# I See You Blockchain User, or Not! Privacy in the Age of Blockchains

**Ghada Almashaqbeh**

**UConn**

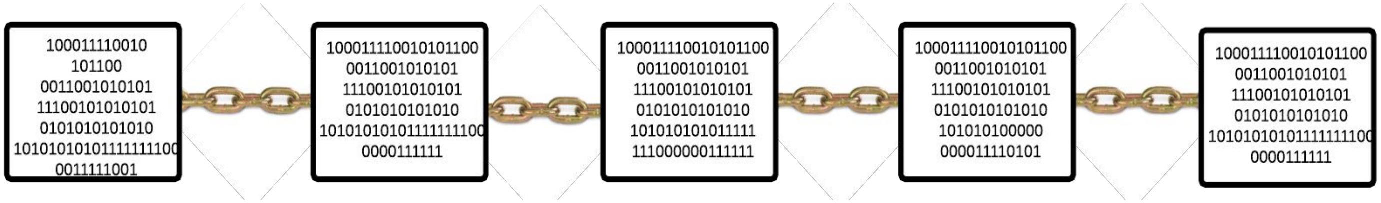
@g_almashaqbeh

**Enigma 2022**

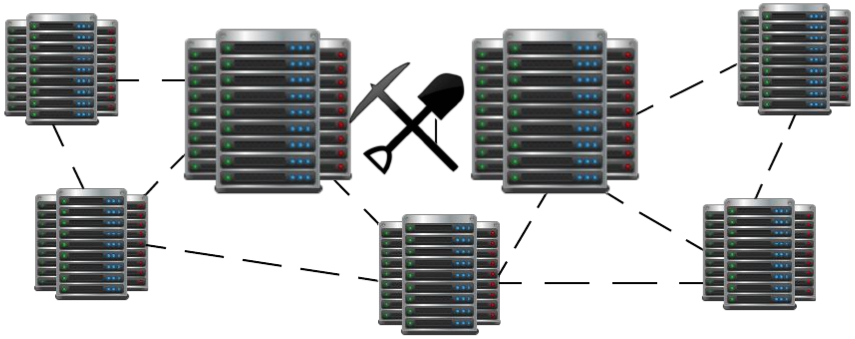
# Big Dreams …

Bitcoin 2009

Blockchain

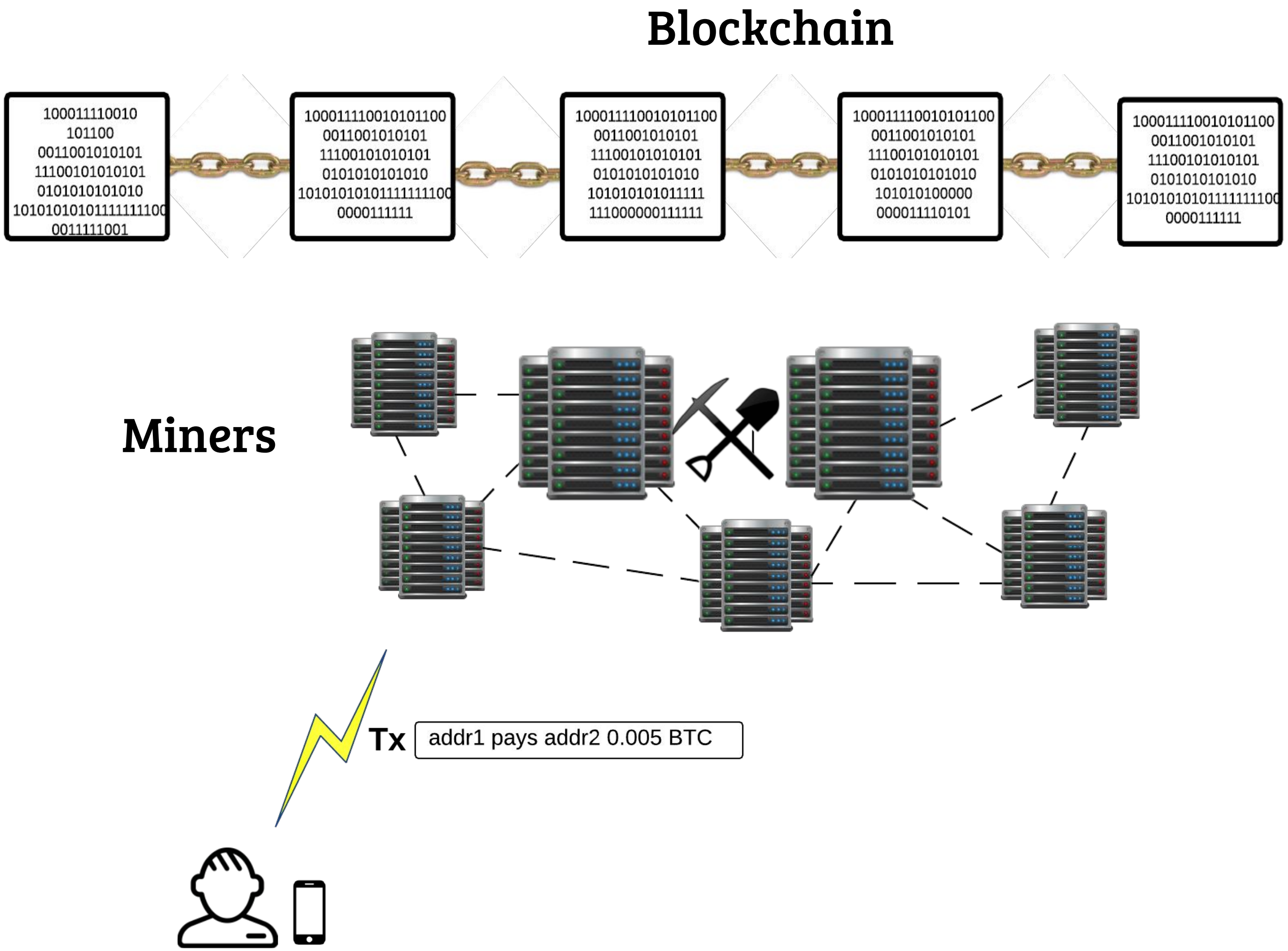


Miners



# Big Dreams …

Bitcoin 2009



Blockchain

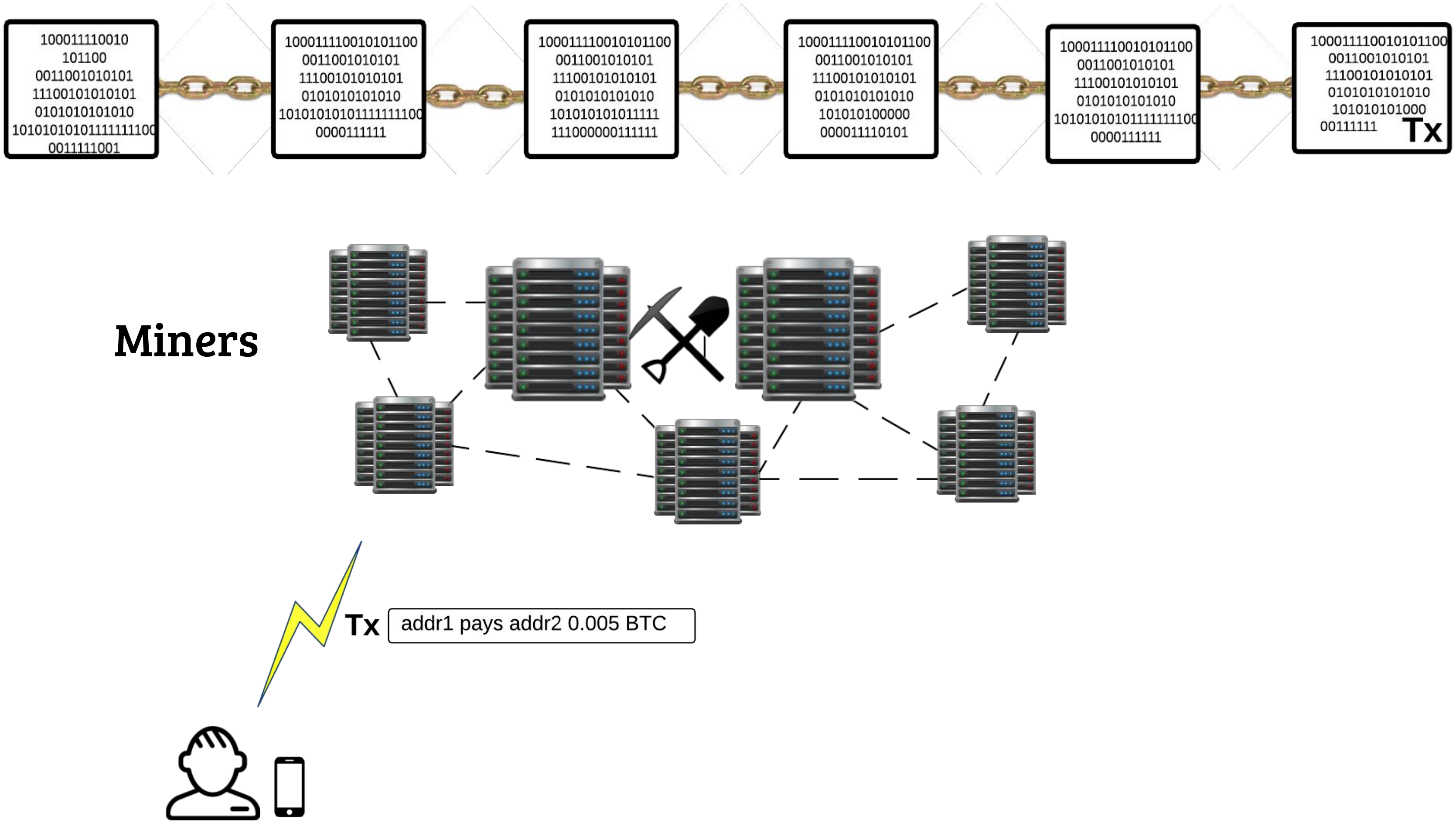
Miners

Tx addr1 pays addr2 0.005 BTC

# Big Dreams …

Bitcoin 2009

Blockchain



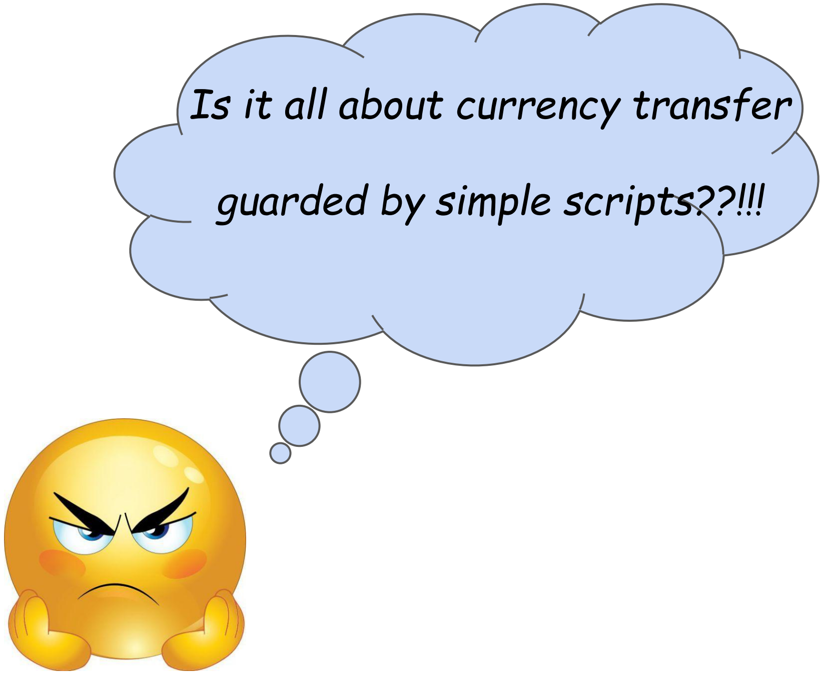
Miners

