HKU Coin: Towards Decentralized Privacy-Preserving Cryptocurrency with Accountability

Dr. Allen Au (allenau@cs.hku.hk)

Associate Professor

Department of Computer Science

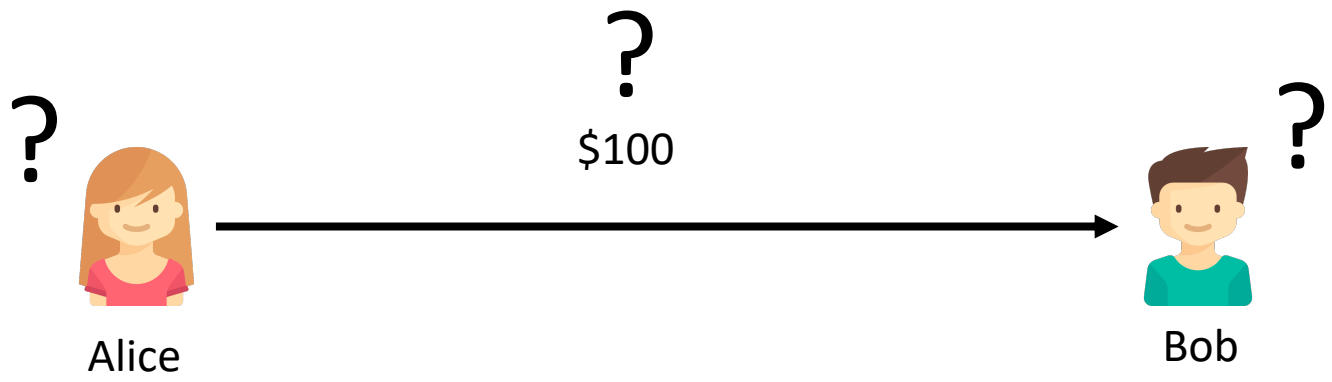
Faculty of Engineering

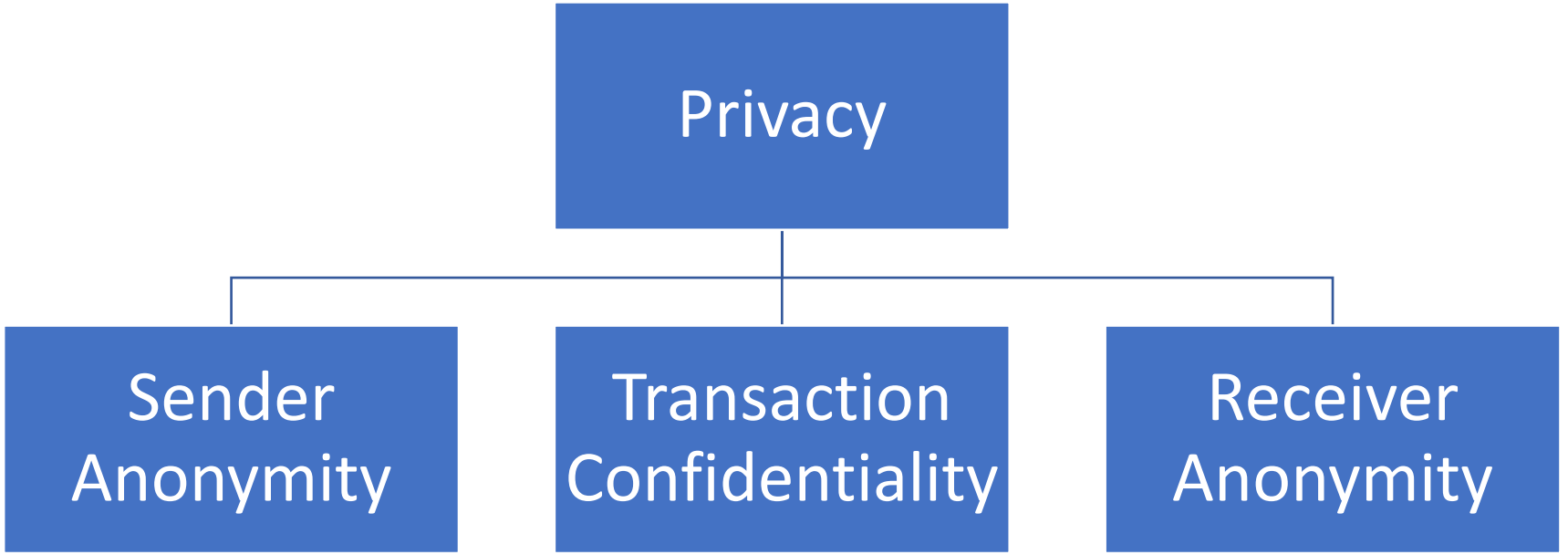
Outline

- Background
- Requirements of HKU Coin
- Design Philosophy of HKU Coin
- Building Blocks
  - Homomorphic Encryption - Twisted ElGamal Encryption
  - Ring Signatures - DualRing
- Conclusion

