Jeremy Clark, Urs Hengartner, & Kate Larson
University of Waterloo

Not So Hidden Information:

Optimal contracts for undue influence in E2E voting systems

Setting

We consider voting systems with end-to-end (E2E) verifiability.

The correctness of these systems rely on mathematical assumptions instead of chain-of-custody, software, or hardware.

(Custody independence *and* software independence)

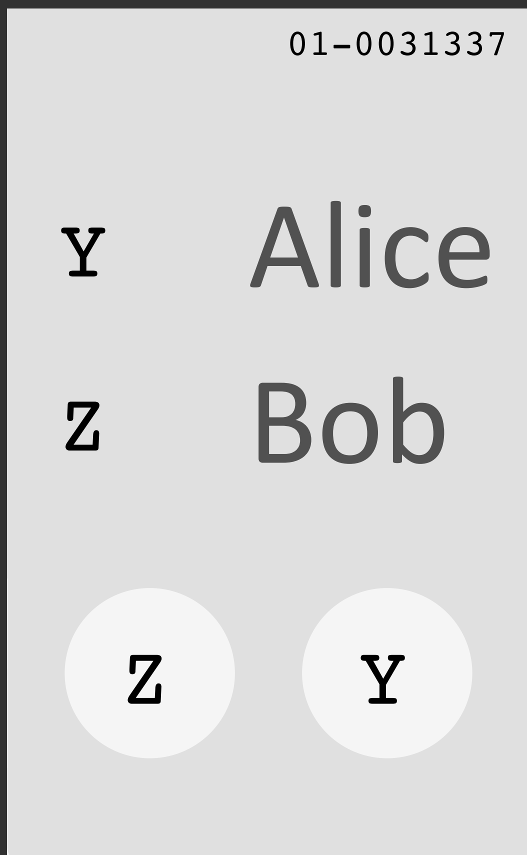
Punchscan

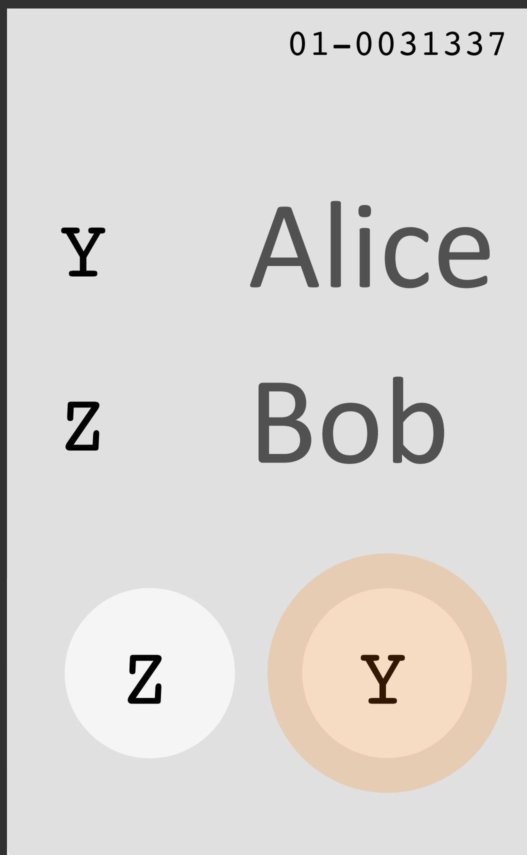
To illustrate the idea of contracts, we focus on one system: Punchscan

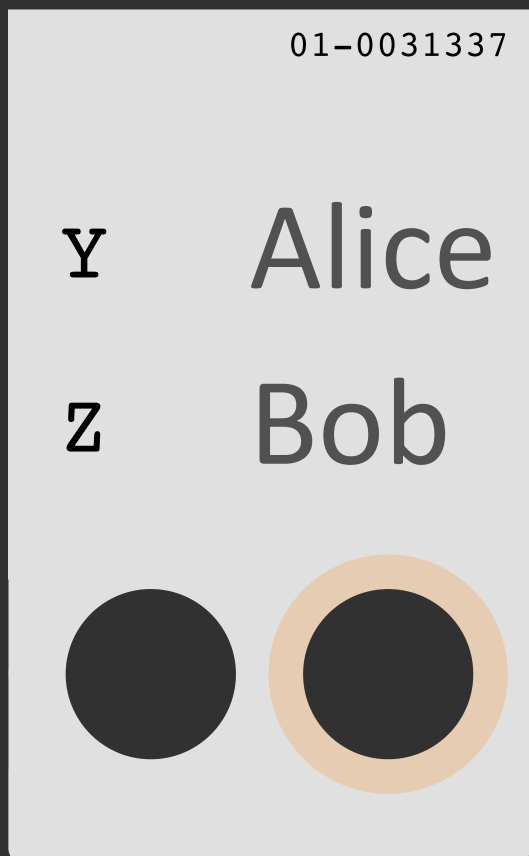
Why just one?

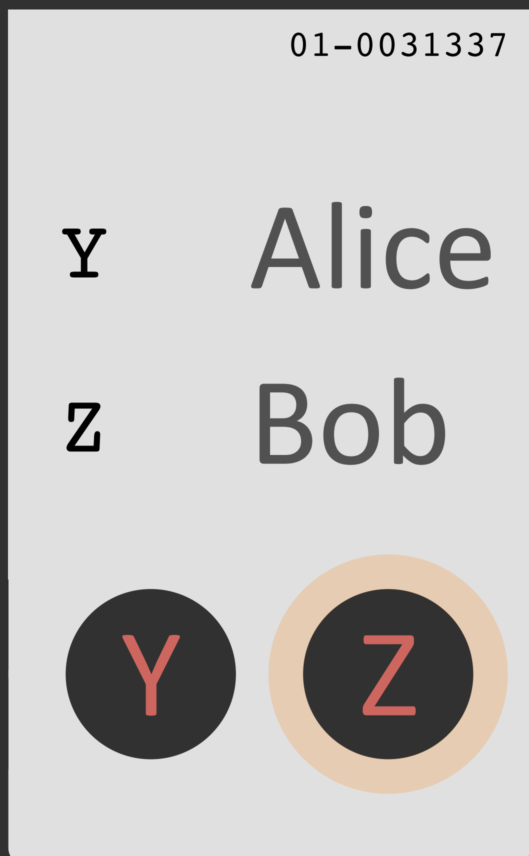
Why this one?

