ShadowEth: Private Smart Contract on Public Blockchain

Rui Yuan(袁睿)
Institute of Parallel and Distributed Systems,Shanghai Jiao Tong University

Yu-Bin Xia(夏虞斌)
Institute of Parallel and Distributed Systems,Shanghai Jiao Tong University

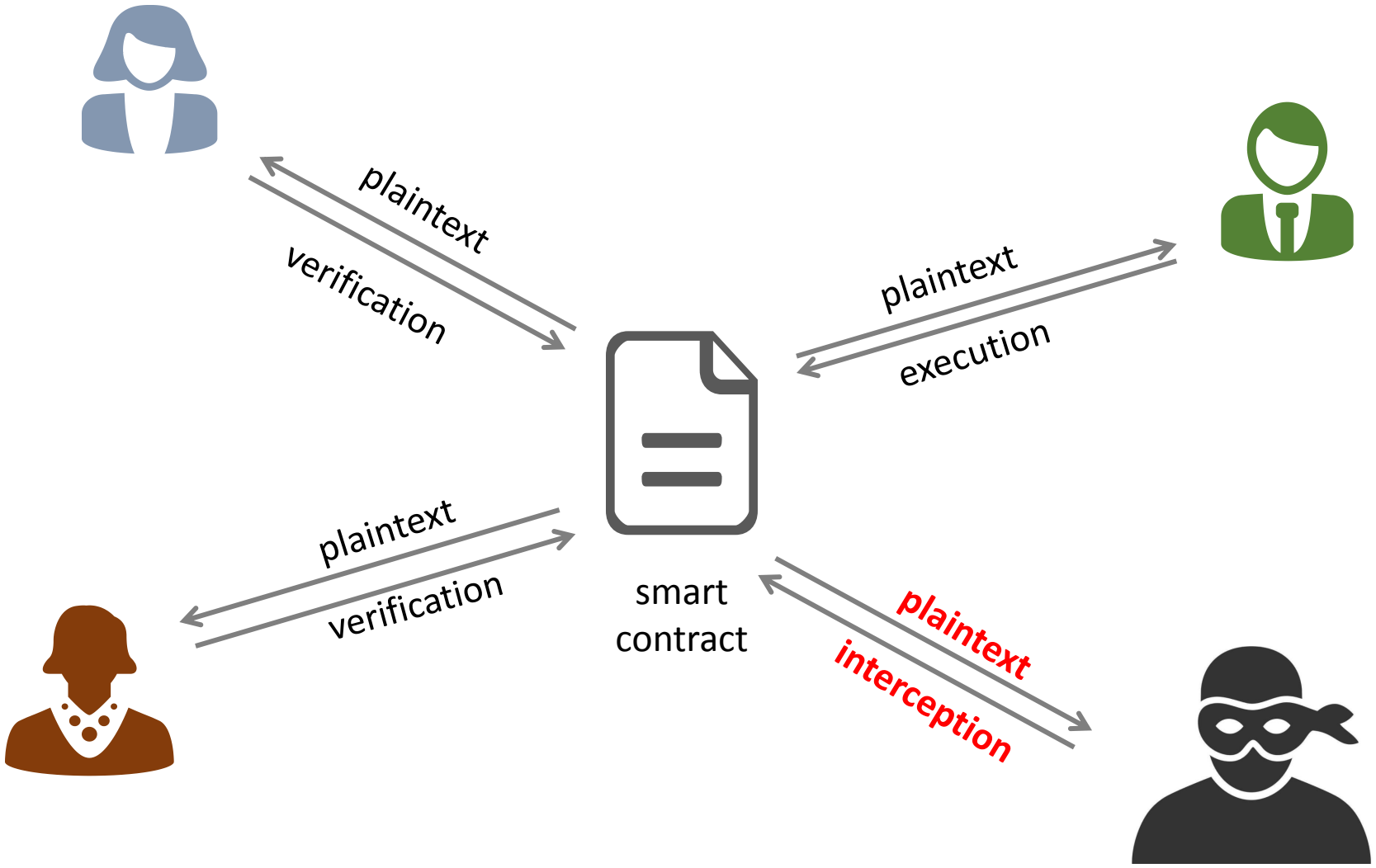
Hai-Bo Chen(陈海波)
Institute of Parallel and Distributed Systems,Shanghai Jiao Tong University