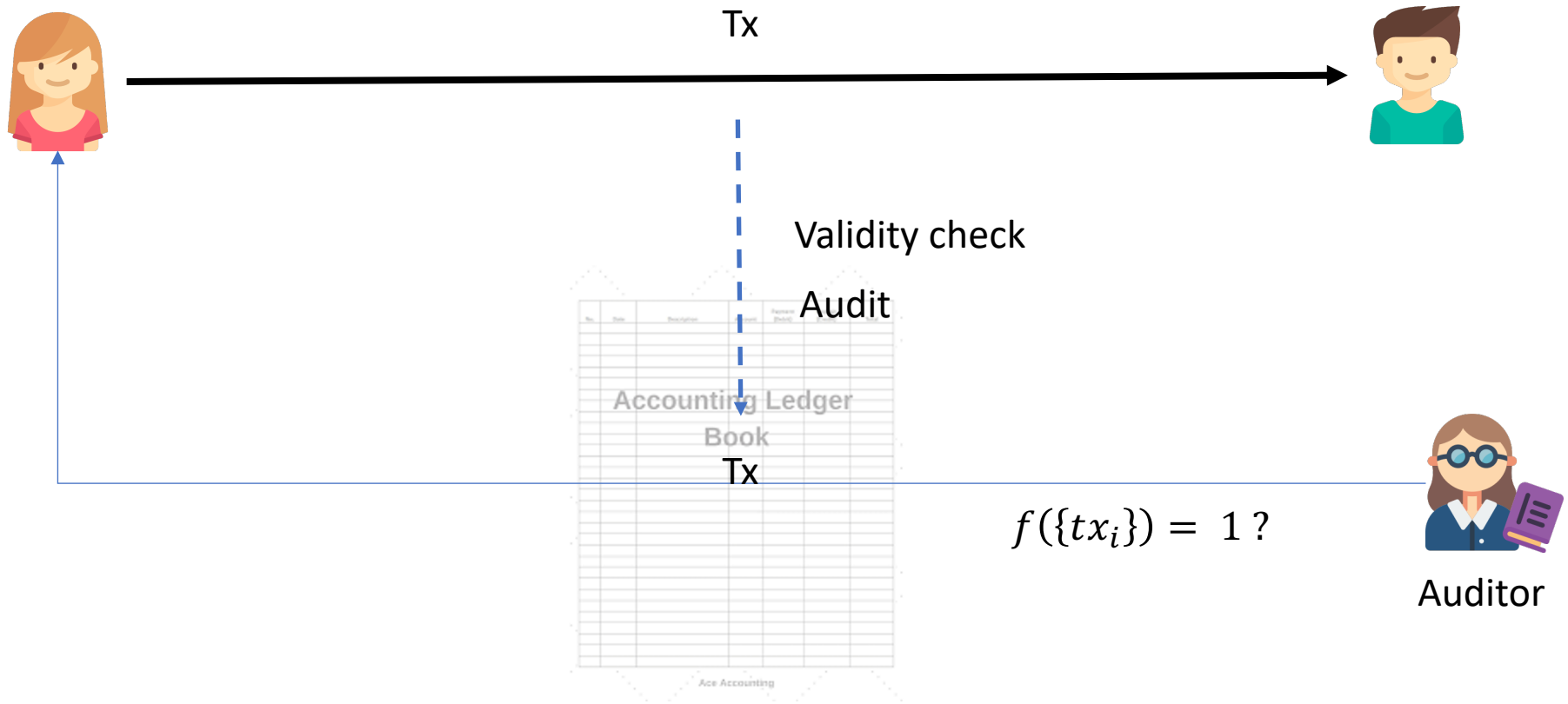
Background

Privacy in Payment System

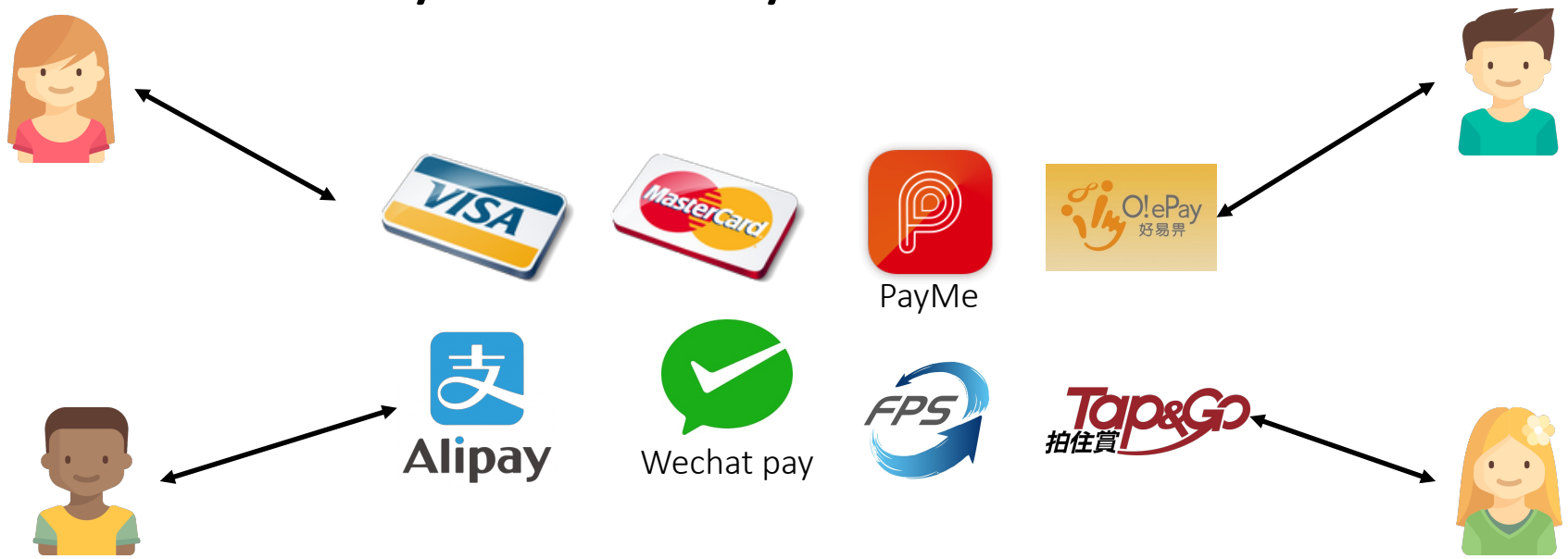




Accountability in Payment System

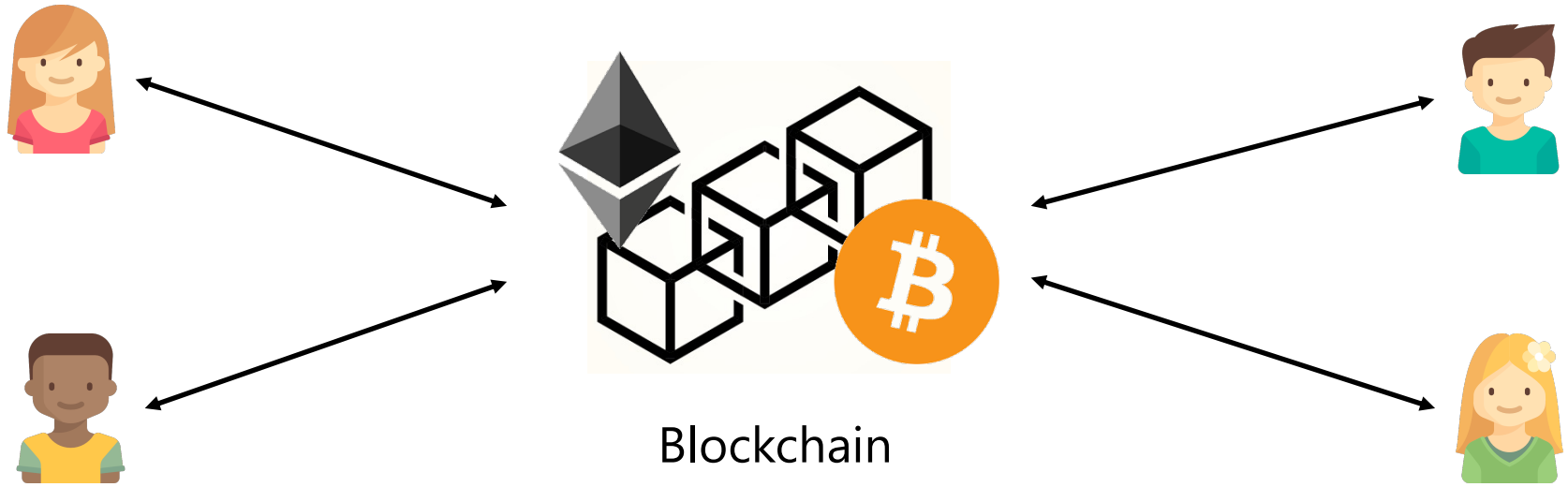


Centralized Payment System



- txs are kept on a private ledger managed by a central authority (e.g., bank)
- The authority is responsible for validity check, conduct audit, as well as privacy protection

