random oracle modified ElGamal Paillier

everlasting privacy commitment scheme Gen

additive homomorphic encryption designated ve

usability eligibility verifiability integrity acco

robustness e-Voting secret-ballot voting sc

cryptographic voting protocols electronic voting

privacy (E2E) verifiability Cast-As-Intende

secrecy of the ballot receipt-freeness Reco

ercion resistance Tallied-As-Recorded

n-interactive zero-knowledge proof blind signa

ixnet-based approach auditability re-encryp

public bulletin board multi-candidate, multi-au

random oracle modified ElGamal Paillier

everlasting privacy commitment scheme Gen

additive homomorphic encryption designated ve

usability eligibility verifiability integrity acco

robustness **E-VOTING** secret-ballot voting sc

cryptographic voting protocols electronic votin

PRIVACY (E2E) **VERIFIABILITY** Cast-As-Intende

secrecy of the ballot receipt-freeness Reco

ercion resistance Tallied-As-Recorded

n-interactive zero-knowledge proof blind signa

ixnet-based approach **AUDITABILITY** re-encryp

public bulletin board multi-candidate, multi-au

Art. 3 Risikobeurteilung

[1] Mit einer Risikobeurteilung muss der Kanton ausführlich und verständlich dokumentieren, dass sich jegliche Sicherheitsrisiken in einem ausreichend tiefen Rahmen bewegen. Die Beurteilung bezieht sich auf folgende Sicherheitsziele:

a. Korrektheit des Ergebnisses;

SECRECY OF THE BALLOT

b. Schutz des Stimmgeheimnisses und Ausschluss vorzeitiger Teilergebnisse;

c. Verfügbarkeit der Funktionalität;

AVAILABILITY

ANONYMITY

d. Schutz der persönlichen Informationen über die Stimmberechtigten;

COERCION-RESISTANCE

e. Schutz der Informationen für die Stimmberechtigten vor Manipulationen;

RECEIPT-FREENESS

f. Ausschluss von Beweisen zum Stimmverhalten.

[2] Jedes Risiko muss mit Bezug auf die Sicherheitsziele, allfällige mit ihnen verbundene Datensätze, Bedrohungen, Schwachstellen und die Dokumentation zum System und zu dessen Betrieb identifiziert und klar beschrieben werden. Der Kanton muss auf dieser Grundlage begründen, weshalb er die Risiken als hinreichend gering einschätzt.

[3] Die Minimierung von Risiken darf sich nicht darauf abstützen, sicherheitsrelevante Informationen zum System und dessen Betrieb geheim zu halten.

https://www.admin.ch/opc/de/classified-compilation/20132343/index.html

– **Art. 4** Anforderungen an die Zulassung von mehr als 30 Prozent des kantonalen Elektorats

INDIVIDUAL VERIFIABILITY

cast-as-intended

[1] Soll ein System für den Einbezug von mehr als 30 Prozent des kantonalen Elektorats zugelassen werden, so müssen die Stimmenden die Möglichkeit haben, zu erkennen, ob ihre Stimme auf der Benutzerplattform oder auf dem Übertragungsweg manipuliert oder abgefangen worden ist (individuelle Verifizierbarkeit, Anhang Ziff. 4.1 und 4.2).

