SECURITY INNOVATION

A METACASH CASE STUDY:

PREVENTING PHISHING ATTACKS

AGAINST SMART CONTRACTS IN BLOCKCHAIN APPLICATIONS

Blockchain Adoption Challenges:

Price Fluctuation and Transaction Fees

Cryptocurrencies have been slow in their goal to reach mass adoption, in part due to the inherent price fluctuations to the underlying crypto assets. It is easy to see why someone may not want to spend their currency on goods and services if they think the value of the currency will rise by simply waiting.

To combat this, blockchain platforms have converged around the concept of stable coins as a means of exchange. These tokens are mapped 1-to-1 with a stable national currency like the US dollar through various technical mechanisms. This allows users to achieve the benefits of conducting business on a blockchain platform, such as lower fees and the minimization of rent-seeking middle-men, without the risk of holding on to an instable form of money.

The Ethereum blockchain is the most popular public smart contract platform at the time of writing and has many stable coins built on top of its network. Unfortunately, due to the design of the system, all transactions that are made to the blockchain must pay a small transaction fee in the blockchain's native currency, Ether. This presents a conundrum for mass adoption. Users that want to achieve simple, fast, low-friction payments without needing to understand any of the underlying blockchain tech can send stable coins easily over the Ethereum network; however they must still purchase Ether to cover the cost of fees, increasing the friction for onboarding new users.

Blockchain Adoption Solutions:

Stable Coins and Relay Networks

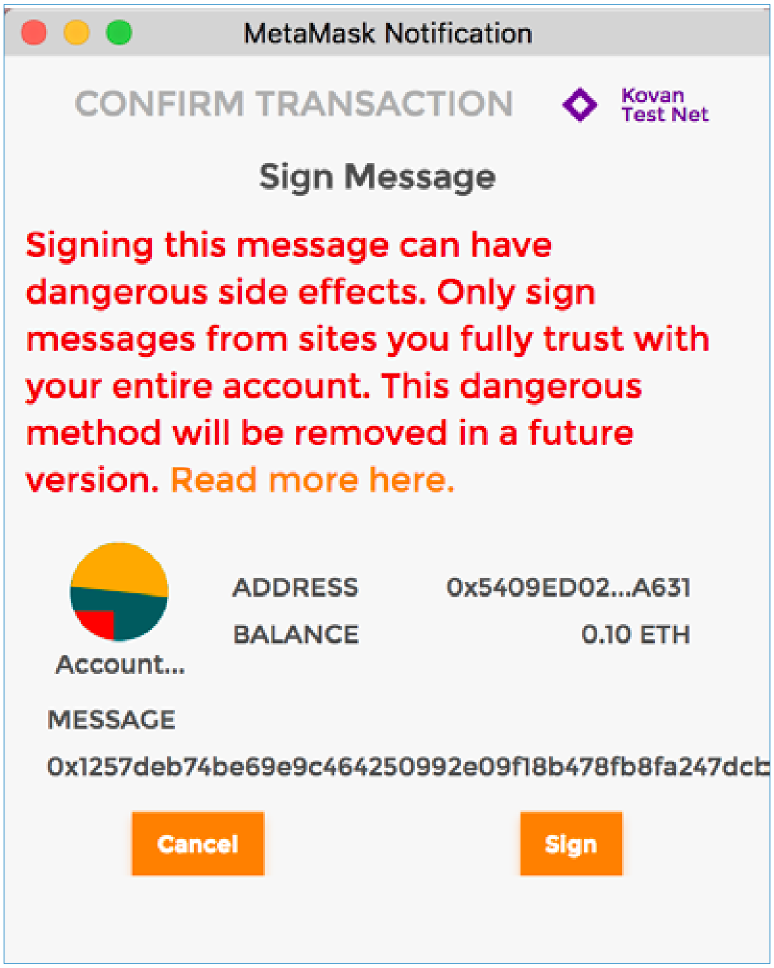
Metacash is a project that aims to solve this problem by creating a network of relayers that will pay your transaction fees for you. By signing a message authorizing a stable coin transaction, a relayer can submit a transaction to the Ethereum network on behalf of the user that transfers the stable coin from that user's Metacash wallet for them. With this system, the relayer can pay all the transaction fees using their personal Ether and collect a small payment from the user's wallet in their stable coin.

