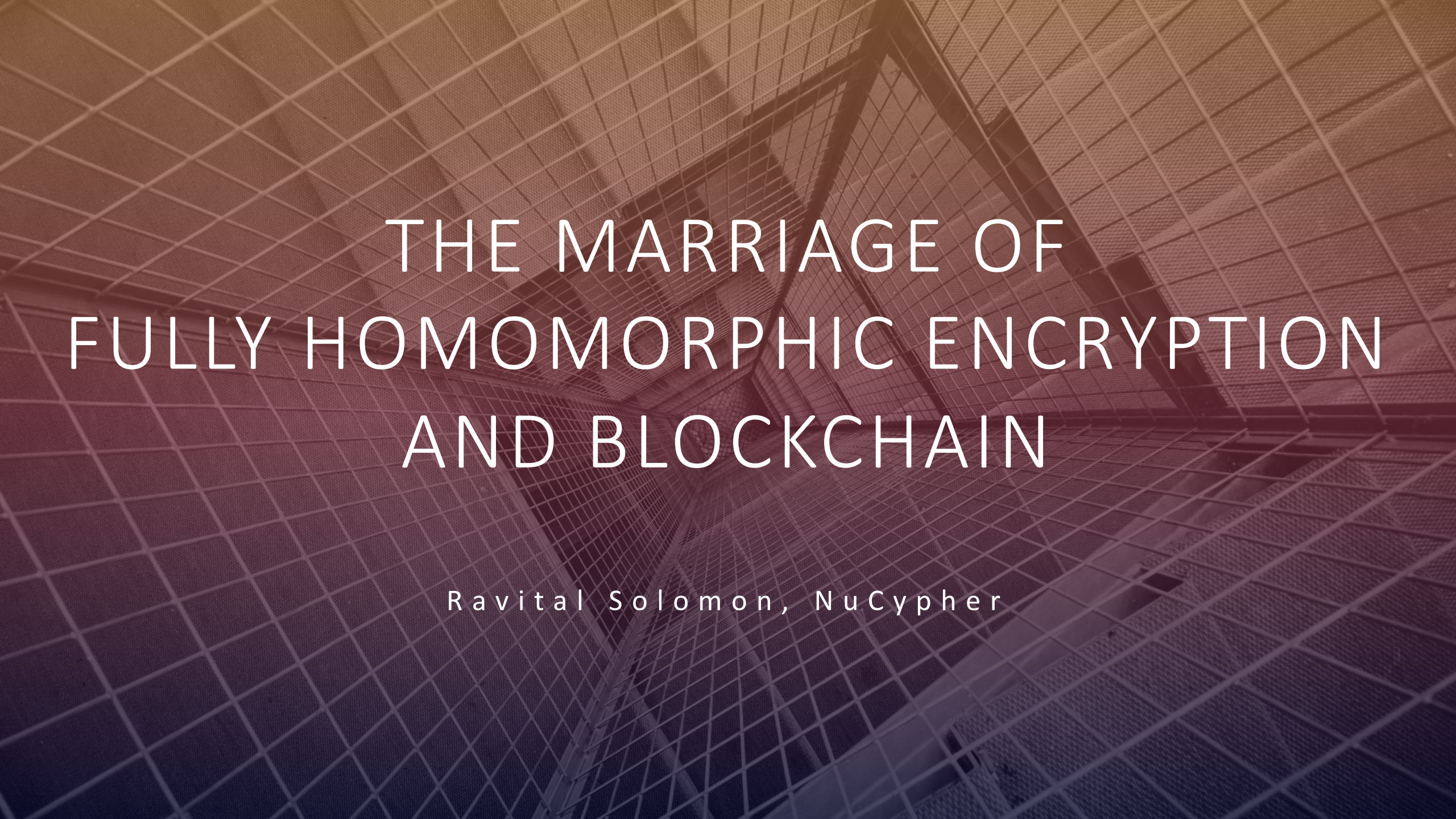


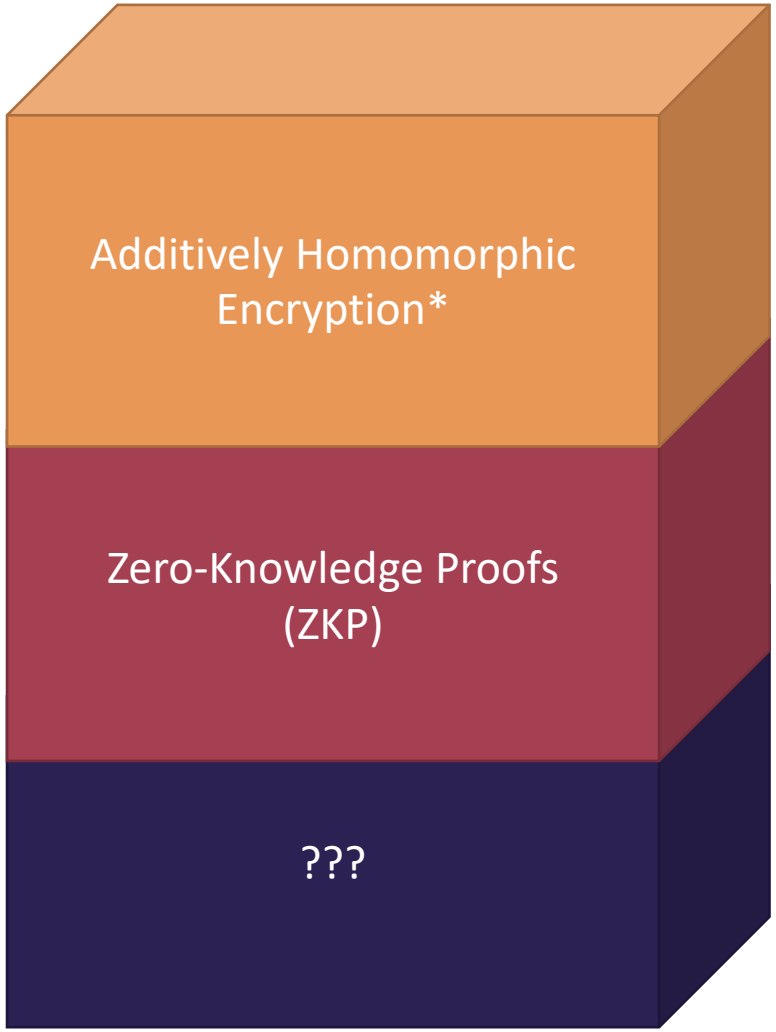
THE MARRIAGE OF FULLY HOMOMORPHIC ENCRYPTION AND BLOCKCHAIN

Ravital Solomon, NuCypher

WHAT IS A PRIVATE TRANSACTION?

- “Privacy”: Confidential vs. Anonymous
  - Confidential = hides inputs/outputs of transaction
  - Anonymous = confidential AND hides users involved
- Private Transaction
  - Minimum: Hides transaction amount, balances
  - Ideal: Hides users involved!
  - Seen in….Zcash, Monero
- Private Smart Contract
  - Viewed as extension to private transactions
  - Simple: Voting, Auctions (+)
  - Advanced: Financial derivatives (·)