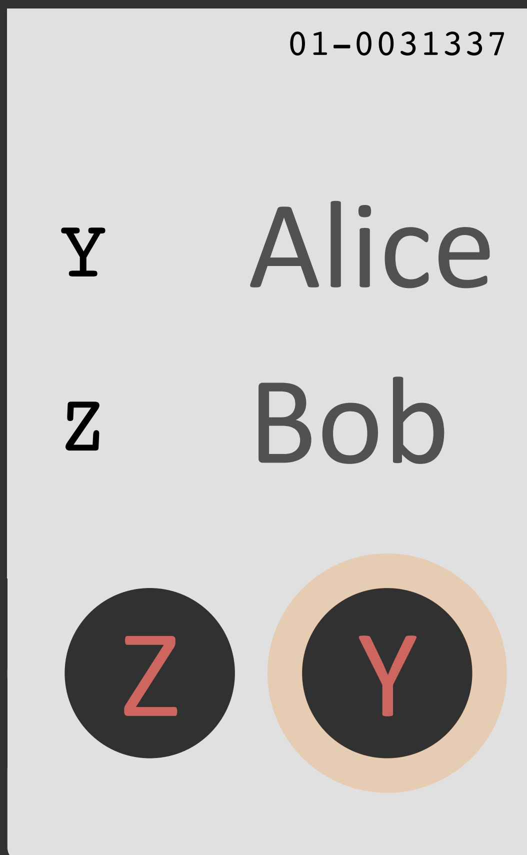
Punchscan

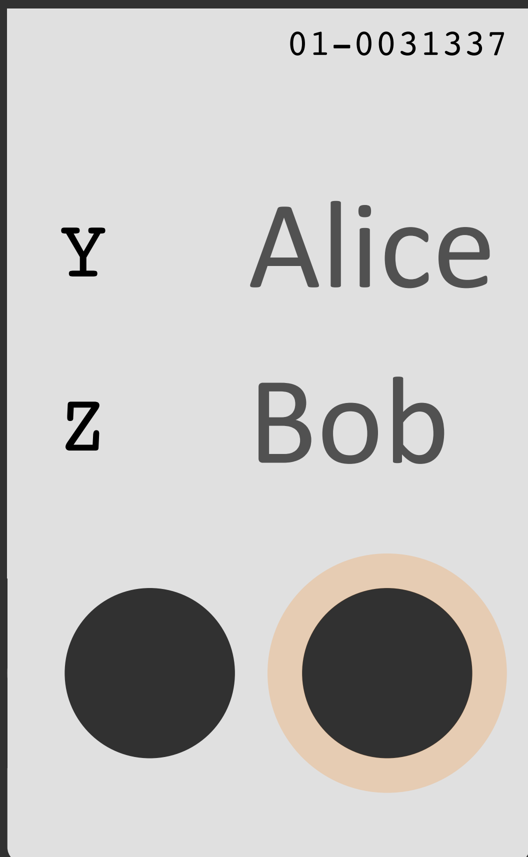


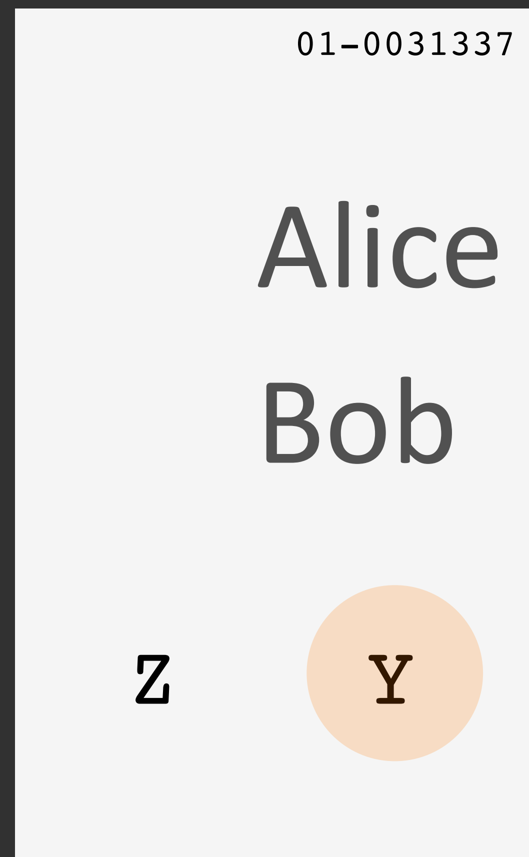

01–0031337
Y Alice
Z Bob
Z
Y


01-0031337
Y
Alice
Z
Bob


01-0031337
Y
Alice
Z
Bob
Y
Z


01-0031337
Y Alice
Z Bob
Z
Y

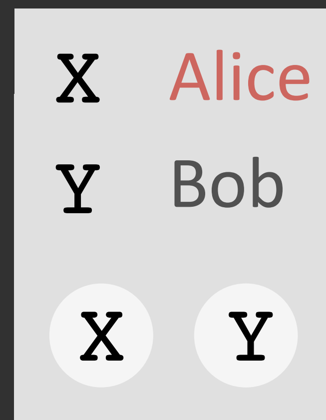

01-0031337
Y
Alice
Z
Bob


01-0031337
Alice
Bob
Z
Y

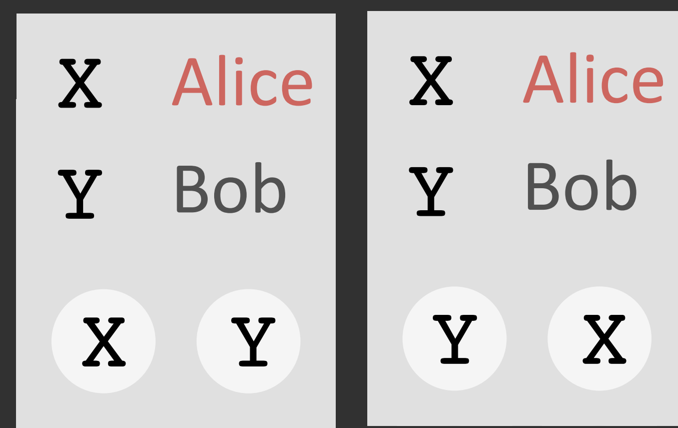
Contracts

$$\begin{cases} u_2 & = \pi_V(L, T \quad | \{YX, \_\_\}) \\ u_1 & = \pi_V(L, B \quad | \{\_\_, XY\}) \\ u_1 & = \pi_V(R, B \quad | \{\_\_, YX\}) \\ u_0 & \text{otherwise} \end{cases}$$

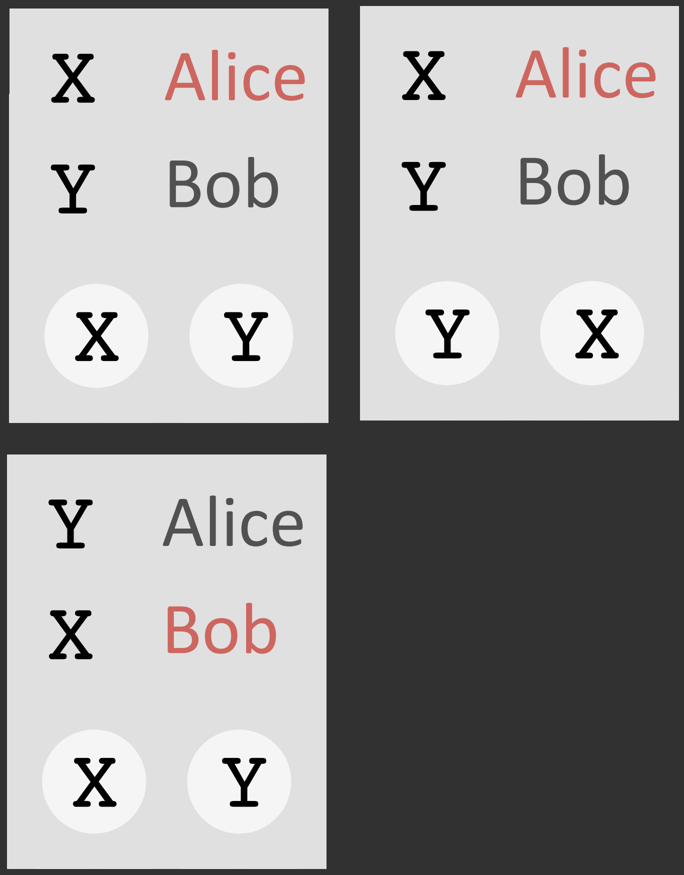
$$
\begin{cases}
u_2 & = \pi_V(L, T \quad |\{YX, \_\_\}) \\
u_1 & = \pi_V(L, B \quad |\{\_\_, XY\}) \\
u_1 & = \pi_V(R, B \quad |\{\_\_, YX\}) \\
u_0 & \text{otherwise}
\end{cases}
$$



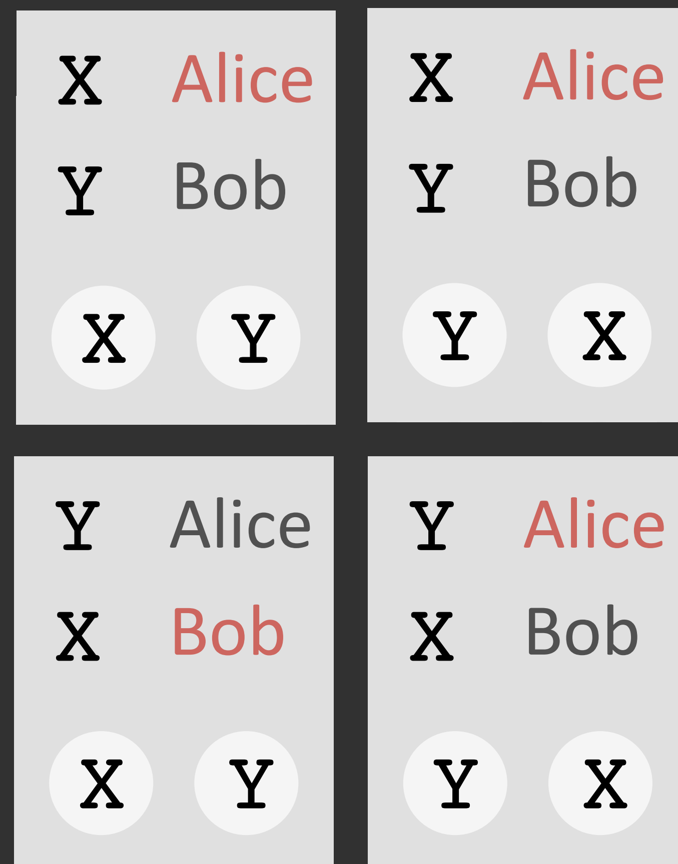
$$\begin{cases} u_2 & = \pi_V(L, T \quad |\{YX, \_\_\}) \\ u_1 & = \pi_V(L, B \quad |\{\_\_, XY\}) \\ u_1 & = \pi_V(R, B \quad |\{\_\_, YX\}) \\ u_0 & \text{otherwise} \end{cases}$$



$$
\begin{cases}
u_2 & = \pi_V(L, T \quad | \{YX, \_\}) \\
u_1 & = \pi_V(L, B \quad | \{\_, XY\}) \\
u_1 & = \pi_V(R, B \quad | \{\_, YX\}) \\
u_0 & \text{otherwise}
\end{cases}
$$



$$
\begin{cases}
u_2 & = \pi_V(L, T \quad |\{YX, \_\_\}) \\
u_1 & = \pi_V(L, B \quad |\{\_\_, XY\}) \\
u_1 & = \pi_V(R, B \quad |\{\_\_, YX\}) \\
u_0 & \text{otherwise}
\end{cases}
$$



A Simple Fix

Order matters.

If the voter choose top or bottom prior to seeing the ballot, the best possible contract is forced randomization.

This, however, does increase the role of poll worker procedure in the security of the system. We are aiming for custody-independence.

Questions about Contracts

What tool is best for analysis?

Of the existing contracts, which are best?

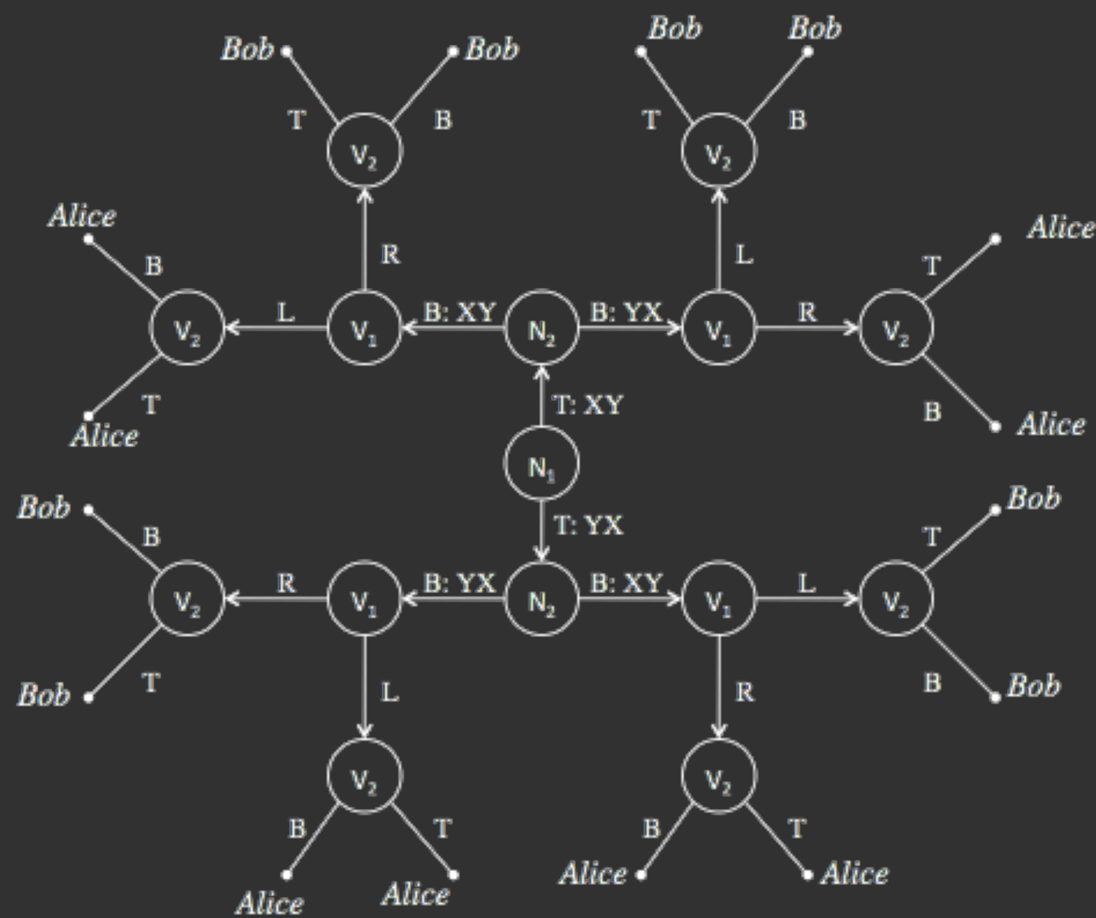
Can we define the best possible contract?