Signing a transaction or message with the user's private key is the only way to move funds from their wallet. If relayers become unavailable or act malicious, the user will still have full control of their funds. This allows users to interact with the growing blockchain ecosystem in a safe manner, using only stable coins and not exposing themselves to volatility or confusion when dealing with other crypto-assets.

Security Innovation Assessment:

Phishing Threats to Message Signing

Security Innovation approached Metacash shortly after the initial release of their beta contract after identifying a possible threat to their design. Due to the way many Ethereum wallets sign messages (using the eth_sign web3.js function), it is difficult for users to verify what their signed message does or ensure that the message is only used in the intended smart contract. By default, wallet interfaces will just display a blob of hex data to be signed with no context whatsoever.


MetaMask Notification

CONFIRM TRANSACTION

Kovan Test Net

Sign Message

Signing this message can have dangerous side effects. Only sign messages from sites you fully trust with your entire account. This dangerous method will be removed in a future version. Read more here.

Account...

ADDRESS 0x5409ED02...A631

BALANCE 0.10 ETH

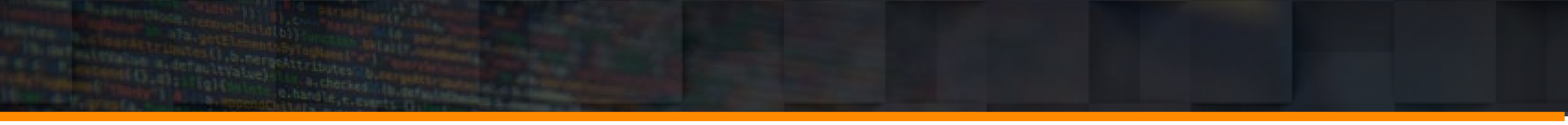
MESSAGE

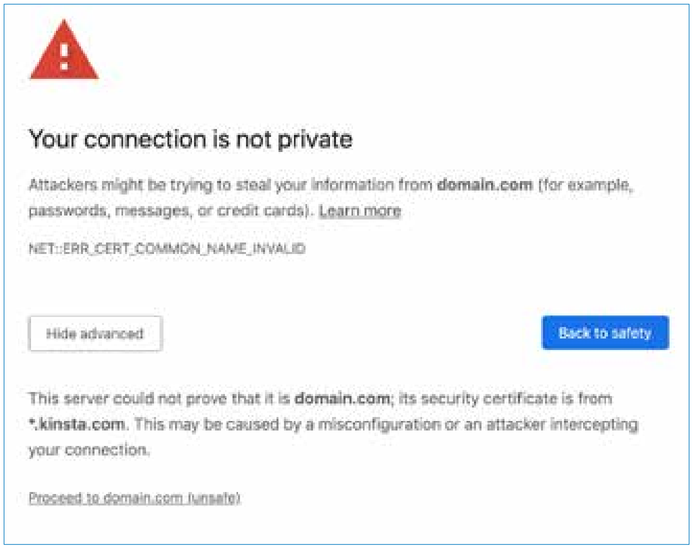
0x1257deb74be69e9c464250992e09f18b478fb8fa247dcb

Example UX of signing a message with "eth_sign"
source: http://eips.ethereum.org/EIPS/eip-712

This issue presented a unique challenge for Metacash. Let's assume there is a malicious DApp (De- centralized application that interacts with a smart contract) called CryptoBullDogs. This DApp might have a feature that requires a user to sign a message with their wallet in order to perform a standard operation, such as registering or authenticating to the DApp. Despite seeing potential warnings, a user is likely to sign the random hex data if this is the user experience that they are used to with other DApps.

