Hello!

Both Bitcoin and Ethereum systems are known to provide pseudo-anonymity for its users:
the real identity can be revealed only if a user discloses his public key that
hashes to his address.

There were several works showing that at least in Bitcoin world, this kind
of anonymity does not guarantee privacy [1] [2]. Using some
statistical methods, one can trace all the addresses belonging to the same party.

This fact explains new research projects towards privacy-preserving blockchain platforms [3].

But what about Ethereum? From Bitcoin, it differs in a sense that by doing a transaction,
you can transfere value and/or mutate some contract state.

Are there any ongoing research regarding privacy issues that arise in the context of
smart-contracts. By privacy, I do not mean non-disclosure of contract's state, but rather
concerns of using the same address for each transaction call, for example.

I appreciate any thoughts/pointers regarding this topic.

Thanks.

[1] Ron, Shamir - Quantitative Analysis of the Full Bitcoin Transaction Graph [2012]

[2] Meiklejohn et al - A Fistful of bitcoins [2013]

[3] Kosba et al - Hawk: The BlockChain Model of Cryptography and Privacy-Preserving Smart Contracts (2016)