



A.D. 1308  
**unipg**  
UNIVERSITÀ DEGLI STUDI  
DI PERUGIA



Politecnico  
di Bari

5th Distributed Ledger Technology Workshop (DLT 2023)  
Bologna, Italy | 25–26 May 2023

# Towards a quantum-safe transaction signature in Ethereum

## Authors:

S. Bistarelli

M. Fiore

I. Mercanti

M. Mongiello

---

Dipartimento di Matematica e Informatica, University of Perugia, Perugia, Italy

Department of Electrical & Information Engineering, Polytechnic University of Bari, Bari, Italy

# Our proposal

---

- Interface implementation of an Ethereum node for supporting different signature methods.
- Post-quantum resistant Blockchain
- No fork needed

# Background

---

- Blockchain systems depend heavily on cryptographic methods to ensure security, protect user privacy, and enhance system performance.
- Blockchain uses wallets with key-pairs for authentication and signing processes.
  - Private key: sign transactions
  - Public key: verify transactions
- The development of quantum computing prompts growing worries on the chain security.

# State of the art

---

- Several related work in literature.
  - Secure cryptocurrency scheme<sup>[1]</sup>.
  - Quantum key distribution<sup>[2]</sup>.
  - Management of cryptographic primitives in smart contracts<sup>[3]</sup>.
- Introducing new features and applying fixes to a Blockchain cause forks in the chain.
- Proposal: development of an interface to support different signature methods in an Ethereum client.

[1] Yulong Gao, et al. A Secure Cryptocurrency Scheme Based on Post-Quantum Blockchain. *IEEE Access* (2018).

[2] Evgeniy O, et al. Quantum-secured blockchain. *CoRR* (2017).

[3] Riccardo Longo, et al. Adaptable Cryptographic Primitives in Blockchains via Smart Contracts. *Cryptography* (2022).

# Post-quantum algorithms

---

- **Key-pair generation**: generation of a user's private key starting from his public key.
- **Transaction signature**: generation of a user's private key starting from the signature of a transaction.
- **Block hashes**: writing new data in a block, rebuilding the chain.