Tx addr1 pays addr2 0.005 BTC

# Limited Functionality

*Decentralized currency transfer*

*Limited scripting language*



*Is it all about currency transfer guarded by simple scripts??!!!*

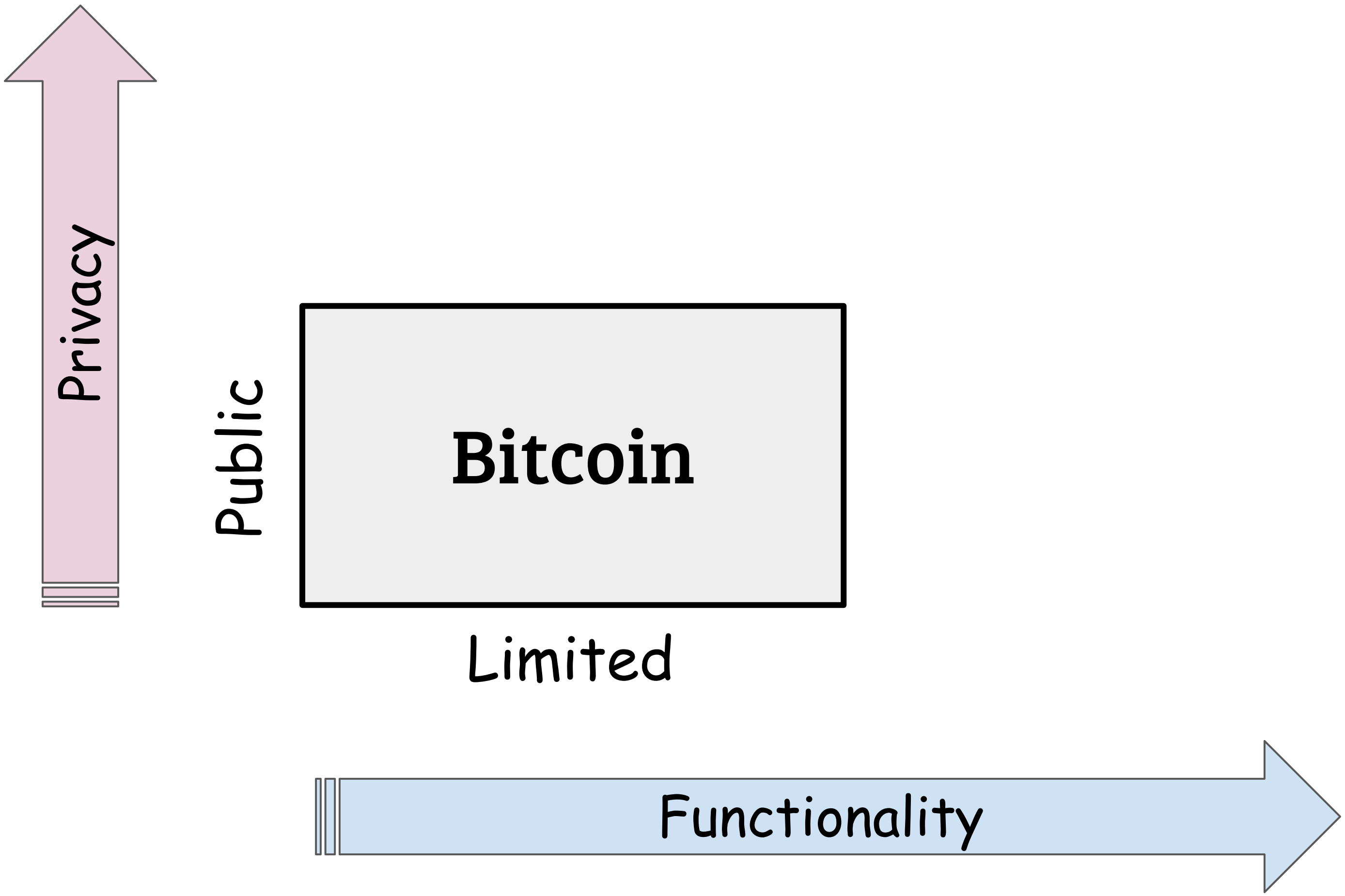
# No Privacy

*Pseudo-anonymity*

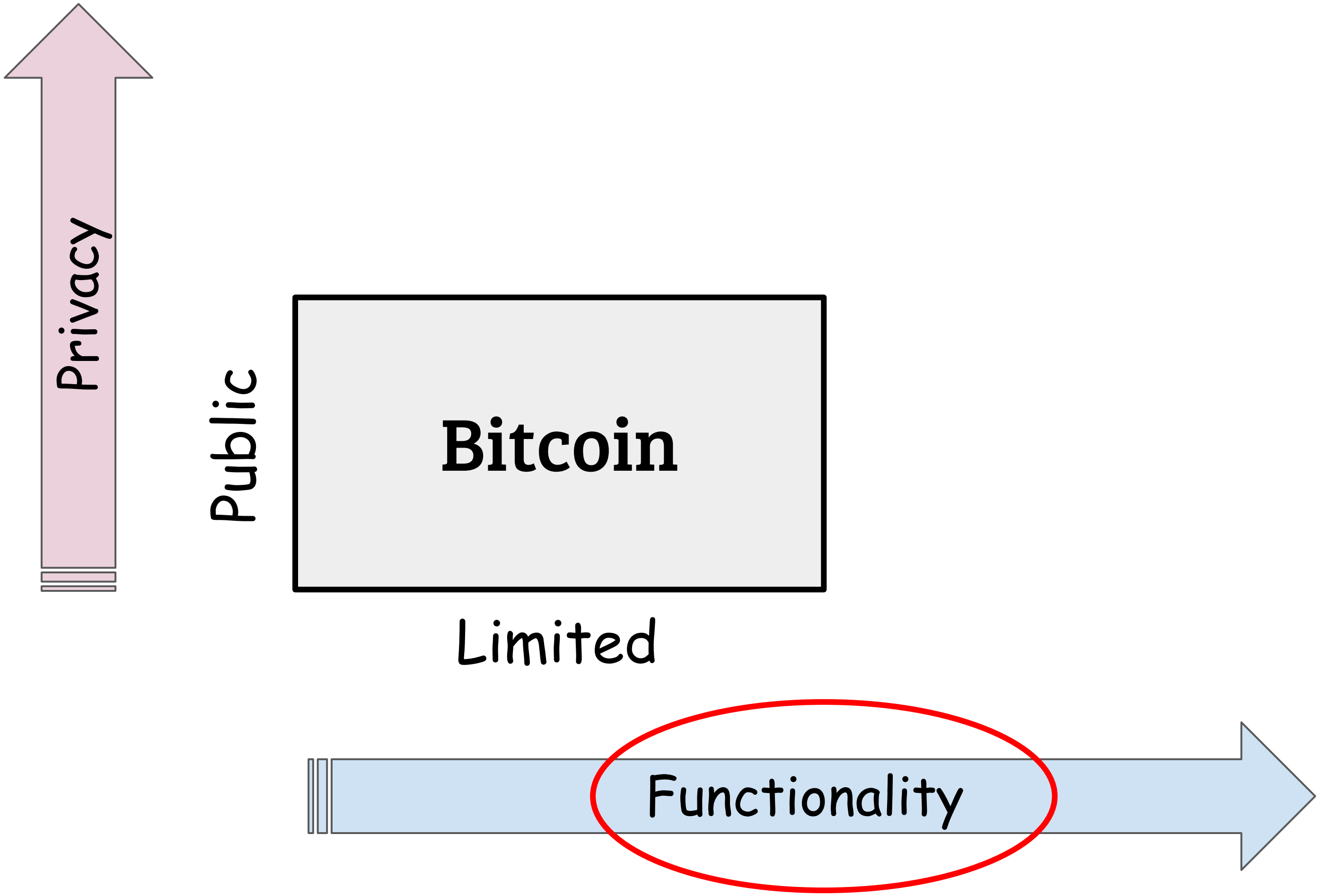
*Transaction Linkability*

Reid et al. "An analysis of anonymity in the Bitcoin system." In Security and privacy in social networks, 2013
Koshy et al "An analysis of anonymity in Bitcoin using p2p network traffic." In Financial Cryptography, 2014