Bing-yu Zang(臧斌宇)
Institute of Parallel and Distributed Systems,Shanghai Jiao Tong University

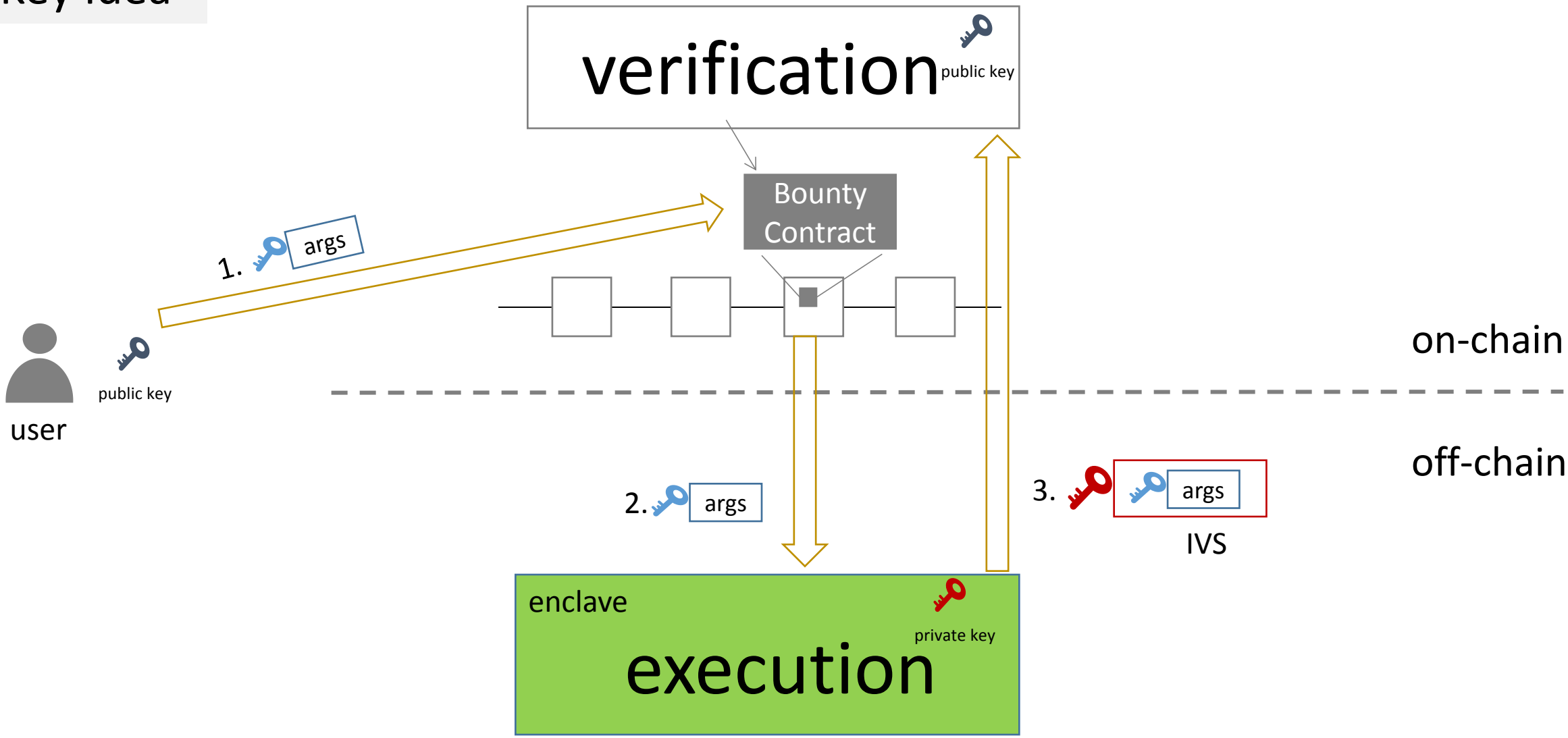
Jan Xie(谢晗剑)
Cryptape Inc.

