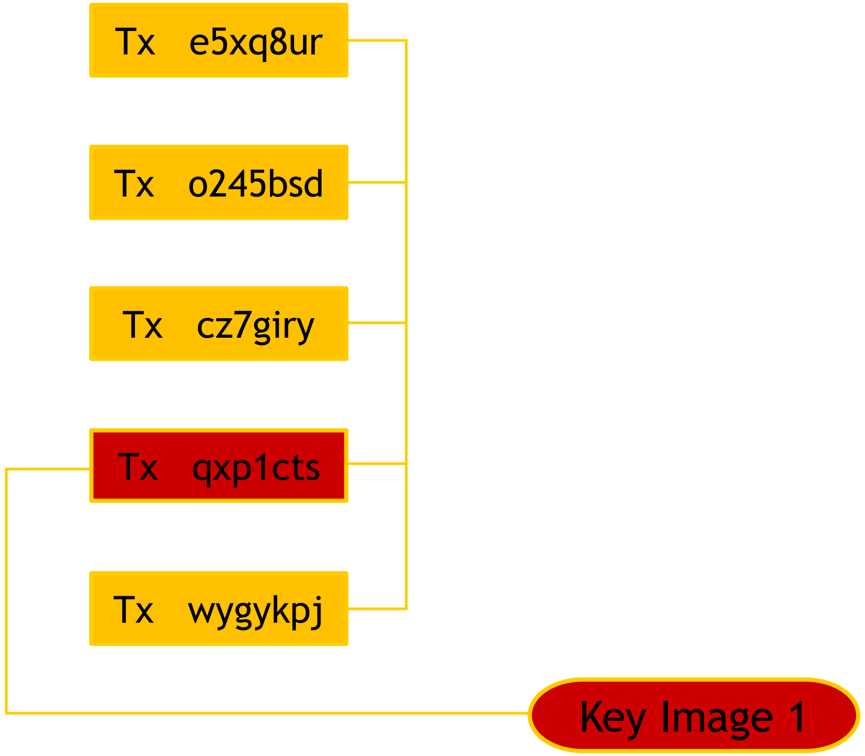
- Inherits the 33GB Monero blockchain
- Inherits said ~13kb tx size
- Best estimate is Q4, 2019
  - No demonstrable efforts to show this is obtainable
- MoneroV’s intermittent scaling problem can be solved by…
- Monero likely releasing Bulletproofs in September
  - Code already published and working in testnet

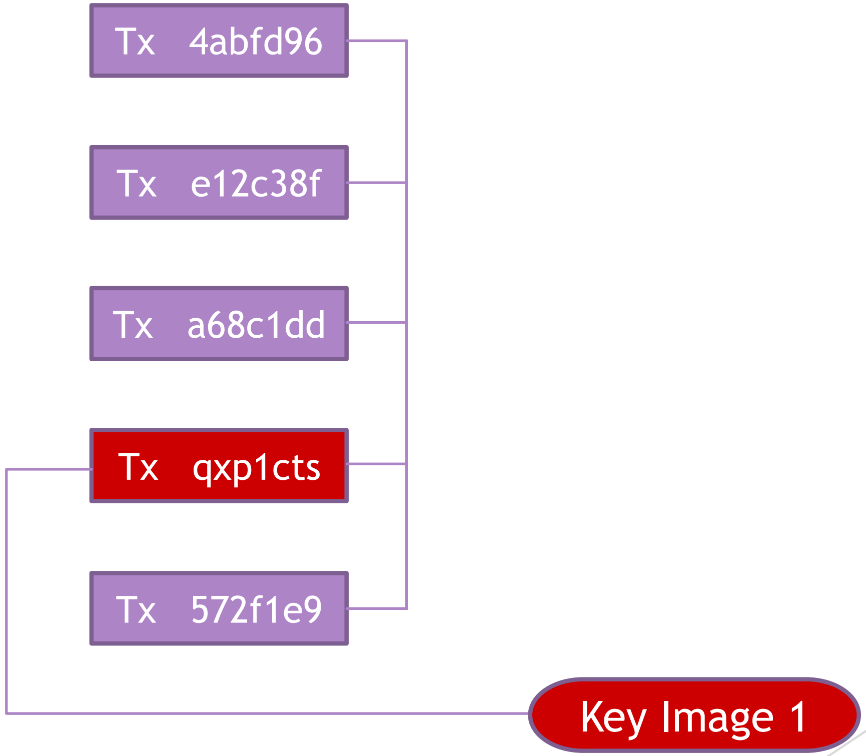
Ring Confidential Transactions (RingCT)



