Актуальные проблемы систем дистанционного электронного голосования

Петр Мурзин
аспирант ВИНИТИ РАН,
разработчик проекта Polys
АО «Лаборатория Касперского»

kaspersky

Polys

Определения

Электронное голосование *(electronic voting / e-voting)* - голосование, в котором применяются электронные технические средства (как минимум на этапе подачи голоса).

Два класса систем электронного голосования (условно):

- ***традиционные*** - голосование производится на избирательных участках с применением специальных технических средств (DRE / Optical Scan Voting Systems);
- ***дистанционные*** - личная явка избирателя на избирательный участок не требуется.

Требования к системам электронного голосования

- Приватность (privacy);
- Полнота (completeness);
- Устойчивость (soundness);
- Правомочность (eligibility);
- Невозможность «двойного» голосования (unreusability);
- Равнодоступность (fairness);
- **Проверяемость (verifiability);**
- **Всеобщая проверяемость (universal verifiability);**
- Сопротивление принуждению (coercion-resistance) *

Системы голосования с прямой записью / КОИБы

DRE (Paper trail – опционально)

КОИБ

Не обеспечивают свойства проверяемости и всеобщей проверяемости

kaspersky

Polys

Технологии обеспечения требований к системам ДЭГ

Требования	Обеспечиваются
Приватность (privacy)	Слепая подпись, HE, ZK-Proofs
Полнота (completeness) / Устойчивость (soundness)	Смарт-контракт
Правомочность (eligibility)	Система идентификации
Невозможность «двойного» голосования (unreusability)	Блокчейн
Равнодоступность (fairness)	Шифрование бюллетеня
Проверяемость / Всеобщая проверяемость (verifiability / universal verifiability)	Блокчейн, расшифрование бюллетеней
Сопротивление принуждению (coercion-resistance)	Переголосование / receipt-freeness *

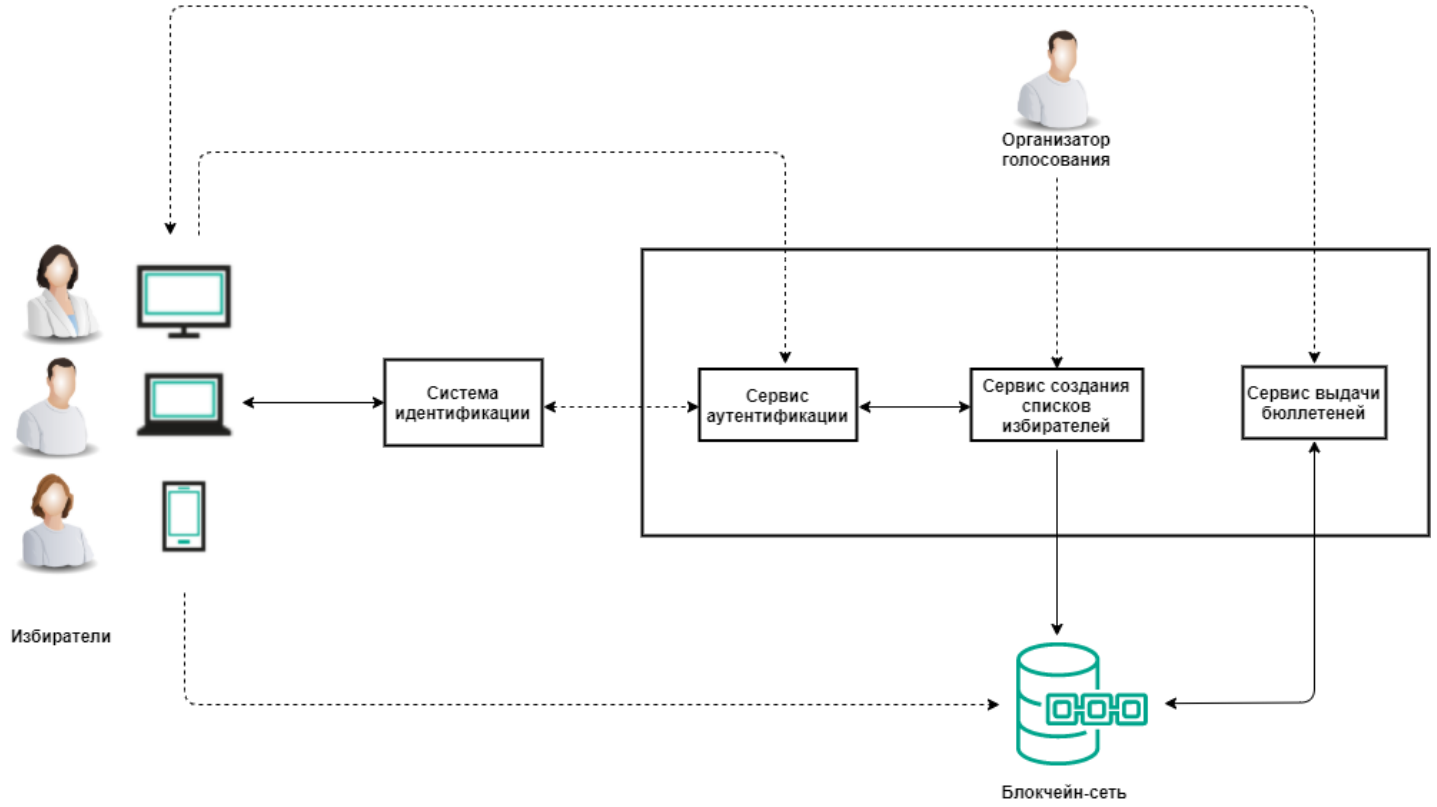
А нужен ли блокчейн в голосовании?

