Practical Applications of Zero-Knowledge Proofs

JUNE 2019

A FRAMEWORK FOR ZERO-KNOWLEDGE COMPUTATIONS

- Isekai (https://github.com/sikoba/isekai)
- Prove the execution of arbitrary programs in Zero-Knowledge
- For any language
- Using any Zero-Knowledge Proof scheme

INTRODUCTION

Blockchain

Voting and Auctions

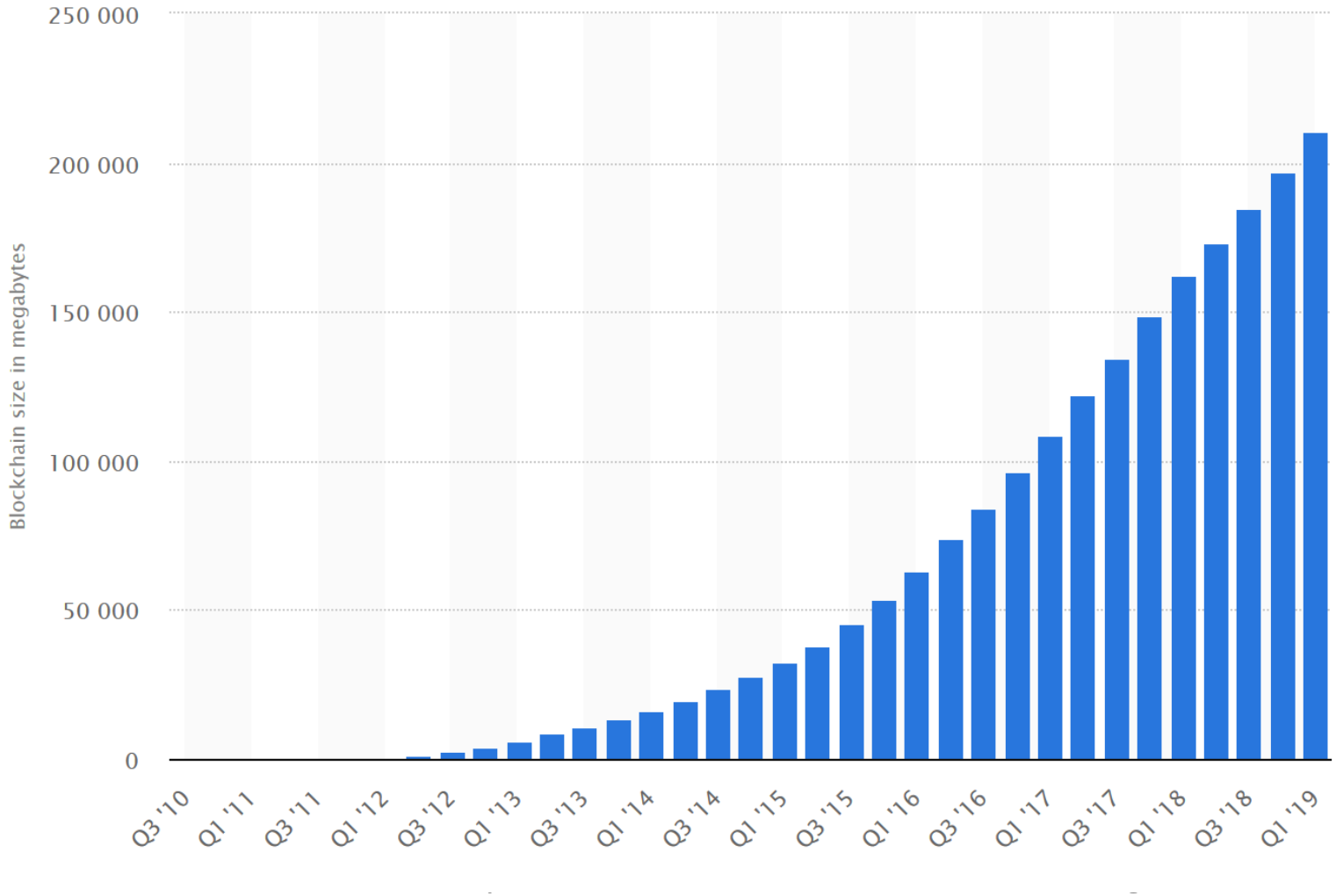
Supply Chain

Finance

Physical Cryptography


BLOCKCHAIN

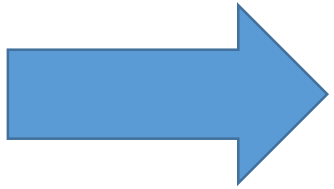
BLOCKCHAIN


250 000
200 000
150 000
100 000
50 000
0
Blockchain size in megabytes
Q3 '10
Q1 '11
Q3 '11
Q1 '12
Q3 '12
Q1 '13
Q3 '13
Q1 '14
Q3 '14
Q1 '15
Q3 '15
Q1 '16
Q3 '16
Q1 '17
Q3 '17
Q1 '18
Q3 '18
Q1 '19