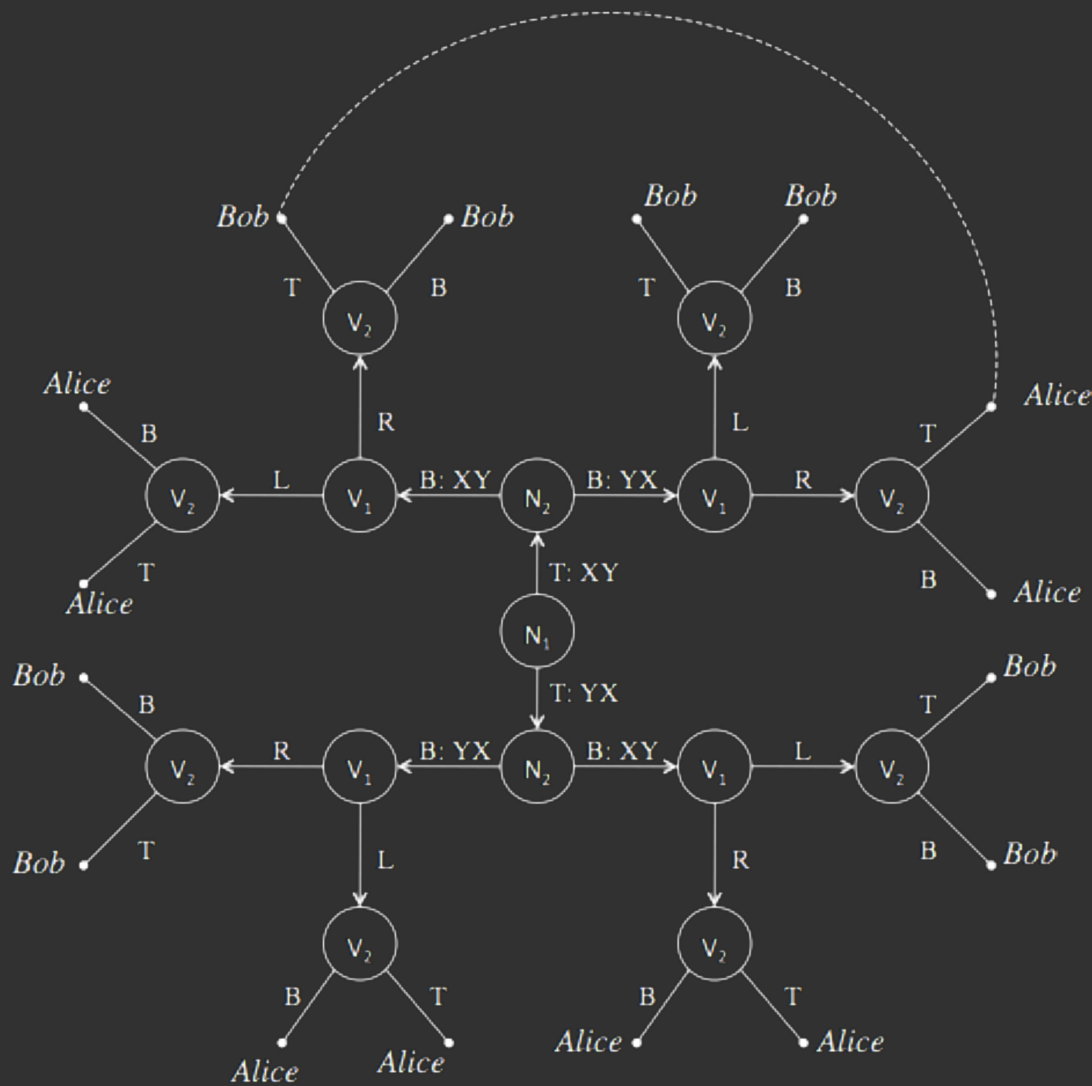
What if we have more than 2 candidates?

What if voters do not behave correctly and follow the contract?

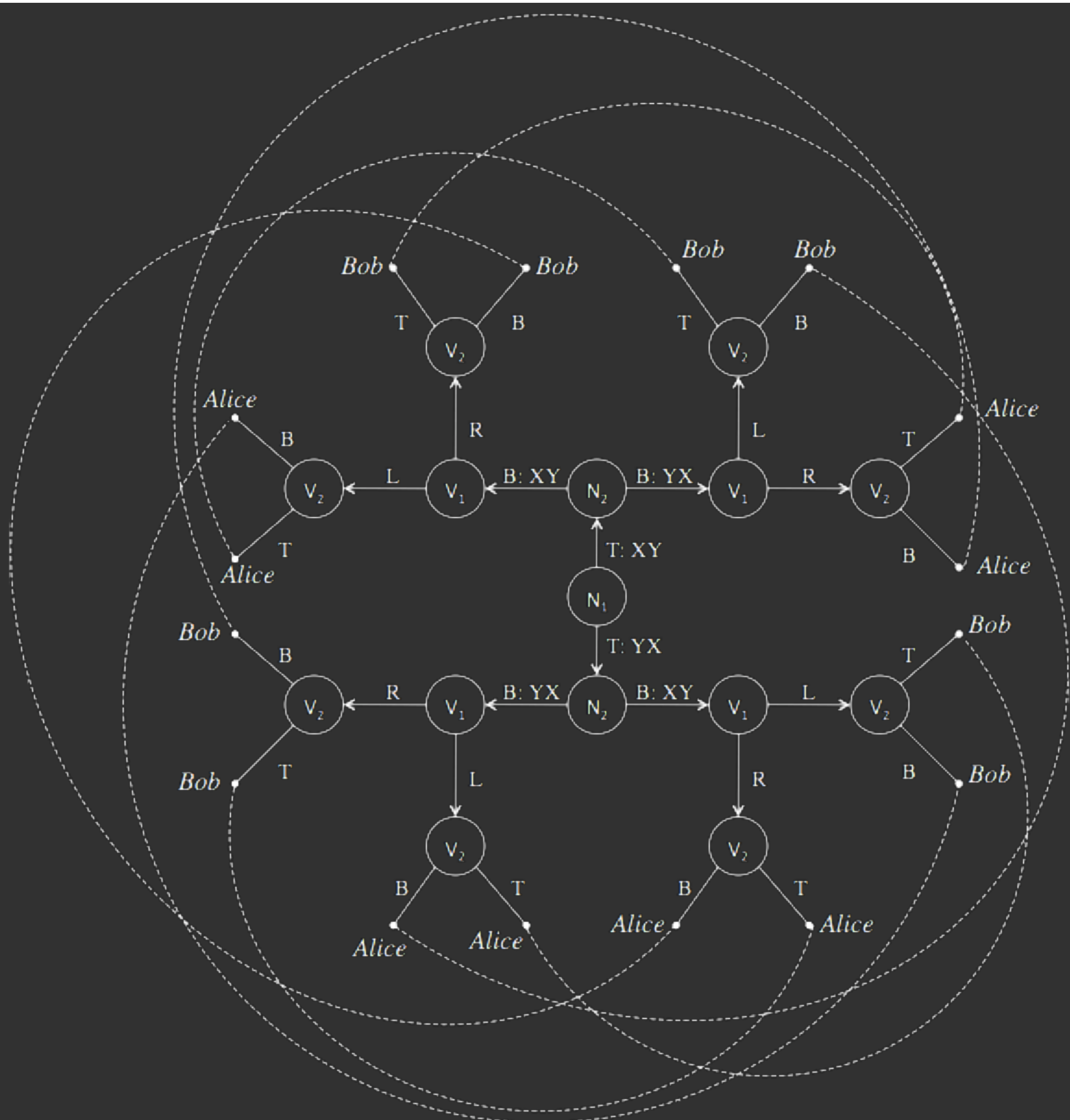
Is the contract financially sensible?