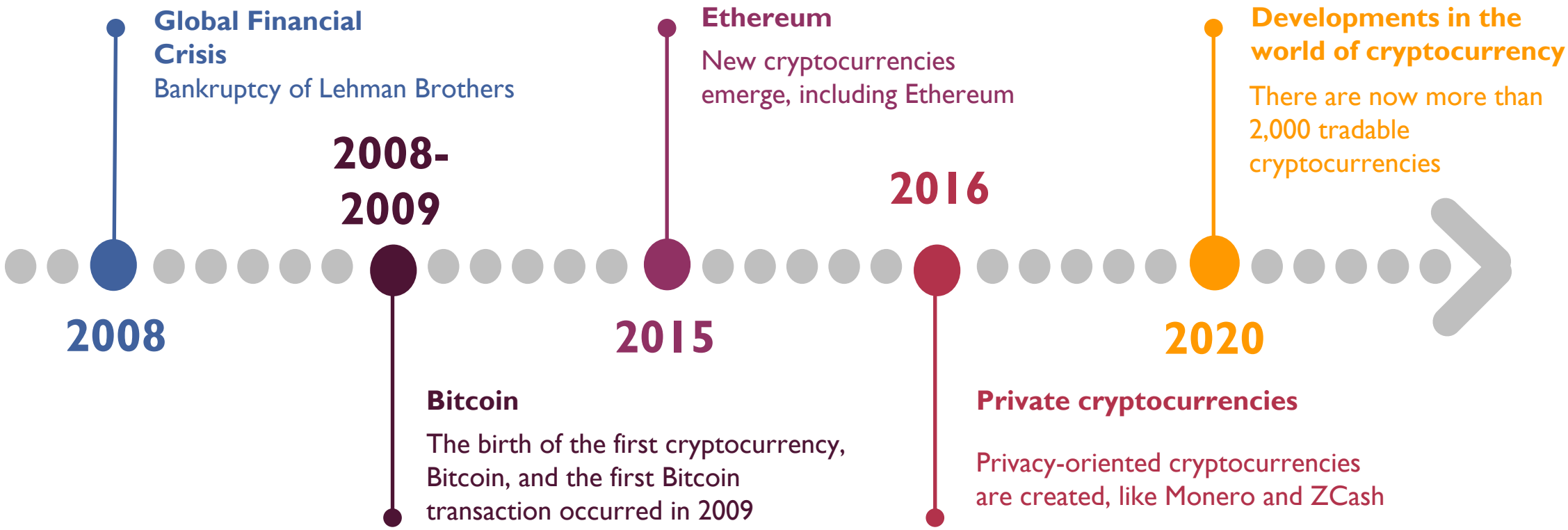
Decentralized Payment System (Blockchain-Based Cryptocurrencies)



- txs are kept on a global distributed public ledger - blockchain
- To allow validity check by all nodes in the system, blockchain-based cryptocurrencies Bitcoin and Ethereum, among others, simply expose all tx information publicly, i.e., there is no privacy in these systems

Motivation of HKU Coin

- Privacy and Accountability are crucial in any financial system



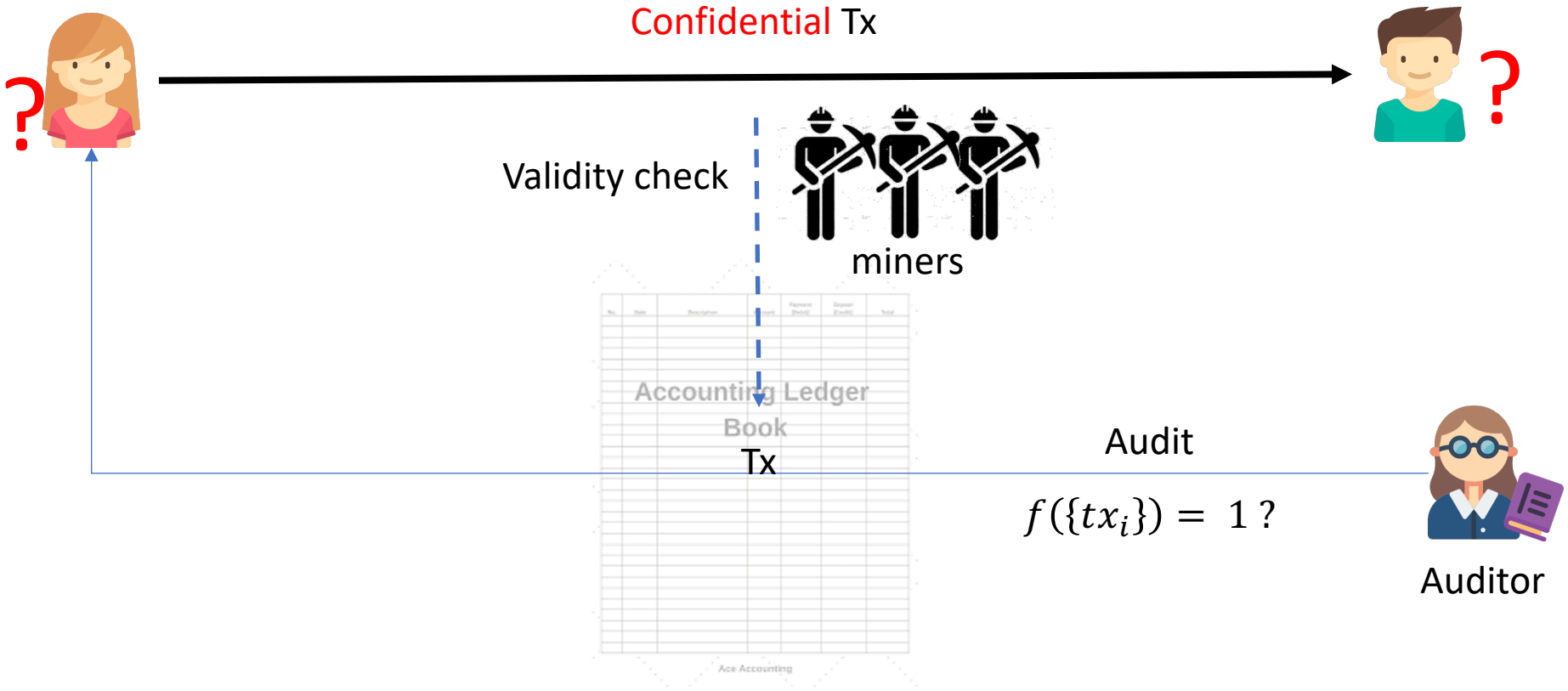
Can we achieve privacy and accountability simultaneously in the decentralize setting?