ZCASH: THE NEED FOR ANONYMITY

EVERY BITCOIN PAYMENT IS **PUBLIC**

BITCOIN ADDRESS CAN BE PARTLY DE-ANONYMIZED



LOCATION

MEDICAL INFORMATION

BUSINESS INFORMATION

FUNGIBILITY

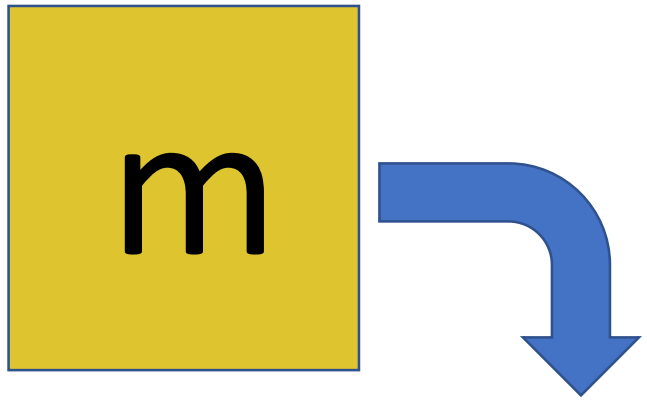
COMMITMENT

Commitment of m

$$Cm \equiv g^m h^r \ [p]$$

r is random, chosen to hide the commitment

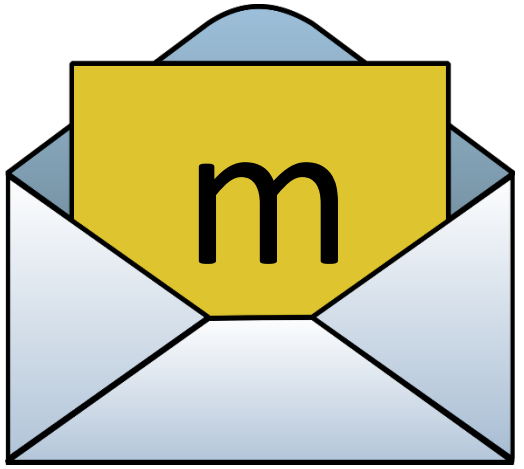
p, g and h are parameters chosen publicly before



COMMITMENT

Opening a commitment

- Prover gives m and r
- Verifiver checks $Cm \equiv g^m h^r$ [p]



ZCASH

MINT

- Consume some bitcoins v
- Create a commitment for a serial number linked to a public key

SPEND

- Reveal the serial number
- Create another coin
- Compute π a zero-knowledge proof of the following:
  - Serial number was previously committed
  - Serial number was not revealed in previous blocks
  - I can generate the public key linked to the serial number
  - Values match

VOTING

Privacy Vs Integrity

VOTING

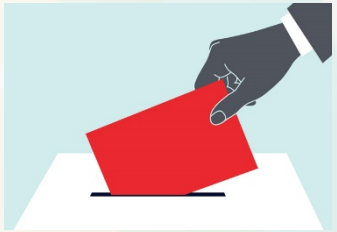
Privacy Vs Integrity

Vote must remain private

VOTING

Privacy Vs Integrity

Vote must remain secret

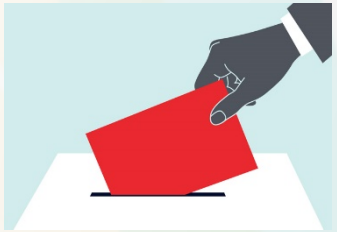


VOTING

Privacy Vs Integrity

Vote must remain secret

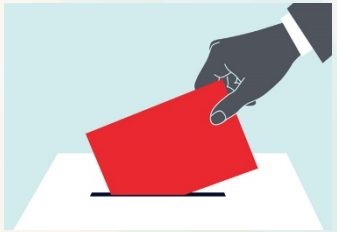
Transparent process



VOTING

Privacy Vs Integrity

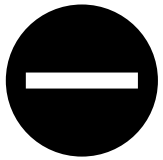
Vote must remain secret



Transparent process

E-VOTING

Basic e-voting zkp protocol



Voters send zkp that their vote is valid

Authorities send zkp they tallied the votes properly

Authorities know who voted what

SECURE AUCTION

- Real world use case: Sugar beet auction in Denmark, in 2008
- Similar protocol as the e-voting scheme
- Bids are processed by 3 servers:
  - Farmers syndicate
  - Danisco
  - Company in charge of the project

SUPPLY CHAIN MANAGEMENT

Products authentication

- Track and trace goods and parts
- Proof of origin

1. Producers creates tokens on a permission blockchain
2. They spend the tokens when goods are exchanged
   - Shipping company
   - Factories
   - Shops

