PGC: Pretty Good Confidential Transaction System with Accountability

PGC Team
June 2019

Why (Ethereum's) Privacy Matters?

加密货币交易记录太过透明，有可能泄露隐私

Blockchain is so transparent that might scare users away

“Hey Bill, can you send me 0.1 ETH? Here’s my wallet address.”

Now Bill knows how much money you have.

加密货币交易记录太过透明，有可能泄露隐私

Blockchain is so transparent that might scare users away

“It’s fundamentally essential if you want corporations and large-scale investors. If you want them to use public blockchains, you’ve got to provide them with privacy … We believe that without privacy you won’t have a lot of serious enterprise users.”

Paul Brody, EY global innovation leader for blockchain

需要为加密货币提供隐私能力

What shall we build to support privacy (on Ethereum)?

- ✓ 隐藏账户余额和交易金额

  Hide balance and transaction amount.

- ✓ 支持可追责性(Accountability)，抗抵赖

  Addressing accountability to settle disputes.

- ✓ 支持ETH和ERC20

  Support ETH and ERC20 tokens.

- ✓ 基于现有公链如Ethereum，而不是开发一条新的区块链

  Build based on existed chains such as Ethereum, rather than to build a new chain.

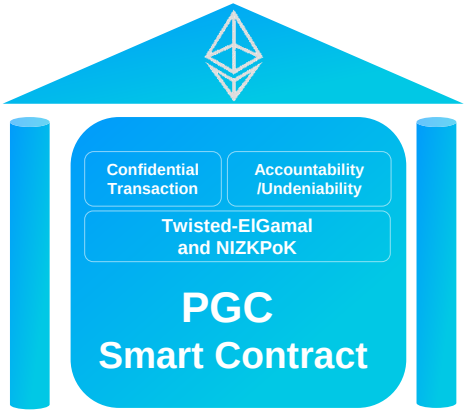
What is PGC ?

PGC Overview

PGC

加密货币银行

Practical Crypto bank

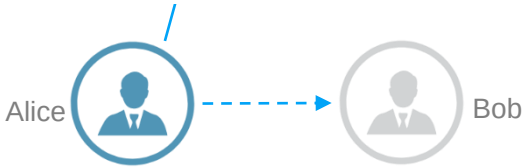


1.2) Verify CTx
Check the validity of a CT using range proof

1.3) Updates the encrypted balance of Alice and Bob

1. Alice transfers *v* coins to Bob

1.1) Creates a CTx
Alice provides a statement



2. Auditing and Accounting
Alice/Bob provides a statement
Auditors Run NIZK.Verify to check the amount hidden in the CT is indeed *v*.

General Framework of Accountable CT

Framework of Accountable Confidential Transaction System

SIG + Homomorphic PKE + NIZK

$\mathsf{Setup}(1^\lambda) \to pp$

$\mathsf{CreateCTx}(\mathsf{nonce}_1, C_1^*, pk_1, sk_1, v, pk_2)$

$C_1 \leftarrow \mathsf{Enc}(pk_1, v; r_1),\ C_2 \leftarrow \mathsf{Enc}(pk_2, v; r_2)$

$\mathsf{meta} = (\mathsf{nonce}_1, C_1^*, pk_1, C_1, pk_2, C_2)$

witness (sk_1, r_1, r_2)

π_{valid} for $(C_1^*, pk_1, C_1, pk_2, C_2) \in L_{\mathsf{valid}}$

$L_1 = \{\exists r_1, r_2 \text{ s.t. } C_i = \mathsf{Enc}(pk_i, v; r_i)\}$

$L_2 = \{\exists r_1 \text{ s.t. } C_1 = \mathsf{Enc}(pk_1, v; r_1) \wedge v \in [0, 2^\ell]\}$

$L_3 = \{\exists sk_1 \text{ s.t. } \mathsf{Dec}(sk_1, C_1^* - C_1) \in [0, 2^\ell]\}$