# Solutions Went Different Directions



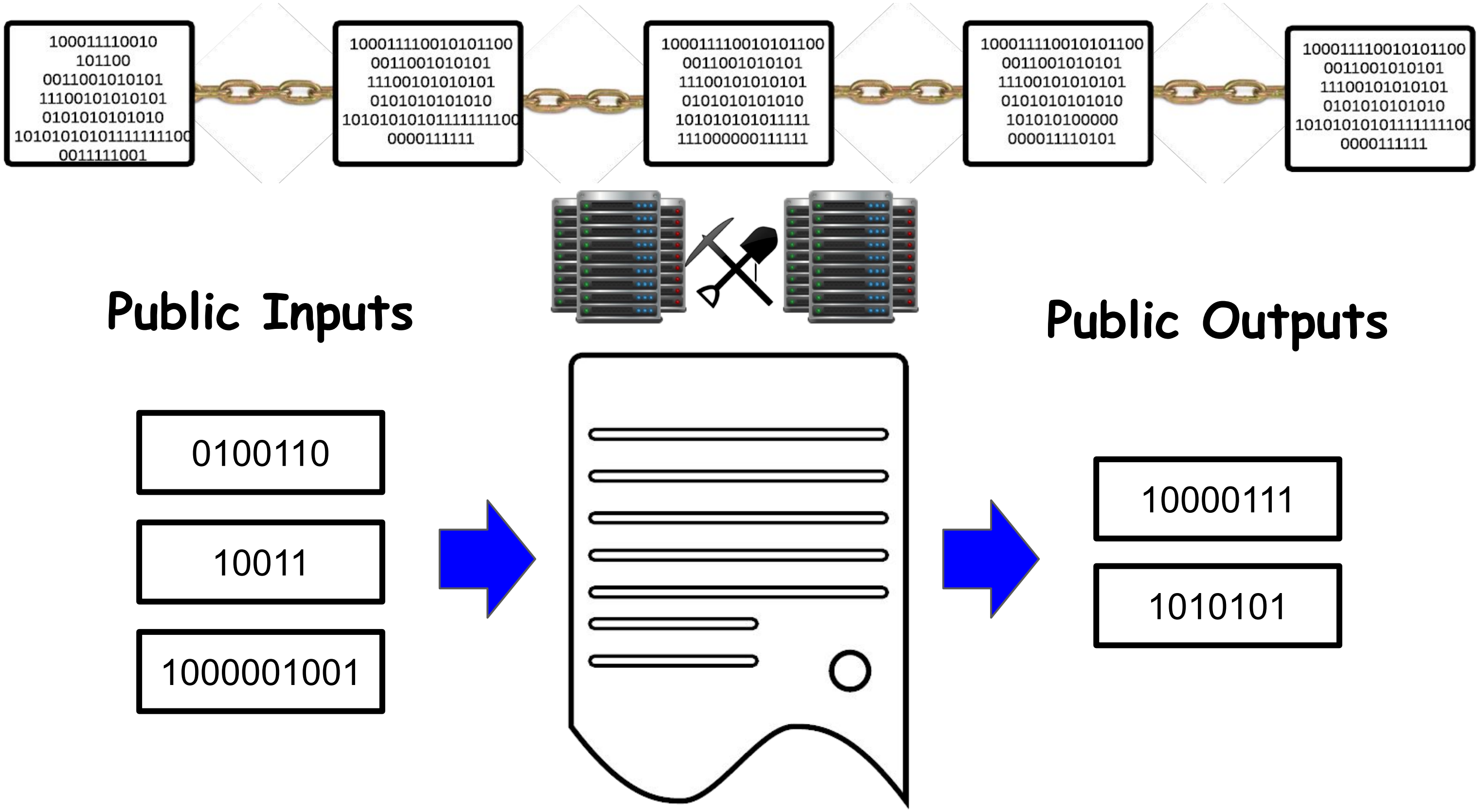
# Solutions Went Different Directions



# Ethereum was Born in 2015

Other systems: Algorand, Cardano, …

# Smart Contracts



Public Inputs

0100110

10011

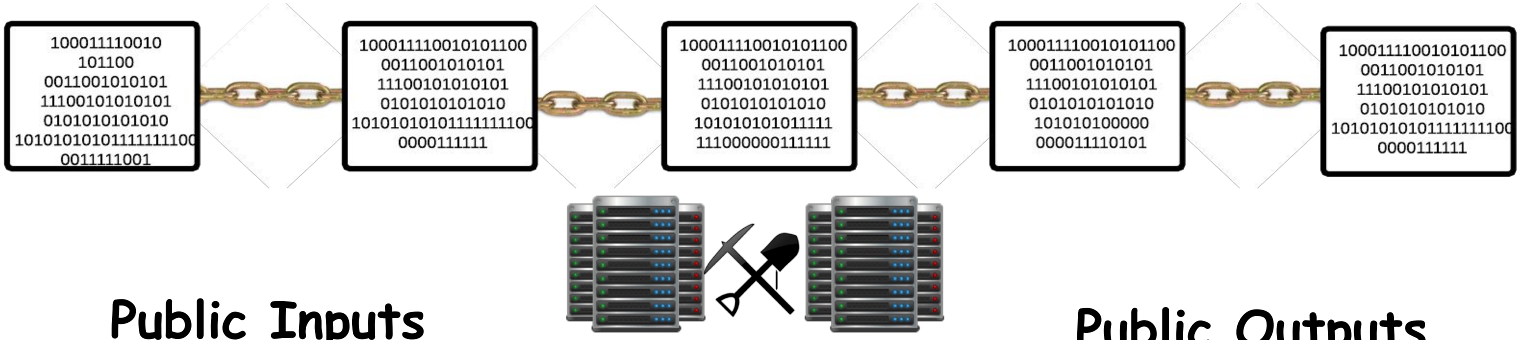
1000001001

Public Outputs

10000111

1010101

# Smart Contracts

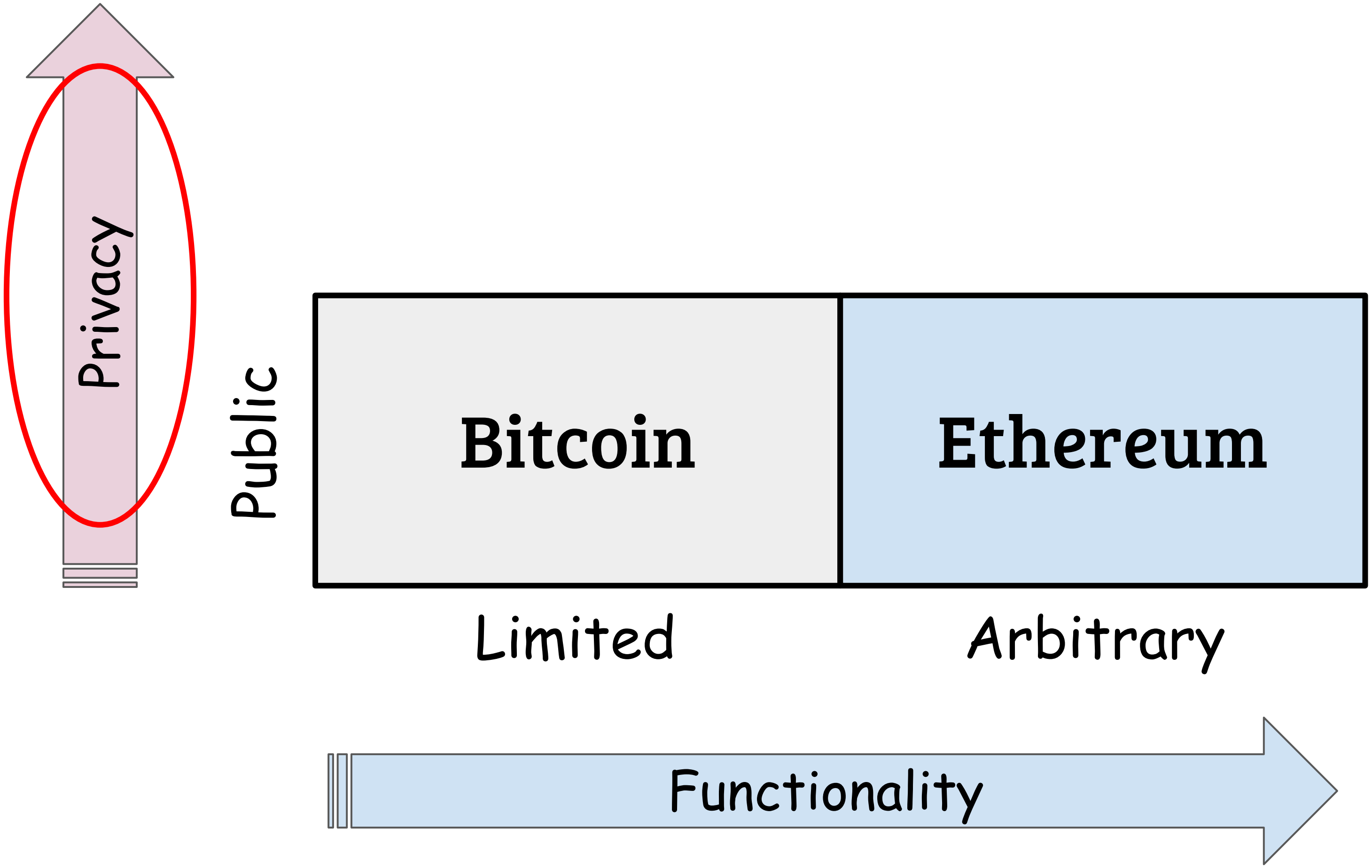


Public Inputs

Public Outputs

Computing on demand!