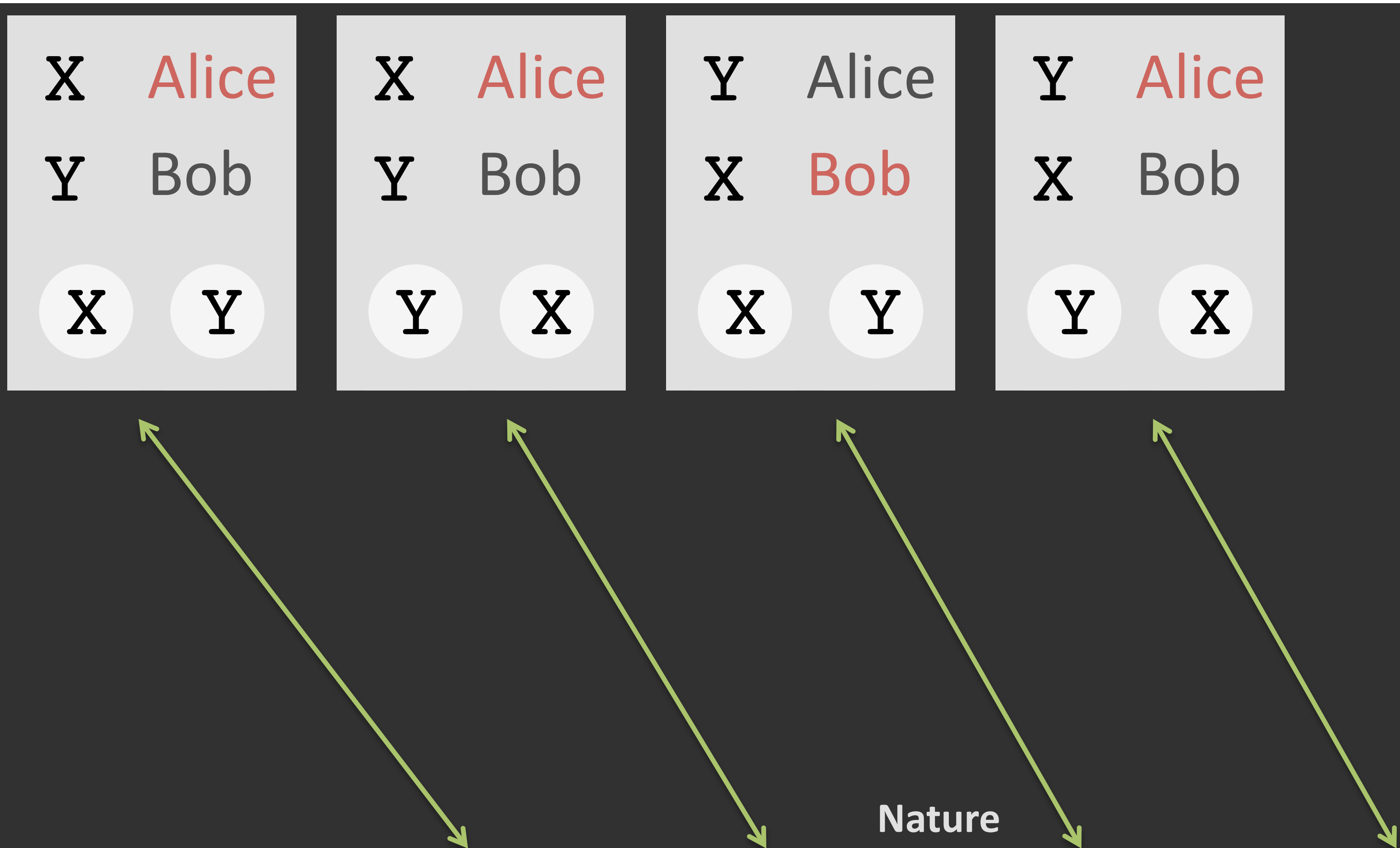
Game Theory


Bob
Bob
T
B
V2
Bob
Bob
T
B
V2
Alice
B
R
L
Alice
T
V2
L
V1
B: XY
N2
B: YX
V1
R
V2
T
Alice
T: XY
B
Alice
N1
Bob
T: YX
Bob
B
T
V2
R
V1
B: YX
N2
B: XY
V1
L
V2
Bob
T
L
R
B
Bob
V2
V2
B
T
B
T
Alice
Alice
Alice
Alice



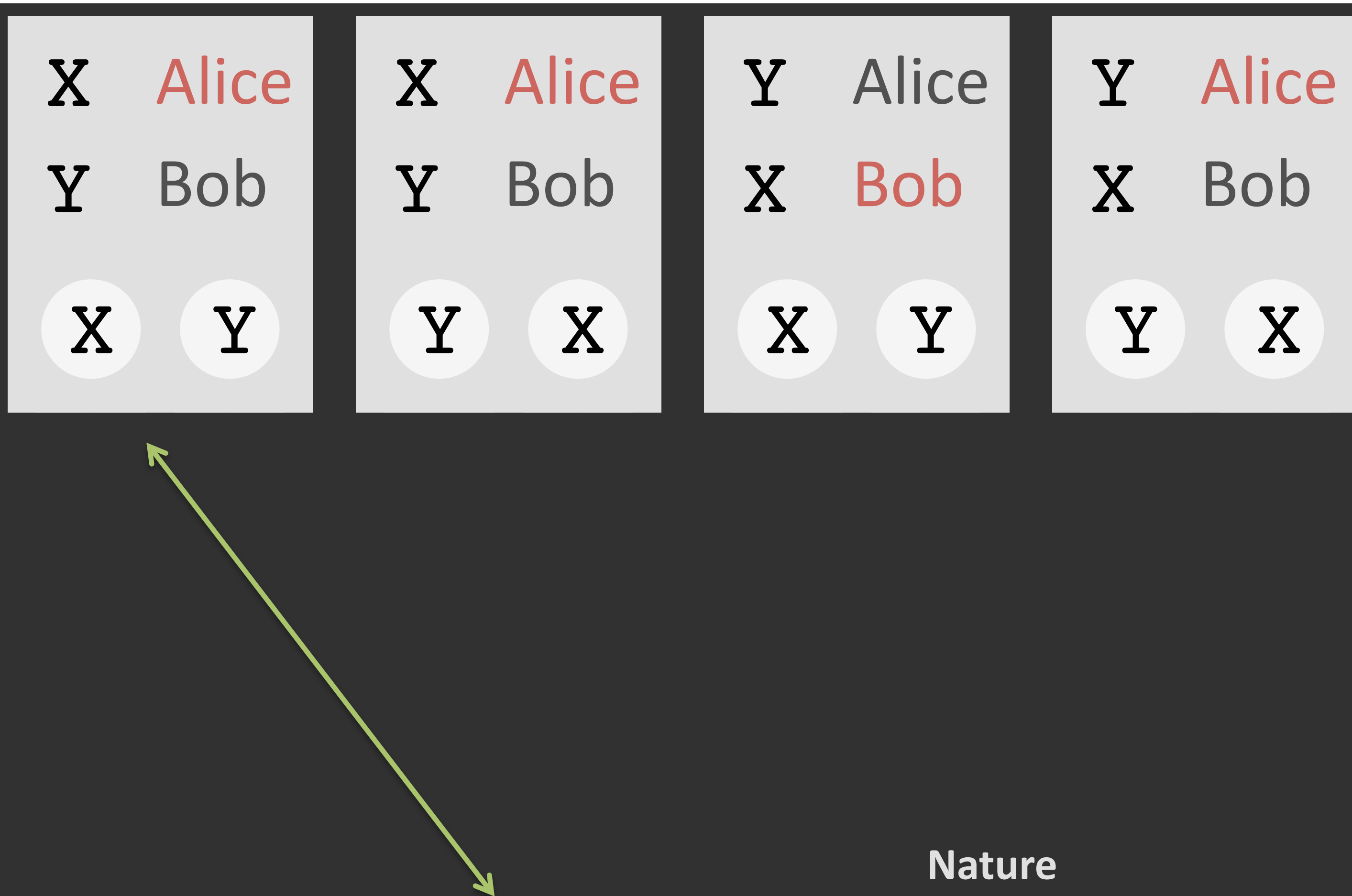
Bob
T
B
Bob
Bob
Bob
T
B
V2
V2
R
L
Alice
B
Alice
T
L
V1
B: XY
N2
B: YX
V1
R
V2
V2
T
B
Alice
Alice
T: XY
N1
T: YX
Bob
B
V2
R
V1
B: YX
N2
B: XY
V1
L
V2
T
Bob
T
Bob
B
Bob
L
R
V2
V2
B
T
Alice
Alice
B
T
Alice
Alice


Bob
Bob
T
B
V2
Bob
Bob
T
B
V2
R
L
Alice
B
V2
L
V1
B: XY
N2
B: YX
V1
R
V2
Alice
T
T
Alice
T: XY
B
Alice
N1
T: YX
Bob
B
V2
R
V1
B: YX
N2
B: XY
V1
L
V2
Bob
T
Bob
T
L
R
B
Bob
V2
V2
B
T
B
T
Alice
Alice
Alice
Alice



Nature

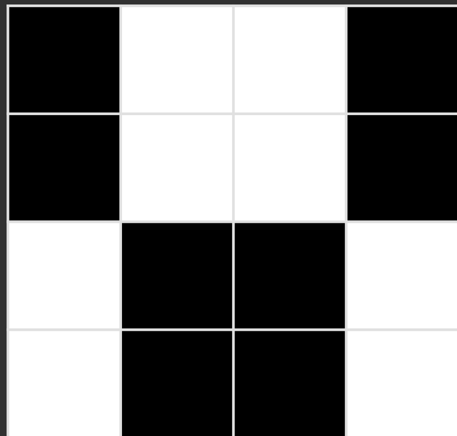
		{XY,XY}	*{XY,YX}*	*{YX,XY}*	*{YX,YX}*
Voter	*L,T*	u_0, 1	u_0, -1	u_2, -1	u_2, 1
	L,B	u_1, 1	u_0, -1	u_1, -1	u_0, 1
	R,T	u_0, -1	u_0, 1	u_0, 1	u_0, -1
	R,B	u_0, -1	u_1, 1	u_0, 1	u_1, -1



		Nature			
		{XY,XY}	*{XY,YX}*	*{YX,XY}*	*{YX,YX}*
Voter	*L,T*	u_0, 1	u_0, -1	u_2, -1	u_2, 1
	L,B	u_1, 1	u_0, -1	u_1, -1	u_0, 1
	R,T	u_0, -1	u_0, 1	u_0, 1	u_0, -1
	R,B	u_0, -1	u_1, 1	u_0, 1	u_1, -1

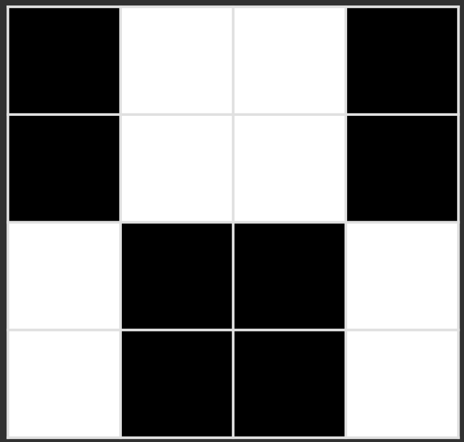
$$
\begin{cases}
u_2 & = \pi_V(L, T \quad | \{YX, \_\_\}) \\
u_1 & = \pi_V(L, B \quad | \{\_\_, XY\}) \\
u_1 & = \pi_V(R, B \quad | \{\_\_, YX\}) \\
u_0 & \text{otherwise}
\end{cases}
$$