This issue is similar in nature to the risk of self-signed certificates in web 2.0 applications. If a user becomes accustomed to clicking past the warnings for their internal company tool, they are more likely to ignore the warning in a legitimate Man-in-the-Middle attack.





Your connection is not private

Attackers might be trying to steal your information from **domain.com** (for example, passwords, messages, or credit cards). Learn more

NET::ERR_CERT_COMMON_NAME_INVALID

This server could not prove that it is **domain.com**; its security certificate is from ***.kinsta.com**. This may be caused by a misconfiguration or an attacker intercepting your connection.

Proceed to domain.com (unsafe)

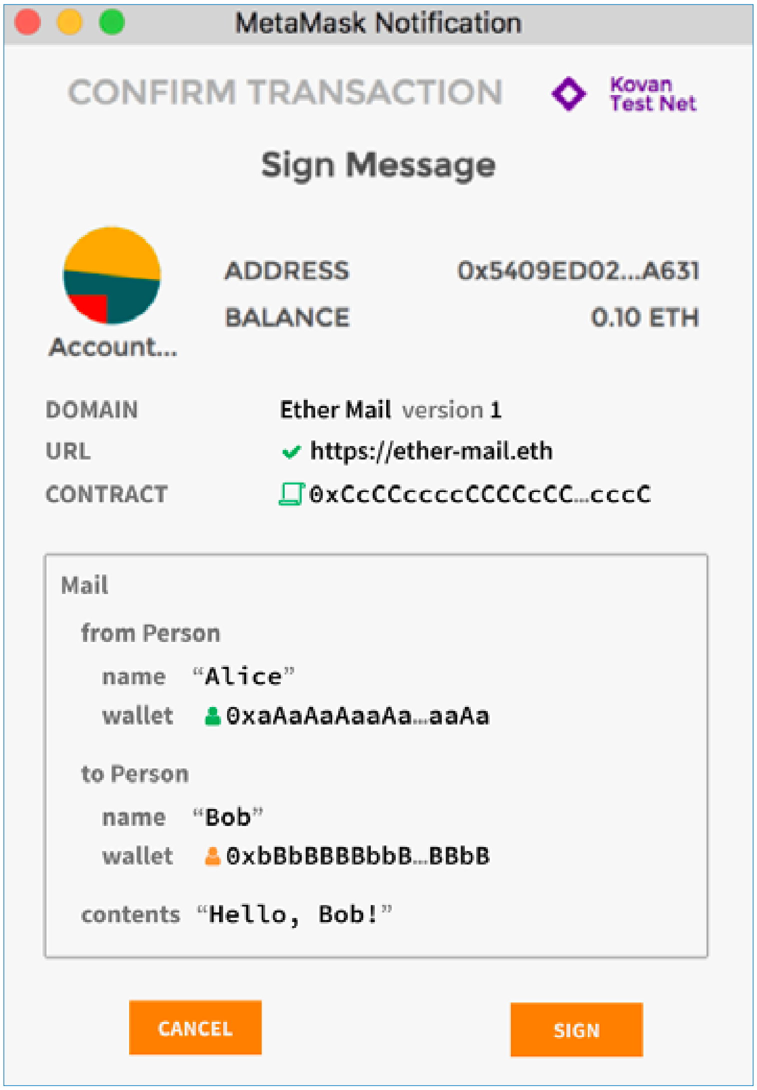
Once the user has signed the message, CryptoBullDogs can collect the signed message and replay this to a Metacash relayer. Depending on what malicious message CryptoBullDogs has tricked the user into signing, they may be able to steal all the funds stored in the user's Metacash wallet.

Addressing the Signing Issues

Security Innovation worked closely with Metacash to identify remediation options for this issue. Our top recommendation was for Metacash to implement the EIP 712 structured signed data standard. This standard is a current work in progress that is an active development among major wallet software and libraries. It provides clear UI indications of the "domain" that the signed message is for, as well as details about the parameters being signed. That way the user can clearly see that CryptoBullDogs is signing a message intended for Metacash and will reject it.