# Solutions Went Different Directions



Privacy

Public

Bitcoin

Ethereum

Limited

Arbitrary

Functionality

# Several Initiatives Out There

***Zcash***

***Monero***

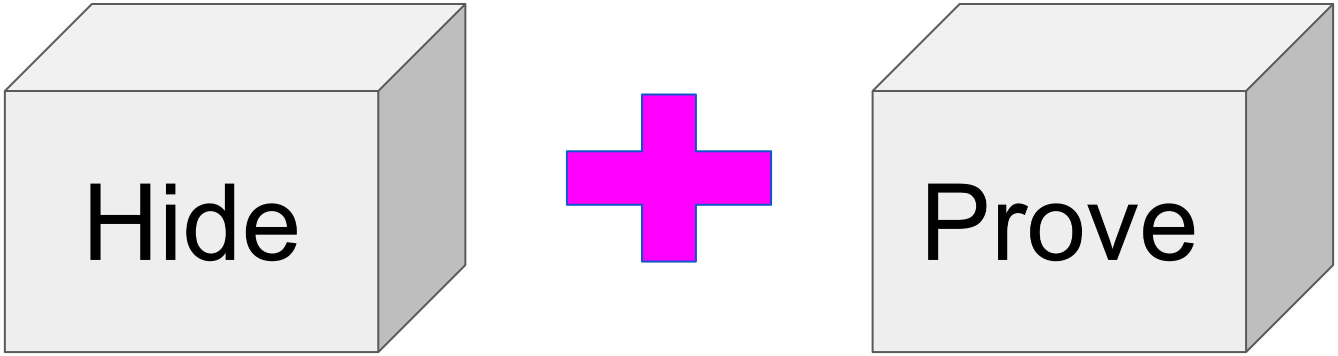
***Quisquis***

***Zerocoin***

**...**

G. Almashaqbeh and R. Solomon. “SoK: Privacy-Preserving Computing in the Blockchain Era“, 2021

# General Paradigm



Hide

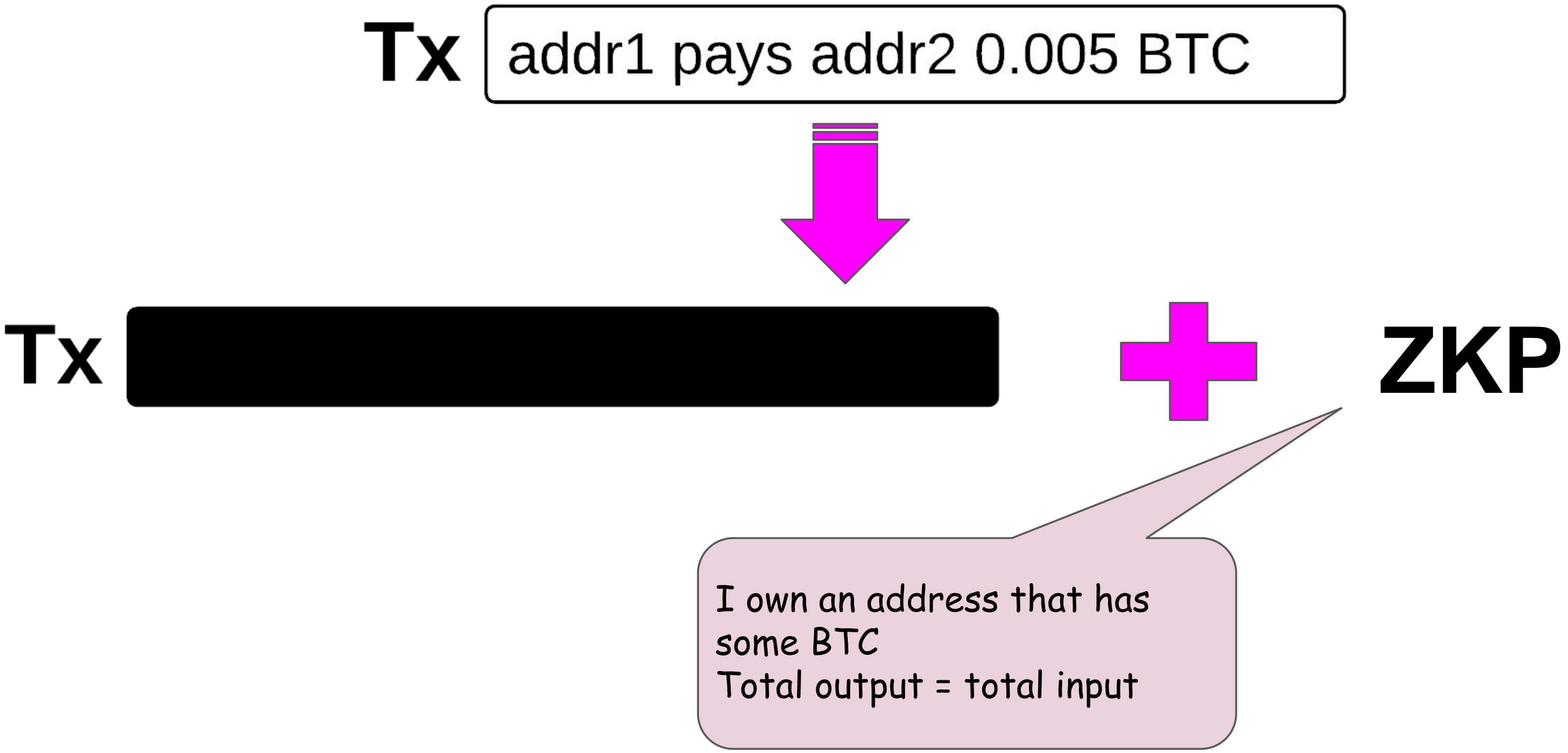
Prove

**Starring:**

Commitment/encryption +

Zero knowledge proofs (ZKP)

