



# Policy Effects of Privacy Coins

Nigel Nderi <ncn@andrew.cmu.edu>, Karim Helmy <khelmy@andrew.cmu.edu>



## Introduction

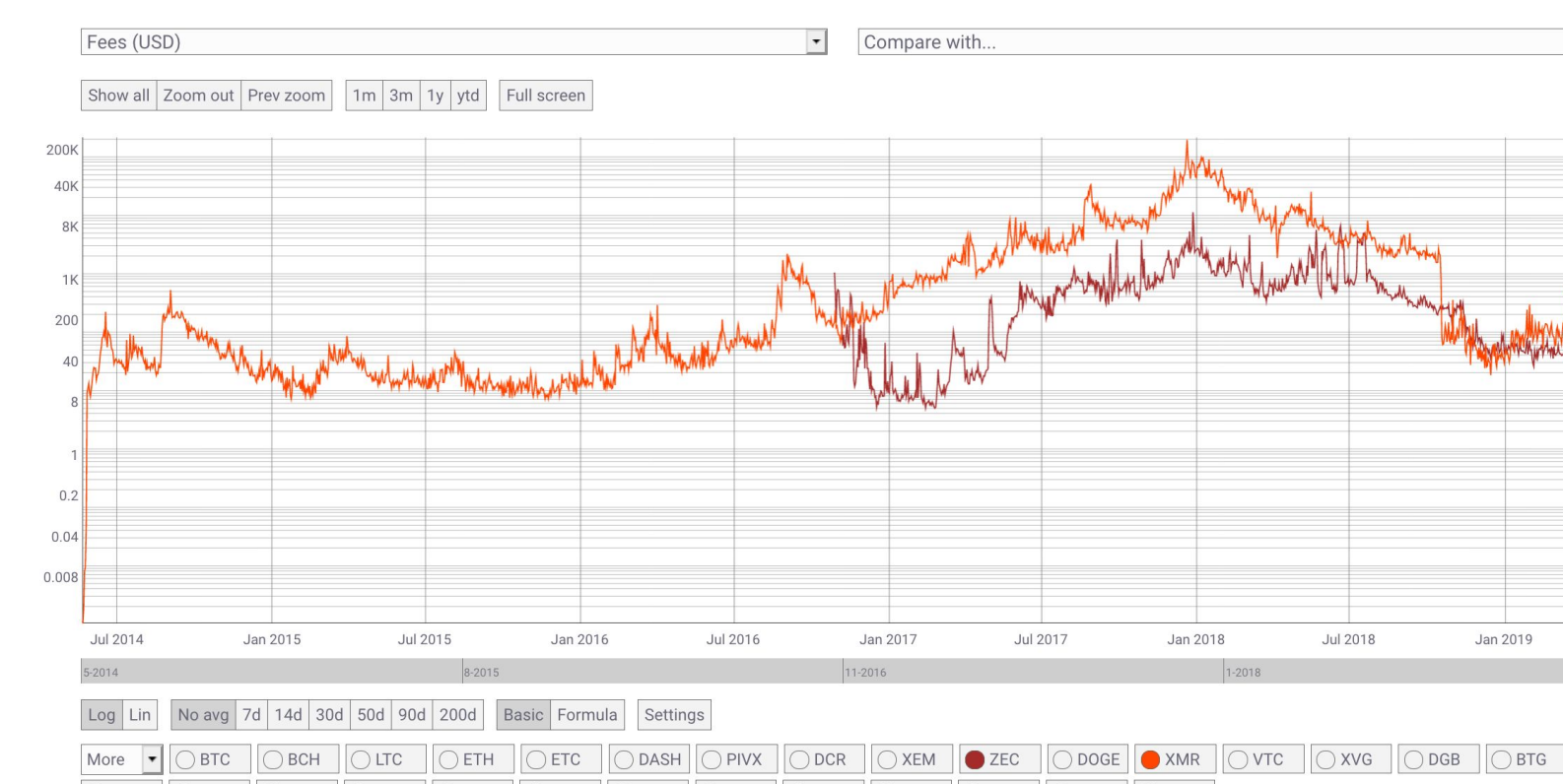
- What are privacy coins?
  - Cryptocurrencies with private transactions
  - Examples: Zcash and Monero
- Importance:
  - Enable digital financial privacy
  - Not government issued
- Issues surrounding their regulation, benefits and potential for misuse

## Benefits and Risks<sup>(3)</sup>

- Security in transactions
  - Limits agents aware of transaction details
  - Easier transaction error detection and handling
- Consumer privacy
  - Reduces risk of theft
  - Minimizes risk when partaking in illicit transactions

## Findings

- Treat privacy coins like cash
  - KYC/AML requirements to financial institutions involved in their use.
  - Large transactions must legally be reported.
- Banning privacy coins:<sup>(2)</sup>
  - Adopted in Japan
  - Disproportionately affects developers rather than users
  - Businesses could move offshore



Fees, a proxy for network usage, Monero (bright) and Zcash (dark) are recently trending up<sup>(4)</sup>

- Likely to be ineffective and to disincentivize innovation
- Requiring merchants to follow KYC/AML procedures:
  - Recently proposed in a Texas bill (Texas HB4371)<sup>(1)</sup>
  - Would be burdensome for users
  - Would infringe on financial privacy

## Conclusion

- Privacy coins:
  - Good for freedom and financial privacy
  - Reduce dependence on banks
  - Introduce significant challenges
- Regulation should take into account characteristics of privacy coins
  - Regulate them like cash



Zcash



## References

- (1) Janus, E. *Texas' 'Worse than Bitlicense' Crypto Bill is Dead on Arrival*.2019.
- (2) Viglione,R. *Japan's Ban is a Wake-Up Call to Defend Privacy Coins*.2018.
- (3) Kahn, C. et. all. *Money is Privacy*.2005.
- (4) Generated with Coin Metrics



The values of Monero (bright orange) and Zcash (dark red) are climbing rapidly in spite of bear market<sup>(4)</sup>