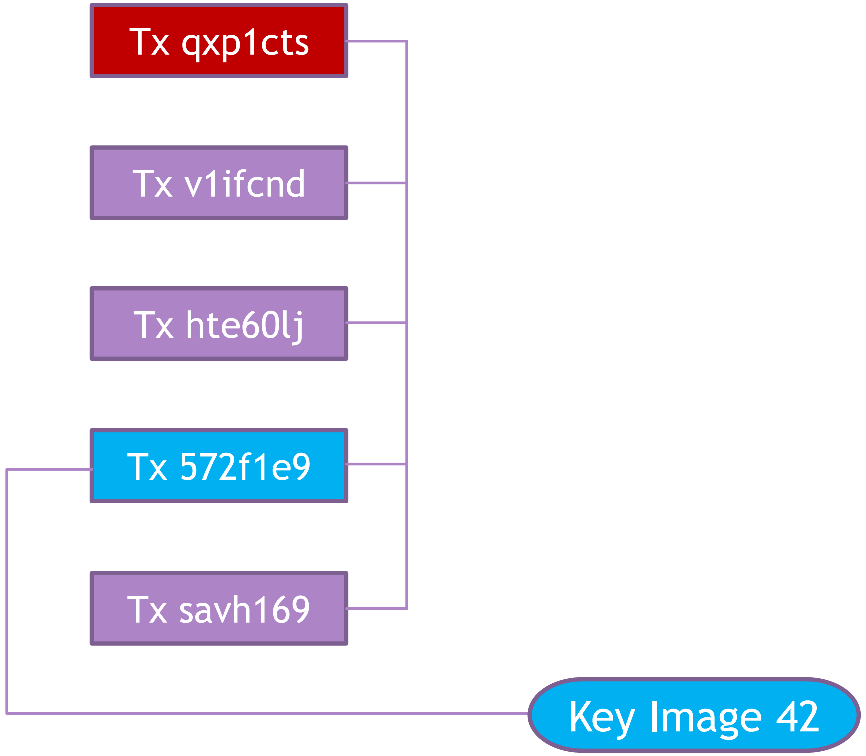
See: https://lab.getmonero.org/pubs/MRL-0005.pdf

