MCC VR

Privacy: The Collision of Theory and Practice

Sarang Noether, Ph.D.

01 Goals and Risks

MCC VR

What are our goals?

I can make a transaction that is accepted by the network.

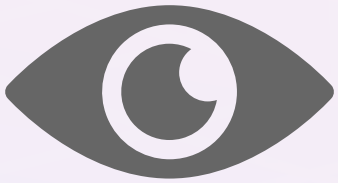
MCC VR

What are our goals?

I can accept a transaction without worrying about asset history.

MCC VR

What are our goals?



Snoops can't infer details about my transaction or its participants.

MCC VR

What are our goals?

Snoops can't link my transactions to each other.

MCC VR

What are our goals?

I can share information about my transactions selectively.

Privacy is informed, affirmative consent.

MCC VR

What are the risks?

I buy a coffee from Clara's Coffee. Clara buys an illegal Beanie Baby. I get a visit from a person in dark sunglasses.

MCC VR

What are the risks?

I run Dave's Donuts. A customer buys a donut, but got the money from selling an illegal Beanie Baby. My exchange refuses the funds.

MCC VR

What are the risks?

I hold large sums of digital assets, but don't wish to broadcast this fact. Evildoers observe my funds and balances and target me for theft.

What are the risks?

I run Sam's Supply Shop. I don't want my competitors to know my business dealings, or those of my clients.

02 Privacy Theory

MCC VR

Transparent chain + mixer

Compatibility with existing protocols/chains, liquidity

Slow, expensive, fragile to analysis

Think Bitcoin with your fave mixer

MCC VR

Transparent + side hustle

- Compatibility with existing protocols/chains, liquidity
- Transparent endpoints, increasing analysis
- Think Bitcoin with Lightning

MCC VR

Limited signer ambiguity

Obscures sender, recipient, amount; easy without trust

Fragile against repeated targeted attacks; statistical heuristics

Think Monero

MCC VR

Mimblewimble-ish

Obscures amount and decouples from addresses; efficient blocks

Fragile against network monitoring and/or evil nodes

Think Grin or Beam

MCC VR

Generalized ambiguity

Obscures sender (maximally), recipient, amount; small and fast

Soundness requires trust; optional in practice with poor ecosystem support

Think Zcash

MCC VR

03 Privacy Practice

MCC VR

Theory/Practice: Part 1

Theory: You can use a transparent asset privately if you do it right.

Practice: It's expensive, slow, generally ad-hoc, and gets flagged by analysis snoops at your exchange. If you bother at all.

MCC VR

Theory/Practice: Part 2

Theory: Offering strong optional privacy means users can choose to operate safely. Yay choice!

Practice: Nobody uses the privacy feature, or has to play jump-between-features and links their transactions anyway.

MCC VR

Theory/Practice: Part 3

Theory: Using off-chain features against a transparent layer gives liquidity and privacy!

Practice: Current solutions are the subject of research showing a disappointing number of analyses and failure modes.

MCC VR

Theory/Practice: Part 4

Theory: This new privacy-focused implementation works fine, if you assume the network is full of honest people.

Practice: Network snoops will… snoop the network. Your transaction graph is exposed, and the protocol's intended use breaks.

04 Lessons Learned

MCC VR

It can't be optional

If privacy-focused features aren't mandatory at the protocol level:

- The ecosystem won't adopt them
- Most users won't use them
- Those who do will use them poorly

Things that work great in the lab might catch on fire in the real world.

MCC VR

Users are humans

Theory and implementation are identical… in theory.

Your implementation needs to honor that users are not experts.

Don't blame users for not getting it.

MCC VR

Sweat the big stuff first

You can't solve for every threat model, and it's easy to nitpick the worst threats at the expense of the broader ones.

Design and build against risks that are most likely to affect the most people.

Communicate this clearly.

MCC VR

Thank you!


magicalcryptoconference.com


@magicalcrypto


@magicalcryptoconference


@magicalcrypto

MCC VR