		Nature			
		{XY,XY}	*{XY,YX}*	*{YX,XY}*	*{YX,YX}*
Voter	*L,T*	u_0, 1	u_0, -1	u_2, -1	u_2, 1
	L,B	u_1, 1	u_0, -1	u_1, -1	u_0, 1
	R,T	u_0, -1	u_0, 1	u_0, 1	u_0, -1
	R,B	u_0, -1	u_1, 1	u_0, 1	u_1, -1

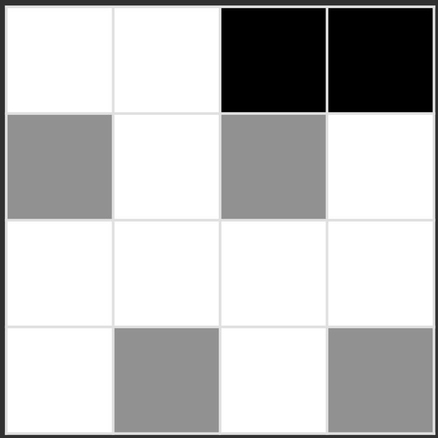


Adversary

		Nature			
		{XY,XY}	*{XY,YX}*	*{YX,XY}*	*{YX,YX}*
Voter	*L,T*	u_0, 1	u_0, -1	u_2, -1	u_2, 1
	L,B	u_1, 1	u_0, -1	u_1, -1	u_0, 1
	R,T	u_0, -1	u_0, 1	u_0, 1	u_0, -1
	R,B	u_0, -1	u_1, 1	u_0, 1	u_1, -1

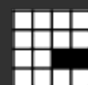


Adversary



Voter

		Nature			
		{XY,XY}	*{XY,YX}*	*{YX,XY}*	*{YX,YX}*
Voter	*L,T*	u_0, 1	u_0, -1	u_2, -1	u_2, 1
	L,B	u_1, 1	u_0, -1	u_1, -1	u_0, 1
	R,T	u_0, -1	u_0, 1	u_0, 1	u_0, -1
	R,B	u_0, -1	u_1, 1	u_0, 1	u_1, -1

Contract Clause		MN	BMR	KMRC
L,T | {XY,___}		u_1	u_0	u_0
L,T | {YX,___}		u_1	u_1	u_2
R,T | {XY,___}		u_1	u_0	u_0
R,T | {YX,___}		u_0	u_0	u_0
L,B | {___,XY}		u_1	u_1	u_1
L,B | {___,YX}		u_1	u_0	u_0
R,B | {___,XY}		u_1	u_0	u_0
R,B | {___,YX}		u_0	u_0	u_1
Perfect: 				

What percent of the time, on average, will utility maximizing voters cast a vote for Alice?

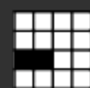
- Forced Randomization: 50.0%
- MN (Moran, Naor 07): 54.2% (or 62.5%)
- BMR (Bohli, Muller-Quade, Rohrich 07): 62.5%
- KRMC (Kelsey, Regenscheid, Moran, Chaum 09): 75.0%

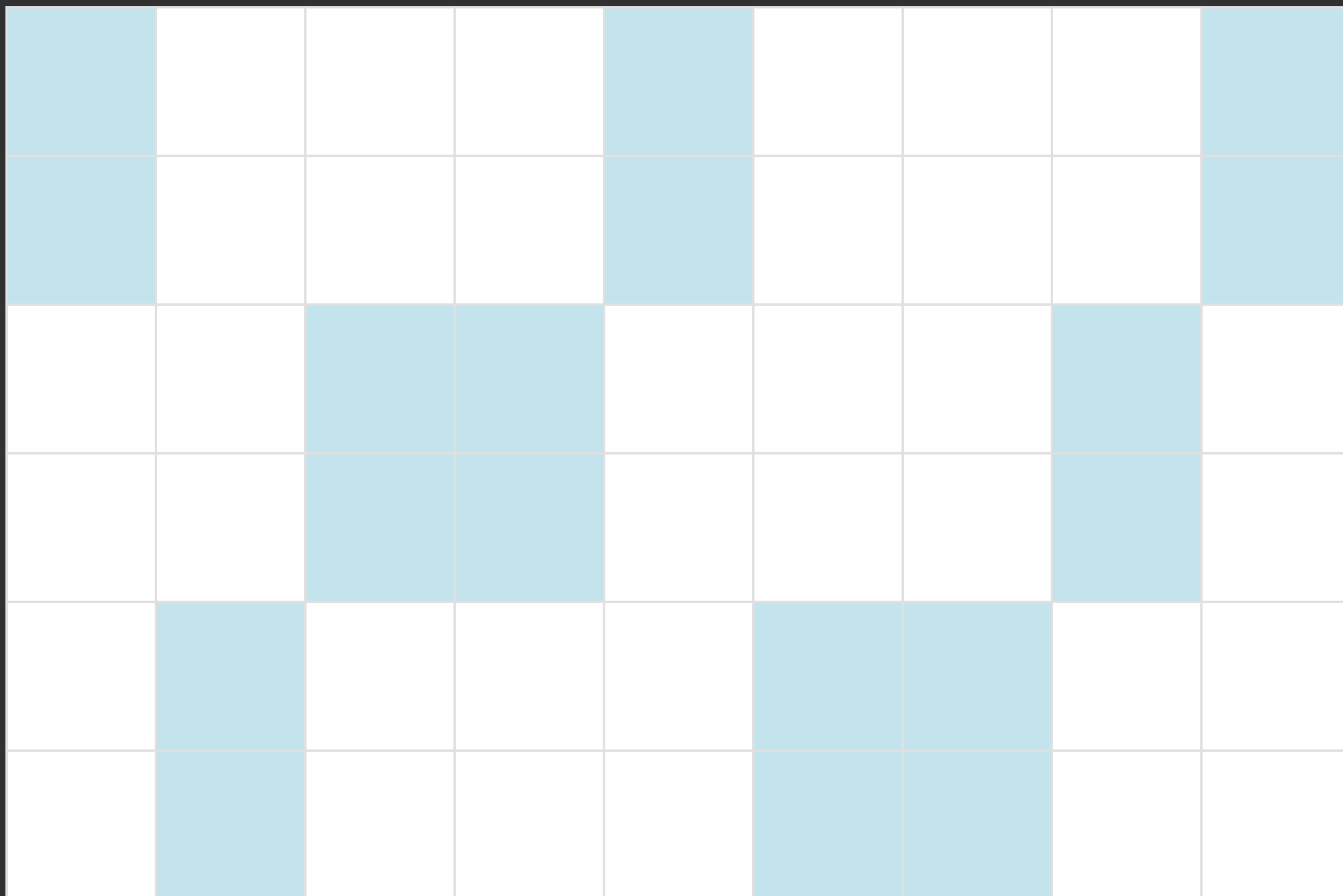
Optimal Contract

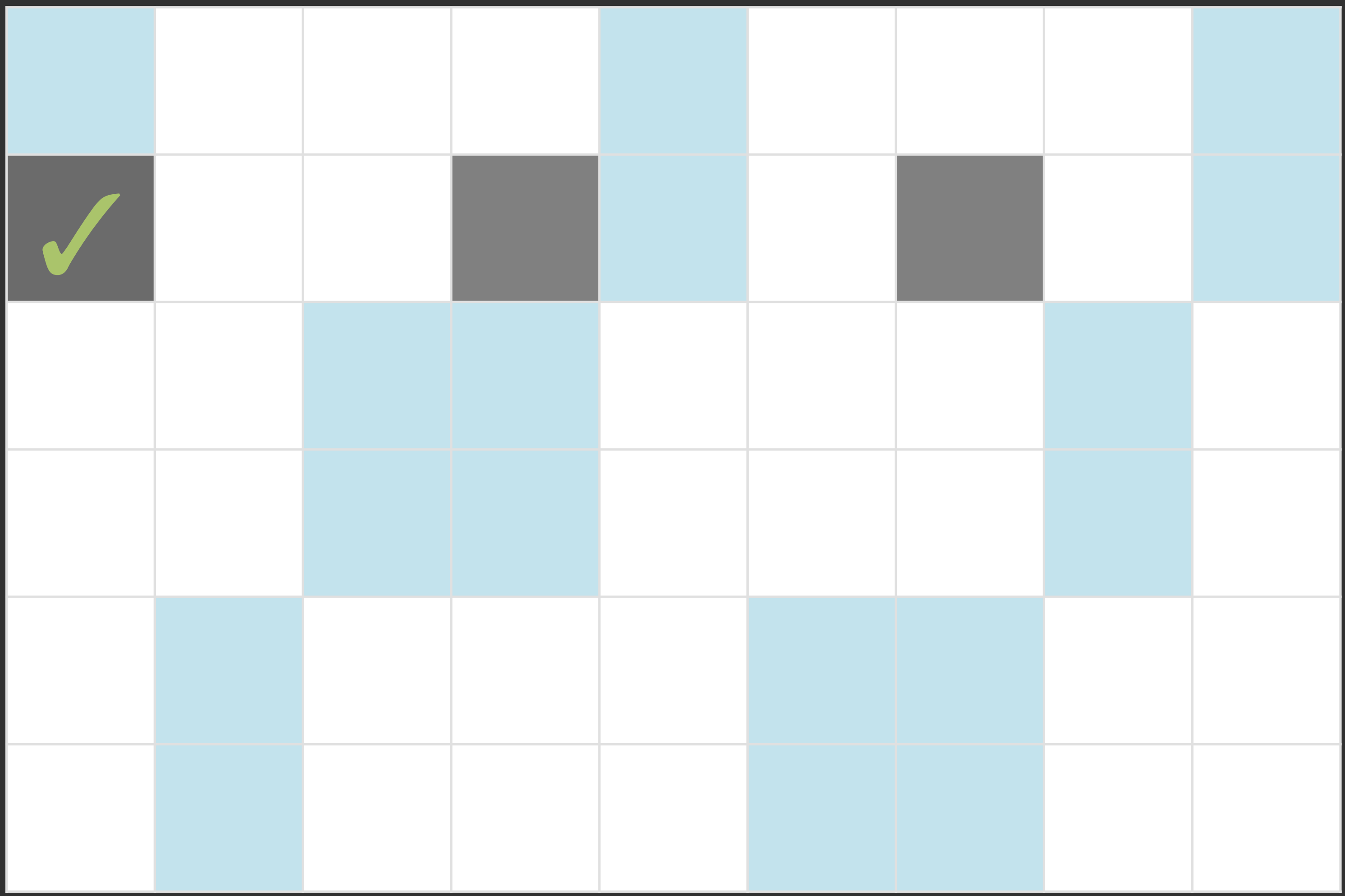
KRMC has the best properties but is it the best contract possible? Yes (for two candidates).

