zkFOCIL

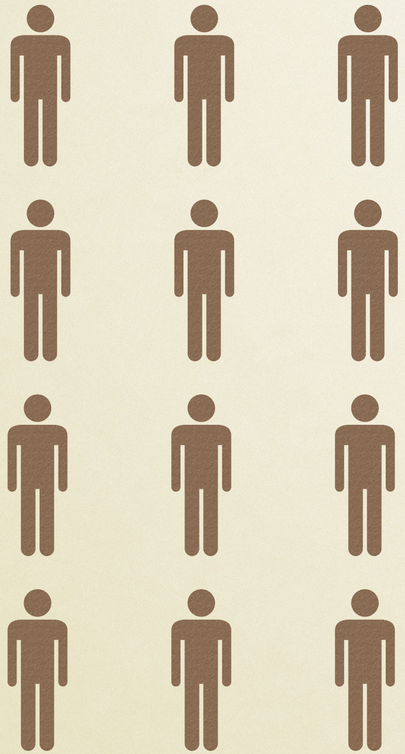
George, Thomas, Benedikt

Talk By Benedikt

Ethereum Foundation Cryptography Research

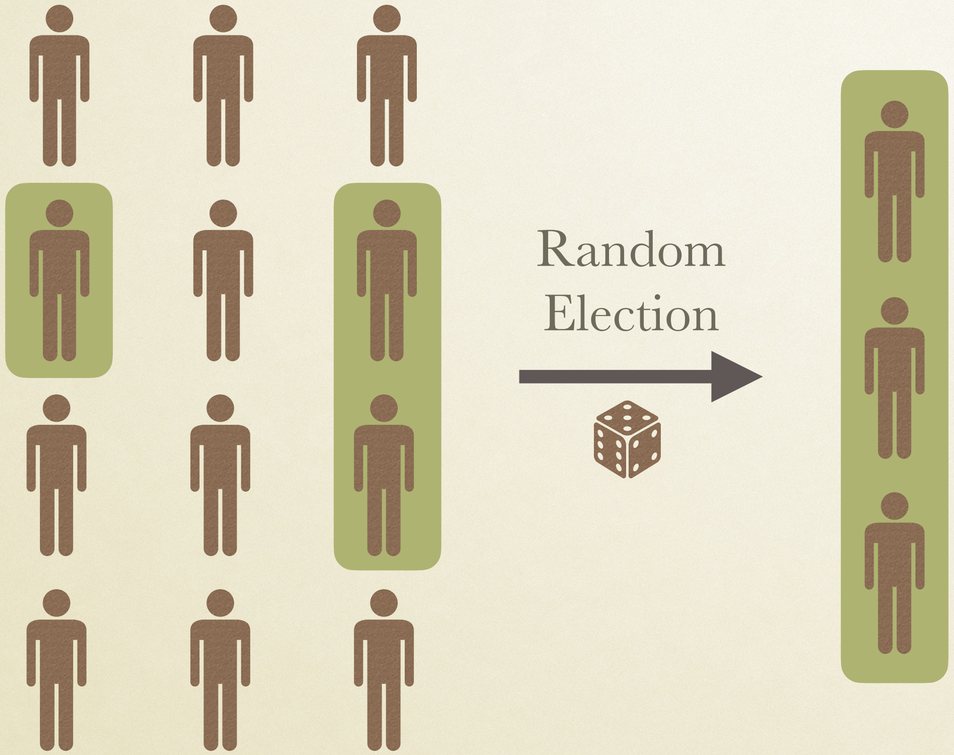
Recap: FOCIL

Recap: FOCIL



Validators

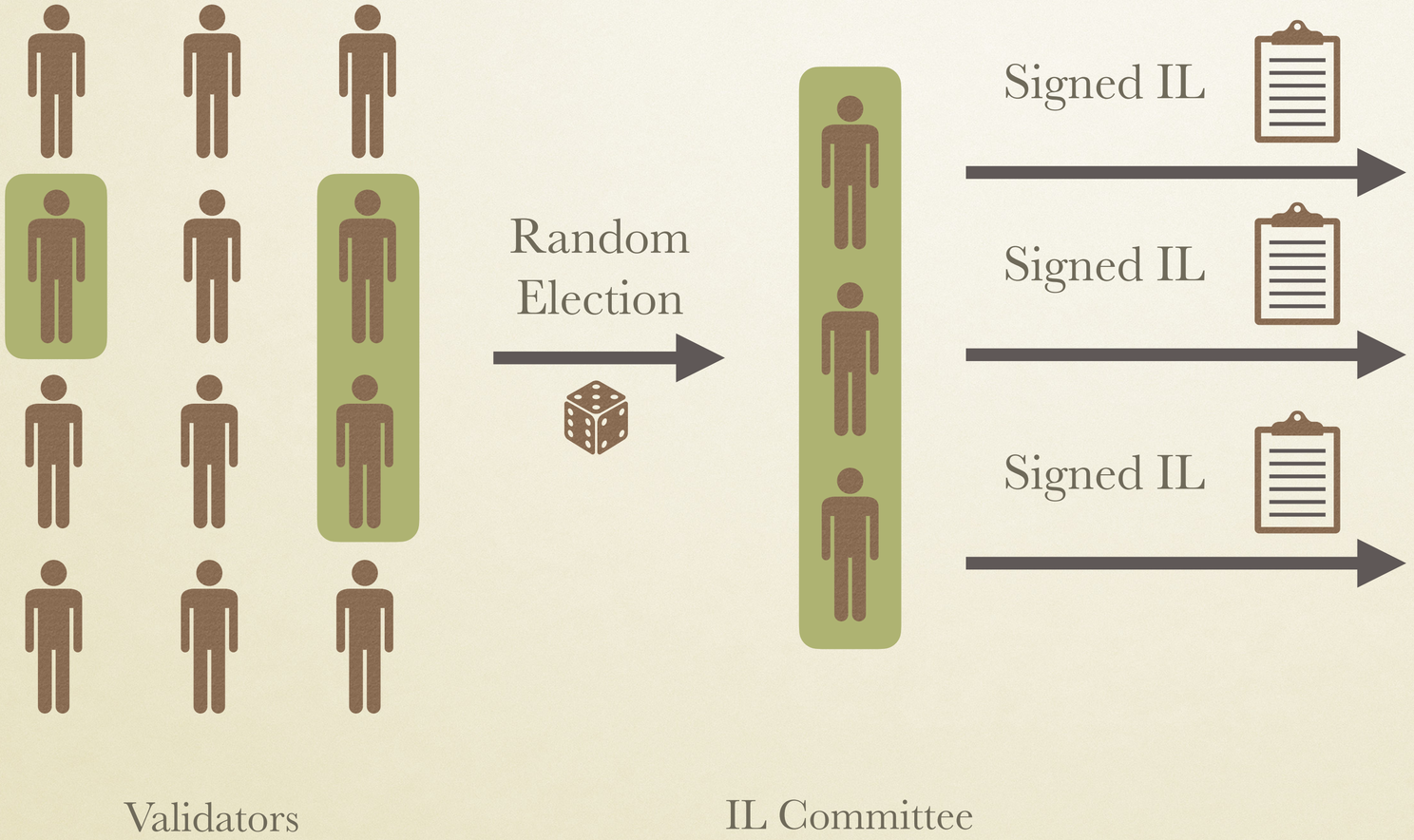
Recap: FOCIL



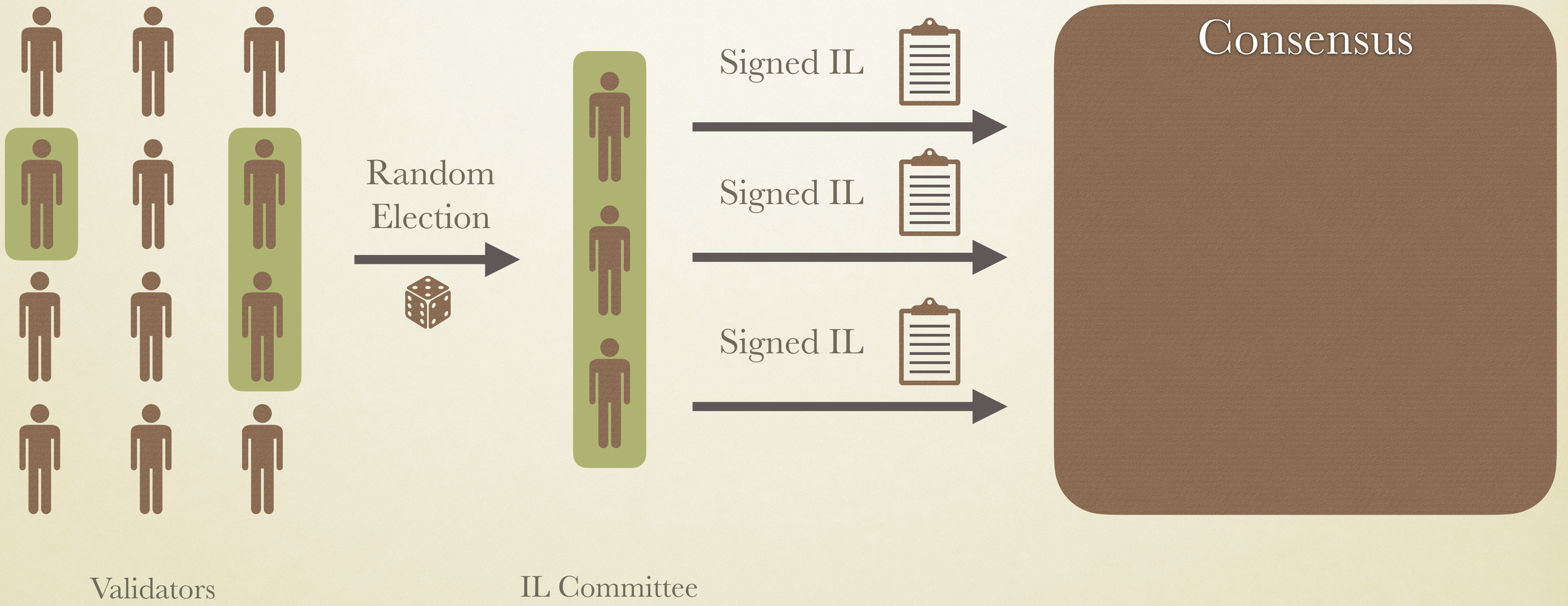
Validators

IL Committee

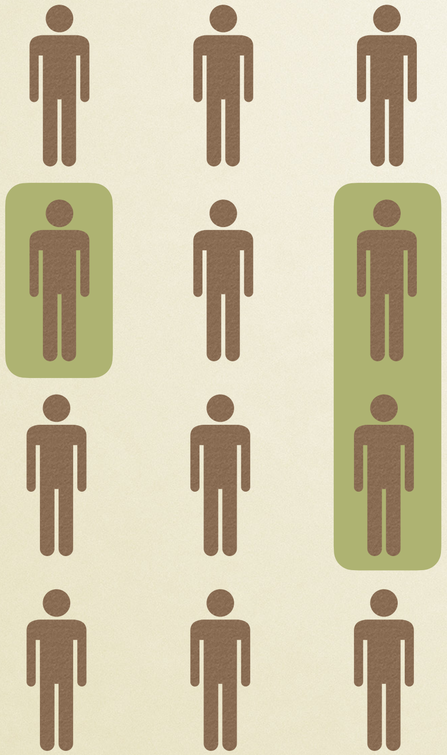
Recap: FOCIL


Random
Election
Signed IL
Signed IL
Signed IL
Validators
IL Committee

Recap: FOCIL


Random
Election
