qedit

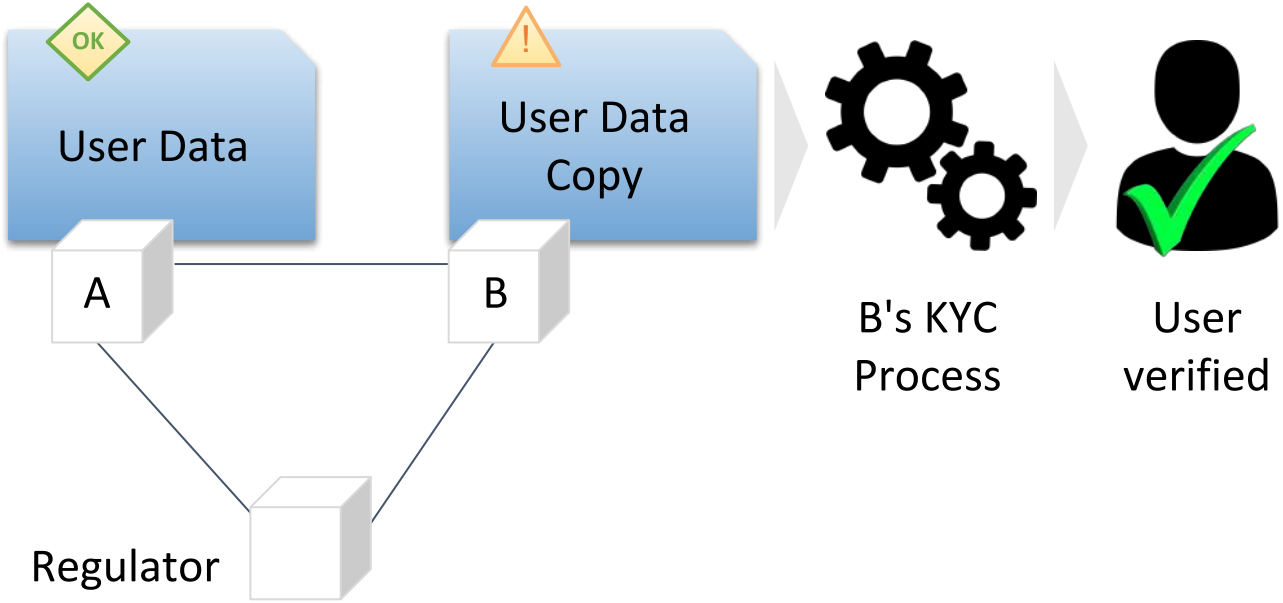
Building a Trust Ecosystem for Adoption of ZKP

Presented at ZKProof.org Amsterdam, October 2019

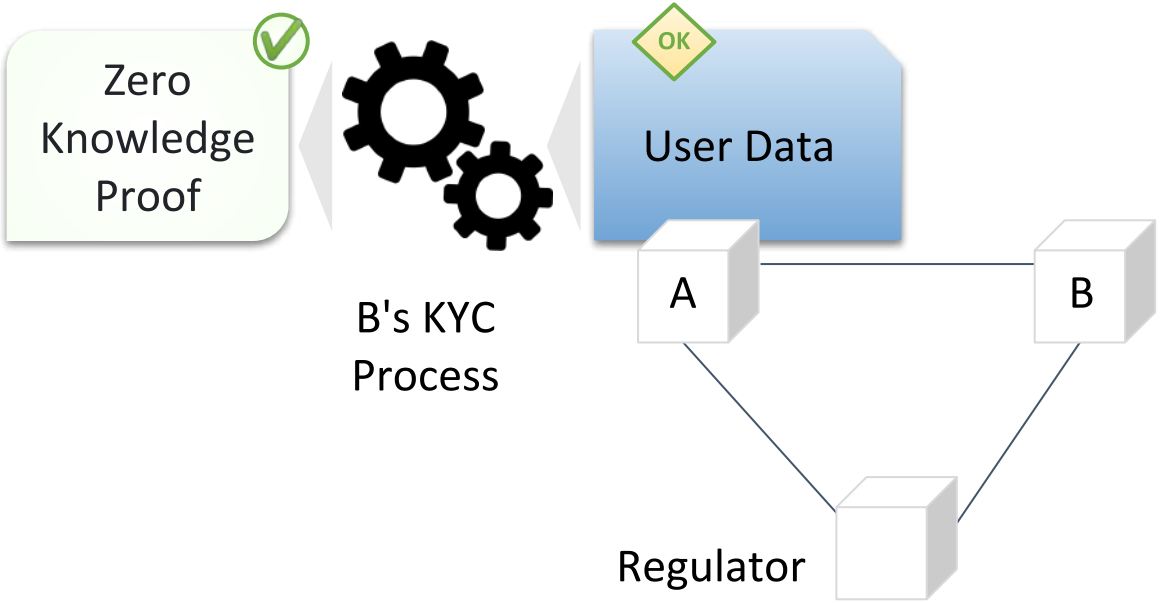
Jonathan Rouach
QEDIT CEO, co-founder

How to foster ZKP adoption in the enterprise world?