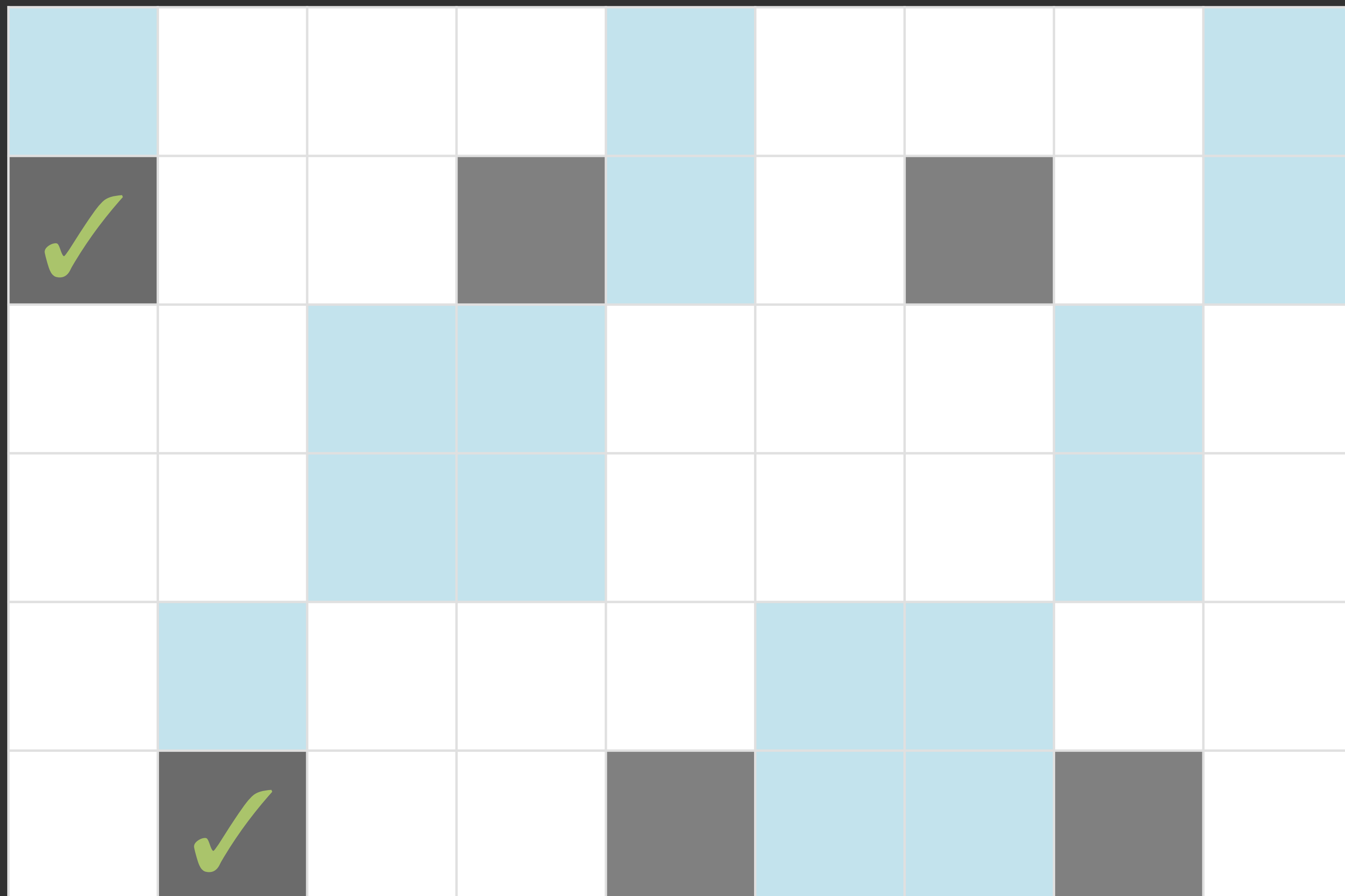
What if there are more than 2 candidates? We provide an algorithm for generating optimal contracts of any number of candidates.

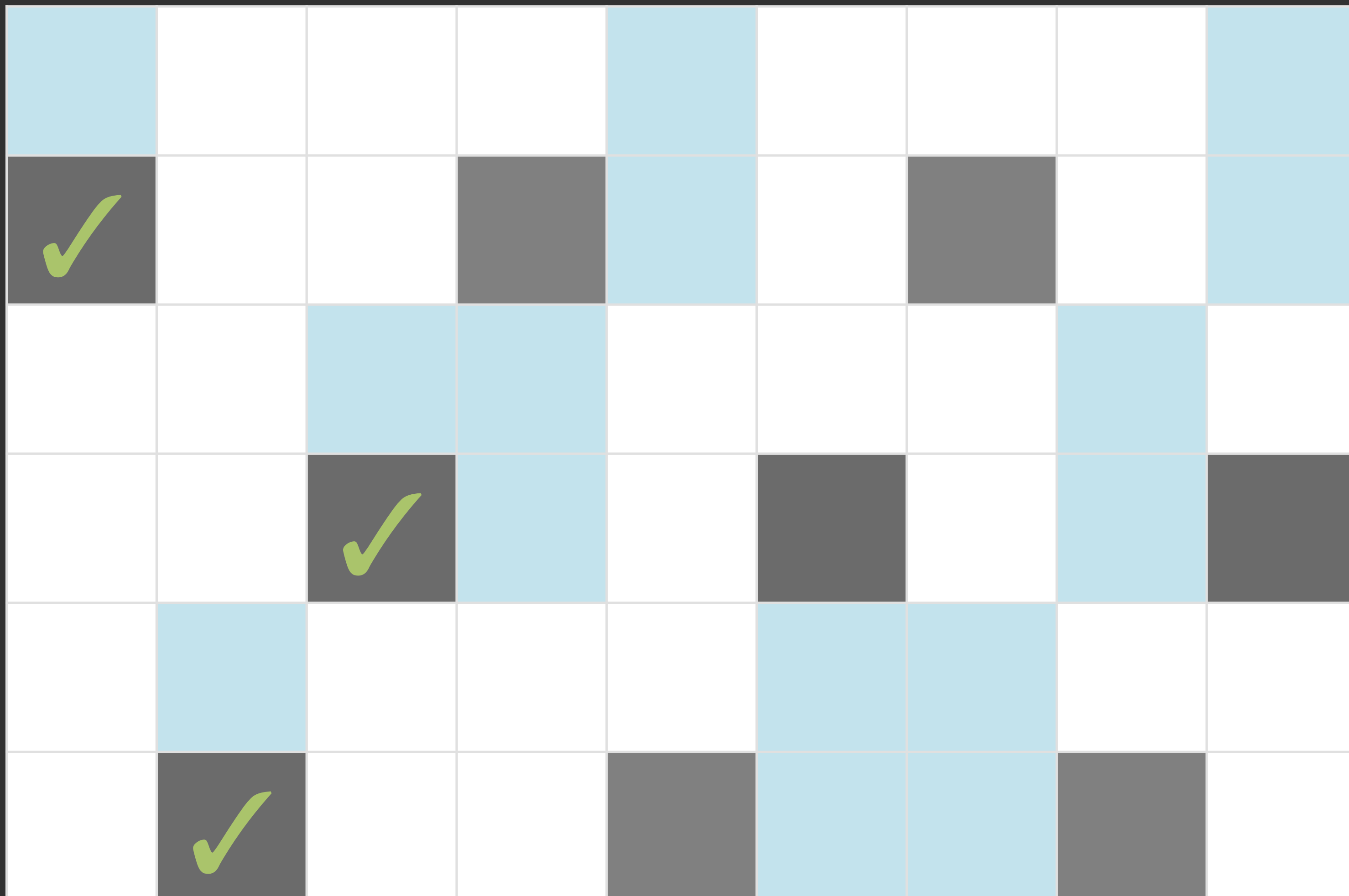
KRMC improved on the previous contracts by adding a second level of utility. Could we not improve further by adding more levels of utility? No.