Signed IL
Signed IL
Signed IL
Consensus
Validators
IL Committee

Recap: FOCIL



Validators

Random Election

IL Committee

Signed IL

Signed IL

Signed IL

Consensus

IF

Signed by committee member

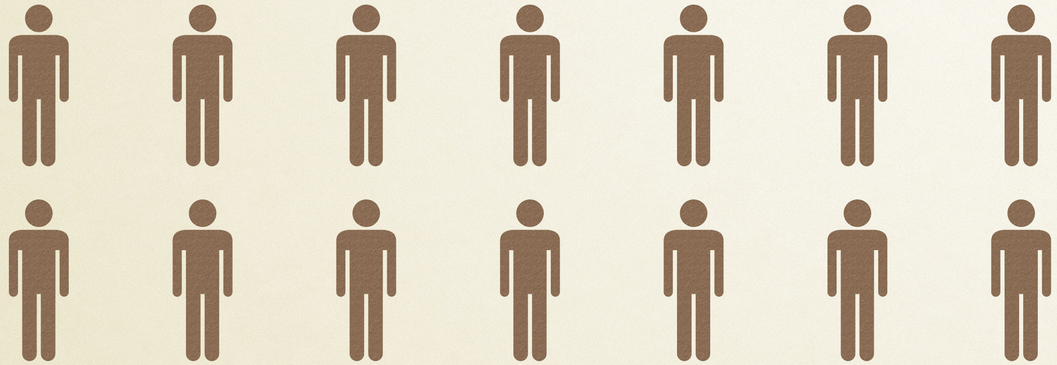
THEN

Force inclusion

Recap: FOCIL

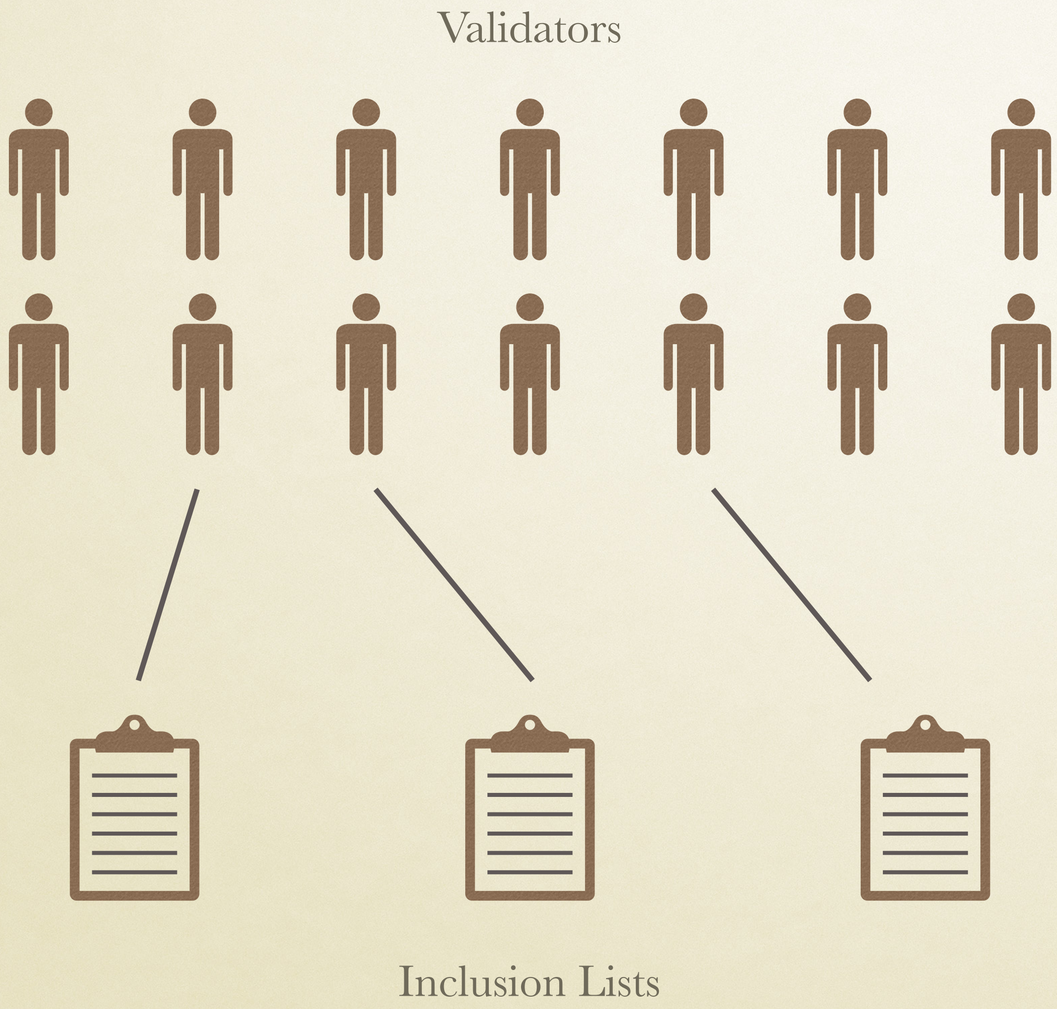
Recap: FOCIL

Validators

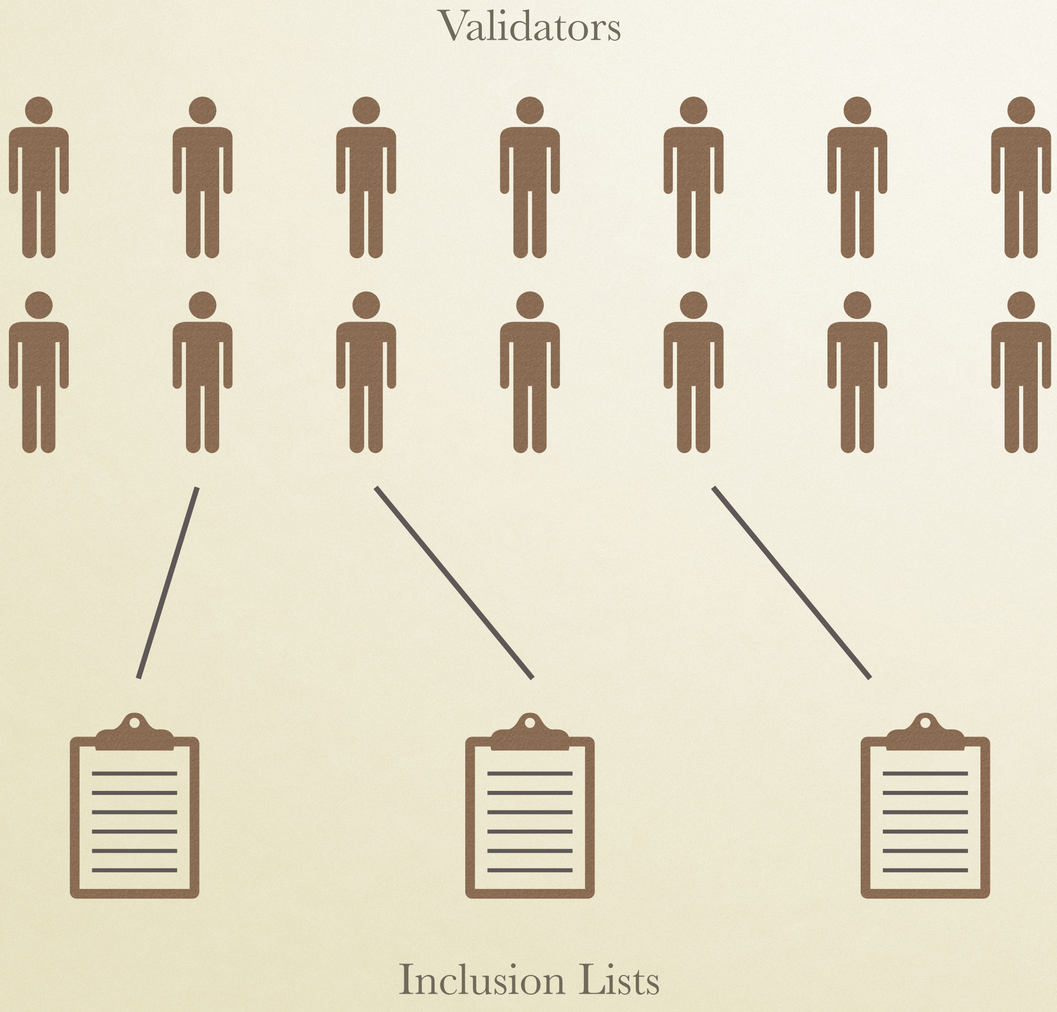


Inclusion Lists

Recap: FOCIL



Recap: FOCIL



Can we hide the link?

Goals of zkFOCIL