MoneroV attacks its own privacy

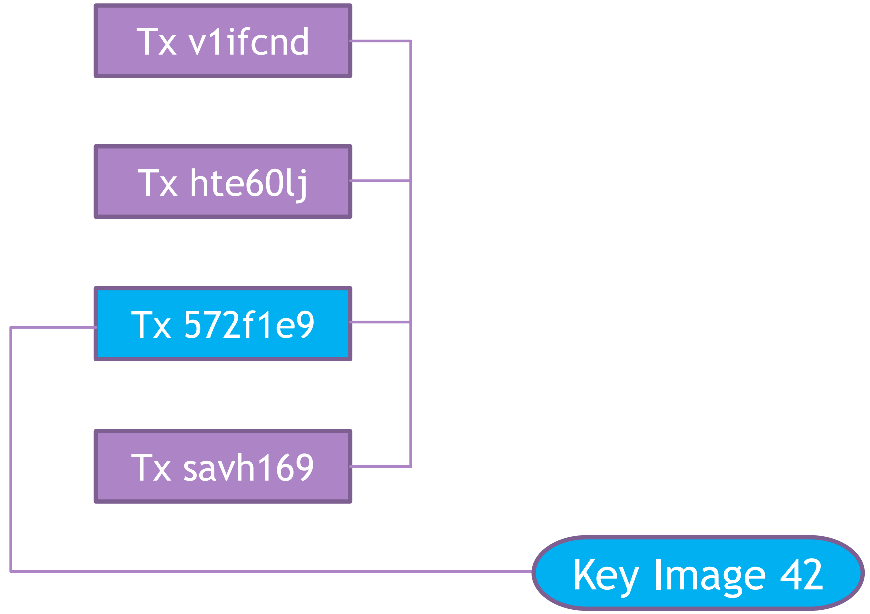




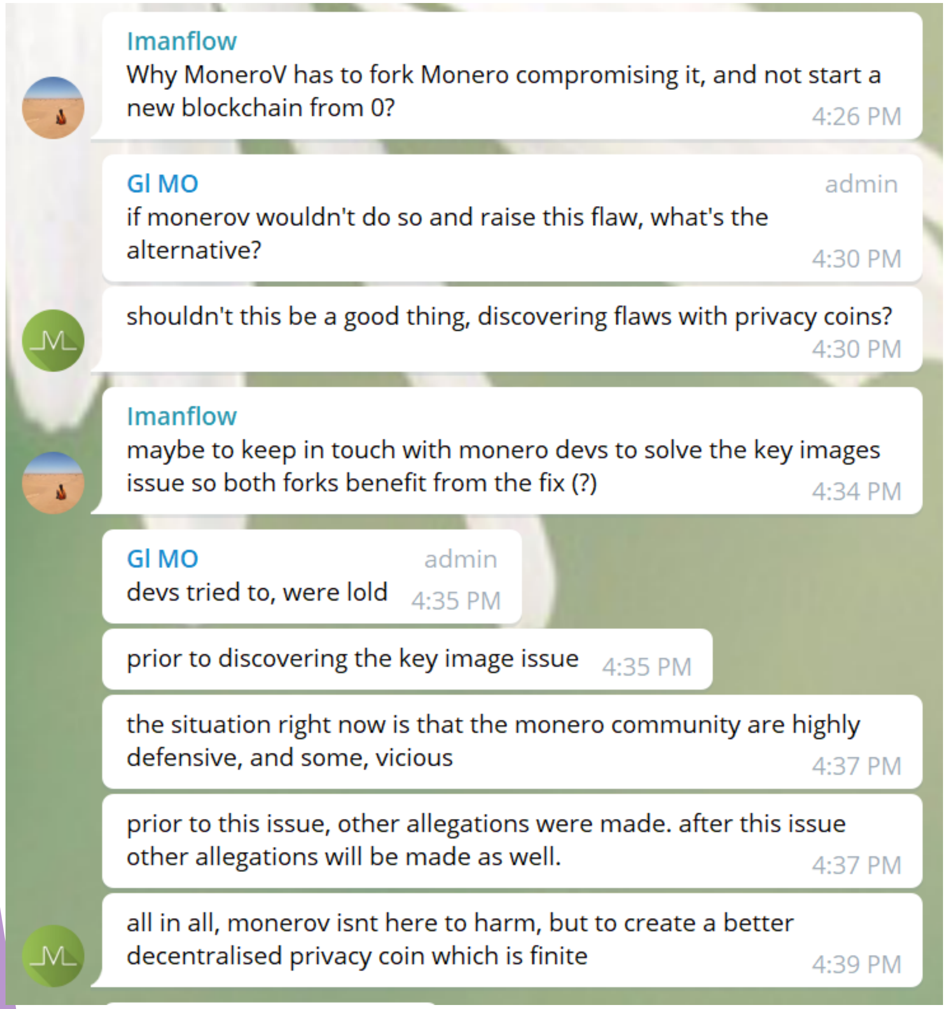
MoneroV attacks its own privacy (Cont’d)



MoneroV attacks its own privacy (Cont’d)



Primum non nocere



Imanflow
Why MoneroV has to fork Monero compromising it, and not start a new blockchain from 0? 4:26 PM

Gl MO admin
if monerov wouldn't do so and raise this flaw, what's the alternative? 4:30 PM

shouldn't this be a good thing, discovering flaws with privacy coins? 4:30 PM

Imanflow
maybe to keep in touch with monero devs to solve the key images issue so both forks benefit from the fix (?) 4:34 PM