- Блокчейн может помочь достичь некоторых желаемых свойств [1, 2] при определенных условиях
- Блокчейн – не панацея[3]

[1] K. Wüst, A. Gervais. “Do you need a Blockchain?”
[2] T. Dimitriou. “Efficient, Coercion-free and Universally Verifiable Blockchain-based Voting”
[3] Y. Nasser, C. Okoye, J. Clark, and P. Y A Ryan. “Blockchains and Voting: Somewhere between hype and a panacea”

Архитектура системы

- Сервис выдачи бюллетеней подписывает ослепленный идентификатор избирателя
- Узлы-валидаторы у представителей партий / ЦИК
- Узлы-аудиторы доступны общественности



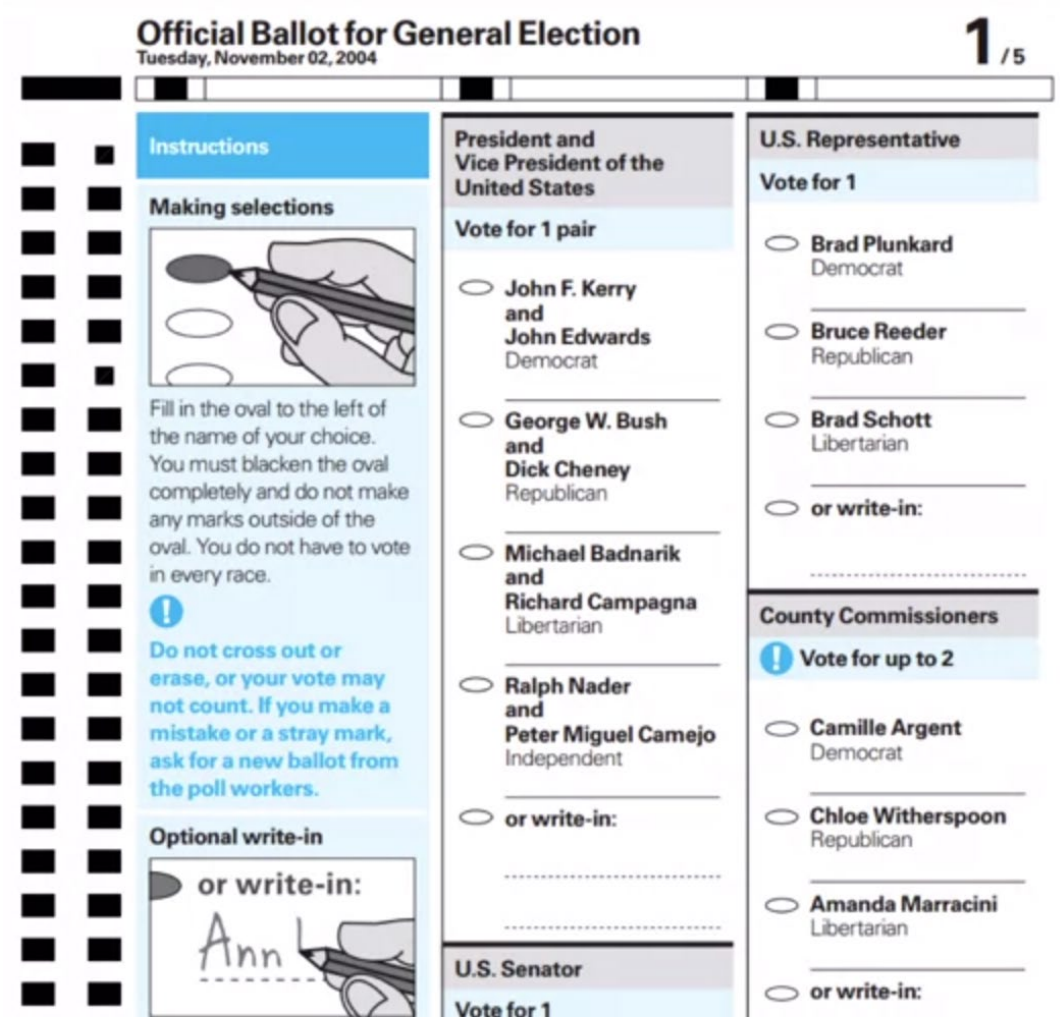
kaspersky

Polys

Анонимизация в системах ДЭГ

- Сети перемешивания
- Гомоморфное шифрование
- Доказательства с нулевым разглашением
- Кольцевые подписи
- Слепая подпись

Важность UX / UI



Official Ballot for General Election
Tuesday, November 02, 2004
1 /5

Instructions

Making selections

Fill in the oval to the left of the name of your choice. You must blacken the oval completely and do not make any marks outside of the oval. You do not have to vote in every race.

Do not cross out or erase, or your vote may not count. If you make a mistake or a stray mark, ask for a new ballot from the poll workers.

Optional write-in

or write-in: Ann

President and Vice President of the United States
Vote for 1 pair

- John F. Kerry and John Edwards — Democrat
- George W. Bush and Dick Cheney — Republican
- Michael Badnarik and Richard Campagna — Libertarian
- Ralph Nader and Peter Miguel Camejo — Independent
- or write-in:

U.S. Senator
Vote for 1

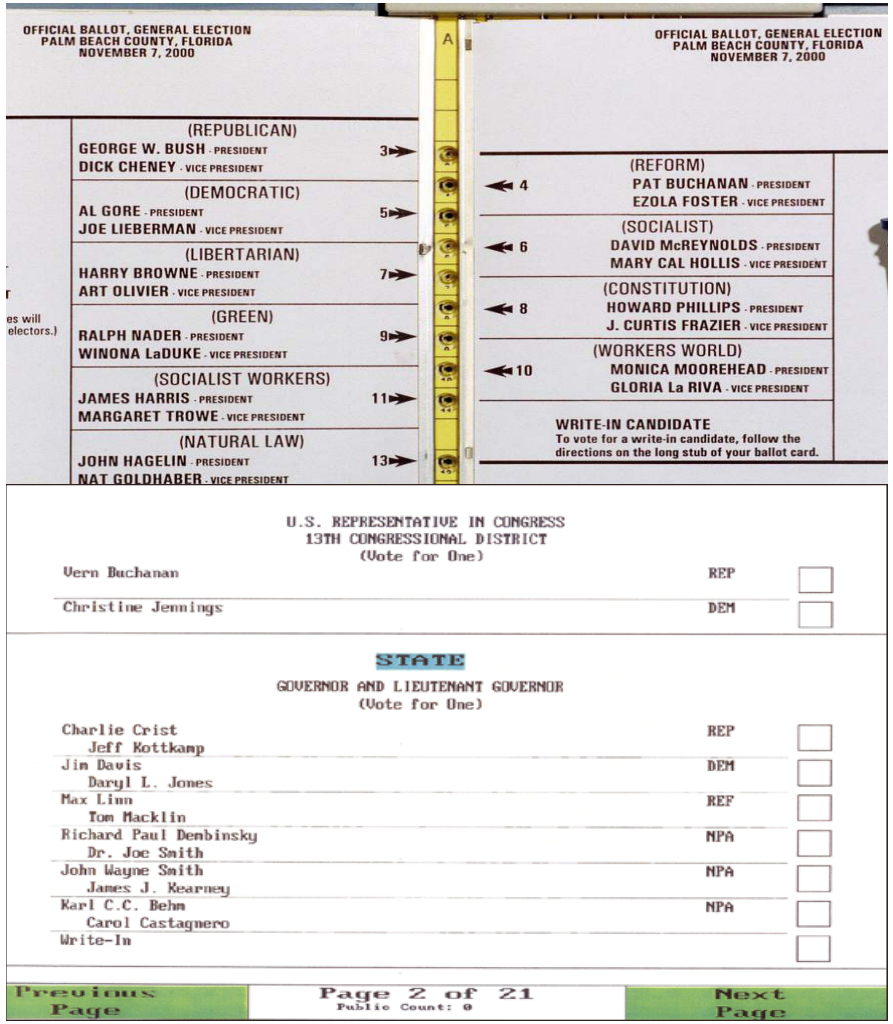
U.S. Representative
Vote for 1

- Brad Plunkard — Democrat
- Bruce Reeder — Republican
- Brad Schott — Libertarian
- or write-in:

County Commissioners
Vote for up to 2

- Camille Argent — Democrat
- Chloe Witherspoon — Republican
- Amanda Marracini — Libertarian
- or write-in:

VS.



OFFICIAL BALLOT, GENERAL ELECTION
PALM BEACH COUNTY, FLORIDA
NOVEMBER 7, 2000

(REPUBLICAN)
GEORGE W. BUSH - PRESIDENT
DICK CHENEY - VICE PRESIDENT — 3

(DEMOCRATIC)
AL GORE - PRESIDENT
JOE LIEBERMAN - VICE PRESIDENT — 5

(LIBERTARIAN)
HARRY BROWNE - PRESIDENT
ART OLIVIER - VICE PRESIDENT — 7

(GREEN)
RALPH NADER - PRESIDENT
WINONA LaDUKE - VICE PRESIDENT — 9

(SOCIALIST WORKERS)
JAMES HARRIS - PRESIDENT
MARGARET TROWE - VICE PRESIDENT — 11

(NATURAL LAW)
JOHN HAGELIN - PRESIDENT
NAT GOLDHABER - VICE PRESIDENT — 13

(REFORM)
PAT BUCHANAN - PRESIDENT
EZOLA FOSTER - VICE PRESIDENT — 4

(SOCIALIST)
DAVID McREYNOLDS - PRESIDENT
MARY CAL HOLLIS - VICE PRESIDENT — 6

(CONSTITUTION)
HOWARD PHILLIPS - PRESIDENT
J. CURTIS FRAZIER - VICE PRESIDENT — 8

(WORKERS WORLD)
MONICA MOOREHEAD - PRESIDENT
GLORIA La RIVA - VICE PRESIDENT — 10