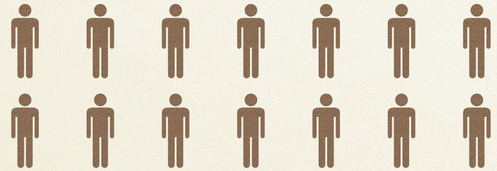
Goals of zkFOCIL

Security

Goals of zkFOCIL

Security

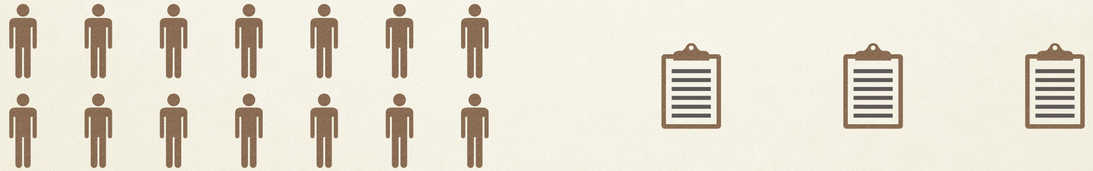
ILs Unlinkable + Hidden Committee



Goals of zkFOCIL

Security

ILs Unlinkable + Hidden Committee

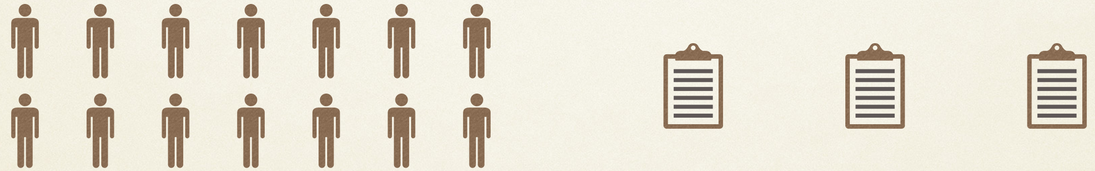


Unbiased Committee Election

Goals of zkFOCIL

Security

ILs Unlinkable + Hidden Committee



Unbiased Committee Election

Applicability

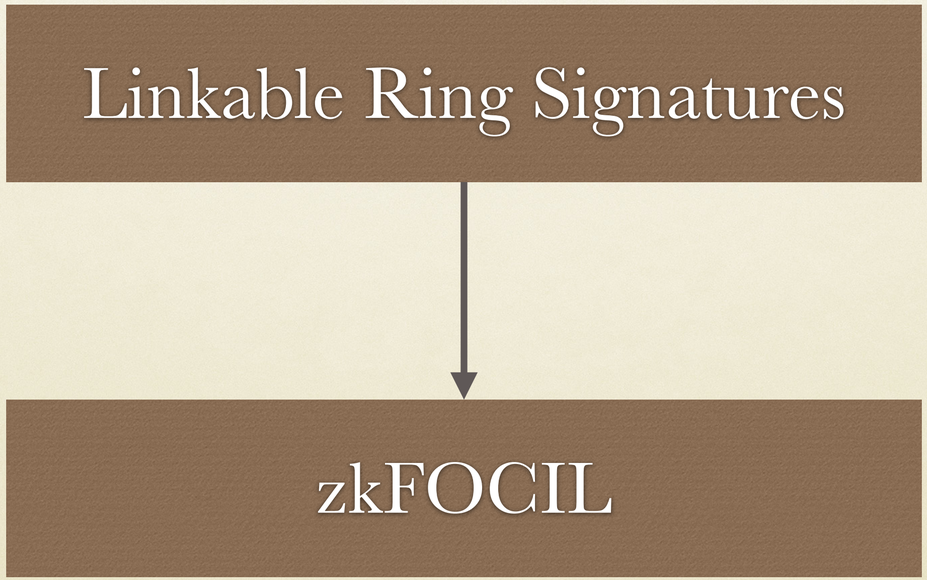
Efficiency Conceptual Simplicity Minimal Protocol Changes