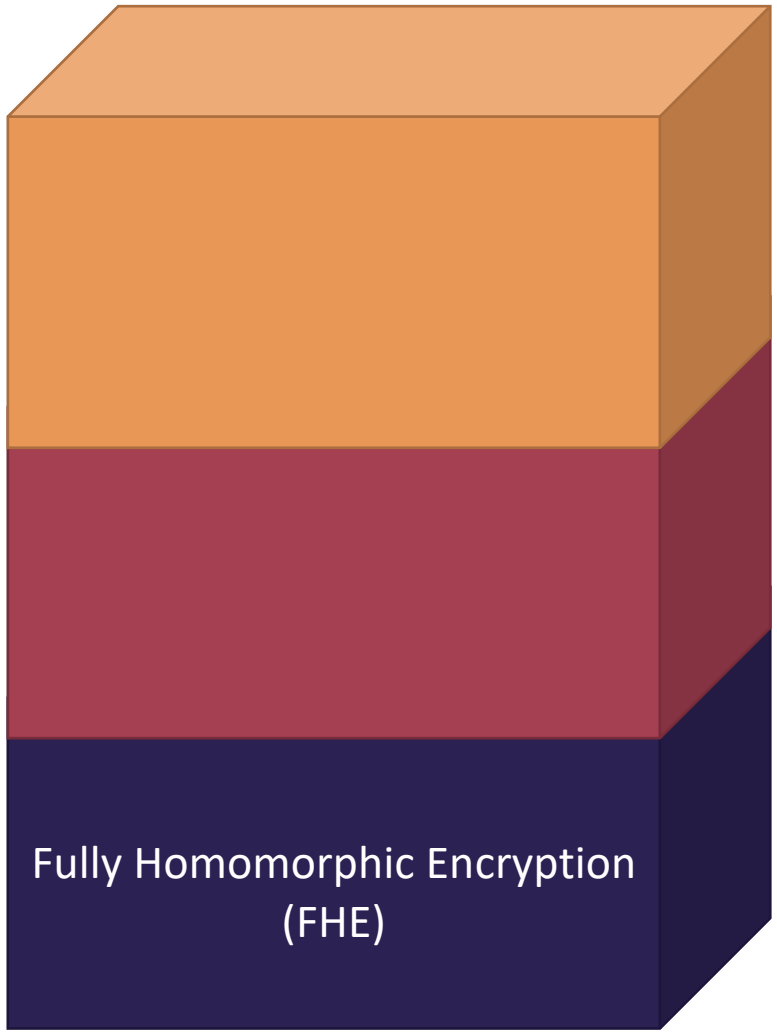
DISSECTING A PRIVATE TRANSACTION



Ingredients:

1. **Additively Homomorphic Encryption/Commitments**
   - Enc(a) + Enc(b) = Enc(a+b)
   - Enc(user's balance) + Enc(trans amnt) = Enc(user's balance after transfer)
2. **Zero-Knowledge Proofs (ZKP)**
   - Prove transfer was done correctly without revealing balances, amount to others
   - Efficient ZKPs: SNARKs (Zcash), STARKs, Bulletproofs (Monero)

THE FINAL BUILDING BLOCK?



Fully Homomorphic Encryption (FHE)

- *Additively* Homomorphic: Enc(a) + Enc(b) = Enc(a + b)
- *Multiplicatively* Homomorphic: Enc(a) · Enc(b) = Enc(a · b)
- Will allow for greater variety of functions to be represented in private smart contracts!

CHALLENGES USING FHE IN BLOCKCHAIN

1. Efficiency
   - Newer schemes more efficient for certain use cases (e.g. Microsoft's SEAL, HELib)
   - "Basic" encryption scheme—Ring-LWE encryption
2. Combining Efficient ZKPs with FHE
   - Efficient ZKPs: Elliptic curves (often)
   - FHE: Lattices
   - Recent results ([DLS19]) provide ideas for efficient combination

PRELIMINARY RESULTS

- Dual key-pair construction—best of both worlds (inspired by Zether [BAZ+19])
  - Allows for interaction between public and private accounts
  - Basic Ring-LWE Encryption Scheme (for confidential transactions)
  - Elliptic Curves/Hashes (for public transactions)
  - Ring-LWE encryption scheme sits inside certain FHE schemes
- Prototype of [DLS19]
  - Ring-LWE Encryption + Bulletproofs
  - Backbone of confidential transactions

PRELIMINARY RESULTS

- Prototype of [DLS19]*
  - Performed on Intel i7 @ 2.6 GHz
  - Application to verifiable encryption (using ring-lwe encryption + bulletproofs variant)
  - Encrypt in <1.3ms; decrypt in <600µs on average

Secp256k1	1 thread	6 threads
Prover time	70s	14.9s
Verifier time	47s	9.7s
Initial proof generation	16s	3.23s

Curve25519	1 thread	6 threads
Prover time	34.6s	8.2s
Verifier time	23.7s	5.2s
Initial proof generation	2.15s	434ms