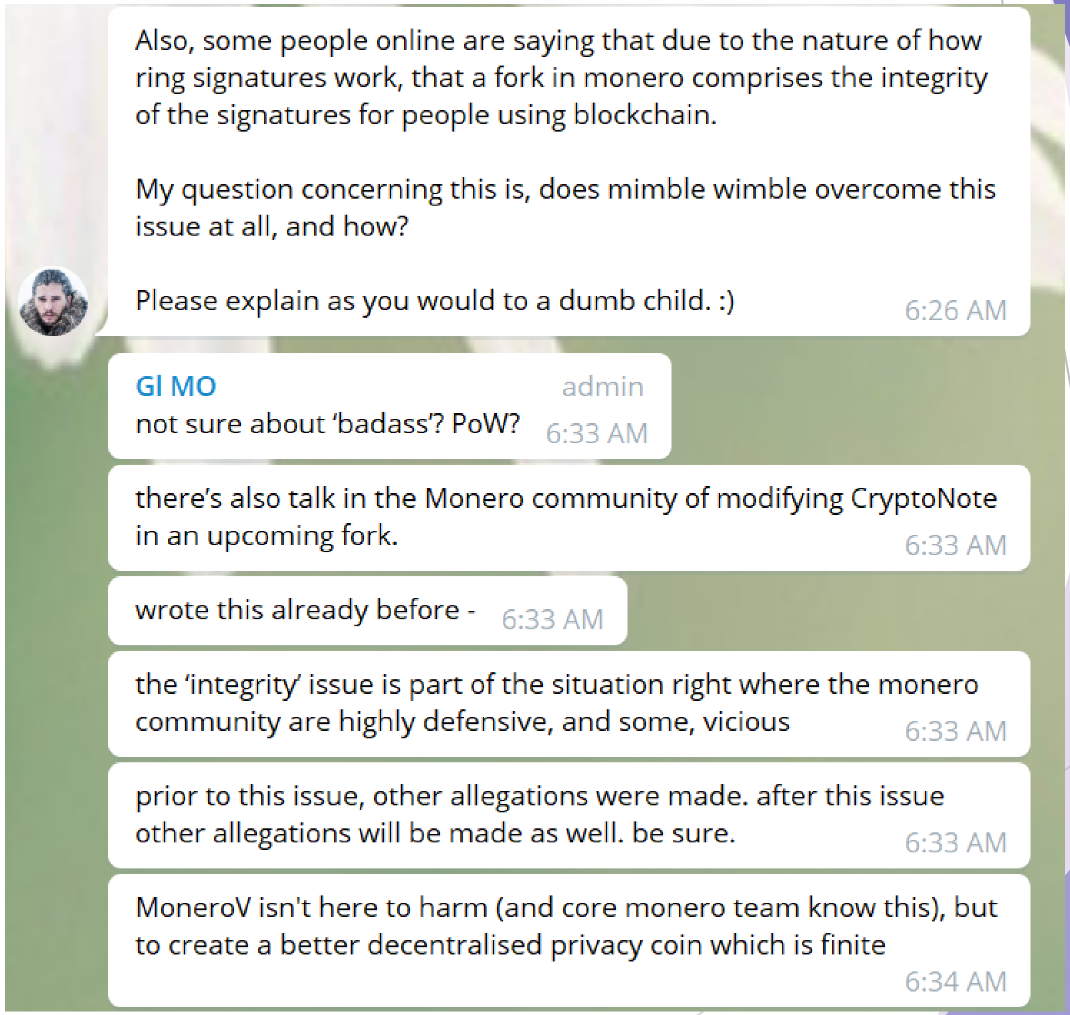
Gl MO admin
devs tried to, were lold 4:35 PM

prior to discovering the key image issue 4:35 PM

the situation right now is that the monero community are highly defensive, and some, vicious 4:37 PM

prior to this issue, other allegations were made. after this issue other allegations will be made as well. 4:37 PM

all in all, monerov isnt here to harm, but to create a better decentralised privacy coin which is finite 4:39 PM



Also, some people online are saying that due to the nature of how ring signatures work, that a fork in monero comprises the integrity of the signatures for people using blockchain.

My question concerning this is, does mimble wimble overcome this issue at all, and how?

Please explain as you would to a dumb child. :) 6:26 AM

Gl MO admin
not sure about 'badass'? PoW? 6:33 AM

there's also talk in the Monero community of modifying CryptoNote in an upcoming fork. 6:33 AM

wrote this already before - 6:33 AM

the 'integrity' issue is part of the situation right where the monero community are highly defensive, and some, vicious 6:33 AM

prior to this issue, other allegations were made. after this issue other allegations will be made as well. be sure. 6:33 AM

MoneroV isn't here to harm (and core monero team know this), but to create a better decentralised privacy coin which is finite 6:34 AM

Between a rock and a hard place

- MoneroV knew about it beforehand before Monero community raised the issue
  - Are still proceeding with hurting their own users
- MoneroV didn't know about it before Monero community
  - Are still proceeding with hurting their own users
- How could this be avoided again…?

How can you protect yourself?

