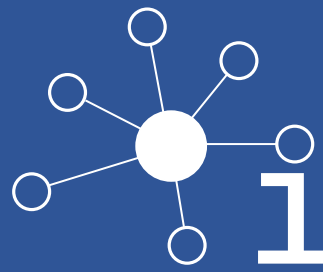


itugen

Transparent and anonymous voting on blockchain

We believe that e-voting has the potential
to become a blockchain Killer App.
We are now seeking investors who can help us
to bring itugen from protocol to product.

Powered by:

sikoba RESEARCH isekai

v Dec 20

The itugen technical paper was presented by Vincenzo Iovino at ITASEC20 in February 2020

Itugen: Transparent and Anonymous voting without Tallying Authorities

Guillaume Drevon[1], Vincenzo Iovino[2], and Aleksander Kampa[1]

[1]Sikoba Research
{gd,ak}@sikoba.com
[2]University of Salerno,
vinciovino@gmail.com

6 December 2019

Abstract

We propose itugen, a new verifiable e-voting system that enjoys very strong security guarantees. Our scheme strictly divides ballot allocation from voting, and the voting system ensures both privacy and verifiability. Authorities are trusted only to guarantee the validity and independence of the ballots but cannot break the privacy of any individual voter or subvert the result of the election even if they collude.

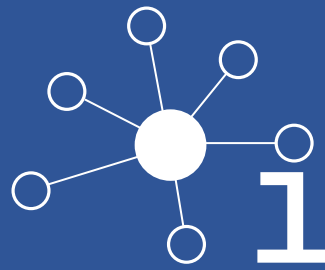
Our system is based on isekai, a versatile and powerful implementation of the major recent variants of succinct zero-knowledge proofs including SNARKs, Aurora, Ligero and Bulletproofs. Integrating these mechanisms in a modular way, our e-voting scheme can be instantiated from a number of currently-mature *post-quantum secure* primitives, with the possibility of adding new schemes in the future.

Keywords: e-voting, zero-knowledge, system design.

Voting is at the heart of every democratic system

The future is clearly in e-voting, but existing systems are not without problems

itugen



itugen

A revolutionary e-voting system

without trusted authority offering

complete transparency

AND

total anonymity

itugen

Transparency

All poll data is published on the itugen blockchain, constituting a public and inalterable record

+ list of all voters

+ all ballots

itugen

Transparency

Anyone can verify that a ballot is valid

(verification of zero-knowledge proof attached to ballot)

itugen

Transparency

Multiple ballots by the same voter are easily identified:

double voting is not possible

itugen

Transparency

After polling ends:

the content of all votes becomes publicly visible
and anyone can verify the result

(no need for a trusted authority)

itugen

Anonymity

Voter identity remains secret forever

(using quantum-resistant cryptography)

itugen

zero-knowledge proofs

blockchain

quantum-resistance

cryptography

complete transparency + total anonymity

https://www.itugen.com

itugen is backed by the team behind Sikoba Research.

Sikoba Research conducts fundamental and applied research in the areas of cryptography, blockchain and distributed systems.

We are the developers of the **isekai** zero knowledge framework.

Zero-knowledge framework supporting:

libsnark (Groth16 and BCTV14a), dalek (Bulletproofs) and libiop (Aurora and Ligero)

a wide subset of C / C++ code

Business model and clients

- Poll organisers pay all fees, voters participate for free
- Initial focus on blockchain and ERC20 token governance
- With COVID-19, e-voting will also become increasingly relevant for state elections.

itugen

Itugen Roadmap

- Technology stack: ready now!
- Technical implementation paper: published December 2019 (*)
- Coding started: January 2020
- POC target: (tbd, will depend on funding)
- MVP target (tbd, will depend on funding)

* Presented at ITASEC20 (www.itasec.it) in February 2020

itugen

We’re looking for:

- Investors
- Partners
- Organisations that need e-voting

itugen

zero-knowledge proofs

blockchain

quantum-resistance

cryptography

complete transparency + total anonymity

https://www.itugen.com

Contact:

Alex Kampa

ak@sikoba.com

+352 691 46 85 81

Links:

Itugen website

Sikoba Research

Isekai 1.0 announcement

itugen