Detect the need | KYC verification on user data copy

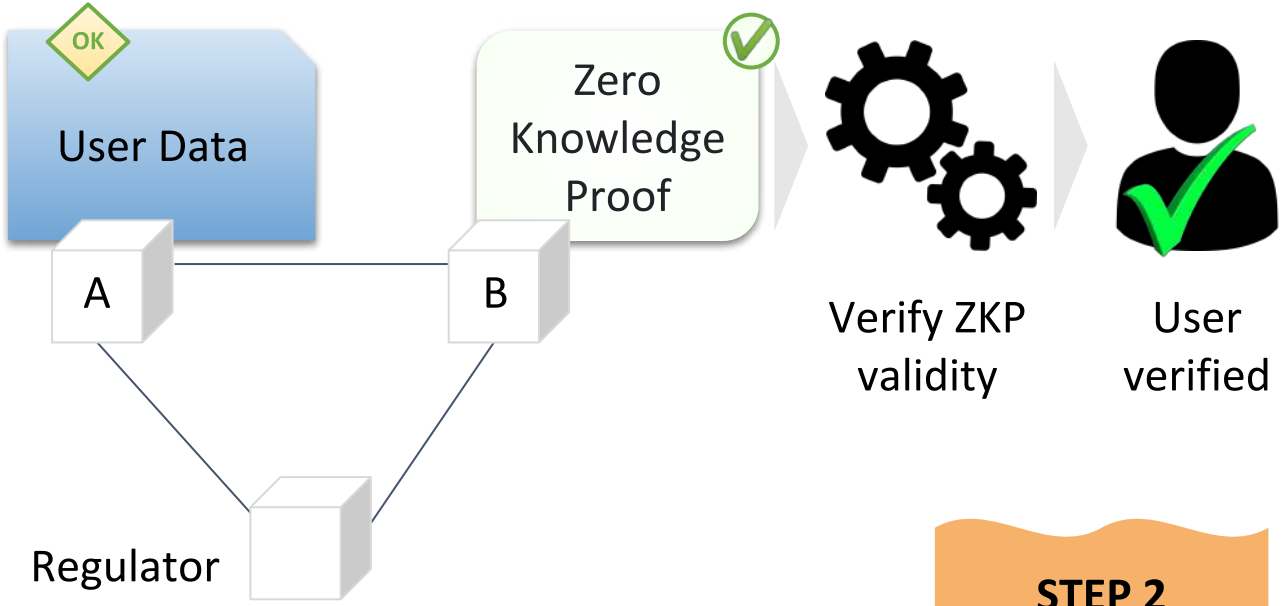


Proposed solution | KYC verification on user data source

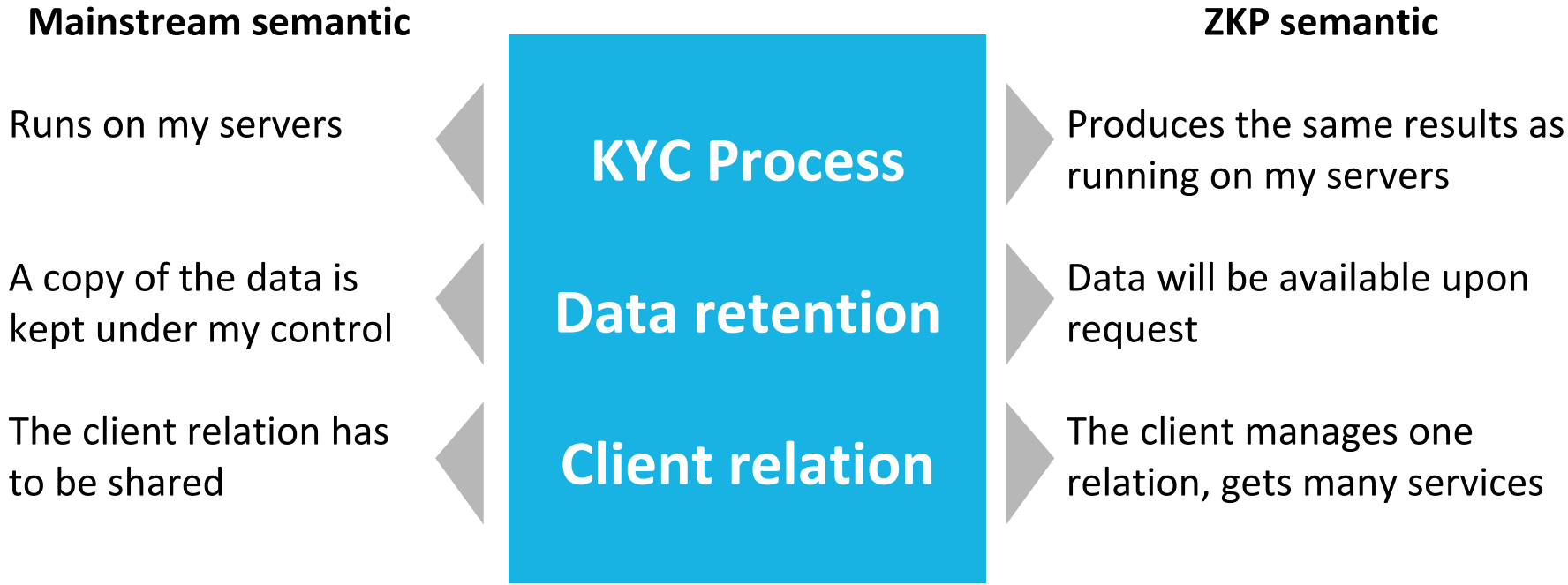


STEP 1

Proposed solution | KYC verification on user data source



ZKP | enables a new separation of concerns



ZKP | A prolific research field

Pinocchio: Nearly Practical Verifiable Computatio

Bryan Parno, Jon Howell — *Microsoft Research*
Craig Gentry, Mariana Raykova — *IBM Research*

Abstract

To instill greater confidence in computations outsourced to

Computing [9–11] or other secure harc
that physical protections cannot be defe
roduced a number
–23] that offer co
ecause they rely c
ofs (PCPs) [17]
4], the performar
ces would take h

Sonic: Zero-Knowledge SNARKs from Linear-Size Universa Updatable Structured Reference Strings

Mary Maller, mary.maller.15@ucl.ac.uk, University College London
Sean Bowe, sean@z.cash, Electric Coin Company
Markulf Kohlweiss, mkohlwei@ed.ac.uk, University of Edinburgh, IOHK
Sarah Meiklejohn, s.meiklejohn@ucl.ac.uk, University College London

ABSTRACT

Ever since their introduction, zero-knowledge proofs have become an important tool for addressing privacy and scalability concerns in a variety of applications. In many systems each client downloads and verifies every new proof, and so proofs must be small and cheap to verify. The most practical schemes require either a trusted setup, as in (pre-processing) zk-SNARKs, or verification complexity that scales linearly with the complexity of the relation, as in Bulletproofs. The structured reference strings required by most zk-SNARK schemes can be constructed with multi-party computation protocols, but the resulting parameters are specific to an individual relation. Groth et al. discovered a zk-SNARK protocol with a universal structured reference string that is also updatable, but the