cast-as-recorded

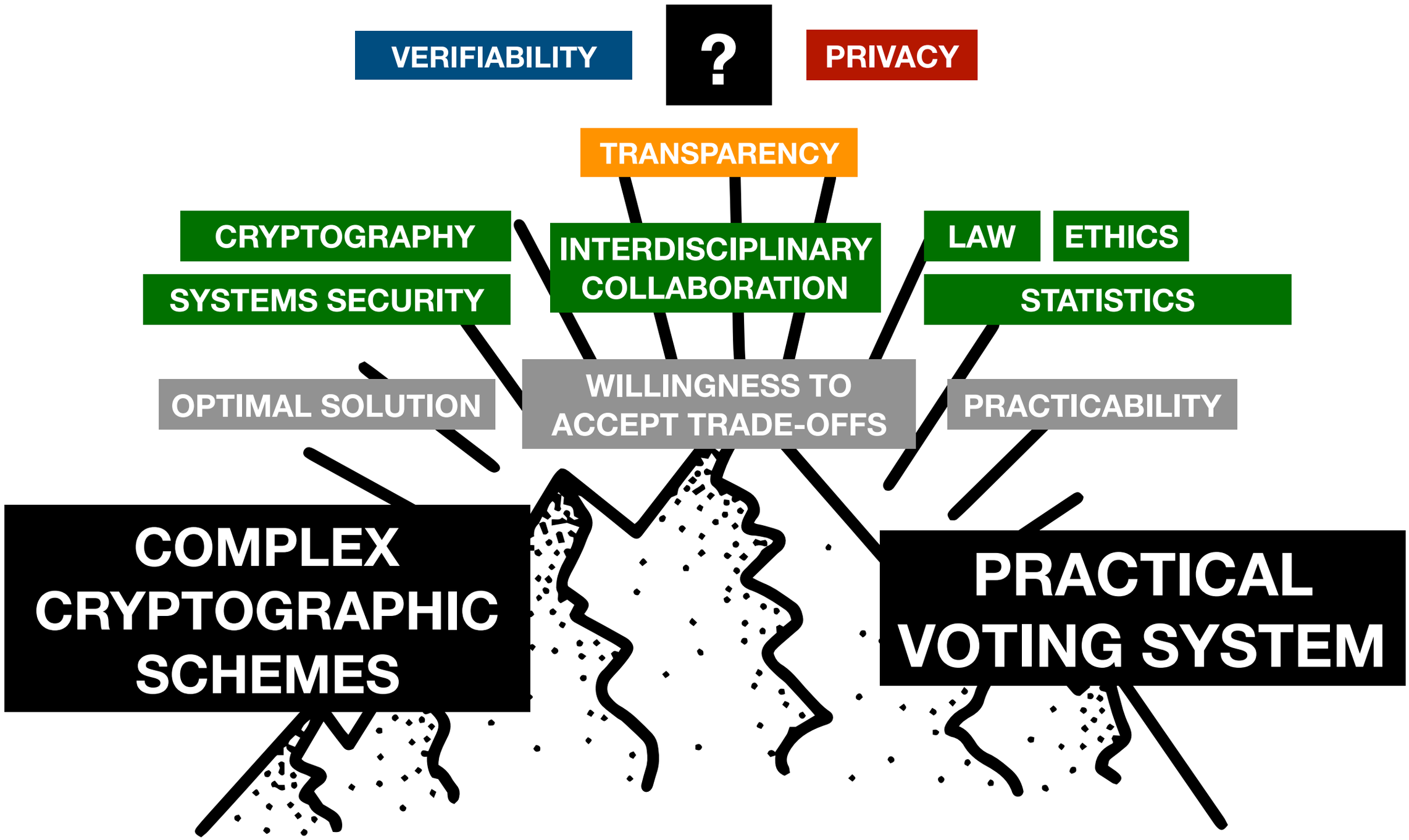
[2] Zur individuellen Verifizierung muss die stimmende Person einen Beweis erhalten, dass das serverseitige System die Stimme so, wie sie die stimmende Person in die Benutzerplattform eingegeben hat, als systemkonform abgegeben registriert hat. Der Beweis muss für jede Teilstimme die korrekte Registrierung bestätigen.

– **Art. 5** Anforderungen an die Zulassung von mehr als 50 Prozent des kantonalen Elektorats

counted-as-recorded

[1] Soll ein System für den Einbezug von mehr als 50 Prozent des kantonalen Elektorats zugelassen werden, so muss sichergestellt sein, dass Stimmende oder die Prüferinnen und Prüfer unter Einhaltung des Stimmgeheimnisses die Möglichkeit haben, jede Manipulation zu erkennen, die zu einer Verfälschung des Ergebnisses führt (vollständige Verifizierbarkeit, Anhang Ziff. 4.3 und 4.4).

