iteratec

DecentraVote

Elektronische Beschlussfassung mit Blockchain-Unterstützung

Dr. Zoltan Fazekas

TL;DR Was als Forschungsprojekt und Eigenentwicklung für die Mitarbeitergenossenschaft der iteratec begann, ist durch Corona zum Produkt für dezentralisiertes anonymes e-Voting für Vereine, Genossenschaften, Gemeinderäte uvm. geworden

Welche Funktionen bieten wir?

- ✓ Mitglieder, Organe erfassen
- ✓ Versammlung, Anmeldungen, Stimmvollmachten verwalten
- ✓ Wahlen und Abstimmungen, spontane Änderungsanträge
- ✓ Stimmberechtigte festlegen
- ✓ Anonyme Abgabe von geheimen Stimmen
- ✓ Stimmauszählung und Ergebnisermittlung gemäß Beschlussanforderungen
- ✓ Anhang zur Niederschrift erstellen

Was müssen wir sicherstellen?

- ✓ Nur stimmberechtigte Mitglieder, Bevollmächtigte
- ✓ Jeder nur eine Stimmabgabe
- ✓ Abgegebene Stimmen nicht zuordenbar
- ✓ Abgegebene Stimmen nicht veränderbar
- ✓ Abgegebene Stimme durch das Mitglied verifizierbar
- ✓ Zwischenergebnis nicht einsehbar
- ✓ Endergebnis durch jedes Mitglied überprüfbar
- ✓ Eigene Entscheidung durch das Mitglied nicht beweisbar

DApp Frontend 1

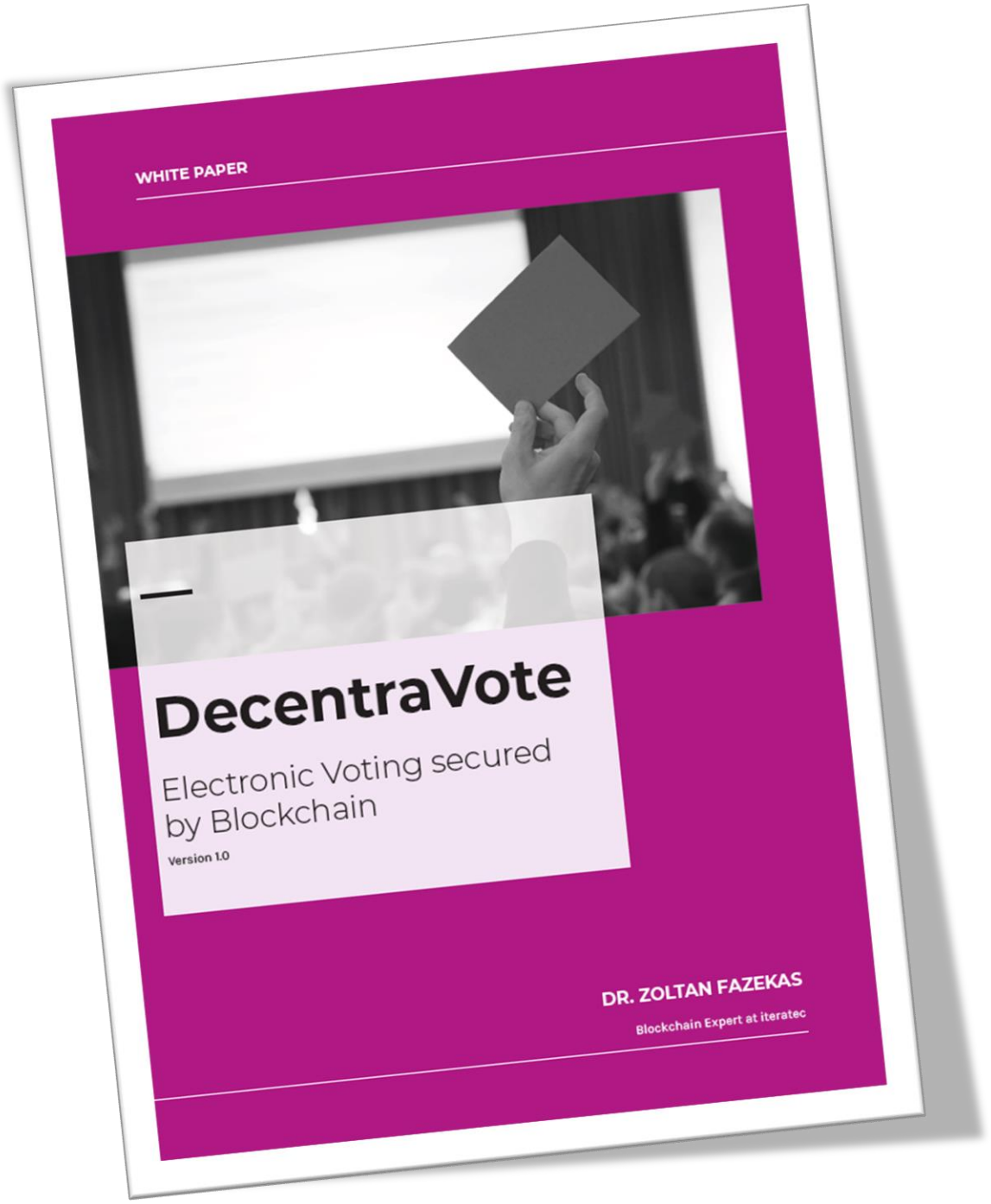
- Sign and submit transactions
- Generate proofs, encrypt votes
- Verify the hash of all files and data loaded by the browser

Smart Contracts 2

- Manage addresses of members, hashes and public keys of votes
- Verify proofs and permissions of addresses to cast a vote

Decentralized Backend 3

- Host files, texts and other data with hashes stored on-chain
- Relay proofs and nullifiers to register one-time accounts



What is coming next?

- Evaluating quinary incremental Merkle trees using Poseidon instead of MiMC hashes
- Migration to wasm based proof generation to make it usable on smartphones
- Anonimity in conjunction with weighted votes
- Wallet without browser extentions like MetaMask, Nifty etc.

iteratec

iteratec
#nurdemteam

Kontakt

Dr. Zoltan Fazekas

Zoltan.Fazekas@iteratec.com

iteratec GmbH, Donau-City-Straße 11, 1220 Wien

www.iteratec.at