Towards a Construction

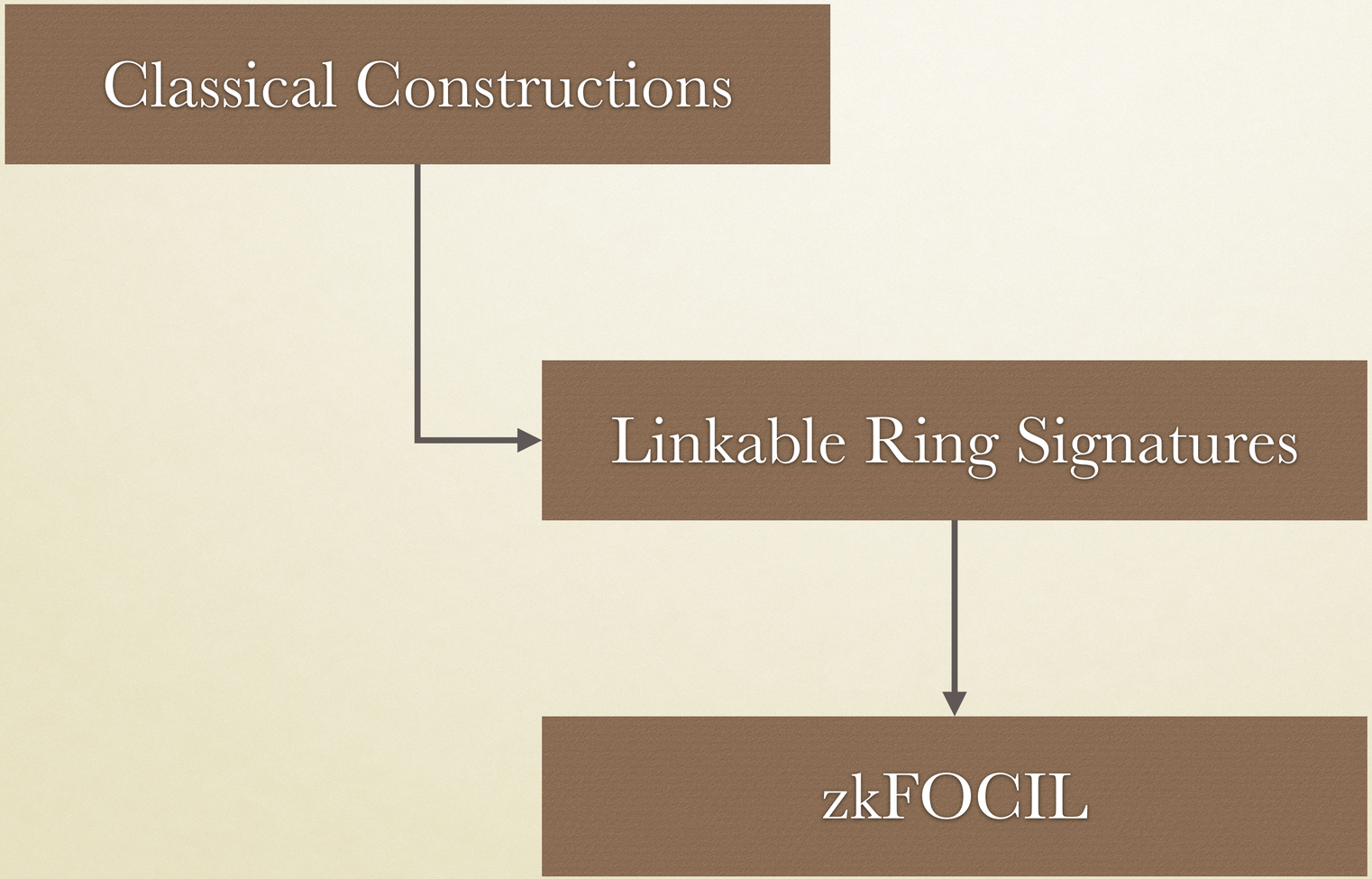
Towards a Construction

zkFOCIL

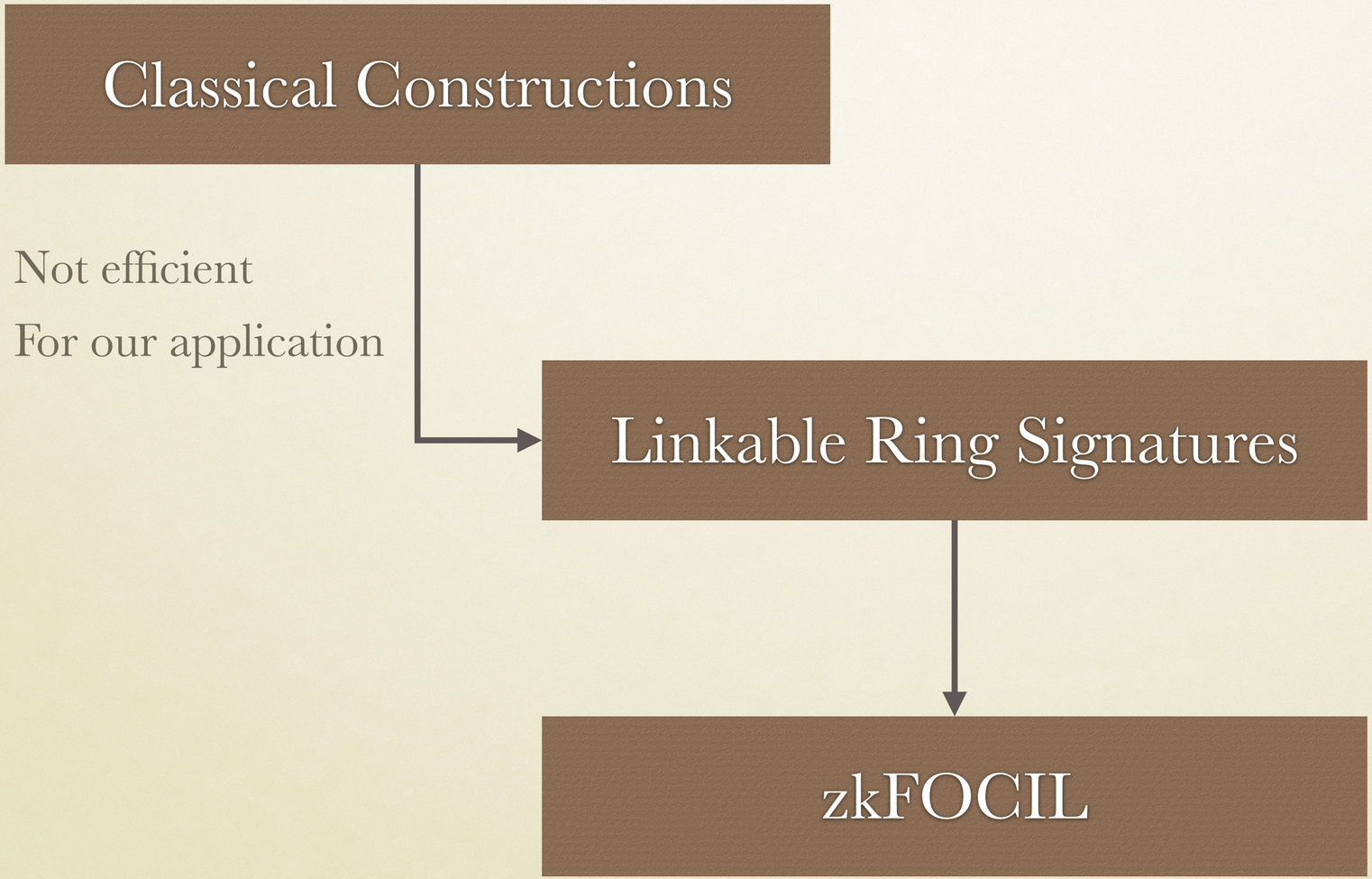
Towards a Construction



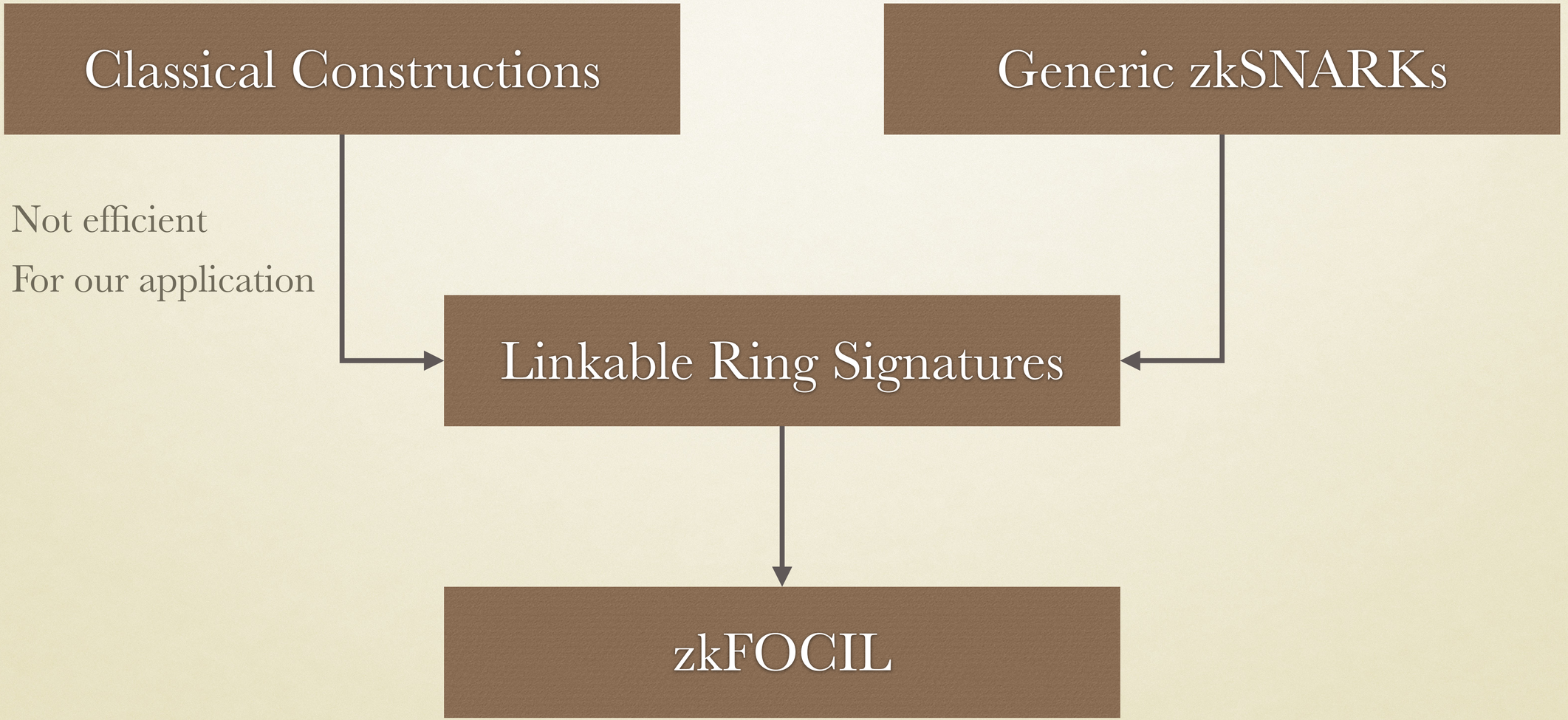
Towards a Construction



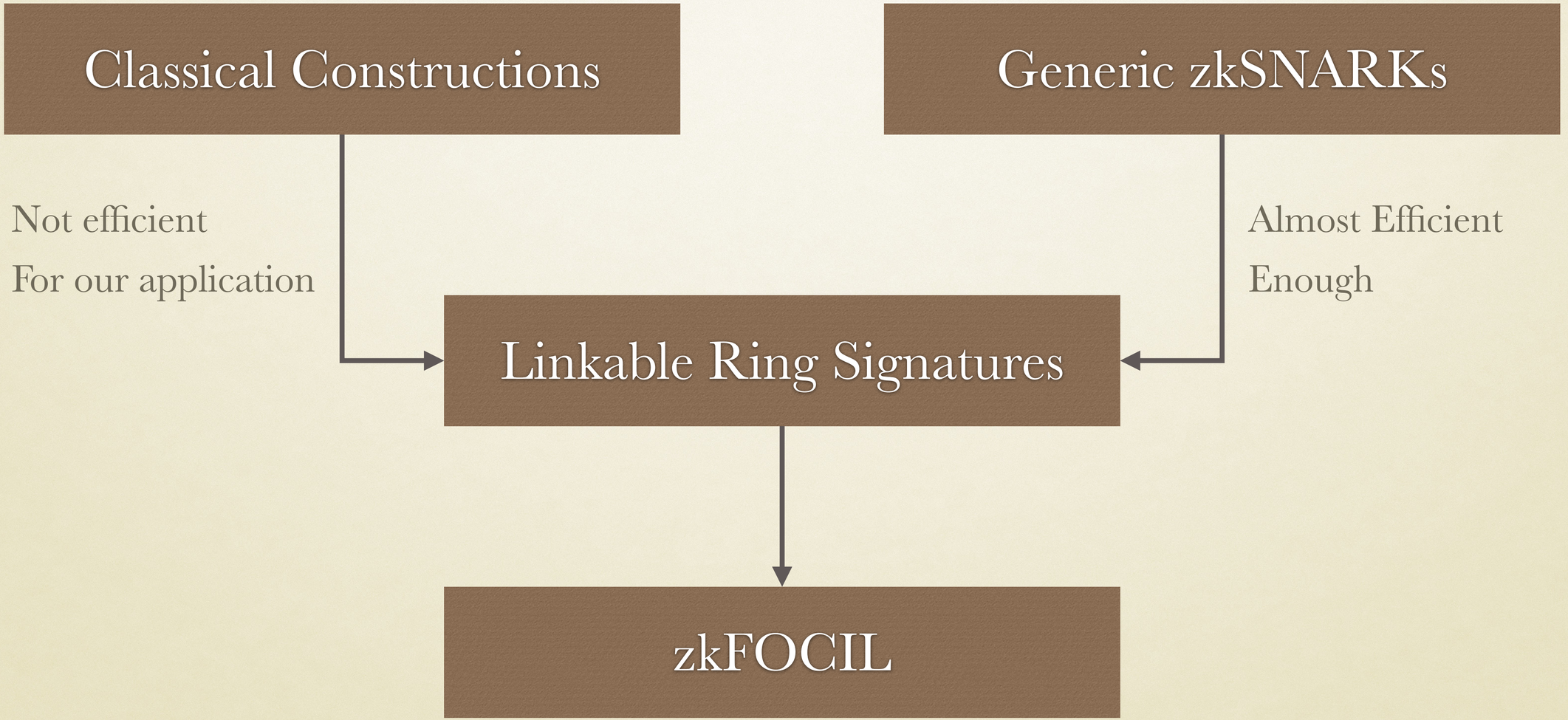
Towards a Construction



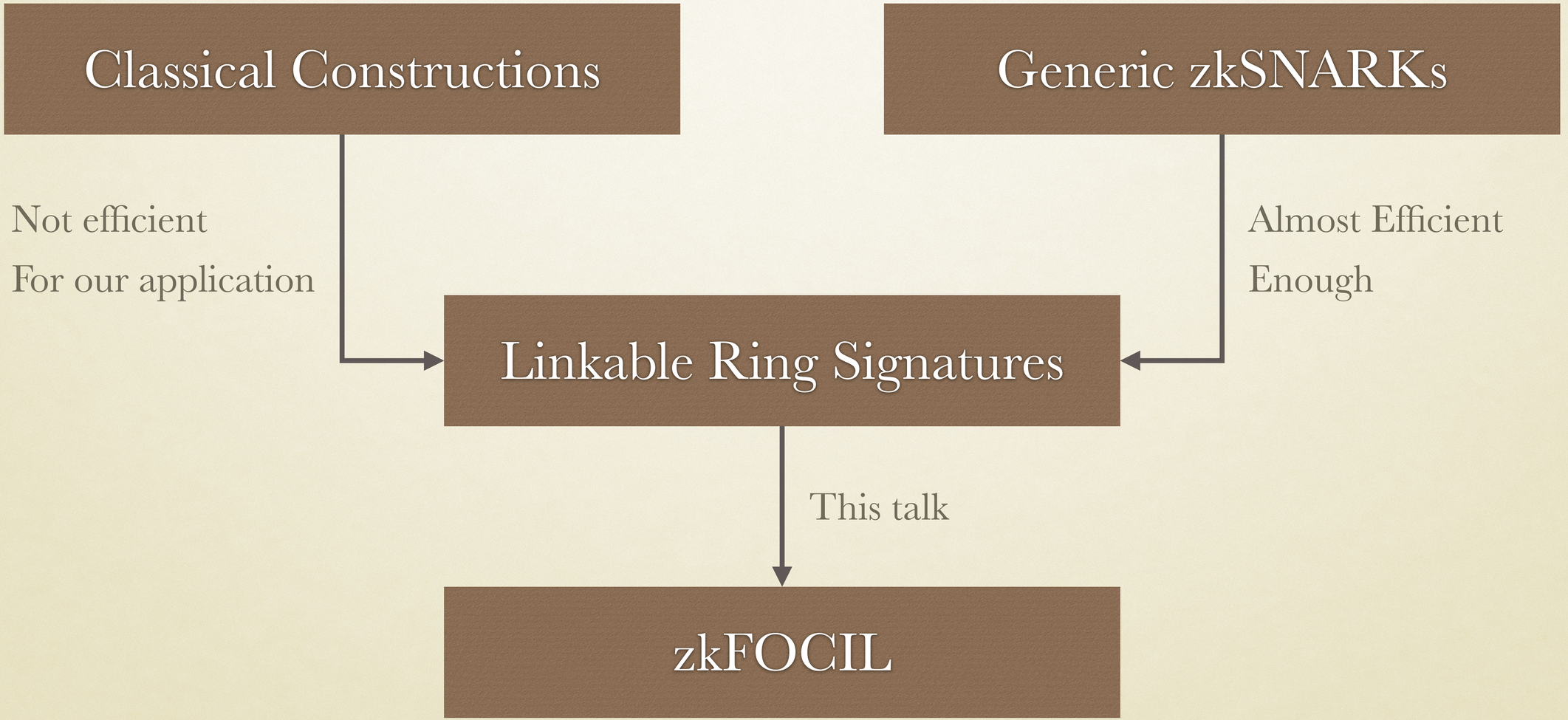
Towards a Construction



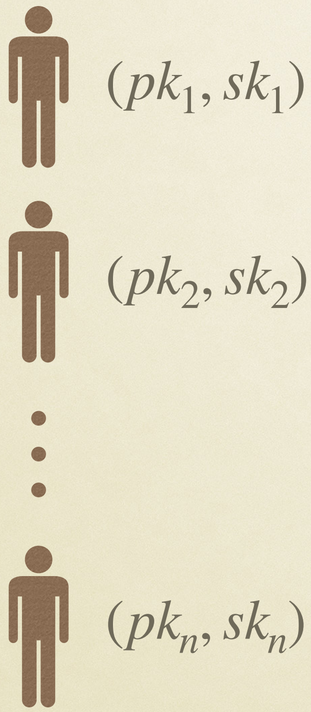
Towards a Construction



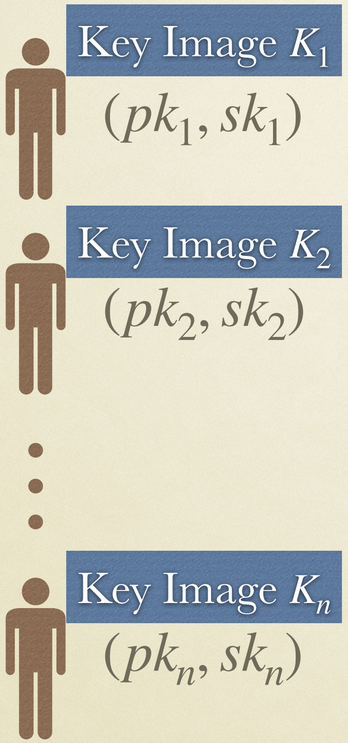