# Private Payments



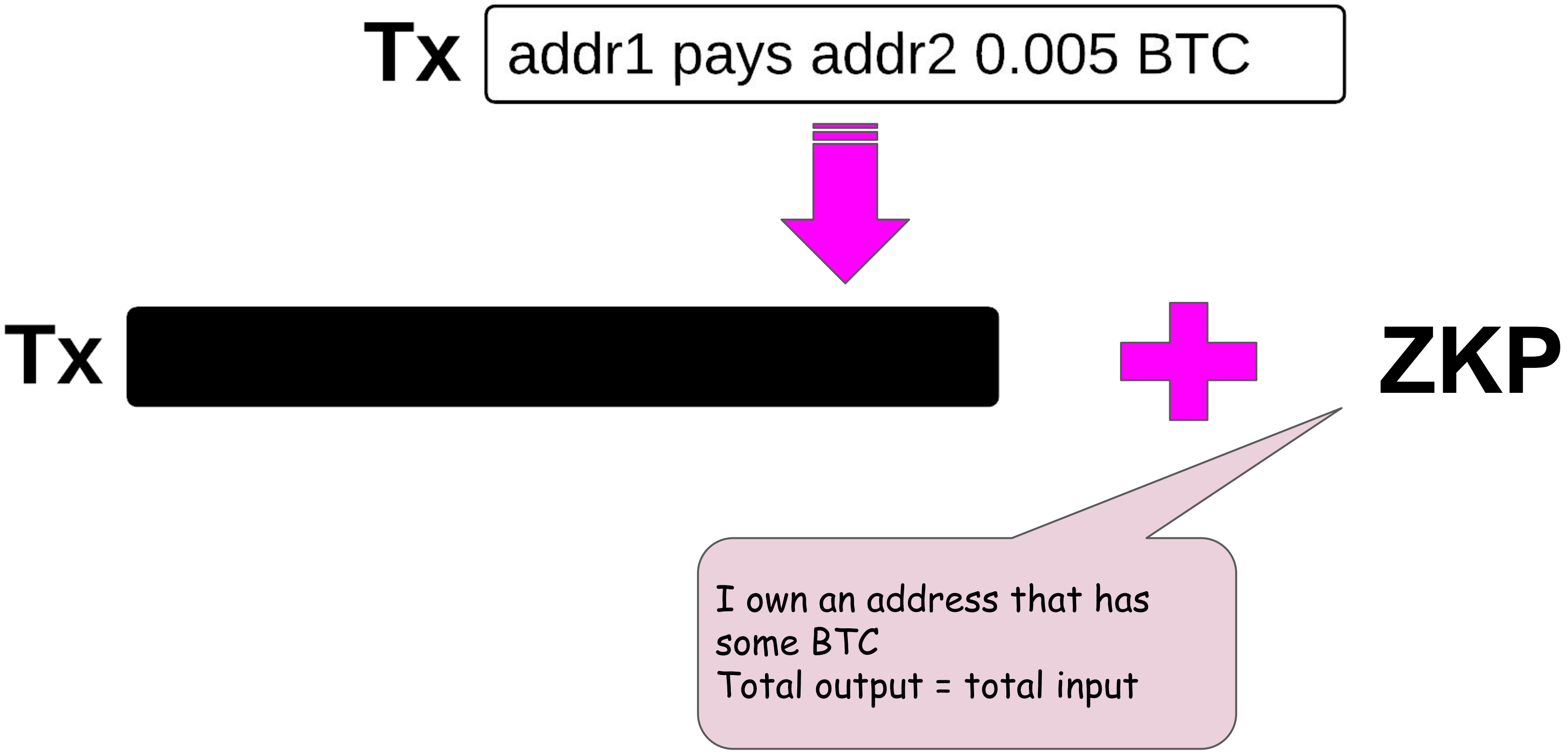
Tx addr1 pays addr2 0.005 BTC

Tx

ZKP

I own an address that has some BTC
Total output = total input

# Private Payments



Tx addr1 pays addr2 0.005 BTC

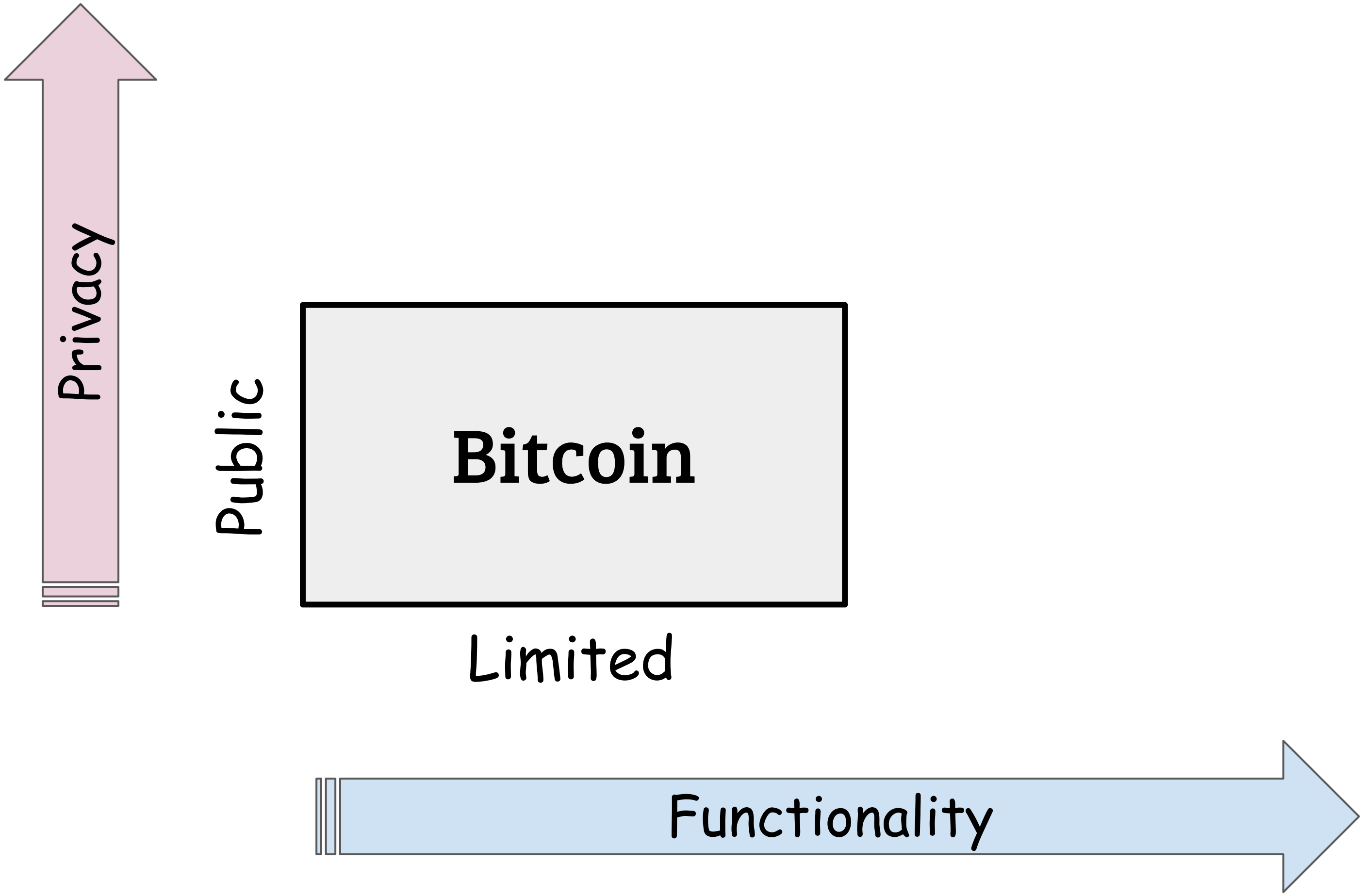
Tx

ZKP

I own an address that has some BTC
Total output = total input

**Bitcoin is still public!!!**

# Bigger Dreams ...



Privacy

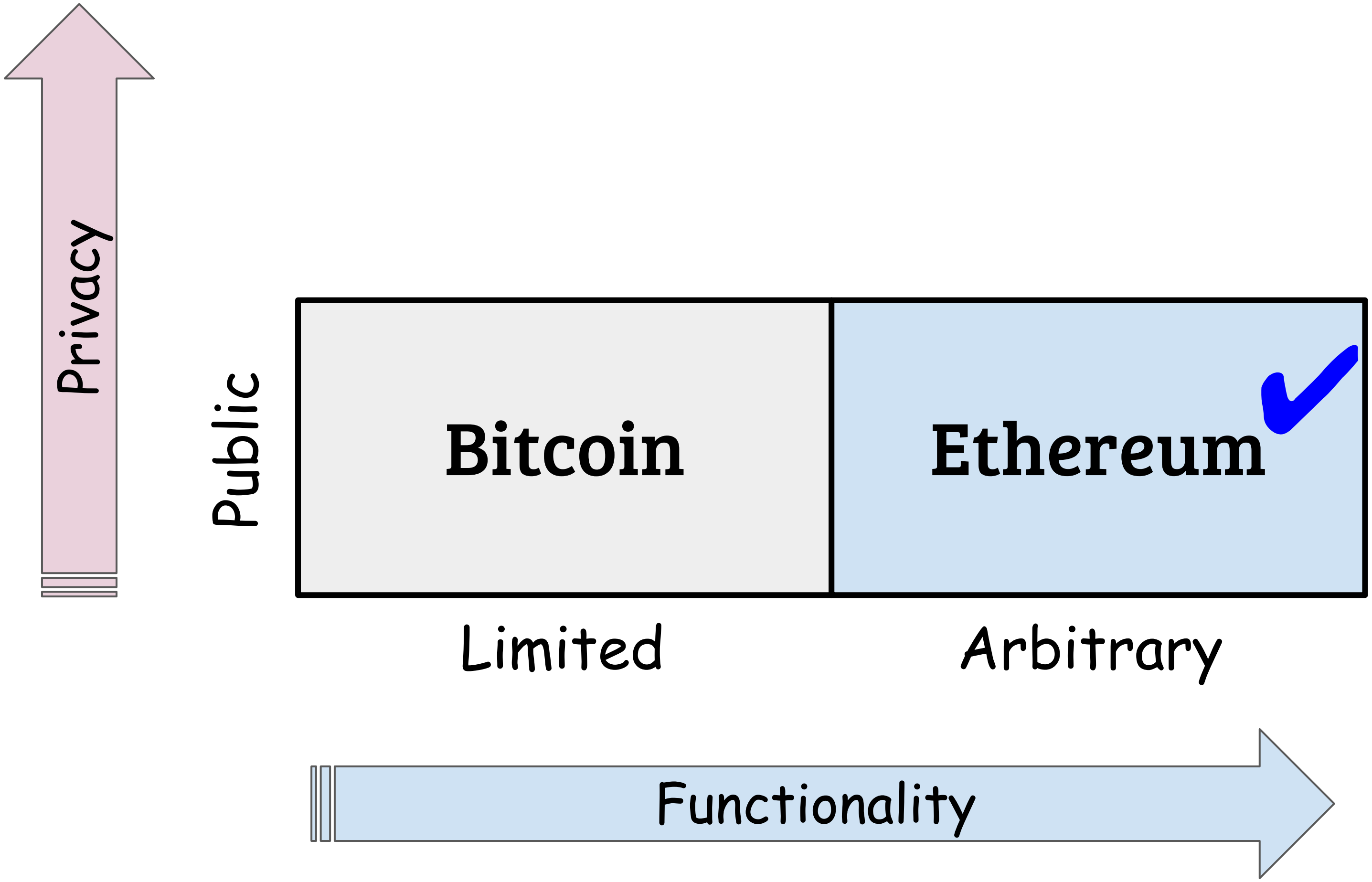
Public

Bitcoin

Limited

Functionality

# Bigger Dreams ...



Privacy

Public

Bitcoin

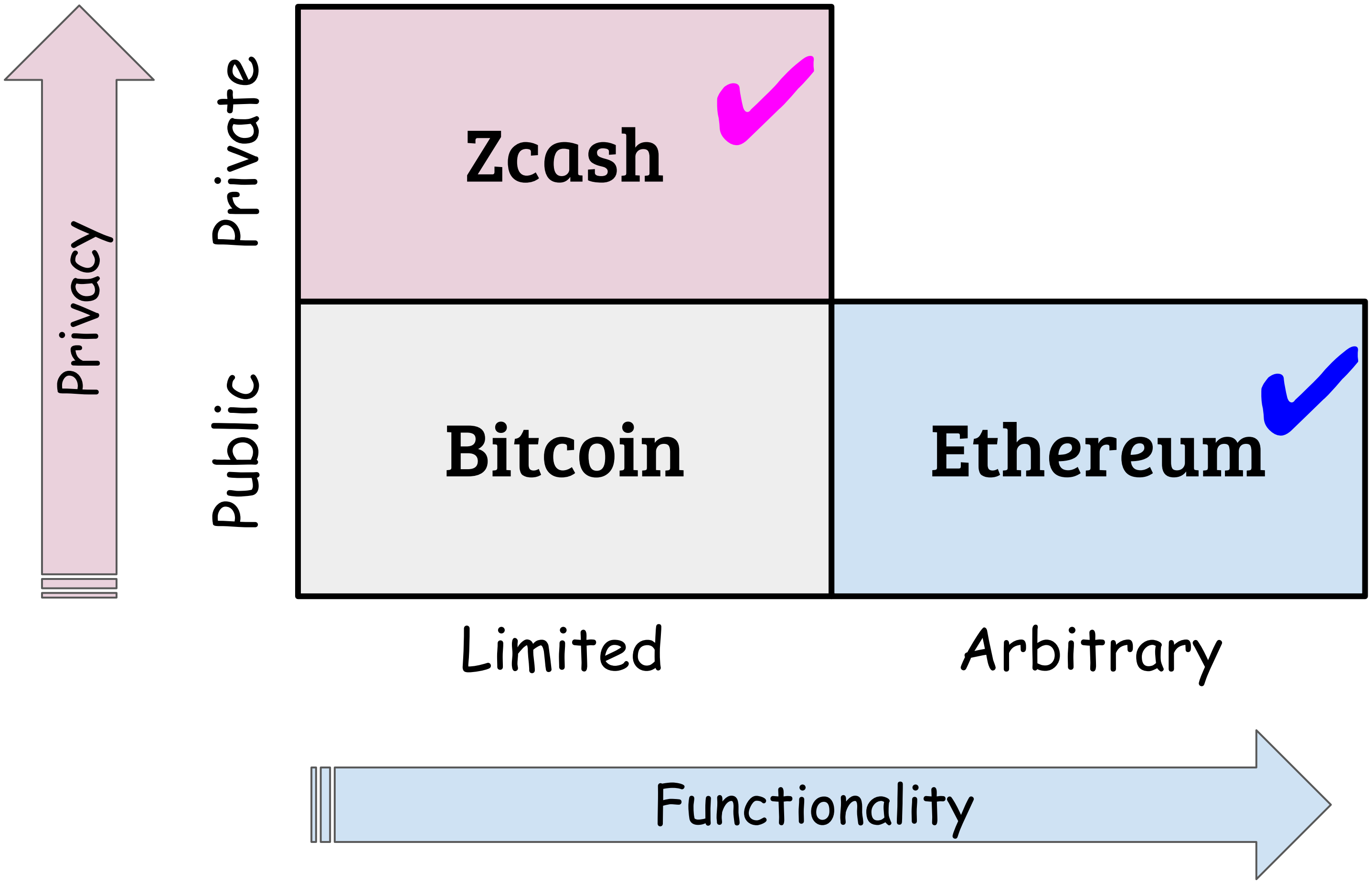
Ethereum ✓

Limited

Arbitrary

Functionality

# Bigger Dreams ...



Privacy

Private

Public

Zcash ✓

Bitcoin

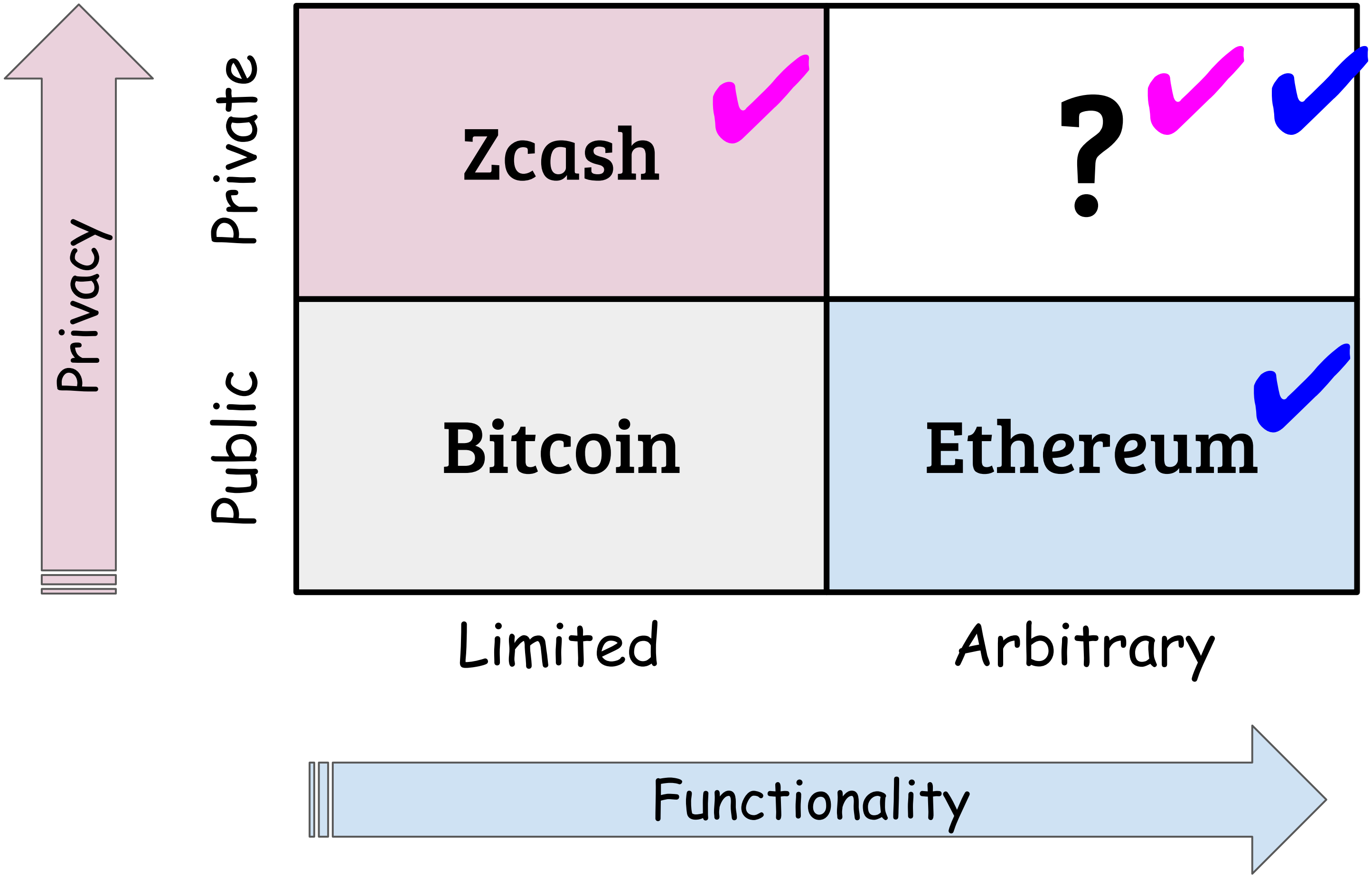
Ethereum ✓

Limited

Arbitrary