- Don’t use XMV that you got from claiming
- Don’t use XMR or XMV for roughly a week after XMV release

Conclusion

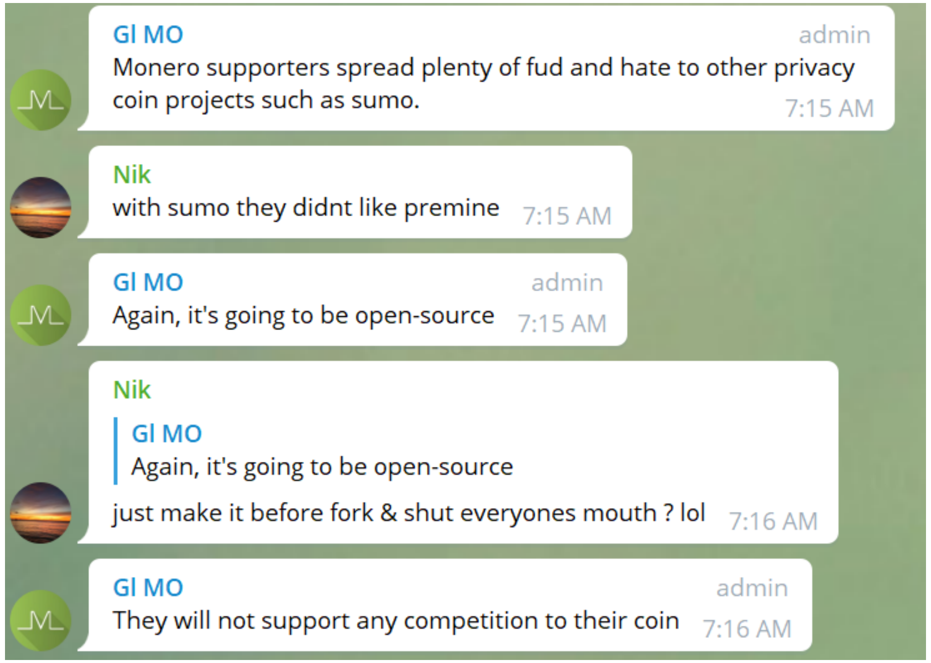
- Coin supply/inflation
  - XMV has more than XMR until ~3,500 AD
- Scalability
  - Hates bloat, but inheriting bloat is ok
- Privacy
  - Claims no intention to harm, proceeds to harm own users

- How can MoneroV avoid all these issues?
  - Say it with me… don’t do a chain split

Bonus Red Flag Round!

- “we have brought many expert developers onboard”
  - Four psuedonyms that took 22 commits to fork and make basic changes to xmr
    - Nospawn last anything commit Feb 18th
    - Vanfactory last commit March 2nd, prior Feb 16th
    - Instanceme, Feb 9th
    - Miltonf, Feb 18th

#1: Monero community hates competition?



Gl MO admin
Monero supporters spread plenty of fud and hate to other privacy coin projects such as sumo. 7:15 AM

Nik
with sumo they didnt like premine 7:15 AM

Gl MO admin
Again, it's going to be open-source 7:15 AM

Nik
> Gl MO
> Again, it's going to be open-source

just make it before fork & shut everyones mouth ? lol 7:16 AM

Gl MO admin
They will not support any competition to their coin 7:16 AM

#1: Not really

“I want competition in the space. It makes privacy as a whole better with innovation. I consider myself a privacy advocate, not a Monero advocate. I welcome competition to Monero, but I just want it to be good.” Diego AKA rehrar, Monero Contributor on a “competitor’s” forum

Smooth, a Monero Core Team member, has been Aeon’s lead developer since April 2015

#2: If I use a temp wallet, I’m still private?