WRITE-IN CANDIDATE
To vote for a write-in candidate, follow the directions on the long stub of your ballot card.

U.S. REPRESENTATIVE IN CONGRESS
13TH CONGRESSIONAL DISTRICT
(Vote for One)

Vern Buchanan — REP
Christine Jennings — DEM

STATE
GOVERNOR AND LIEUTENANT GOVERNOR
(Vote for One)

Charlie Crist / Jeff Kottkamp — REP
Jim Davis / Daryl L. Jones — DEM
Max Linn / Tom Macklin — REF
Richard Paul Denbinsky / Dr. Joe Smith — NPA
John Wayne Smith / James J. Kearney — NPA
Karl C.C. Behm / Carol Castagnero — NPA
Write-In

Previous Page | Page 2 of 21 | Next Page
Public Count: 0

kaspersky

Polys

Актуальные проблемы

- Tradeoff coercion-resistance / receipt-freeness ←→ проверяемость
- Сопротивление принуждению не решается техническими способами
- Доверие избирателей к системе
- Отсутствие национальных стандартов / рекомендаций ТК 26 на слепую подпись

Выводы

- Блокчейн помогает обеспечить некоторые важные свойства
- Существующие государственные криптографические стандарты не закрывают все потребности систем ДЭГ
- Важен публичный аудит систем ДЭГ

Петр Мурзин
аспирант ВИНИТИ РАН,
разработчик проекта Polys
АО «Лаборатория Касперского»
petr.murzin@kaspersky.com

kaspersky

Polys