protocols. There are several practical schemes from wh
with a vast space of tradeoffs in performance and c
assumptions.
Currently, the most attractive proving system from
perspective is a (pre-processing) succinct non-interact
of knowledge, or zk-SNARK for short, which has a c
proof size and constant-time verification costs even f
large relations. The most efficient scheme described in
is a zk-SNARK by Groth [45] which contains only
elemen
friendl
In c
require

PLONK: Permutations over Lagrange-bases Oecumenical Noninteractive arguments o Knowledge

Ariel Gabizon, Protocol Labs
Zachary J. Williamson, Aztec Protocol
Oana Ciobotaru

October 27, 2019

Abstract

Halo: Recursive Proof Composition without a Trusted Setup

Sean Bowe, sean@electriccoin.co, Electric Coin Company
Jack Grigg, jack@electriccoin.co, Electric Coin Company
Daira Hopwood, daira@electriccoin.co, Electric Coin Company

Abstract

Non-interactive proofs of knowledge allow us to publicly demonstrate the faithful execution of arbitrary computations. SNARKs have the additional property of succinctness, meaning that the proofs are short and fast to verify even when the computations involved are large. This property raises the prospect of recursive proof composition: proofs that verify other proofs. All previously known realizations of recursive proof composition have required a trusted setup and cycles of expensive pairing-friendly elliptic curves.