# Post-quantum algorithms

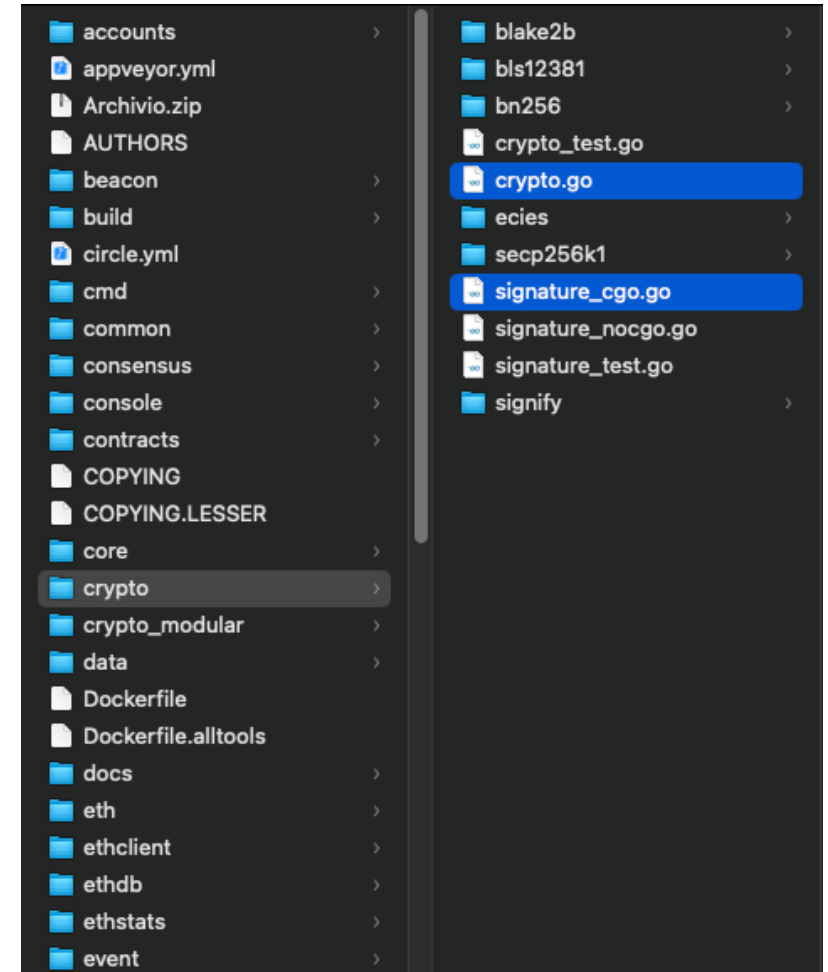
---

- **Key-pair generation:** a post-quantum algorithm can quickly generate a user's private key starting from his public key.
- **Transaction signature:** a post-quantum algorithm can quickly generate a user's private key starting from the signature of a transaction.
- **Block hashes:** a post-quantum algorithm can be used by an attacker to break the hash linking between blocks, writing new data in a block and quickly rebuilding the entire chain.

# Changes in GO code

---

- Geth implementation – v1.11.0.
- Support multiple signature algorithms.
- *crypto.go* and *signature\_cgo.go* files.



# Changes in GO code

---

- We create *crypto\_ecdsa.go* and *signature\_cgo\_ecdsa.go*.
- Constraint: ECDSA-compliant algorithm required.
- Example: generation of a key-pair using the interface.

```
/* Generation of a key-pair using an interface
*/
func GenerateKey() (*privateKey, error) {
    switch actualAlgorithm {
    case "ECDSA":
        return crypto_ecdsa.GenerateKey()
    case "SPHINCS":
        return crypto_sphincs.GenerateKey()
    case "OTHER":
        return crypto_other.GenerateKey()
    default:
        return error("Unknown algorithm")
    }
}
```



# Validation

- A node has been run and tested using the interface.
- Connection to Ethereum mainnet and transaction submission in Sepolia testnet.

The screenshot shows the Etherscan Sepolia Testnet interface for the address `0x836434fCB37dA8125f1d9AFce209764996D0Cb8b`. The interface includes a search bar, navigation links (Home, Blockchain, Tokens, NFTs, Misc), and a 'More' dropdown menu. The main content area is divided into three sections: Overview, More Info, and Multi Chain.

**Overview:** ETH BALANCE: 0.005421840000021 ETH

**More Info:** LAST TXN SENT: `0xa76a1f1de0ec0...` from 8 days 23 hrs ago; FIRST TXN SENT: `0xa76a1f1de0ec0...` from 8 days 23 hrs ago

**Multi Chain:** MULTICHAIN ADDRESSES: N/A

**Transactions:** Token Transfers (ERC-20)

Latest 3 from a total of 3 transactions

Transaction Hash	Method	Block	Age	From	To	Value	Txn Fee
<code>0xb2613d1a3ea494442...</code>	Transfer	3456334	8 days 23 hrs ago	<code>0x80b8e8...bb8c95Eb</code>	<code>0x836434...96D0Cb8b</code>	0.005 ETH	0.00002099
<code>0xa76a1f1de0ec035a4...</code>	Transfer	3456253	8 days 23 hrs ago	<code>0x836434...96D0Cb8b</code>	<code>0x80b8e8...bb8c95Eb</code>	0.01 ETH	0.00002099
<code>0x2a42bec1de6d8acc5...</code>	Transfer	3456241	8 days 23 hrs ago	<code>0x6Cc939...7Ba5F455</code>	<code>0x836434...96D0Cb8b</code>	0.01044284 ETH	0.000042

# Conclusion

---

- Interface implementation of an Ethereum node for supporting different signature methods.
- Post-quantum resistant Blockchain.
- Future work: extension of the interface to support algorithms with a different structure than ECDSA.

Thank you for your attention



[marco.fiore@poliba.it](mailto:marco.fiore@poliba.it)



[@Mackerkun](https://www.instagram.com/Mackerkun)