E-VOTING IN A NUTSHELL



pro-civis

e-government as a service

[PROVOTUM]

PRIVACY, VERIFIABILITY AND AUDITABILITY IN BLOCKCHAIN-BASED E-VOTING

Masters Project University of Zurich, Killer Christian, Matile Raphael

[PROVOTUM]

PRIVACY, VERIFIABILITY AND AUDITABILITY IN BLOCKCHAIN-BASED E-VOTING

VISION

INTERDISCIPLINARY FIELD

ELECTRONIC VOTING

BLOCKCHAIN

ETHEREUM

CRYPTOGRPAHY

HOMOMORPHIC ENCRYPTION

THEORETICAL BUILDING BLOCKS

PRIVACY, VERIFIABILITY & AUDITABILITY

"[…] blockchains do not address any of the fundamental problems in elections, and their use actually makes things worse"

Public Evidence from Secret Ballots

Benaloh, J., Bernhard, M., Halderman, J. A., Rivest, R. L., Ryan, P. Y. A., Stark, P. B., Teague, V., Vora, P. L., and Wallach, D. S. (2017)

STAKEHOLDERS

VOTING AUTHORITY

SETUP & ADMINISTRATION

[PROVOTUM]

VOTER

VOTES & CHALLENGES

MOCK-IDENTITY-PROVIDER

AUTHENTICATE & DISTRIBUTE WALLETS

VOTING PROCESS

SETUP

VOTING

COUNTING

GENERATE GENESIS BLOCK AND WALLETS

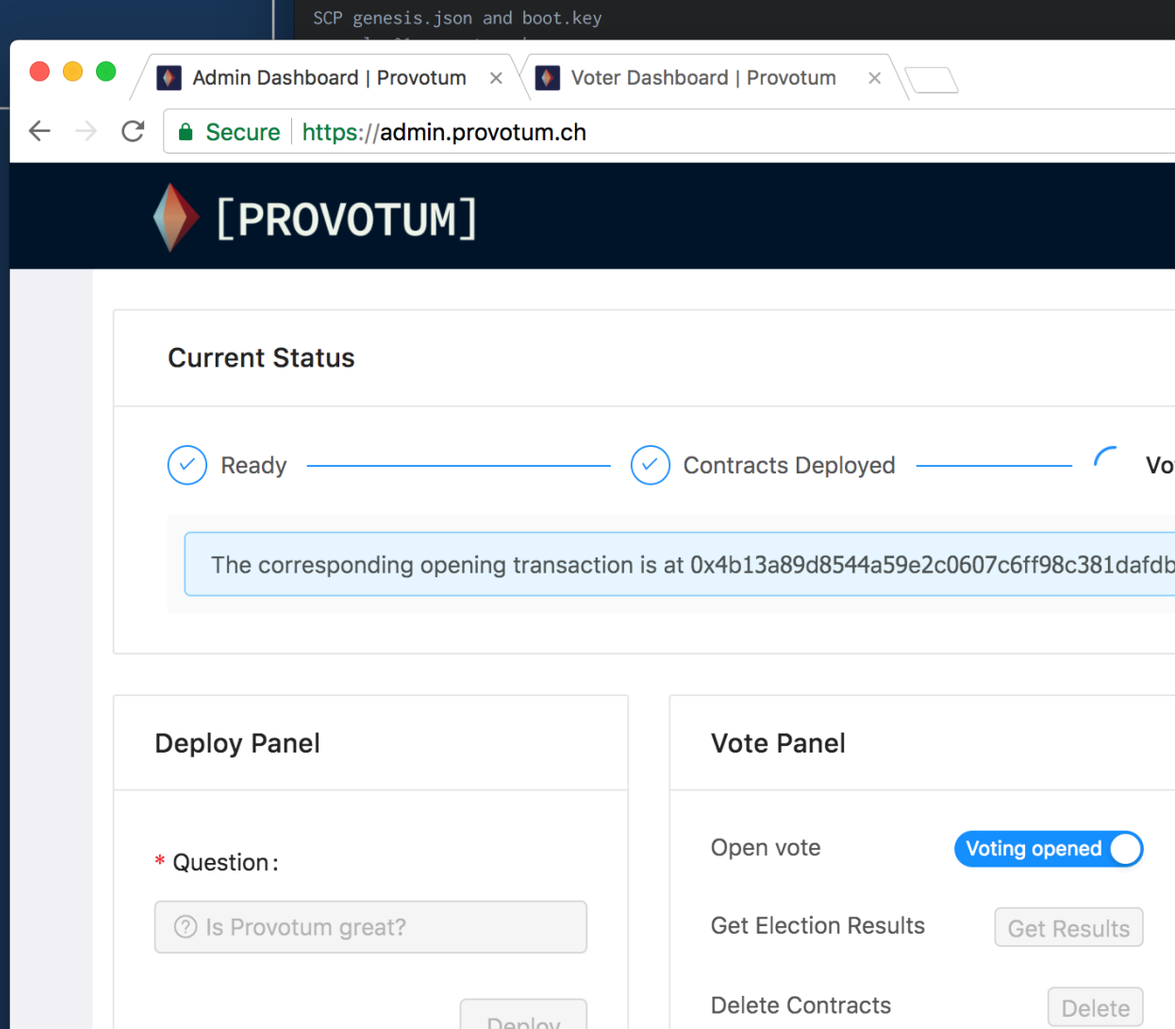
SEND PRIVATE KEYS TO MOCK IDENTITY PROVIDER