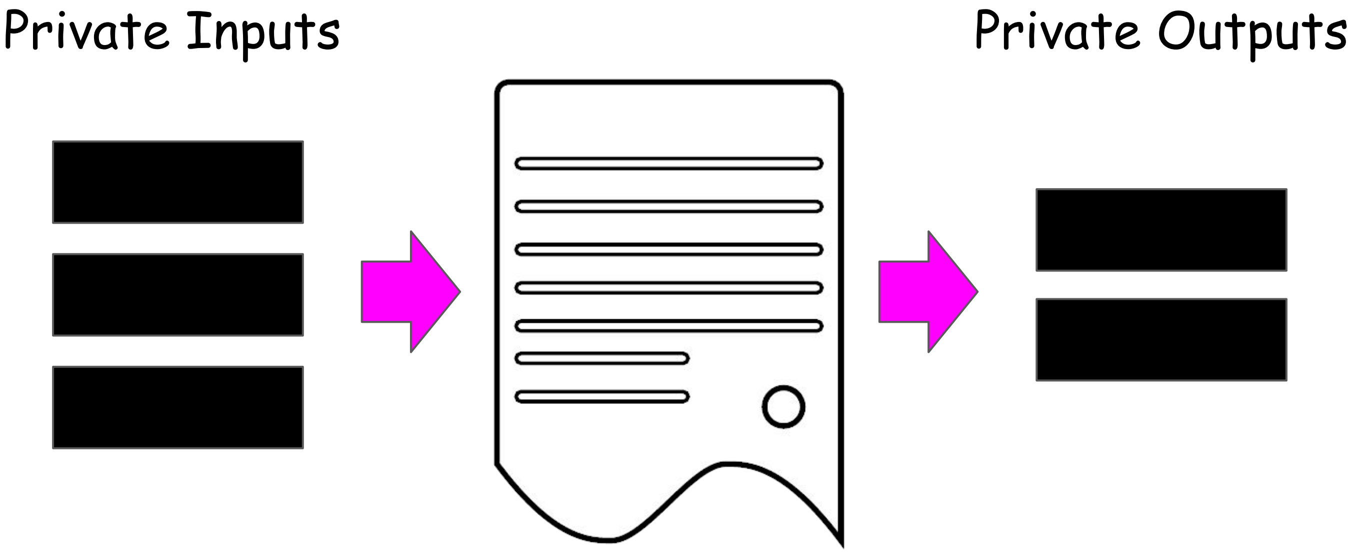
Functionality

# Bigger Dreams ...



| | Limited | Arbitrary |
|---|---|---|
| Private | Zcash ✓ | ? ✓ ✓ |
| Public | Bitcoin | Ethereum ✓ |

# Privacy-preserving Smart Contracts?



Private Inputs

Private Outputs

# More Initiatives

***Hawk***

***Zether***

***Kachina***

***Zexe***

***Ekiden***

***smartFHE***

***Arbitrum***

***Zkay***

G. Almashaqbeh and R. Solomon. “SoK: Privacy-Preserving Computing in the Blockchain Era“, 2021

# Solutions Spectrum

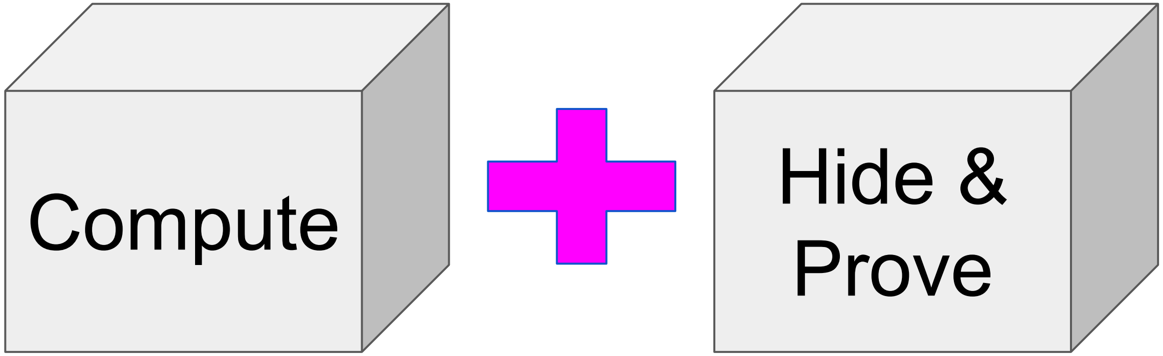
**Off-chain**

**On-chain**

Others compute

Miners compute

# Off-chain Private Computing



**Starring:** ZKP

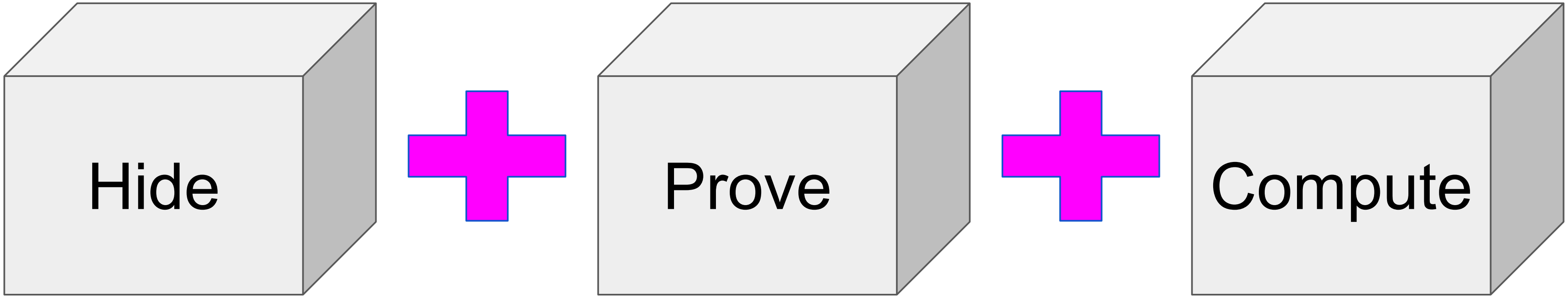
Steffen et al. "zkay: Specifying and enforcing data privacy in smart contracts." ACM CCS. 2019