Requirements of HKU Coin

HKU Coin: Design Goal

- A blockchain-based decentralized cryptocurrency to provide privacy and accountability simultaneously
  - Account-Based Model
  - Sender Anonymity
  - Receiver Anonymity
  - Transaction Confidentiality
  - Decentralization
  - Accountability

Simplified System Model



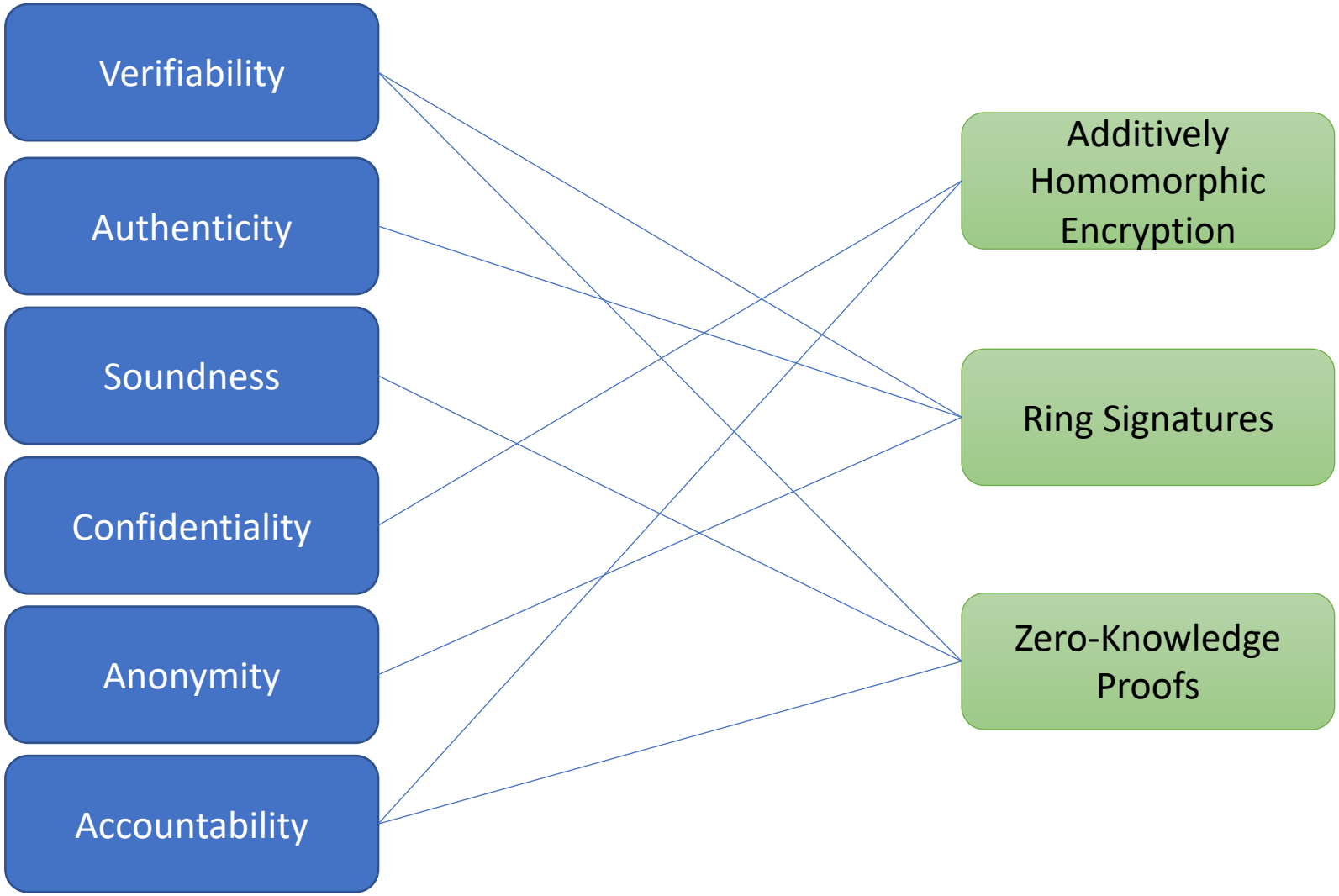
Security Requirements

- Public Verifiability - validity of txs are publicly verifiable
- Authenticity – only the sender can generate txs
- Soundness – no one can generate an illegal tx that passes verification
- Confidentiality – no one can learn the transfer amount
- Anonymity* - no one can learn the identity of the sender and receiver
- Accountability – auditor can conduct audit, users cannot provide incorrect information about all txs it has participated

*we consider a strong form of anonymity which requires that actions from the same user are unlinkable

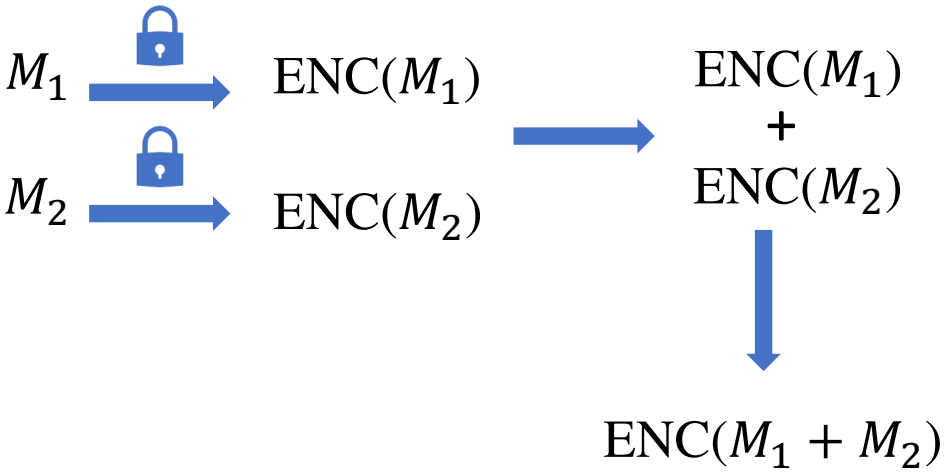
Design Philosophy of HKU Coin

Building Blocks of our Construction



Confidentiality

- All account balances are encrypted by an additively Homomorphic Encryption (HE) so that only the owner can review the details.