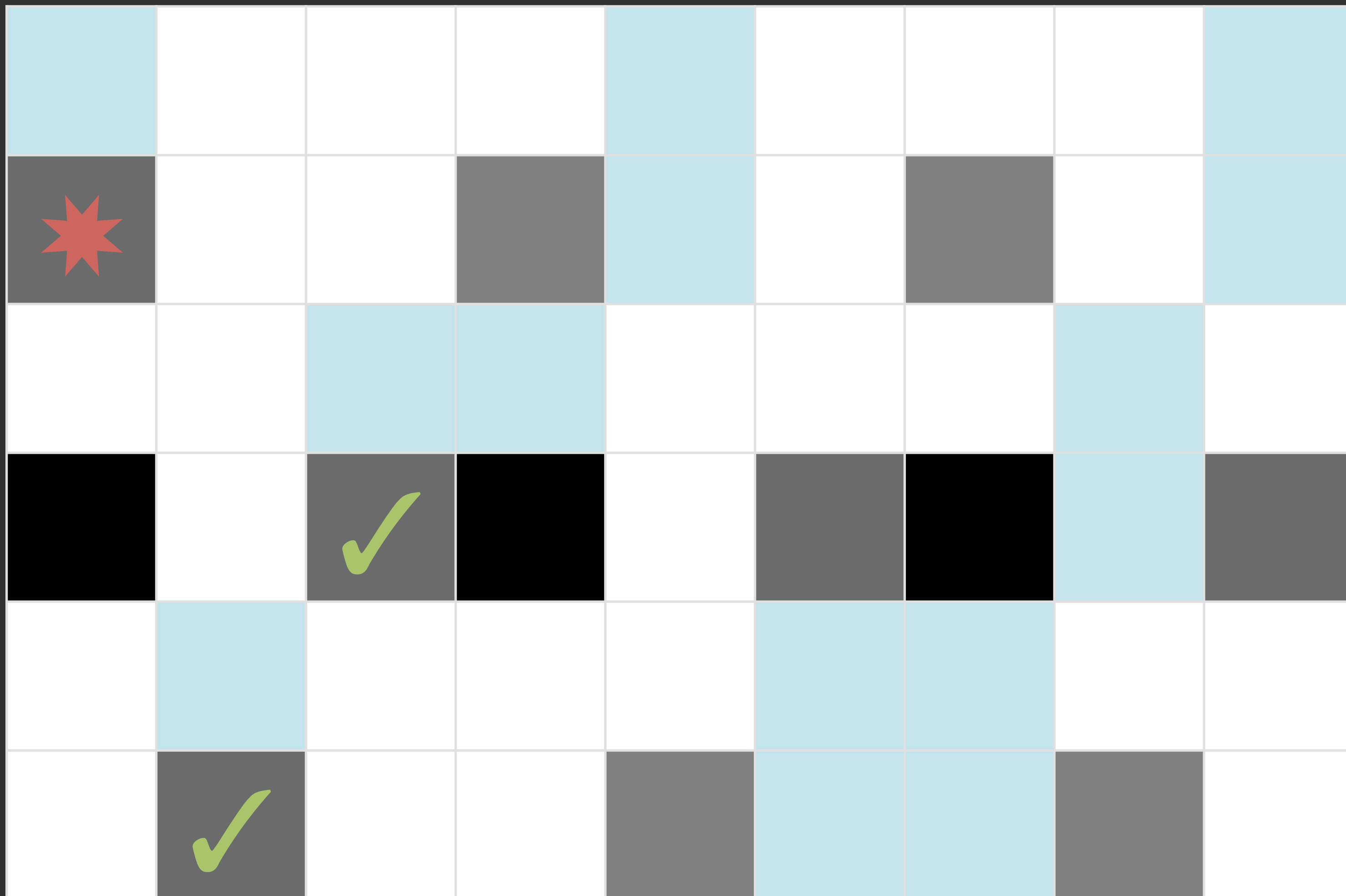
Contract Clause		MN	BMR	KMRC
L,T | {XY,__}		u_1	u_0	u_0
L,T | {YX,__}		u_1	u_1	u_2
R,T | {XY,__}		u_1	u_0	u_0
R,T | {YX,__}		u_0	u_0	u_0
L,B | {__,XY}		u_1	u_1	u_1
L,B | {__,YX}		u_1	u_0	u_0
R,B | {__,XY}		u_1	u_0	u_0
R,B | {__,YX}		u_0	u_0	u_1
Perfect: 				



