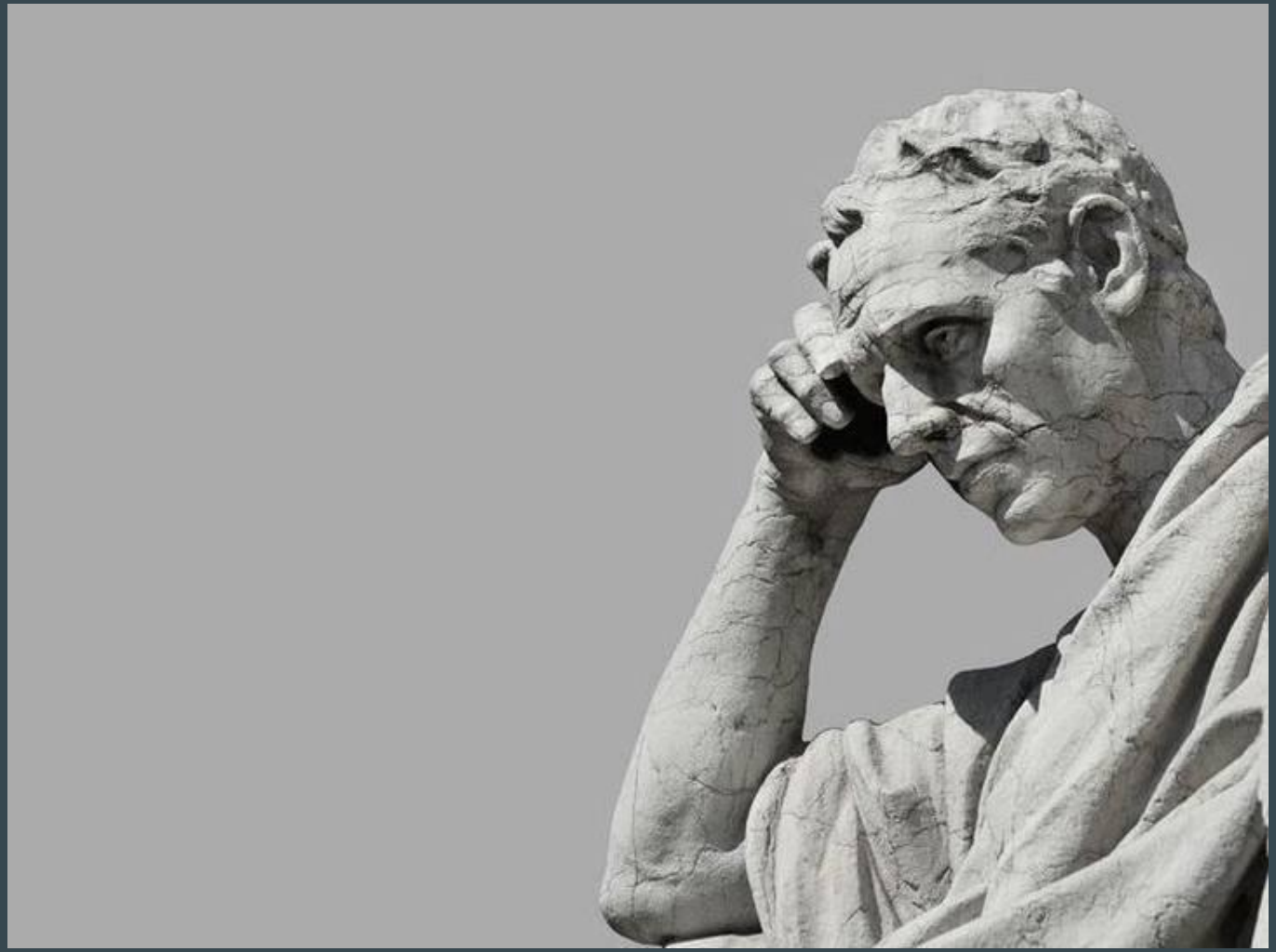
...