Towards a Construction



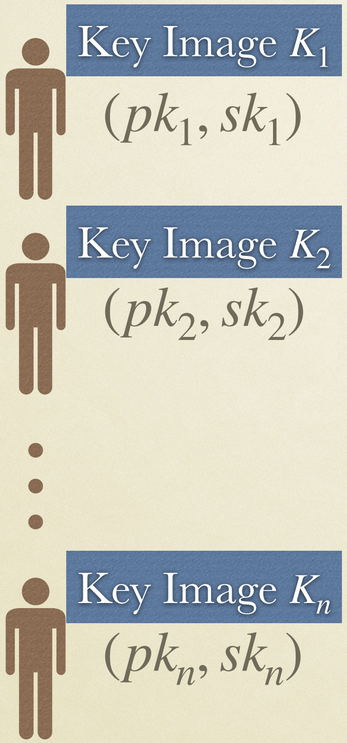
Linkable Ring Signatures



Linkable Ring Signatures

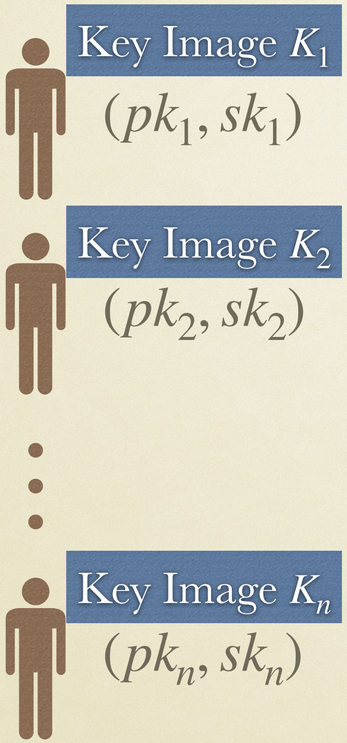


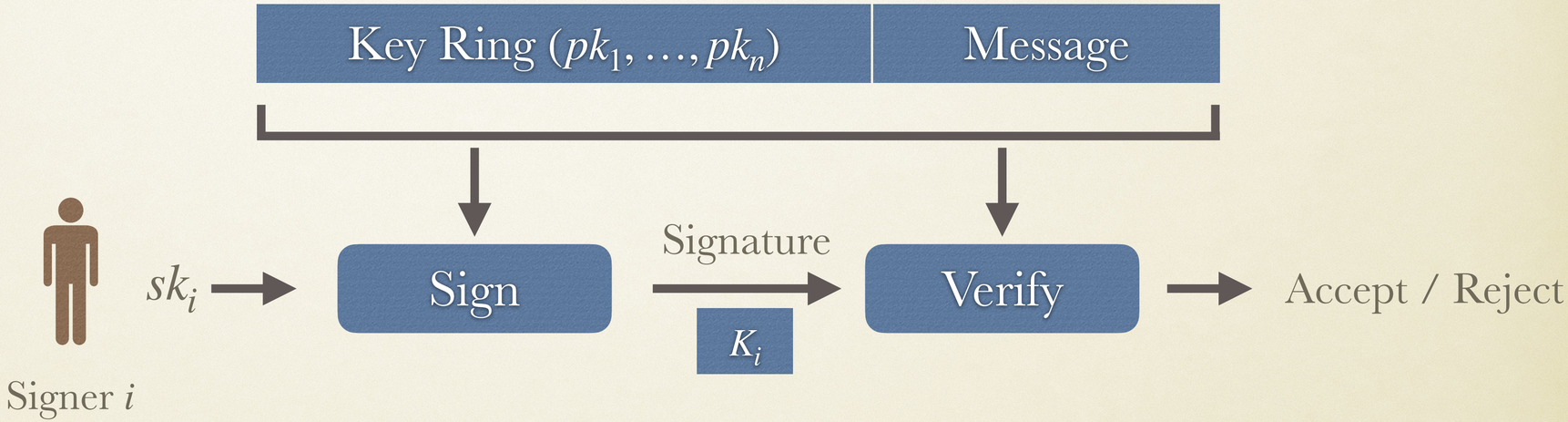
Linkable Ring Signatures



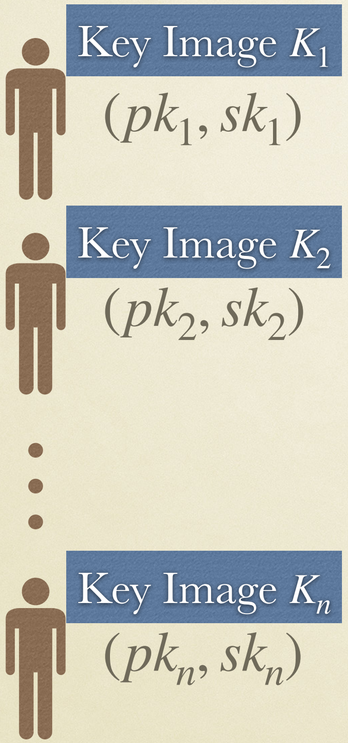
Signer i

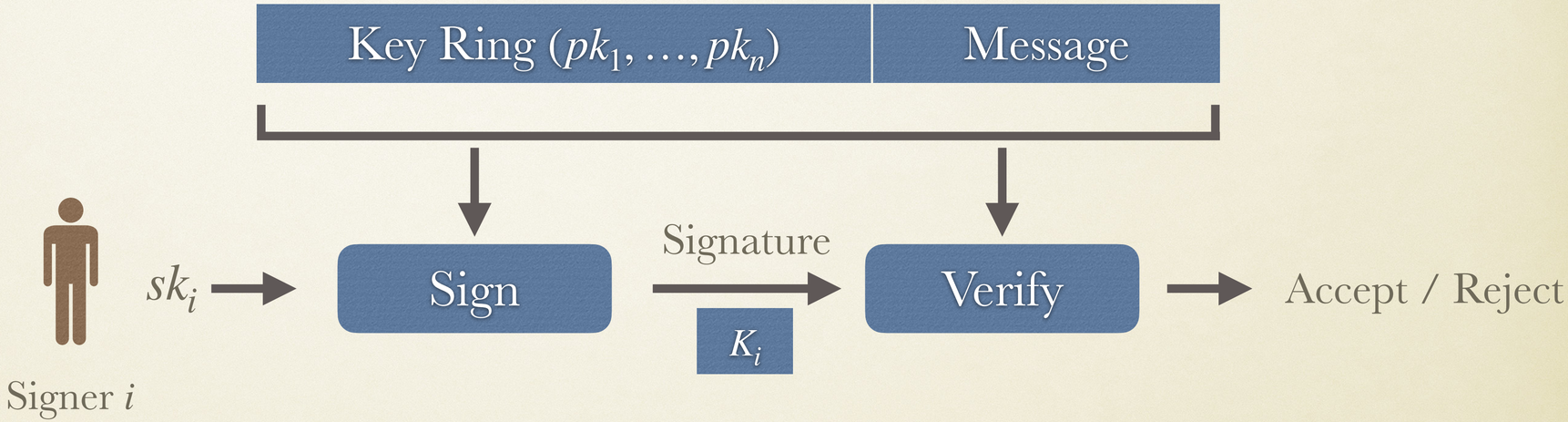
Linkable Ring Signatures





Linkable Ring Signatures





Security

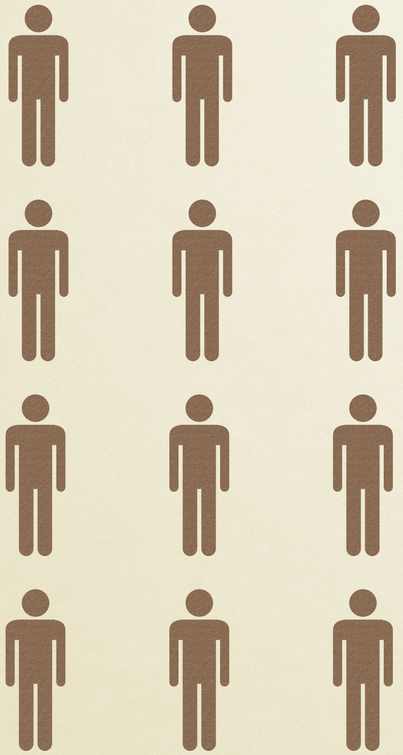
Can only sign using one of the sk_i