➢ The shop can then provide a certificate of authenticity

- Players do not want to share information (especially with their competitors)
- Authorities wants to see everything

3. Zero-Knowledge proofs to make confidential transactions
4. Viewing keys for the authorities to monitor the network

FINANCIAL USE CASES

“ZKRP helps banks to protect data and meet regulatory requirements”

Mariana Gomez de la Villa, global head of ING's blockchain program (2017)

FINANCIAL USE CASES

PERSONAL COMPLIANCE

- Privacy
- Efficiency

Intersection proof that employee holdings are not in the company blacklist

- Employee must not know the company blacklist
- Employee can cheat (commitment)

FINANCIAL USE CASES

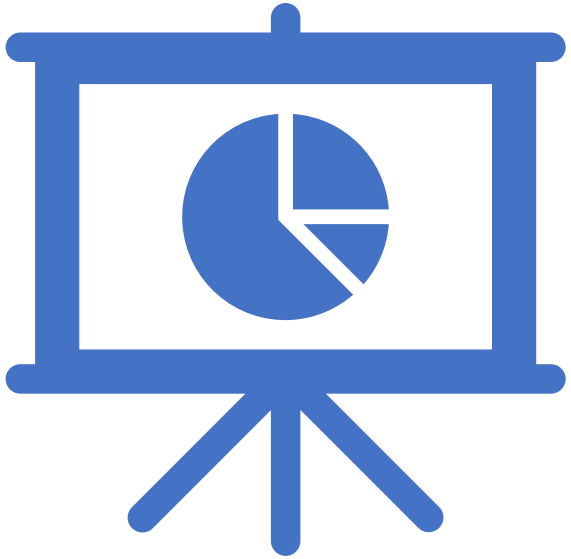
INVESTMENT COMPLIANCE

- Trust
- Misrepresentation

Range proof that the fund follows restrictions
  - f(wi,fi,cmi) =w1*f1+…wn*fn is inside allowed range and cmi is a commitment of wi
- Fund can lie:
  - Regulator can check the commitment for values that are legally reported
  - During investigations, authorities will ask to open the commitment

FINANCIAL USE CASES

FUND COMPLIANCE



- Trust

ZKP sum check for Ponzi scheme

- Each investor/intermediary encrypts their part xi with the fund public key: Xi = E(xi)
- Fund generates a proof that V = f(Xi,sk) where f(.) is decrypting xi using the fund secret key sk and returns their sum
- Authorities check the proof is valid and V is not growing too fast
- If not, they will investigate the fund

OTHER USE CASES

Insurance on a blockchain

Why do we need Zero-Knowledge?

Private smart contracts

Replace the expert with a proof

Anonymous login

Why do we need Zero-Knowledge?

Login with a random ticket T linked to your credential:

$T= (r,r^x)$ where r is random

And a ZKP that:

- the secret key x is corresponding to a valid credential

- your credential is not linked to a revoked ticket

Image authentication

Why do we need Zero-Knowledge?

Photoproof provides robust proof of photography authenticity:

ZKP that the image is the result of photographic filters with private parameters from an authenticated photo.

PHYSICAL CRYPTOGRAPHY

PHYSICAL CRYPTOGRAPHY

Nuclear Disarmament

Why do we need Zero Knowledge?

- ZKP that two nuclear warheads have similar radiograph
- Physical implementation of an **Interactive Zero Knowledge protocol**
  1. Verifier provides several pairs of sensors
  2. Prover initialize each pair at a different offset (for zero-knowledge)
  3. Verifier choose a random angle and random pair, checks they have the same offset
  4. Prover puts the sensors on each warhead
  5. Verifier checks the values are the same
  6. Repeat until desired confidence level is obtained

PHYSICAL CRYPTOGRAPHY

DNA test

- Police tests suspect DNA against a sample from a crime scene
- *Why do we need Zero-Knowledge?*
- Color blind toy example
  - Police inspectors collect DNA sample from the crime scene (C)
  - Defender collects suspect DNA under police supervision (S)
  - Police choose randomly and secretly S or C
  - Defender can tell for sure if it S or C, only if S ≠ C
  - Defender will fail with 50% probability if S==C
  - Repeat until desired confidence level is obtained

➔ Interactivity weakens the protocol, need to use seals and commitment to deal with dishonest parties

PHYSICAL CRYPTOGRAPHY

DNA test (2)

- **Non interactive protocol**, run under police supervision

1. Defender creates several pairs of samples from S and C
2. Each pair is physically analyzed with a different primer chosen randomly (for ZK property)
3. If S==C, all the samples are the same
4. If S<>C, the set of sample is of size 2^k where k is the number of pairs
5. Defender use a Set lower-bound protocol to prove the set is of size one

GUILLAUME DREVON
gd@sikoba.com