We obtain the first practical example of recursive proof composition without a trusted setup, using only ordinary cycles of elliptic curves. Our primary contribution is a novel technique for amortizing away expensive verification procedures from within the proof verification

On the Size of Pairing-based Non-interac

Jens Groth**

University College London, UK
j.groth@ucl.ac.uk

Abstract. Non-interactive arguments enable a prover to convinc
ment is true. Recently there has been a lot of progress both in
constructing highly efficient non-interactive arguments with sm
cation complexity, so-called succinct non-interactive arguments (S
non-interactive arguments of knowledge (SNARKs).
Many constructions of SNARGs rely on pairing-based cryptography
a proof consists of a number of group elements and the verificati

Bulletproofs: Efficient Range Proofs for Confidential Transactions

Benedikt Bünz*[1], Jonathan Bootle[†2], Dan Boneh[‡1], Andrew Poelstra[§3], Pieter Wuille[¶3], and Greg Maxwell[‖3]

[1]Stanford University
[2]University College London
[3]Blockstream

Abstract

We propose Bulletproofs, a new non-interactive zero-knowledge proof protocol with very short proofs and without a trusted setup; the proof size is only logarithmic in the witness size. Bulletproofs are especially well suited for efficient range proofs on committed values: they enable proving that a committed value is in a range using only $2\log_2(n) + 9$ group and field elements, where n is the bit length of the range. Proof

ZKP | Clients don't understand enough to trust it

Academic researchers discover and understand the math

Scientific community review papers and improve schemes

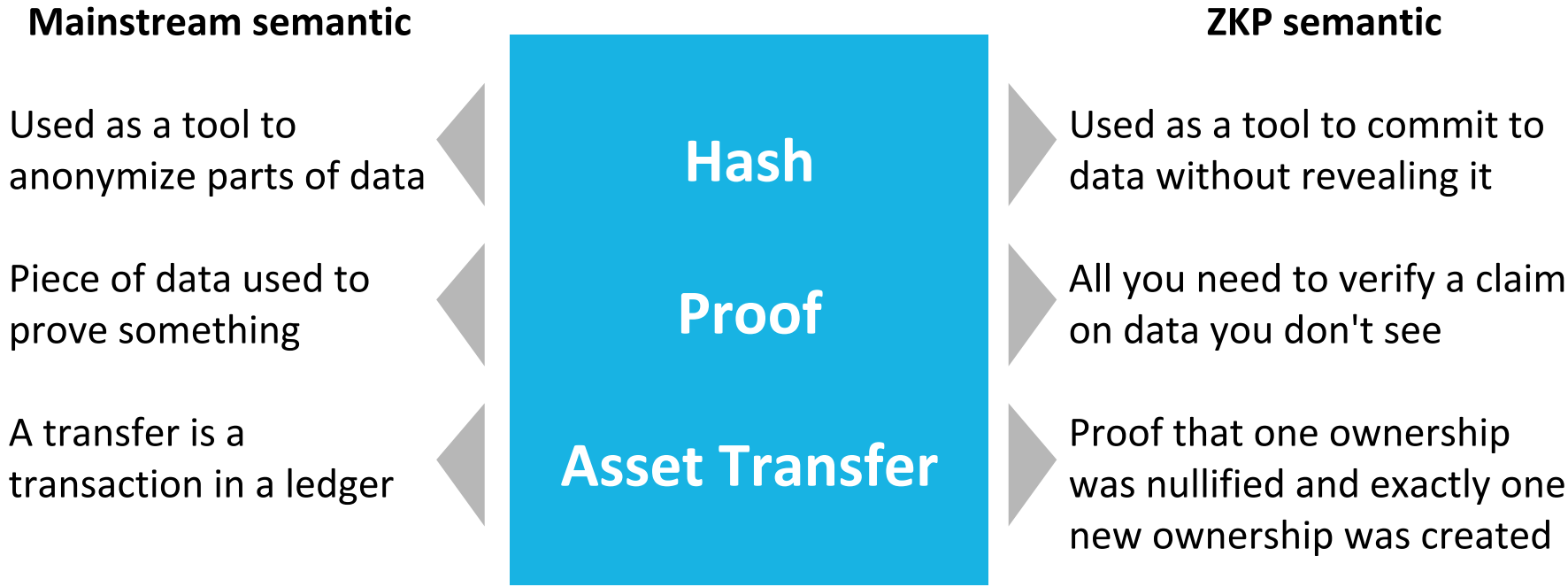
Engineers & Devs implement libraries

Integrators & Clients


ZKProof.org

ZKP adoption | Building ZKP trust ecosystem

ZKP Adoption | We still to bridge semantic gaps



ZKP Adoption | WEF promotes Privacy

Deloitte EduScrypt

A welcome partner in the trust ecosystem

Key ideas| They will adopt it when they trust it

- **Companies want to innovate, be the first to deploy… the standard!**
  - Enterprises have reputation, valuable data at stake, need strong assurances
  - Don't have the people to vet the tech
- **ZKProof gives enterprises the time to adopt, by slowing down the pace**
  - ZKP produces more and more papers, schemes
  - Added benefit of permitting e.g. tools, hardware acceleration
- **It's an ecosystem of trust to review and compare practices**
  - From the lab to the clients, keep the trust going
  - There is no revolution without redefining the meaning of the words

Data is the new gold, ZKP is the new vault