(Signature, K_i) does not reveal i

K_i is *unique* pseudonym of pk_i

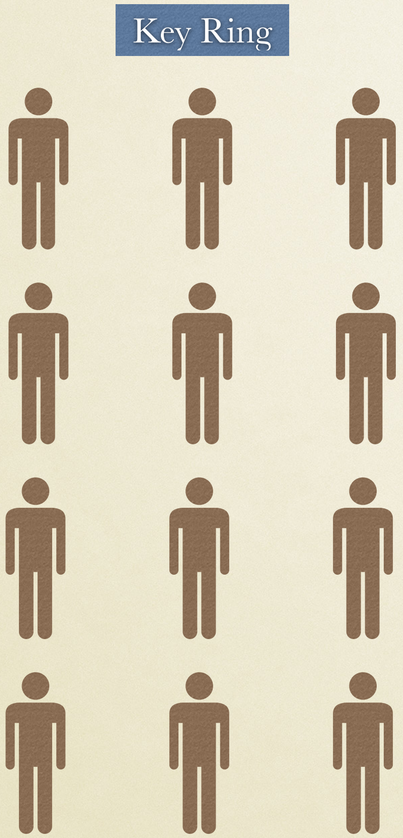
Linkable Ring Signatures in FOCIL

Linkable Ring Signatures in FOCIL



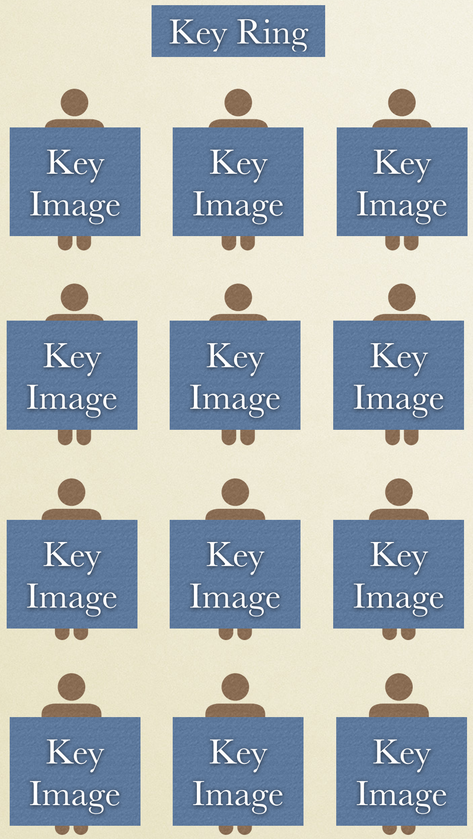
Validators

Linkable Ring Signatures in FOCIL



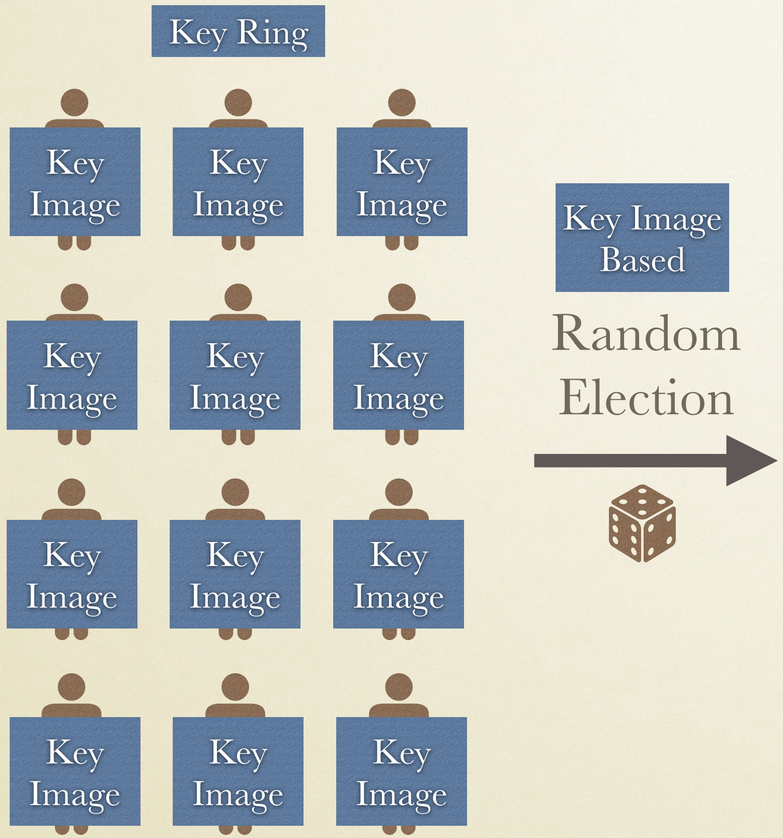
Validators

Linkable Ring Signatures in FOCIL

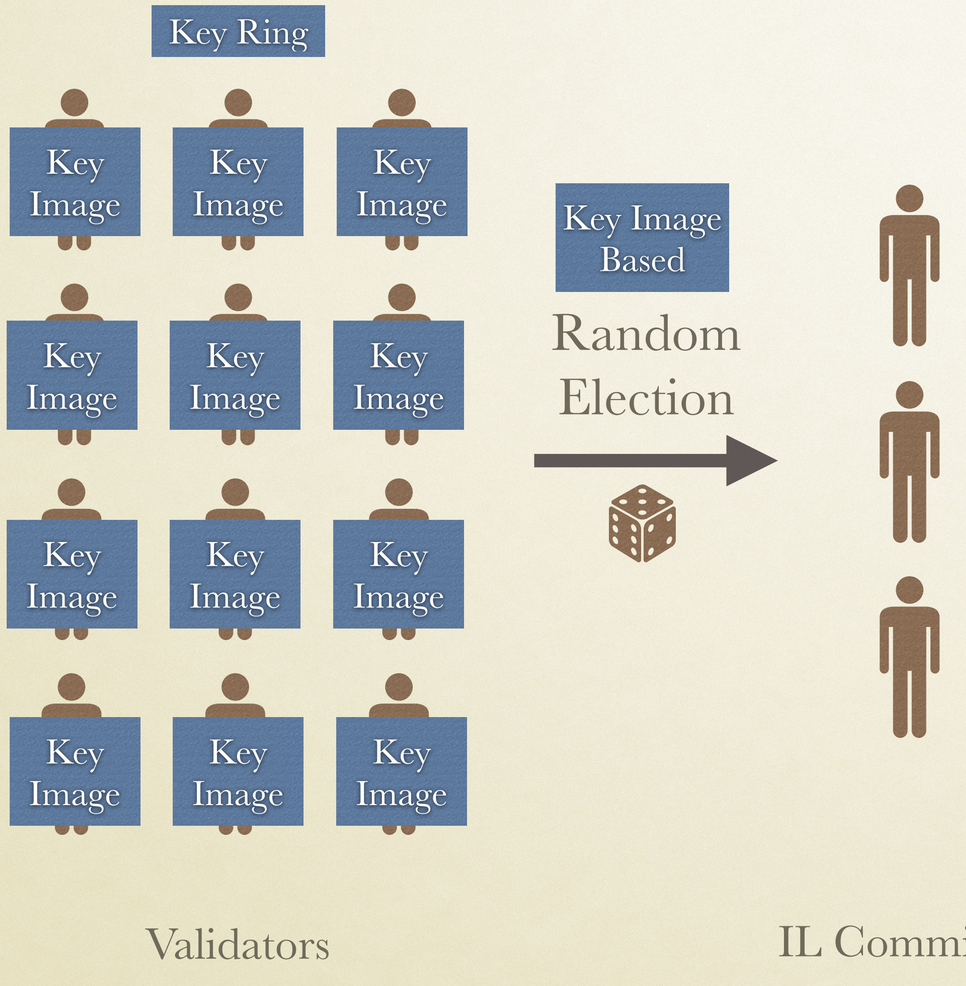


Validators

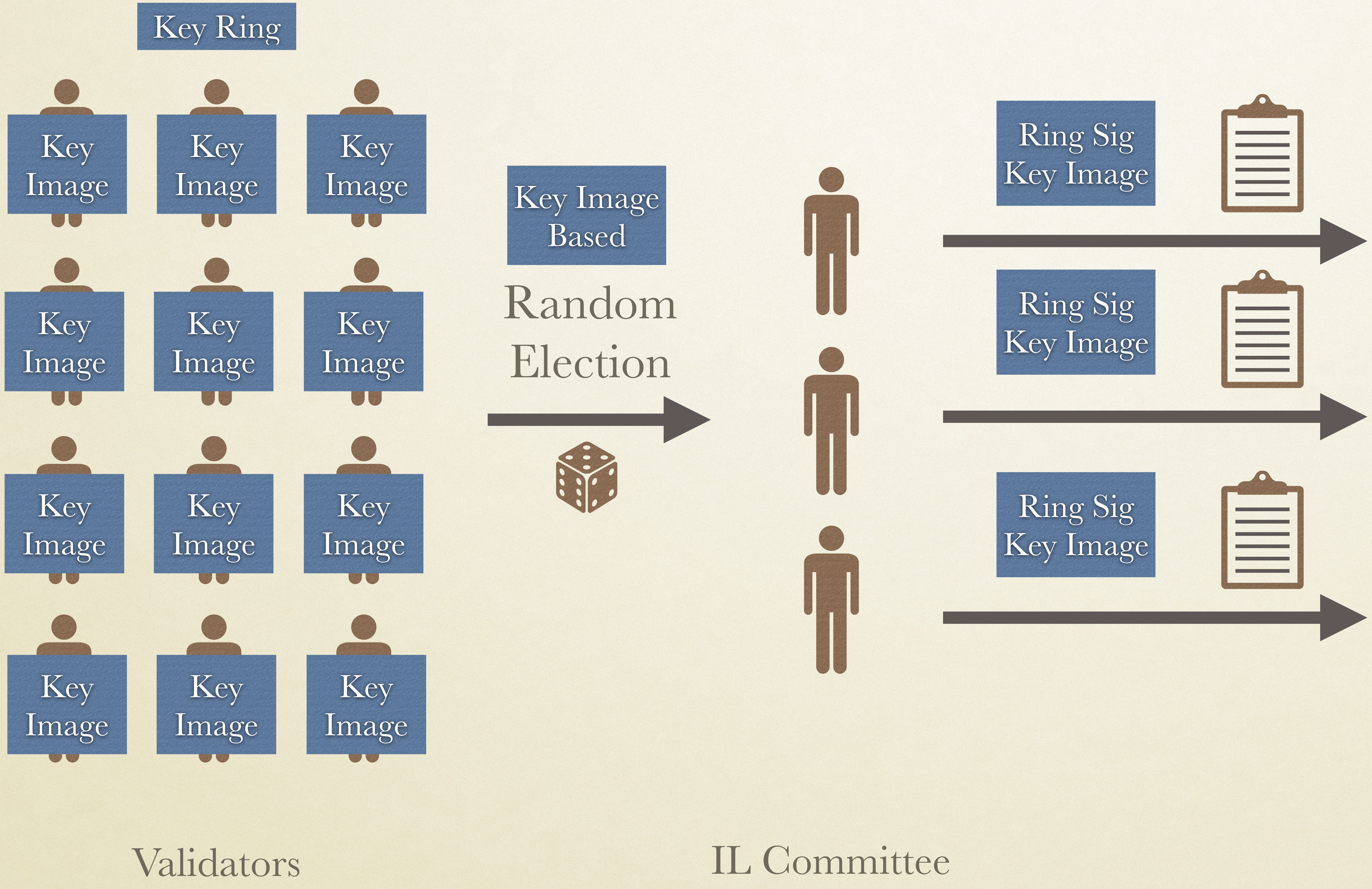