1000 XMR

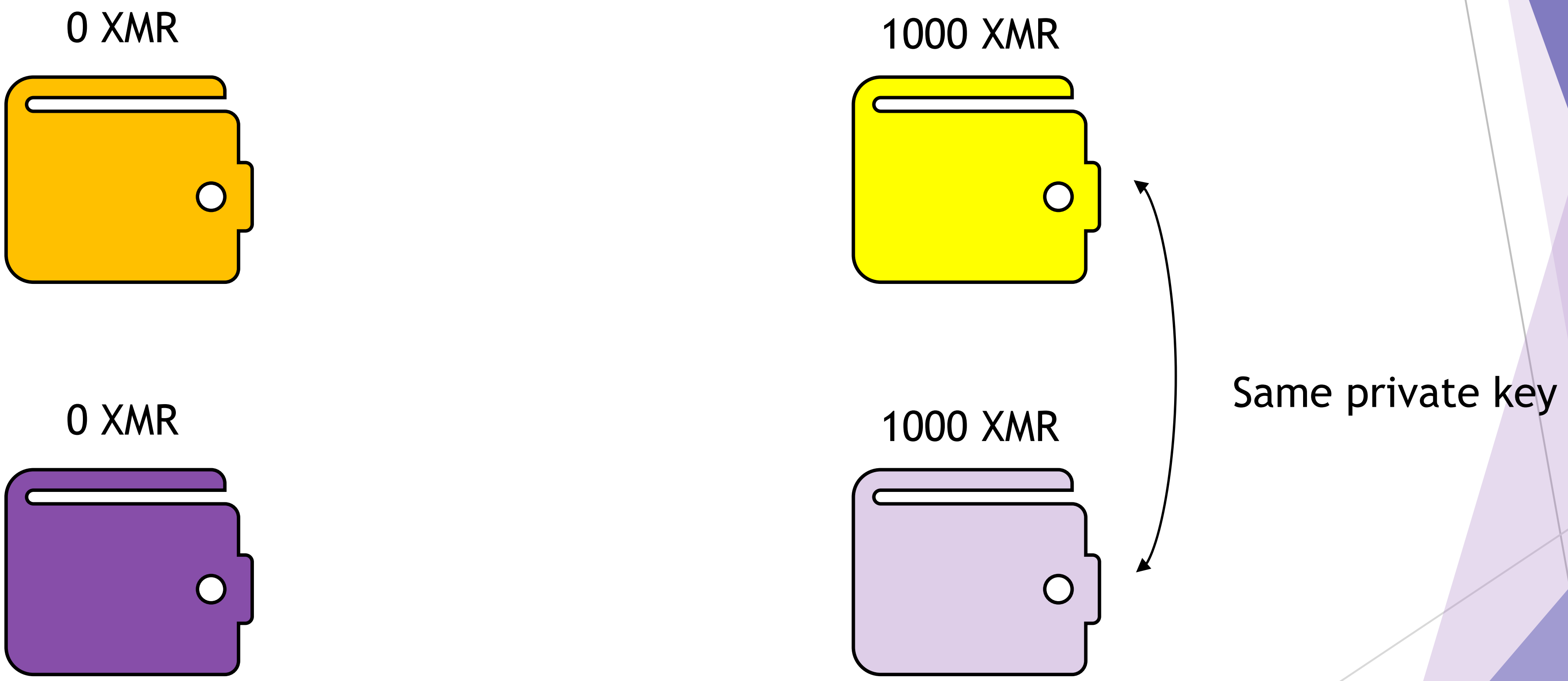
0 XMR

#2: If I use a temp wallet, I’m still private?

0 XMR

1000 XMR

#2: If I use a temp wallet, I’m still private?