While EIP 712 is a promising solution to this problem, it is an incomplete standard and general-purpose libraries are far from finalized. After discussing alternative solutions with Metacash, we concluded that the risk of this issue could be minimized by ensuring users only use the official Metacash wallet software with their Metacash wallets and not with other DApps.

The developers of Metacash were able to come up with an elegant solution to this issue where the prefix string to a signed message would differ in the Metacash wallet and smart contracts than that produced by the generic eth_sign function.



MetaMask Notification

CONFIRM TRANSACTION

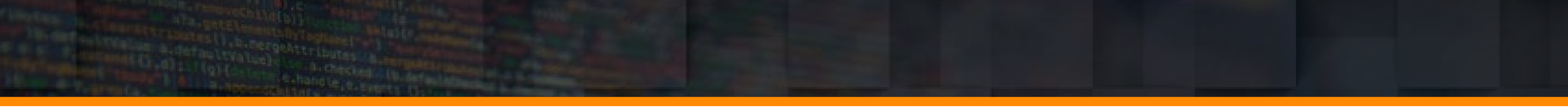
Sign Message

Account...

ADDRESS 0x5409ED02...A631
BALANCE 0.10 ETH

DOMAIN Ether Mail version 1
URL ✓ https://ether-mail.eth
CONTRACT 0xCcCCccccCCCCcCC...cccC

```
Mail
  from Person
    name   "Alice"
    wallet 0xaAaAaAaaAa...aaAa
  to Person
    name   "Bob"
    wallet 0xbBbBBBBbbB...BBbB
  contents "Hello, Bob!"
```



This solution remains compliant with the EIP-191 Signed Data Standard since the version byte 'M' (0x4D) has not been allocated and ensures that any signed message produced by a malicious DApp will be incompatible with the Metacash smart contracts and cannot be used to steal funds.

Typical prefix with eth_sign:	**Prefix used by Metacash wallet & smart contracts:**
"\x19Ethereum Signed Message:\n32"	"\x19Metacash Signed Message:\n32"

Additional Security

Security Innovation additionally preformed a full smart contract audit of the second version of the Metacash smart contracts. In total, 10 security issues were identified, with 2 being ranked high severity that could result in a loss of user funds or theft. Metacash was able to review and respond to each of the findings and patch the issues in their latest release of the contract.

"The report from Security Innovation has really impressed us," says Nour Haridy, lead architect of the Metacash project. "Some issues that were raised could have been completely catastrophic if exploited. We are grateful to have partnered with the engineers at Security Innovation to amplify the security of our code and protect our users' assets."

We at Security Innovation are very excited to support projects like Metacash that seek to bring usability and adoption to this exciting new technological landscape.

The full Metacash Smart Contract Audit Report can be found here: **http://bit.ly/metacash2019.**

> *"The report from Security Innovation has really impressed us. Some issues that were raised could have been completely catastrophic if exploited. We are grateful to have partnered with the engineers at Security Innovation to amplify the security of our code and protect our users' assets."*
>
> **— NOUR HARIDY,** LEAD ARCHITECT OF THE METACASH PROJECT

ABOUT SECURITY INNOVATION

Security Innovation is a pioneer in software security and trusted advisor to its clients. Since 2002, organizations have relied on our assessment and training solutions to make the use of software systems safer in the most challenging environments – whether in Web applications, IoT devices, or the cloud. The company's flagship product, CMD+CTRL Cyber Range, is the industry's only authentic environment to build the skills teams need to protect the enterprise where it is most vulnerable – at the software layer. Security Innovation is privately held and headquartered in Wilmington, MA USA. For more information, visit **www.securityinnovation.com** or connect with us on **LinkedIn** or **Twitter**.

Get in **Touch** |

✉ 187 Ballardvale Road, suite A195
Wilmington, MA 01887

☎ 887.839.7598 x1
🌐 www.securityinnovation.com