Linkable Ring Signatures in FOCIL



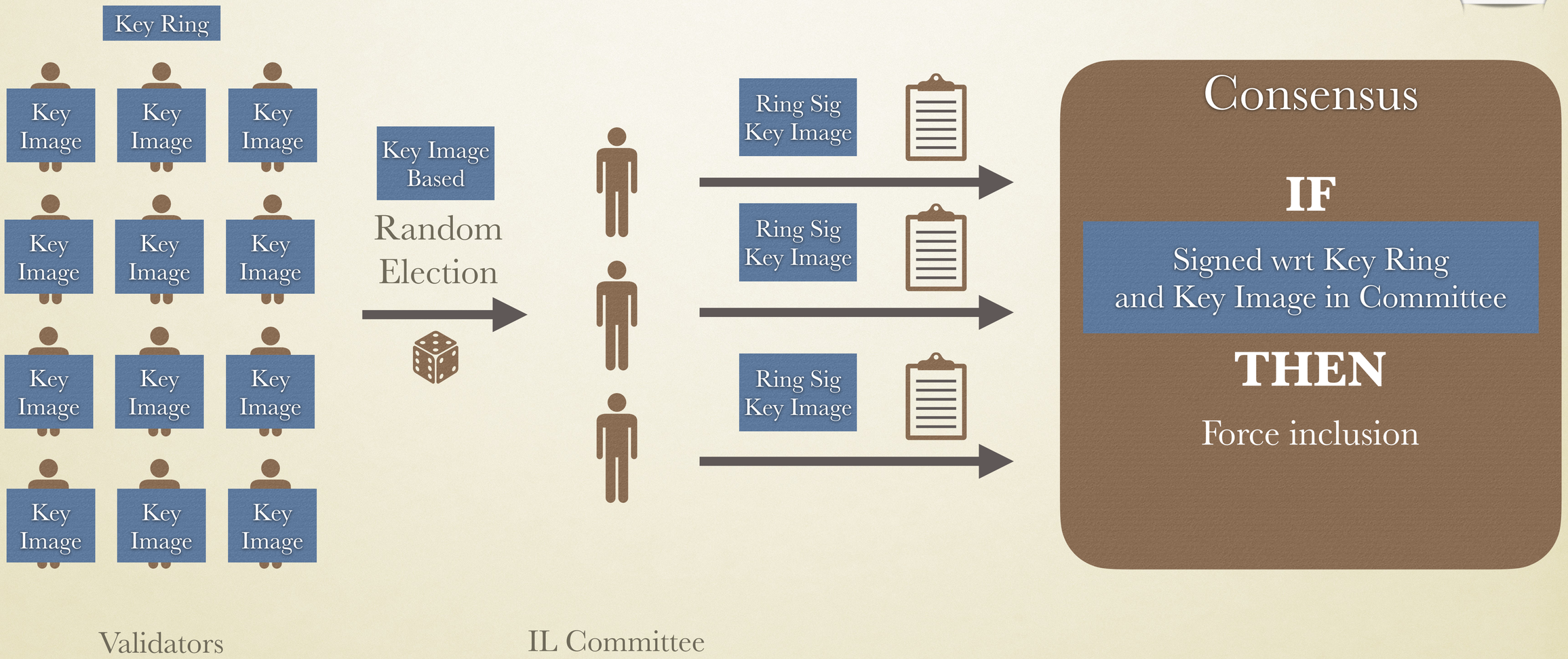
Linkable Ring Signatures in FOCIL



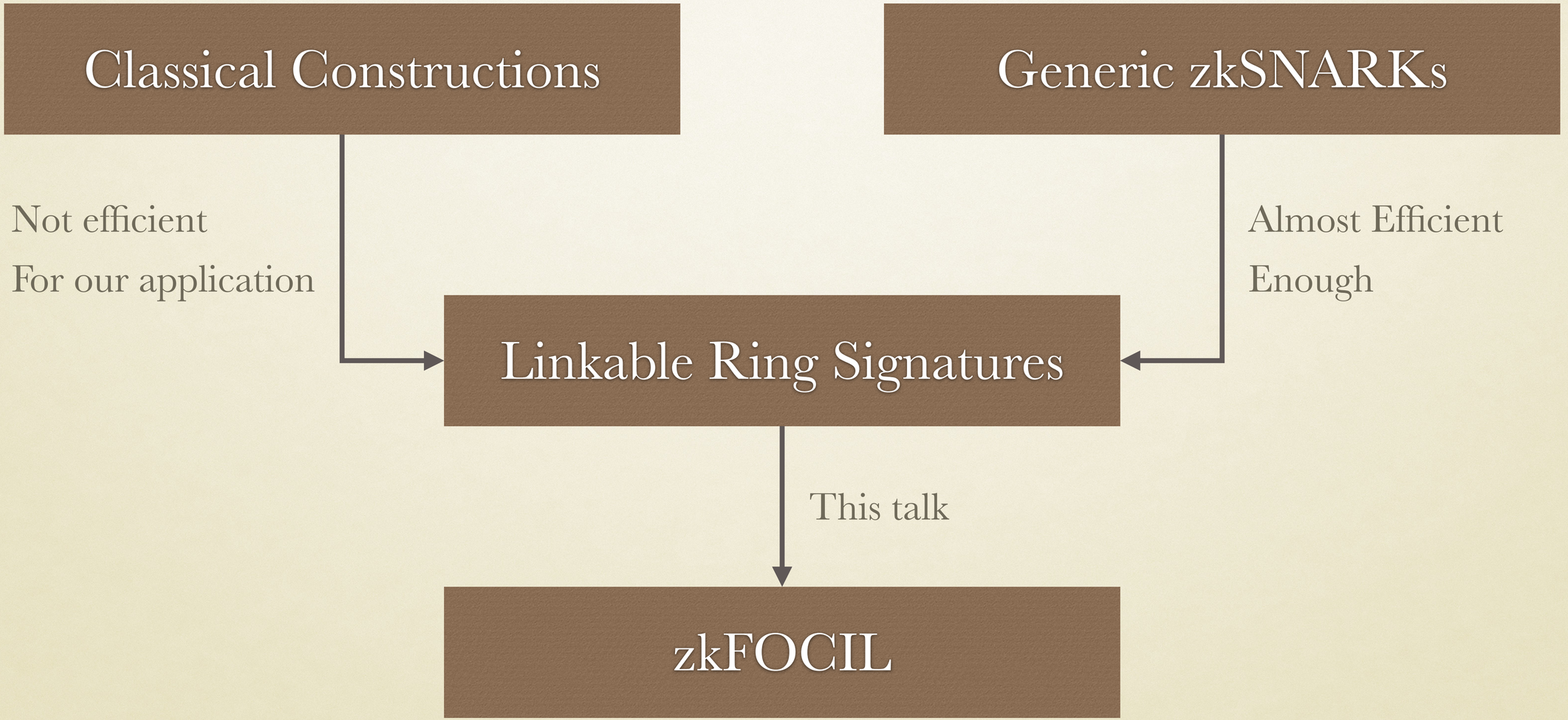
Linkable Ring Signatures in FOCIL



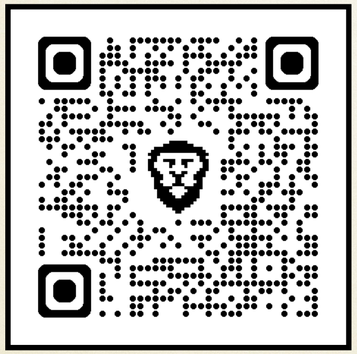
Linkable Ring Signatures in FOCIL



Towards a Construction



Efficiency (from generic zksnarks)



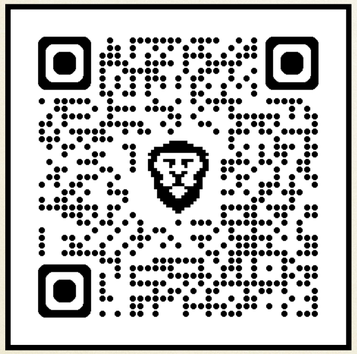
Prototype Implementation

by Shreyas Londhe & Suyash Bagad

* Sig + Key image size ~ 500 Byte

* BN254+IPA / SECP256k1+IPA

Efficiency (from generic zksnarks)



Prototype Implementation

by Shreyas Londhe & Suyash Bagad

Key Image + Proof	< 2.5 s
Sign IL	~ BLS sig
Verify Sig + Key Image	87 ms

* Sig + Key image size ~ 500 Byte

* BN254+IPA / SECP256k1+IPA

Next Steps

Next Steps

More efficient Construction

Next Steps

More efficient Construction

zkFOCIL Combinatorics

Next Steps

More efficient Construction

zkFOCIL Combinatorics

Integration into FOCIL

Thank You