0 XMR

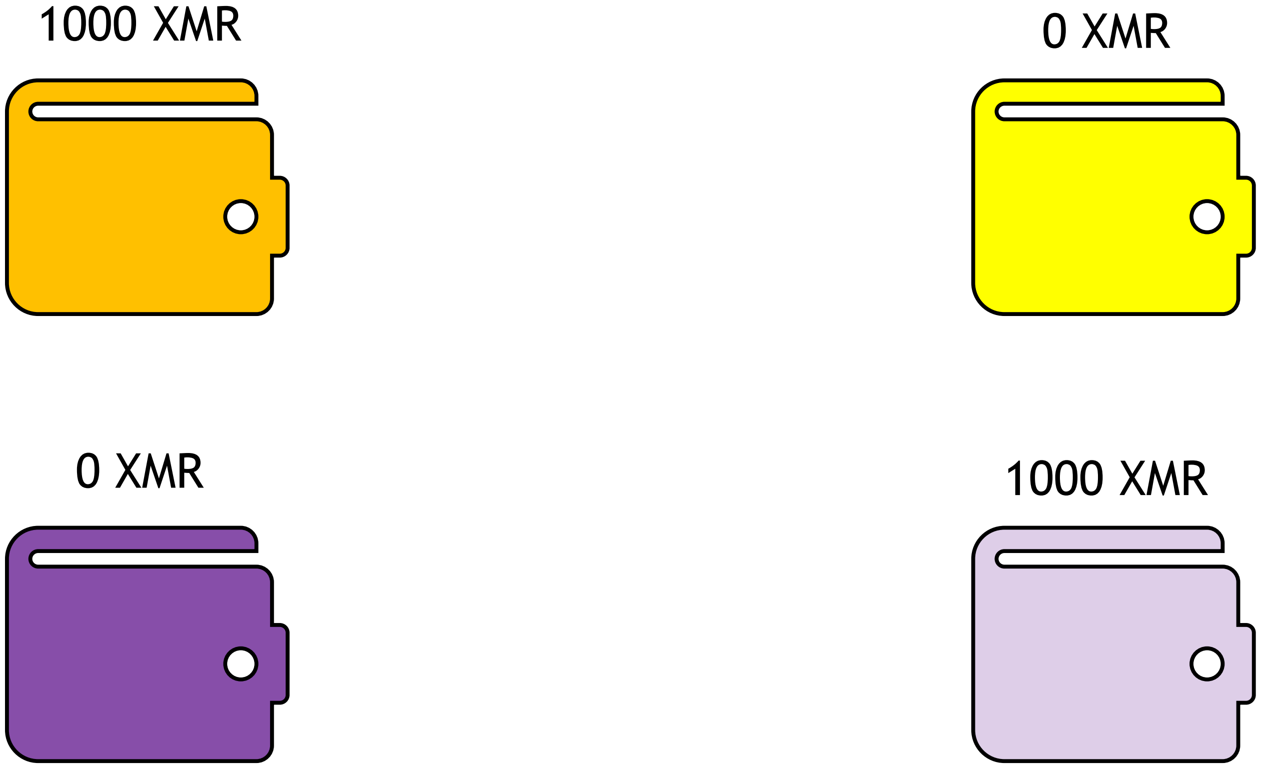
1000 XMR

0 XMR

1000 XMR

Same private key

#2: If I use a temp wallet, I’m still private?