Yuan R, Xia YB, Chen HB et al. ShadowEth: Private smart contract on public blockchain. JOURNAL OF COMPUTER SCIENCE AND TECHNOLOGY 33(3): 542–556 May 2018. DOI 10.1007/s11390-018-1839-y

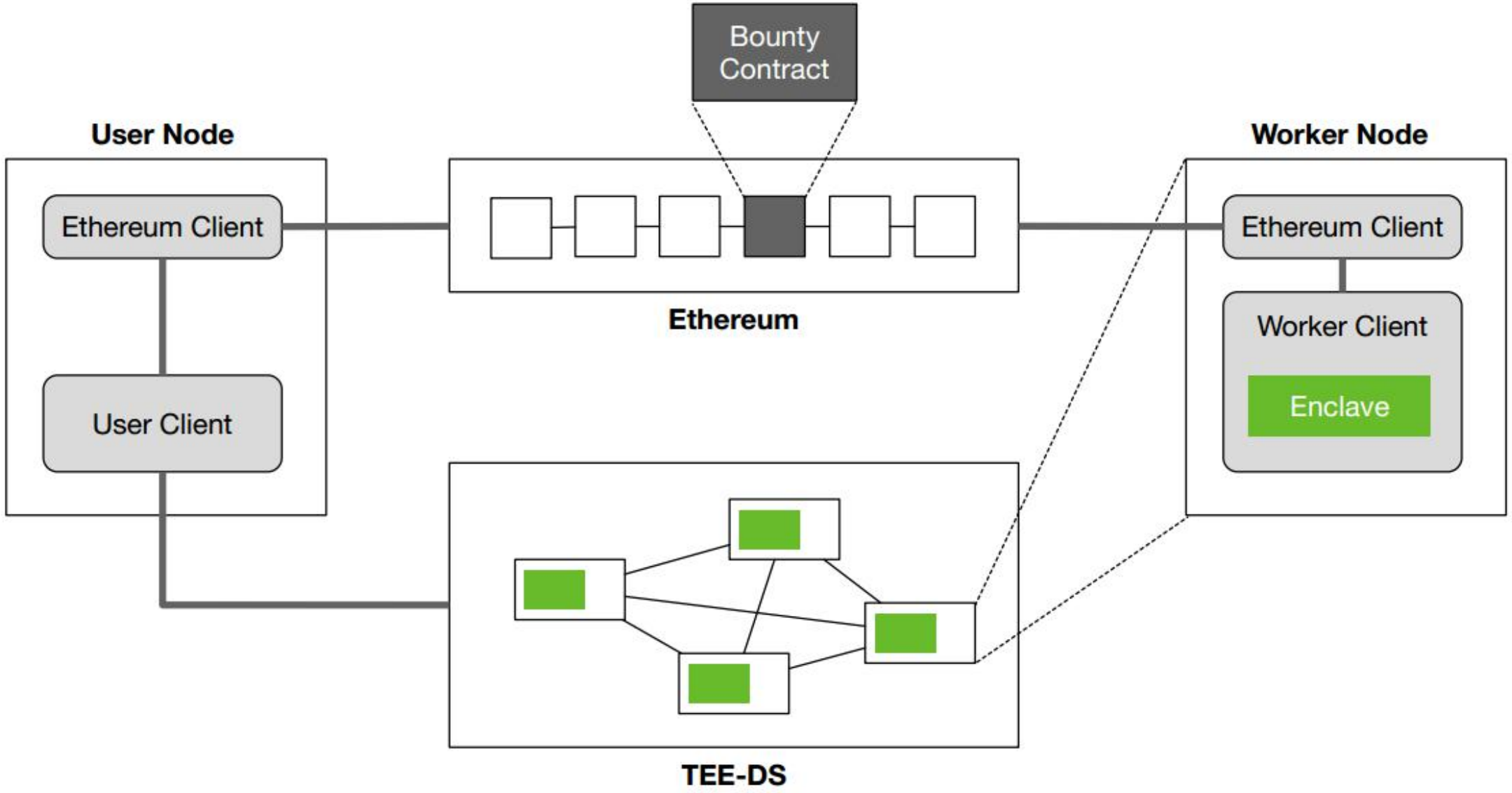
Confidentiality of smart contracts ?



Key Idea


verification
public key
Bounty Contract
1.
args
user
public key
on-chain
off-chain
2.
args
3.
args
IVS
enclave
private key
execution

System Architecture



Contribution

- It presents ShadowEth, a confidential, distributed, trust-less off-chain smart contract system clinging to existing public blockchain network without any modification
- It describes the detailed architecture and protocol of ShadowEth
- It shows the applicability of ShadowEth with three use cases
- It presents a prototype and demonstrates the security and availability of ShadowEth