Account Balance

A	18
B	22
C	32
D	18
E	16

Account Balance in Blockchain

A	Enc(18)
B	Enc(22)
C	Enc(32)
D	Enc(18)
E	Enc(16)

Twisted El Gamal Encryption

Joint work with Yu Chen, Xuecheng Ma and Cong Tang

Twisted El Gamal Encryption

- Public Parameter: g
- Public / Secret key: $(pk, sk) := (g^x, x)$
- Encryption: $(c_1, c_2) := (\mathrm{g}^m pk^r, g^r)$
- Decryption: $\mathrm{g}^m := c_1 c_2^{-x}$, solve* DL of g^m

- Public Parameter: g, h
- Public / Secret key: $(pk, sk) := (g^x, x)$
- Encryption: ~~$(c_1, c_2) :=$~~ $(h^m g^r, pk^r)$
- Decryption: $h^m := c_1 c_2^{-\frac{1}{x}}$, solve* DL of h^m

The same format as a Pedersen Commitment. Can use ZKP directly

ElGamal Encryption ⟺ Twisted ElGamal Encryption

As secure and efficient as the original ElGamal Encryption

* Assume m is small

Twisted ElGamal

Comparison with State-of-the-Art PHE (Paillier Encryption)

Scheme	KeyGen	Encryption	Decryption	Addition	Key Size	Ciphertext Size
Paillier	1644.53ms	32.211ms	31.367ms	0.0128ms	374 bytes	768 bytes
Twisted ElGamal	0.0151ms	0.114ms	1ms	0.0031ms	33 bytes	66 bytes

Scheme	One-time Setup Cost	Public Parameters
Paillier	-	-
Twisted ElGamal	56s	66 bytes