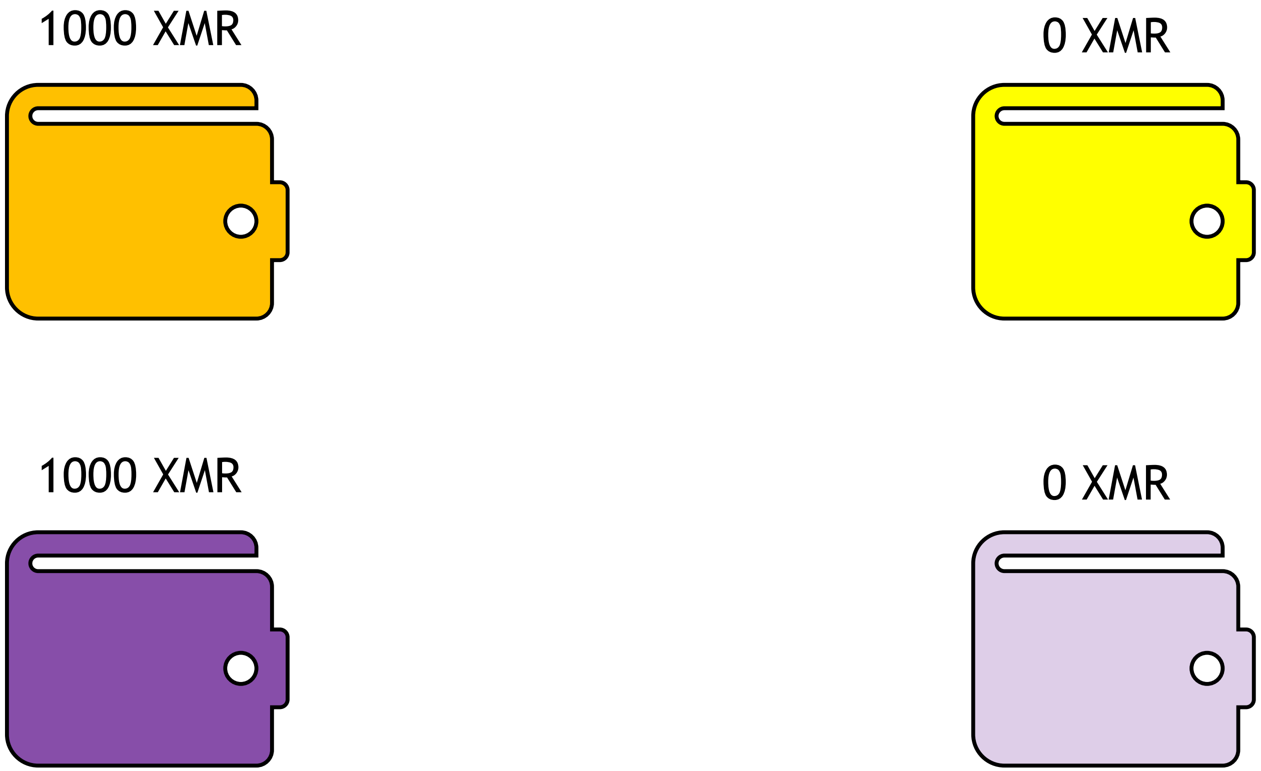
1000 XMR

0 XMR

0 XMR

1000 XMR

#2: If I use a temp wallet, I’m still private?



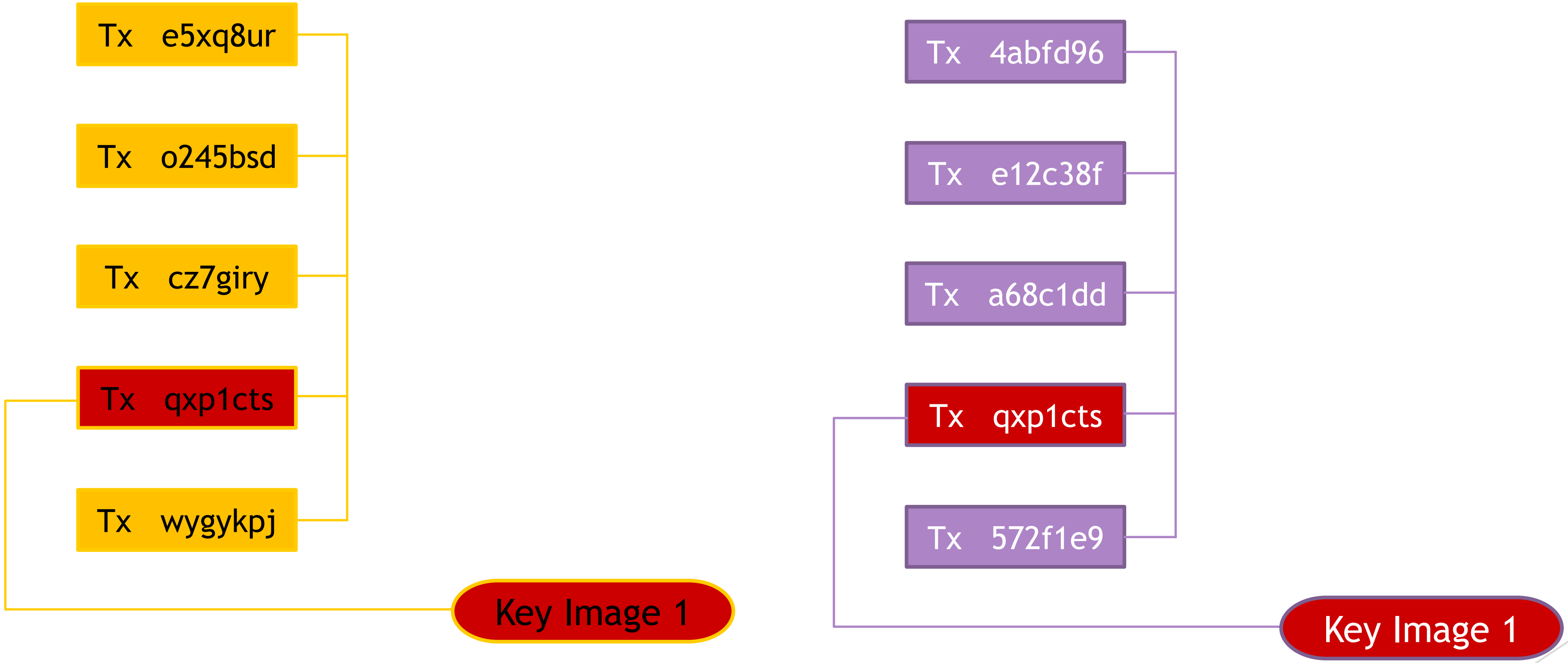
1000 XMR

0 XMR

1000 XMR

0 XMR

#2: No, not if you claim XMV



#3 Devs are anonymous

“With an anonymous team, there is no recourse if something similar happens as did with the fork of bitcoin, bitcoin gold, where the development team promoted wallets containing malware.” – BTC Manager