



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:



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

ITASEC20 ABOUT PROGRAM REGISTRATION NEWS CALLS IMPORTANT DATES PARTNERS ACC

FRI 07 FEB

SESSION 14: CRYPTOLOGY (CRYPTOGRAPHY AND CRYPTANALYSIS)
9:45 Am - 10:45 Am Aula 155/5-6, Facoltà Di Ingegneria | Via Brezze Bianche, 12
Track: 08.Scientific & Technical track | Feb 5-6-7

EVENT DETAILS

Session chair: Massimiliano Sala

Efficient Identity-Based Encryption from RSA groups
Vincenzo Iovino

A Hardware Implementation for Code-based Post-quantum Asymmetric Cryptography
Kristjane Koleci, Marco Baldi, Maurizio Martina and Guido Masera

Itugen: Transparent and Anonymous voting without Tallying Authorities
Guillaume Drevon, Vincenzo Iovino and Aleksander Kampa

Itugen: Transparent and Anonymous voting without Tallying Authorities

Guillaume Drevon¹, Vincenzo Iovino², and Aleksander Kampa¹

¹Sikoba Research

{gd,ak}@sikoba.com

²University of Salerno,
vinciovin@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, Ligerio 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



The screenshot shows a news article from the Swiss Post website. The header features the Swiss Post logo on the left and a 'Menu' button on the right. The main headline is 'Swiss Post temporarily suspends its e-voting system' with a date of '29.3.2019'. Below the headline are three category tags: 'Security', 'Cantons', and 'Public Intrusion Test (PIT)'. The article text discusses a public intrusion test ordered by the Confederation and cantons, which revealed critical errors in the source code of the new e-voting system. Swiss Post is taking action to correct the code and has decided to suspend the system for the May 19 elections.

SWISS POST  Menu 

Swiss Post temporarily suspends its e-voting system

29.3.2019

[Security](#) [Cantons](#) [Public Intrusion Test \(PIT\)](#)

The public intrusion test ordered by the Confederation and the cantons on Swiss Post's new e-voting system is complete. Although the electronic ballot box could not be hacked, feedback on the published source code reveals critical errors. Since the integrity of votes and elections is a top priority, Swiss Post is taking action. It will correct the source code and have it reviewed again by independent experts. It will therefore not provide its e-voting system to the cantons for the votes of 19 May.



**A revolutionary e-voting system
without trusted authority offering**

complete transparency

AND

total anonymity



Transparency

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

+ list of all voters

+ all ballots

Transparency

Anyone can verify that a ballot is valid

(verification of zero-knowledge proof attached to ballot)

Transparency

Multiple ballots by the same voter are easily identified:

double voting is not possible

Transparency

After polling ends:

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

(no need for a trusted authority)

Anonymity

Voter identity remains secret forever

(using quantum-resistant cryptography)

blockchain

zero-knowledge proofs

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 Ligerio)**

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 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

We're looking for:

- Investors
- Partners
- Organisations that need e-voting

blockchain

zero-knowledge proofs

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](#)