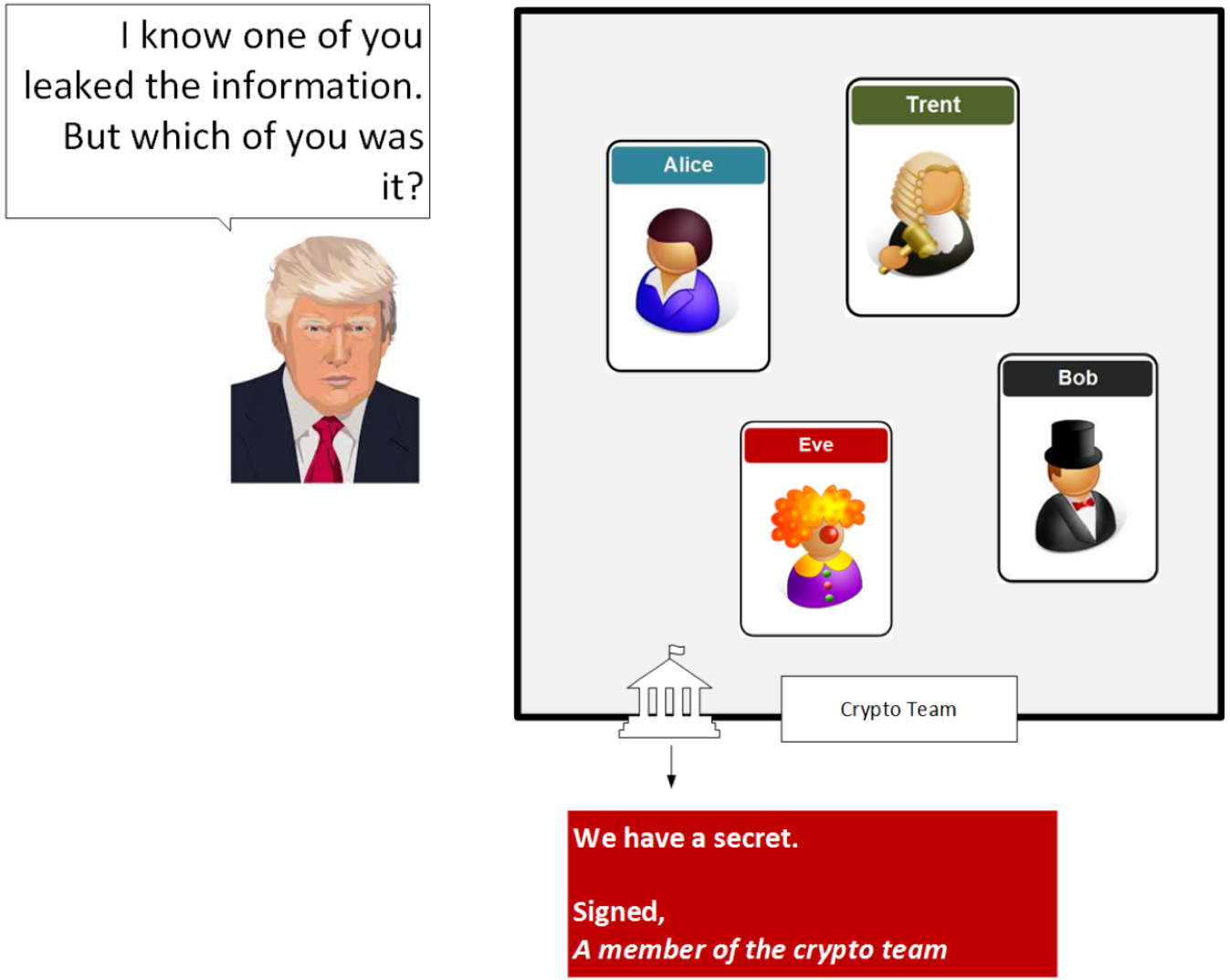
Assume 32-bit message space

DualRing

Joint work with Tsz Hon Yuen, Muhammed F. Esgin, Joseph K. Liu and Zhimin Ding

Slides adapted from Joseph K. Liu's presentation

Ring Signatures



https://medium.com/asecuritysite-when-bob-met-alice/ring-signatures-and-anonymisation-c9640f08a193