$\mathsf{Sign}(sk_1, (\mathsf{meta}, \pi_{\mathsf{valid}})) \to \sigma$

$\mathsf{ctx} = (\mathsf{meta}, \pi_{\mathsf{valid}}, \sigma)$ ✓

$\mathsf{RevealAcct}(sk_1, C_1^*)$

$\mathsf{CreateAcc}(pp)$

$(pk_1, sk_1) \leftarrow \mathsf{Gen}(\lambda)$

$C_1^* \leftarrow \mathsf{Enc}(pk_1, 0; r_{\mathsf{dummy}})$

$C_1^* := C_1^* - C_1$

$\mathsf{RevealAcct}(sk_2, C_2^*)$

$\mathsf{CreateAcc}(pp)$

$(pk_2, sk_2) \leftarrow \mathsf{Gen}(\lambda)$

$C_2^* \leftarrow \mathsf{Enc}(pk_2, 0; r_{\mathsf{dummy}})$

$C_2^* := C_2^* - C_2$

sk_1

sk_2

π_{correct} for $v = \mathsf{Dec}(sk_i, C_i)$

PGC: an Efficient Instantiation

PGC Instantiation

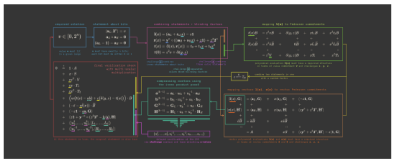
ECDSA $\Rightarrow$ Digital Signature

Twisted ElGamal $\Rightarrow$ Additive Homomorphic PKE

- same key pair for Sig and Enc $\rightsquigarrow$ largely compatible with Bitcoin, Ethereum
- statement are algebra encoded $\rightsquigarrow$ friendly to efficient Σ protocols

Σ-protocol for plaintext equivalence $\Rightarrow$ NIZK for $v_{\mathsf{in}} = v_{\mathsf{out}}$

Bulletproof + Ciphertext Refreshing + Twisted Structure $\Rightarrow$ Range proof



Σ-protocol for DLOG equivalence $\Rightarrow$ NIZK for Accountability

no trusted setup & highly efficient
based on standard DLOG assumption

PGC优势 Highlights of PGC

PGC

- ✓ 不需要在协议级别上对以太坊进行更改，轻松集成到现有钱包

  Seamlessly integrated into wallets, no need to modify any Ethereum protocol.
- ✓ 只需要一个固定的私钥就能操作账户，不需要维护很多中间状态

  Users only need a fixed secret key to check balance and spend coins.
- ✓ 不依赖可信系统设置 (Zcash等需要trust setup)

  Efficient Sigma protocols and zero-knowledge range proofs without trust setup.
- ✓ 无需带外信息交互，交易双方无需同时在线 (Mimblewimble协议需要带外信息交互)

  No out of band blinding factor transmitted.
- ✓ 任意第三方可针对单笔交易进行真实性验证，无需借助交易任一方私钥

  A transaction can be verified by anyone without disclosing secret keys of sender or receiver.

PGC优势 Highlights of PGC

- ✓ 首个支持可审计（Accountability）的机密交易方案

  Address accountability for Confidential Transaction System for the first time.
- ✓ 提出了机密交易的通用框架，数字签名+同态加密+非交互零知识证明

  Propose a generic framework of Confidential Transaction System from Combined Public-Key Scheme (Signature and Homomorphic PKE sharing the same keypair) and NIZK.
- ✓ 给出了强安全模型中的严格的安全性证明

  Give a formal rigorous proof in strong security model.

PGC

04

PGC应用场景

- ✓ 加密基金投资 Crypto funds
- ✓ 发放工资 Paying Salary in crypto
- ✓ 慈善捐助 Charitable donations
- ✓ 密封拍卖 Sealed-bid Auctions
- ✓ 稳定币大额转账 Payment channels

DEMO

PGC Contract Performance

	Avg. Gas Cost	In eth (10 Gwei)	|tx| size	EIP 1108[1] Optimization	EIP 1108[1] Optimization in eth
Deposit	212K	0.002	64 bytes	180K	0.0018
Transfer	6,563K	0.066	2980 bytes	1,100K	0.01
Withdraw All	6,285K	0.005	389 bytes	1,100K	0.004
Withdraw Part	529K	0.062	2611 bytes	410K	0.01

[1] EIP 1108 Reduce alt_bn128 precompile gas costs. https://eips.ethereum.org/EIPS/eip-1108

Hinc itur ad astra.

我们从这里走向繁星

From here the way leads to the stars.

https://pgc.info