DEPLOY BLOCKCHAIN

DEPLOY SMART CONTRACTS

OPEN VOTING

```
10:53:37 killer@dhcp-wlan-uzh-10-12-0-153 ~/setup v8.10.0 b829e9a ✔
$ ./setup.sh
########################################
Executing steps/01-deploy-poa-net/
########################################
Generating keys using keythereum
 Generating [1000] keys
 Adding 5 nodes (sealer01-sealer05) to genesis block.
 Generating   [POA]   genesis block.
 ✔ Sucessfully sent private keys to http://138.68.69.99:8080/wallets
 Killing all running geth instances on the sealer nodes
 → sealer01.provotum.ch
 → sealer02.provotum.ch
 → sealer03.provotum.ch
 → sealer04.provotum.ch
 → sealer05.provotum.ch
 ✔Killed all running geth instances on the sealer nodes
 Deleting old files from the sealer nodes
 → sealer01.provotum.ch
^[^[^[ → sealer02.provotum.ch
 → sealer03.provotum.ch
 → sealer04.provotum.ch
 → sealer05.provotum.ch
 ✔Deleted all old files
 SCP genesis.json and boot.key
```



VOTING PROCESS

SETUP

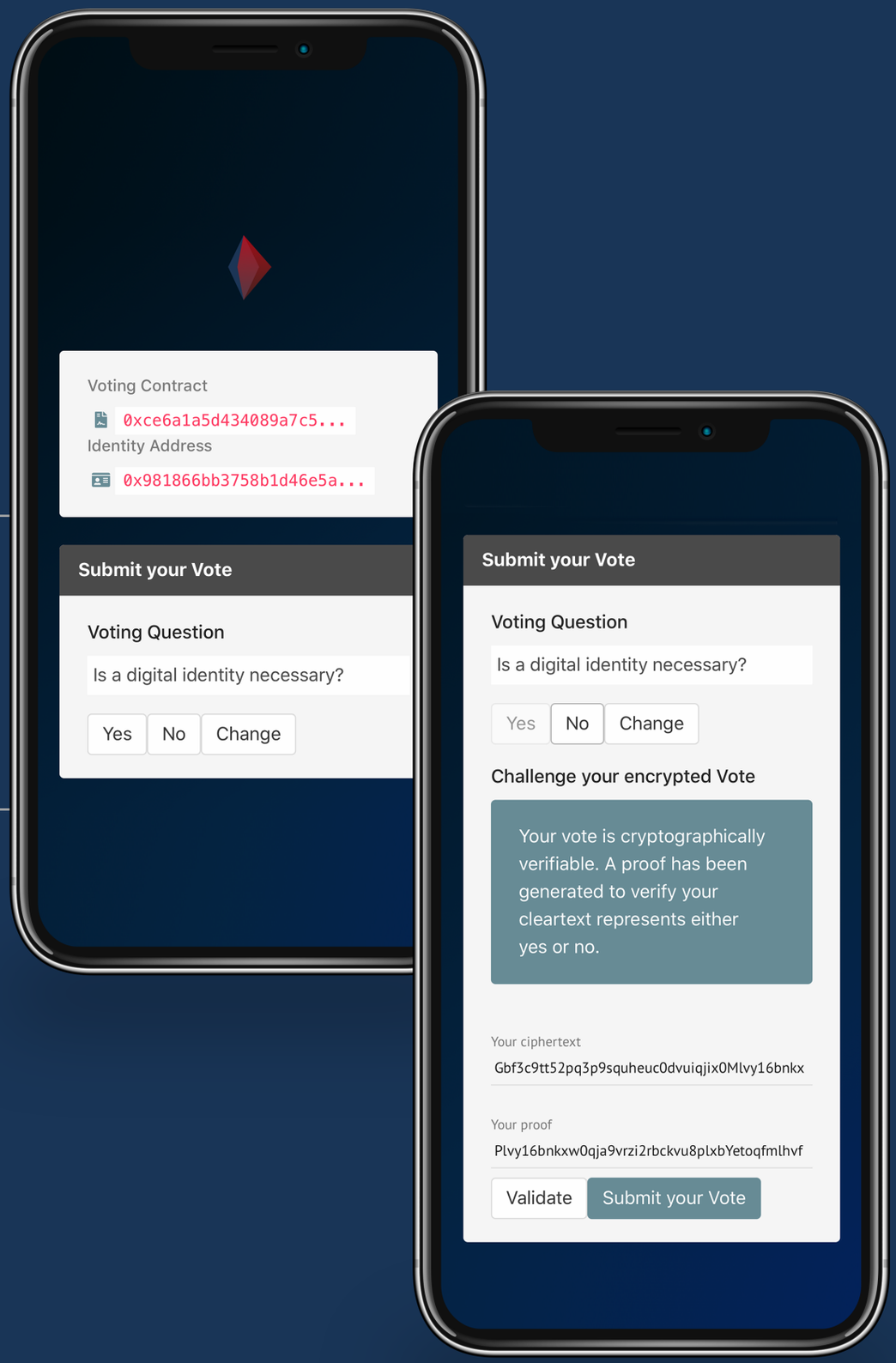
VOTING

COUNTING

VOTER ENCRYPTS VOTE

VOTER CHALLENGES VOTE

VOTER SUBMITS VOTE



VOTING PROCESS

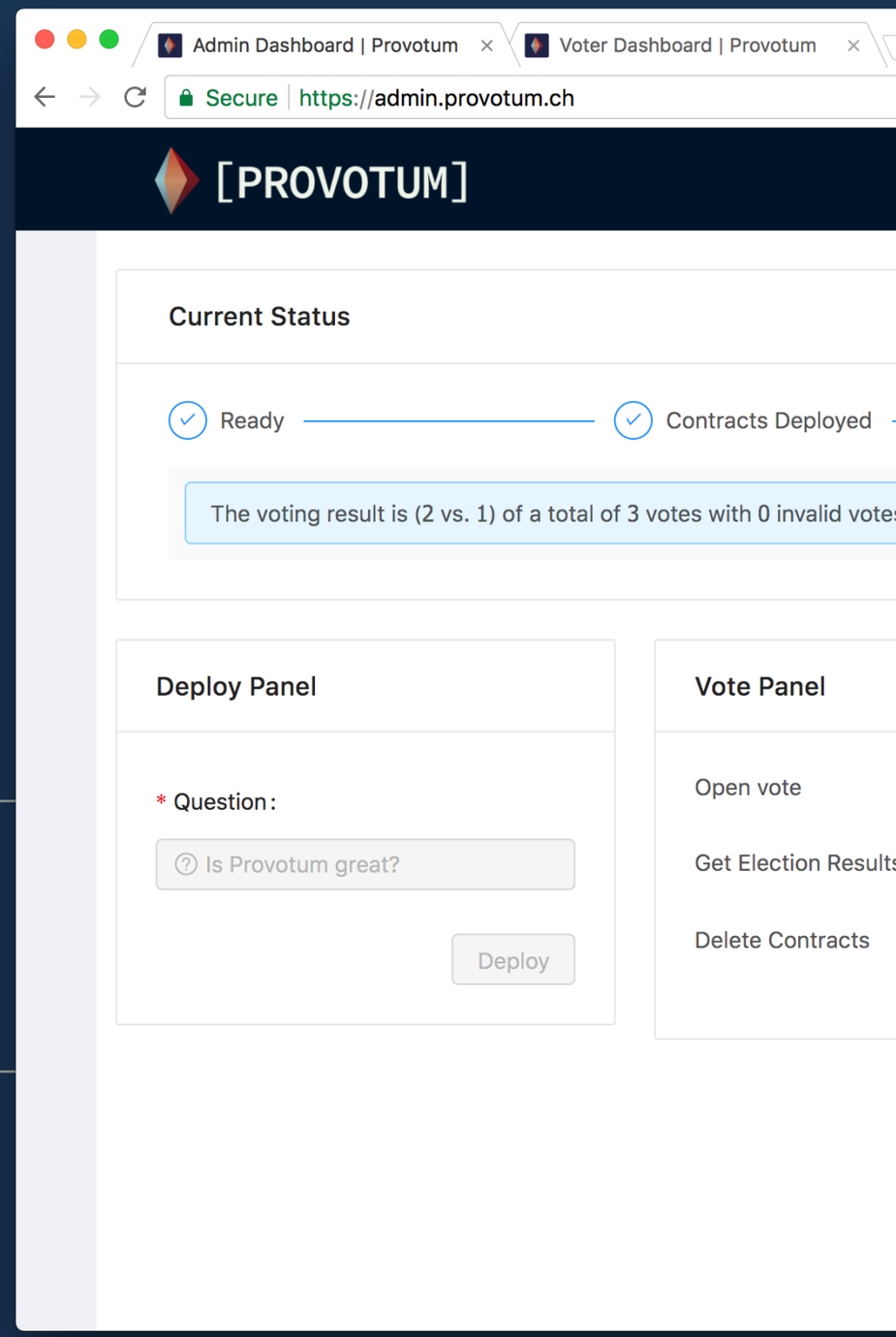
SETUP

VOTING

COUNTING

BACKEND CLOSES VOTE

BACKEND HOMOMORPHICALLY ADDS, DECRYPTS AND PUBLISHES RESULT



EVALUATION

PROPERTY	STATUS	REASON
INDIVIDUAL VERIFIABILITY	**FULFILLED**	*“I QUERY THE BLOCKCHAIN”*
UNIVERSAL VERIFIABILITY	**FULFILLED**	*“I VERIFY THE PROOF”*
END-TO-END VERIFIABILITY	**PARTIALLY**	
├── CAST-AS-INTENDED	**NOT FULFILLED**	*“I **TRUST** THE BACKEND”*
├── RECORDED-AS-CAST	**FULFILLED**	*“I CAN SEE THE TRANSACTION”*
└── COUNTED-AS-RECORDED	**FULFILLED**	*“I VERIFY THE PROOF”*
AUDITABILITY	**FULFILLED**	*“I QUERY THE BLOCKCHAIN (AND LOGS)”*
BALLOT-PRIVACY	**FULFILLED**	*“VA DOESN’T KNOW WHO I AM”*
RECEIPT-FREENESS	**FULFILLED**	*“I CAN NOT PROVE WHAT I VOTED”*
COERCION-RESISTANCE	**NOT FULFILLED**	*“I CAN’T FAKE A VOTE”*

SOLIDITY X CRYPTOGRAPHY *BIG INTEGER & MODULAR ARITHMETICS*

E2E-V FOR SWISS REGULATION *CAST-AS-INTENDED*

@Raphael Matile's Master Thesis:

https://github.com/provotum/node-rs
https://github.com/provotum/client-rs

ELECTIONS INSTEAD OF VOTES *NOT JUST YES OR NO*

THRESHOLD CRYPTOGRAPHY *SPLIT UP PRIVATE KEY*

Thanks for your attention

provotum.ch