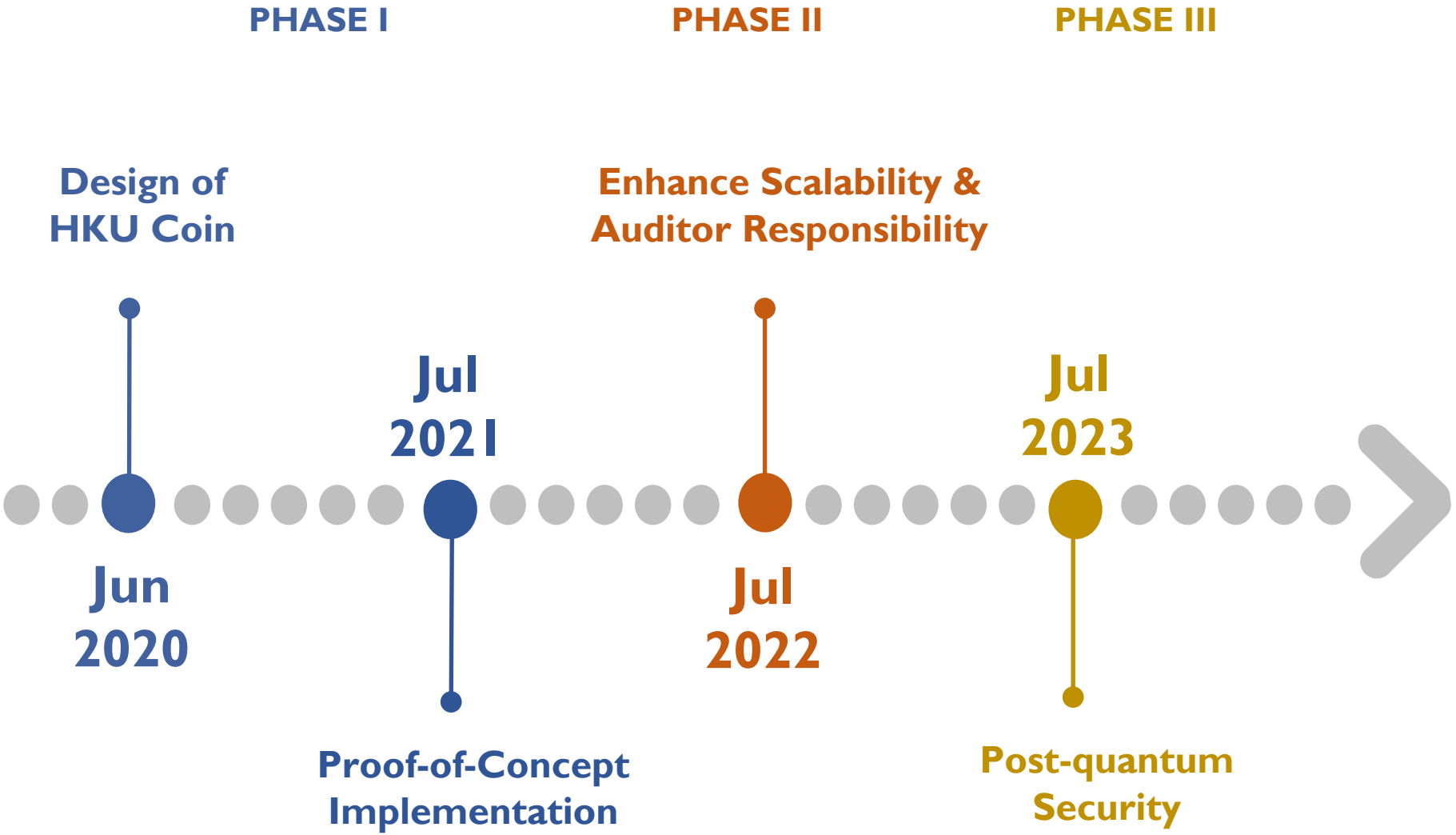
Conclusions

- We present the design of HKU coin, an account-based, efficient privacy-preserving decentralized cryptocurrencies with accountability
- Simple & Modular
- Transparent Setup

Future Work

- Allow users to generate audit report by himself/herself
- More complex audit policy
- Ensure rightful use of data by auditors
- Post-Quantum Security

Timeline


PHASE I
PHASE II
PHASE III
Design of HKU Coin
Enhance Scalability & Auditor Responsibility
Jul 2021
Jul 2023
Jun 2020
Jul 2022
Proof-of-Concept Implementation
Post-quantum Security

References

- [Bulletproofs] B. Bunz, J. Bootle, D. Boneh, A. Poelstra, P. Wuille, G. Maxwell. Bulletproofs: Short Proofs for Confidential Transactions and More. IEEE S&P 2018
- [DualRing] T.H. Yuen, M. F. Esgin, J.K. Liu, M. H. Au, Z. Ding. DualRing: Generic Construction of Ring Signatures with Efficient Instantiations. CRYPTO 2021
- [PGC] Y. Chen, X. Ma, C. Tang, M. H. Au. PGC: Decentralized Confidential Payment System with Auditability. ESORICS 2020.
- [zkLedger] N. Narula, W. Vasquez, M. Virza. Privacy-Preserving Auditing for Distributed Ledgers. NSDI 2018.
- [Zether] B. Bunz, S. Agrawal, M. Zamani, D. Boneh. Zether: Towards Privacy in a Smart Contract World. FC 2020.

Questions and comments are welcome!

Project Team Members

Dr. Allen Au

Ms. Karina Ko

Mr. Franky Lau

Ms. Mengling Liu

Dr. Xingye Lu