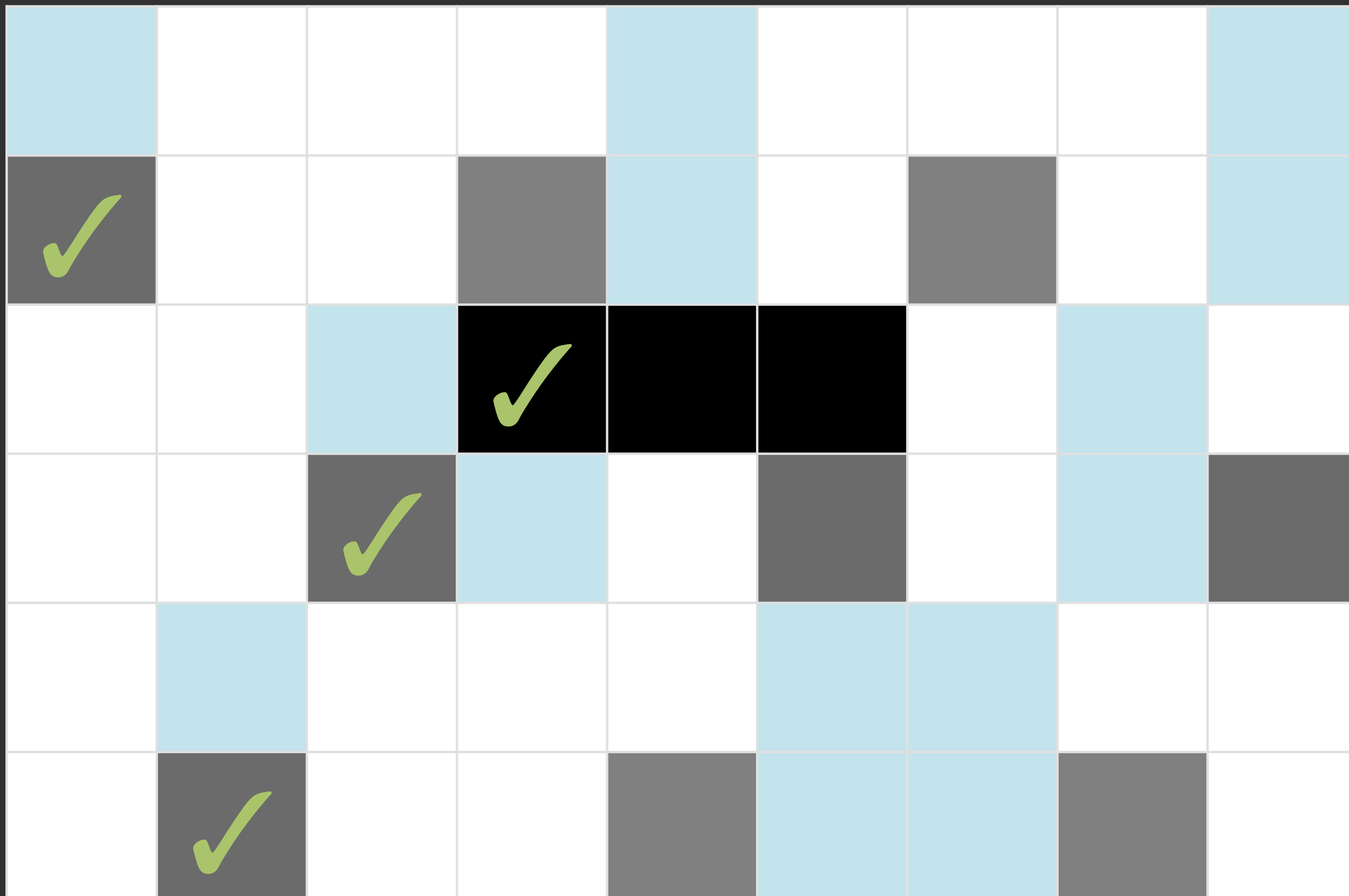


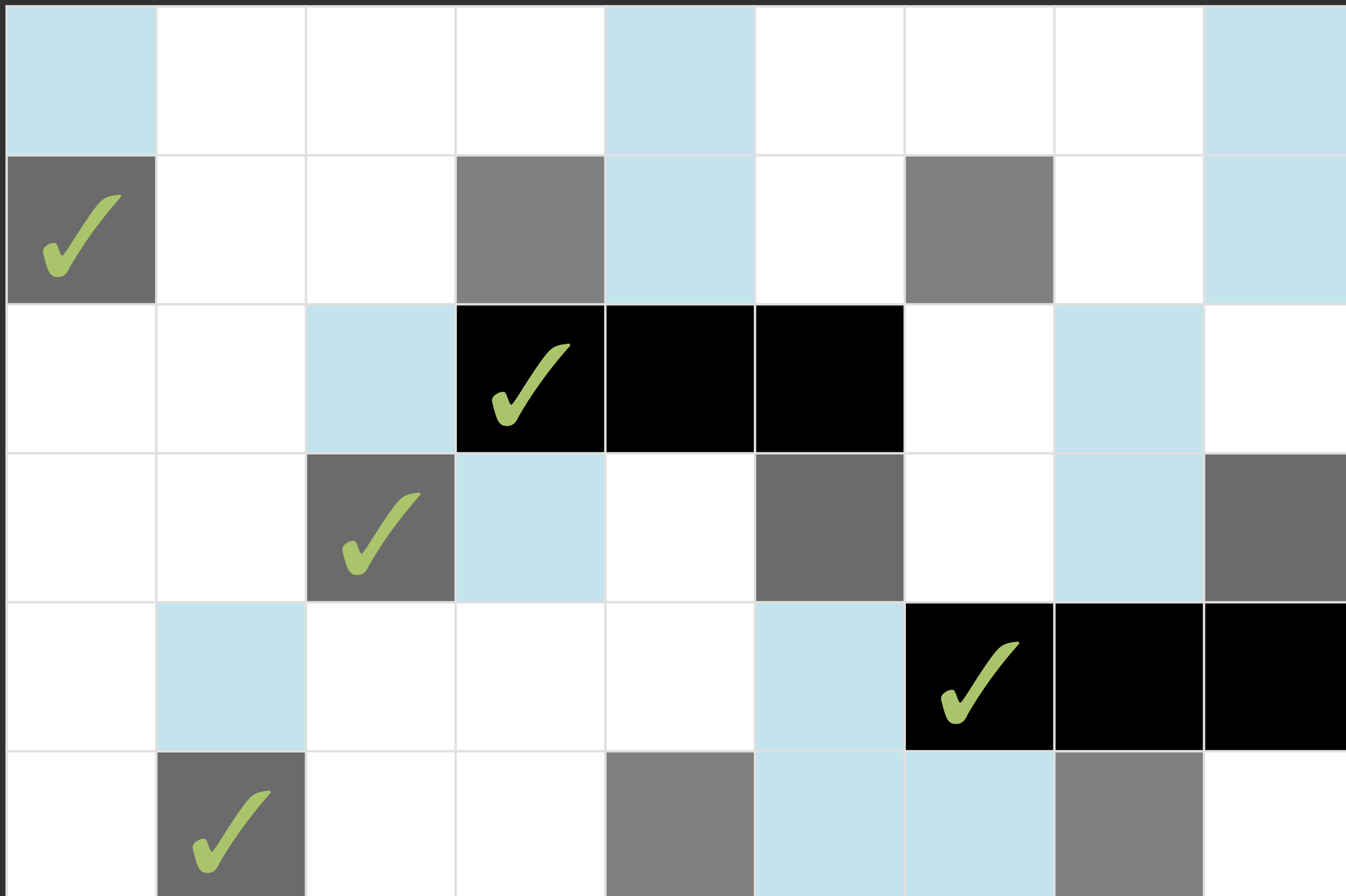


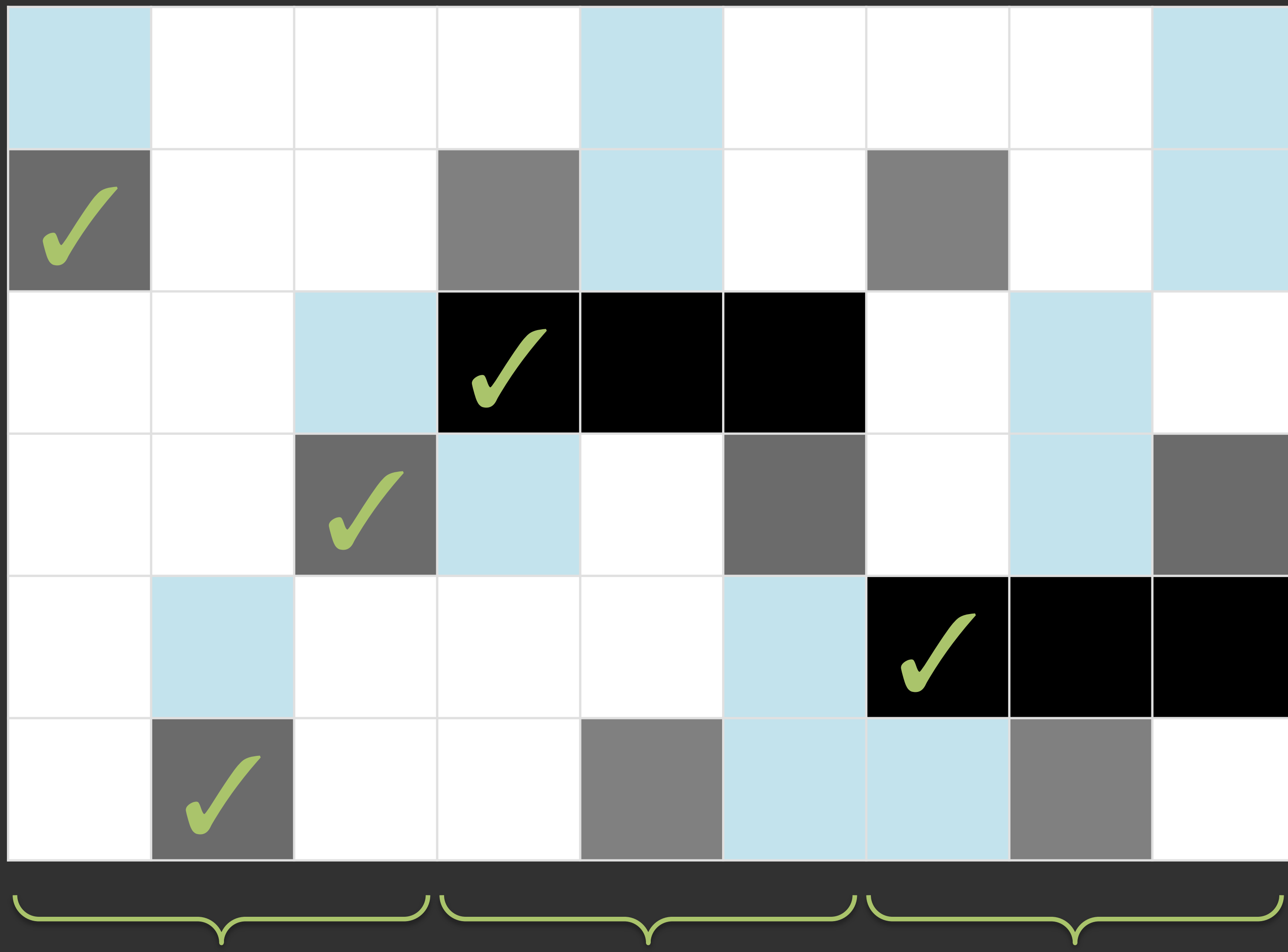




Contract Clause		MN	BMR	KMRC
L,T | {XY,___}		u_1	u_0	u_0
L,T | {YX,___}		u_1	u_1	u_2
R,T | {XY,___}		u_1	u_0	u_0
R,T | {YX,___}		u_0	u_0	u_0
L,B | {___,XY}		u_1	u_1	u_1
L,B | {___,YX}		u_1	u_0	u_0
R,B | {___,XY}		u_1	u_0	u_0
R,B | {___,YX}		u_0	u_0	u_1
Perfect: 				

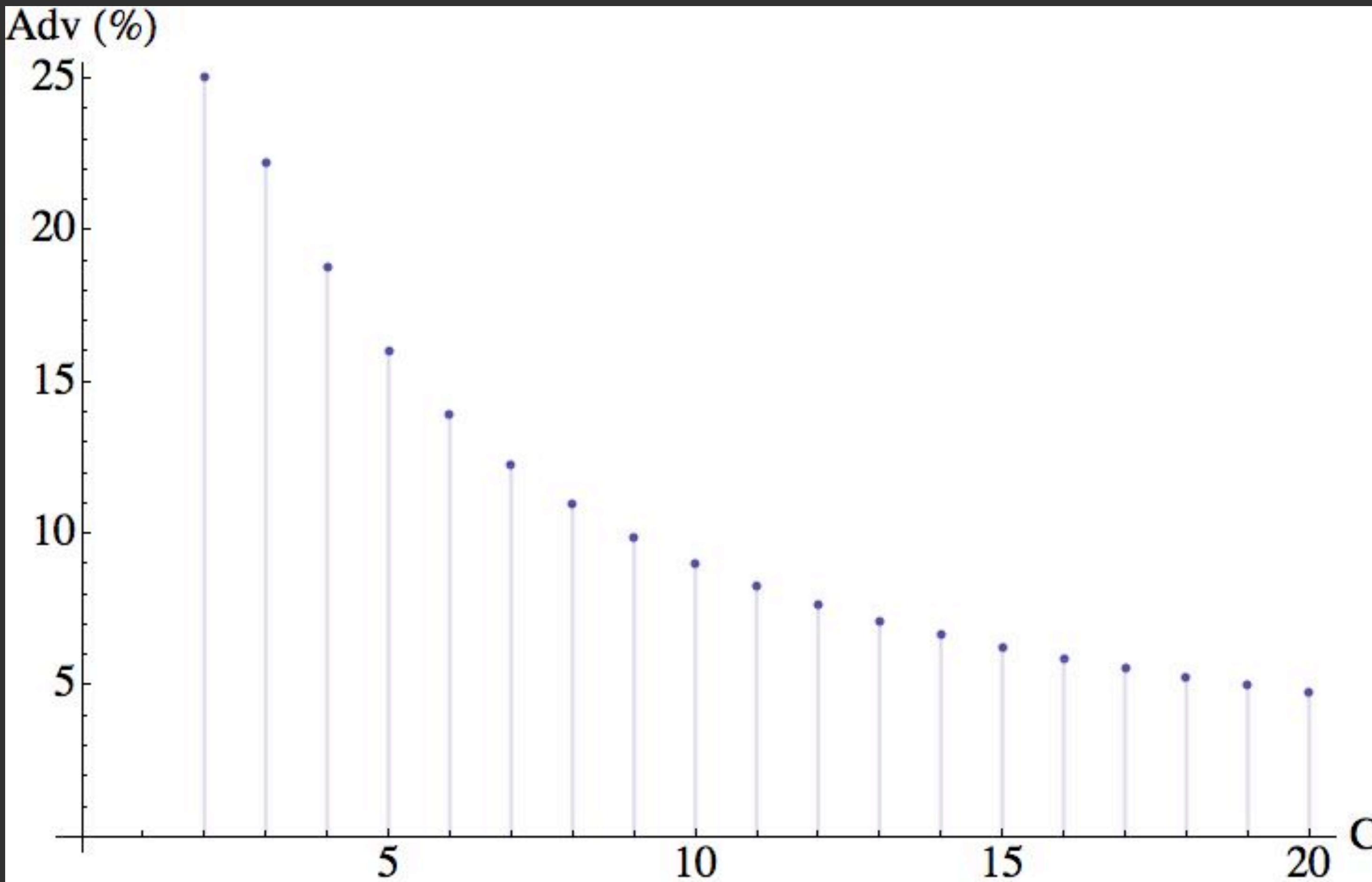






n/n 1/n 1/n

Advantage vs. Number of Candidates



What if voters are not utility-maximizing?

We model voters of four types:

- Always vote for Alice
- Always vote for Bob
- Follow the contract to receive highest payoff ("utility maximizing")
- Always vote contrary to the adversary ("vengeful")

Coercion vs. Vote Buying?

The language of utilities abstracts away the difference: utilities could be possible (vote buying) or negative (coercion).

However vote buying is voluntary while coercion is involuntary: we must this. For example, vengeful voters only matter for coercion.

Influence of vote type in coercion

How many cooperative voters are needed to counter-act the influence of one vengeful voters in coercive contracts?

- MN: at least 6.1
- BMR: at least 4
- KRMC: 0 (any cooperate voters add votes for Alice)

Influence of Voter Type in Buying

With vote-buying contracts, the voters who did not change their vote due to the contract may still coincidentally meet the conditions of the contract and request payment.

How much does the adversary actually pay and how does that relate to how many votes are actually being bought?

We provide some analysis and a general utility equation.

Example numbers: For optimal 2-candidate contracts, assume Alice voters and Bob voters make up 45% of the electorate each. The remaining 10% will vote according to the contract for €10.

The contract becomes profitable when a vote gained is worth at least €89 for the adversary.

For 3 candidates and similar split, the number increases to €96.

Future Work

- A general framework for eliminating contracts is left for future work
- Eliminating, or moving forward, voter choices helps in this specific case
- Screening techniques could improve contracts