Bowe et al. "Zexe: Enabling decentralized private computation." IEEE S&P, 2020

👤 Compute over inputs

👤 Encrypt input/output, provide ZKPs

🖥⚒🖥 Verify ZKPs, apply state changes

# On-chain Private Computing



Hide + Prove + Compute

**Starring:**

Fully homomorphic encryption (FHE) +

Zero knowledge proofs (ZKP)

R. Solomon and G. Almashaqbeh. “smartFHE: Privacy-Preserving Smart Contracts from Fully Homomorphic Encryption“, 2021

**FHE**

$$\mathrm{Enc}(x) + \mathrm{Enc}(y) = \mathrm{Enc}(x + y)$$

$$\mathrm{Enc}(x) . \mathrm{Enc}(y) = \mathrm{Enc}(x . y)$$

**ZKP**

System/application specific conditions

👤 Encrypt inputs, provide ZKPs

🗄⛏🗄 Compute, produce encrypted outputs

👤 Decrypt outputs

Encrypt inputs, provide ZKPs

Compute, produce encrypted outputs

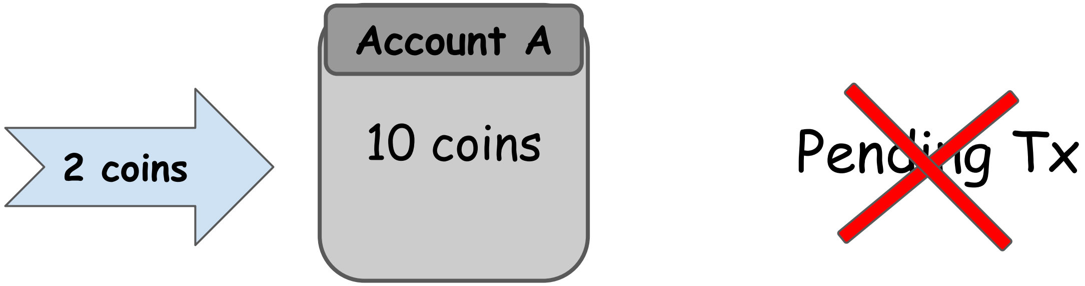
Decrypt outputs

Private computing on demand!

# Several Challenges…

# Concurrency

A state change will invalidate all pending ZKPs



Solutions rely on locking and delaying deposits

# Multi-User Inputs

$PK_G$

$PK_B$

$PK_A$

$PK_C$

$PK_E$

$PK_F$

$PK_D$

Interactivity and high computation cost!

# Efficiency

Efficiency?!
Scalability?!
Throughput?!
...

## Computation cost

- Generating a ZKP can take a minute

## Ciphertext size

- Homomorphic multiplication ciphertext > 100 KB

# The Path Forward?!

**On-chain**

**+**

**Off-chain**

# Take-home Message

Privacy is critical for the future of blockchain systems

Many open questions

**A long path ahead…**
**This is just the beginning!**