По Жицата у Вили

VoteChainge

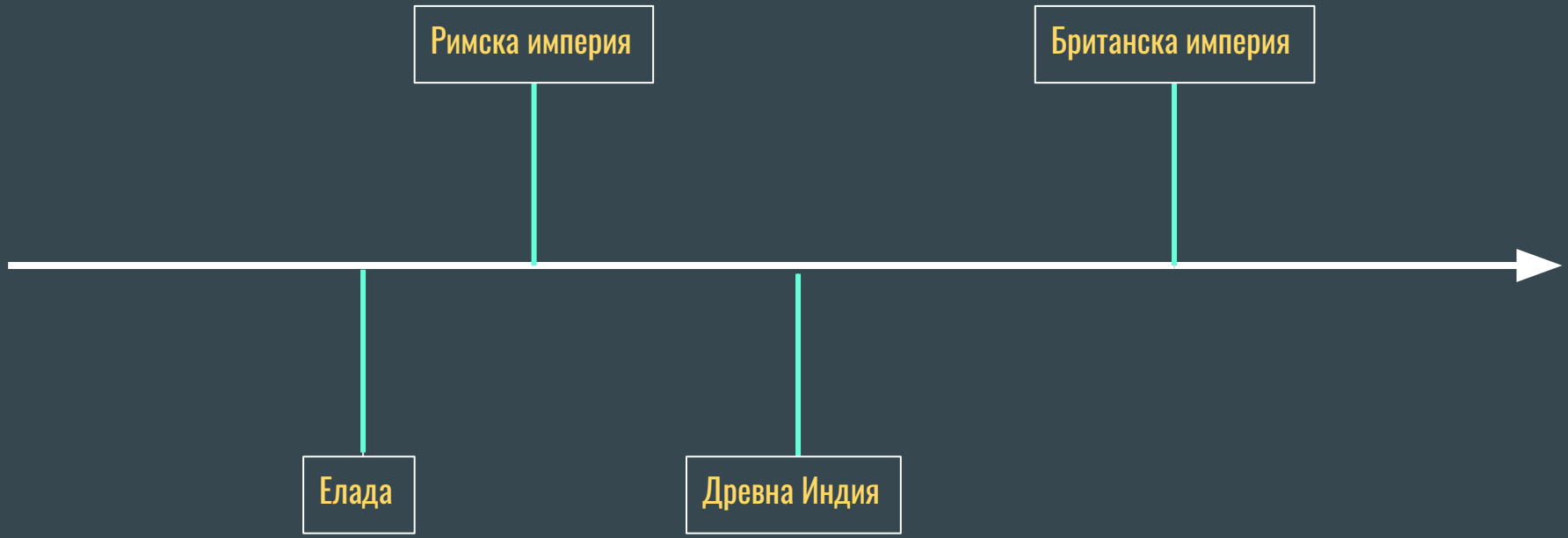
...

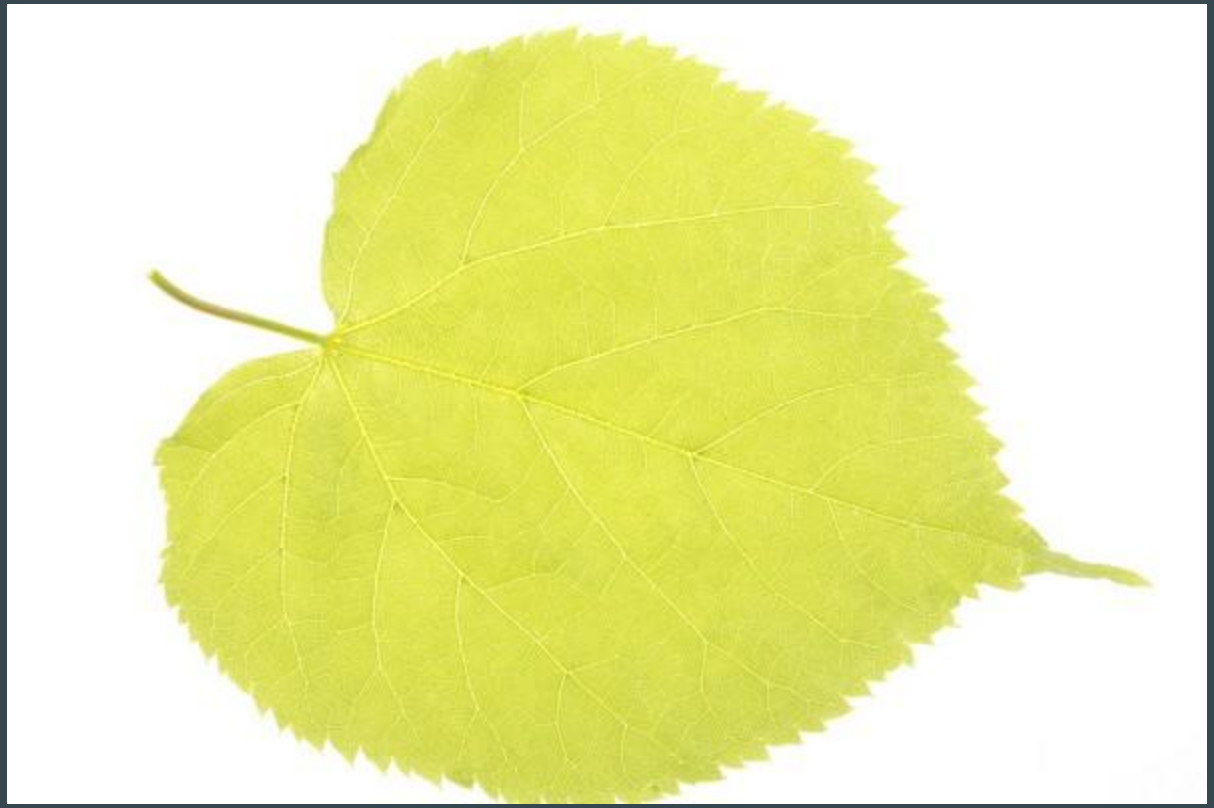
По Жицата у Вили



Малко история

Имало едно време





CARDIGANSHIRE ELECTION,

1880.

MR. L. P. PUGH begs to thank the Electors for the hearty promises of support he has received, and to inform them that his name will be **SECOND** on the Ballot Paper. Each Voter has only *One Vote*, and in Voting for Mr. PUGH, a X should be placed opposite his name as below.

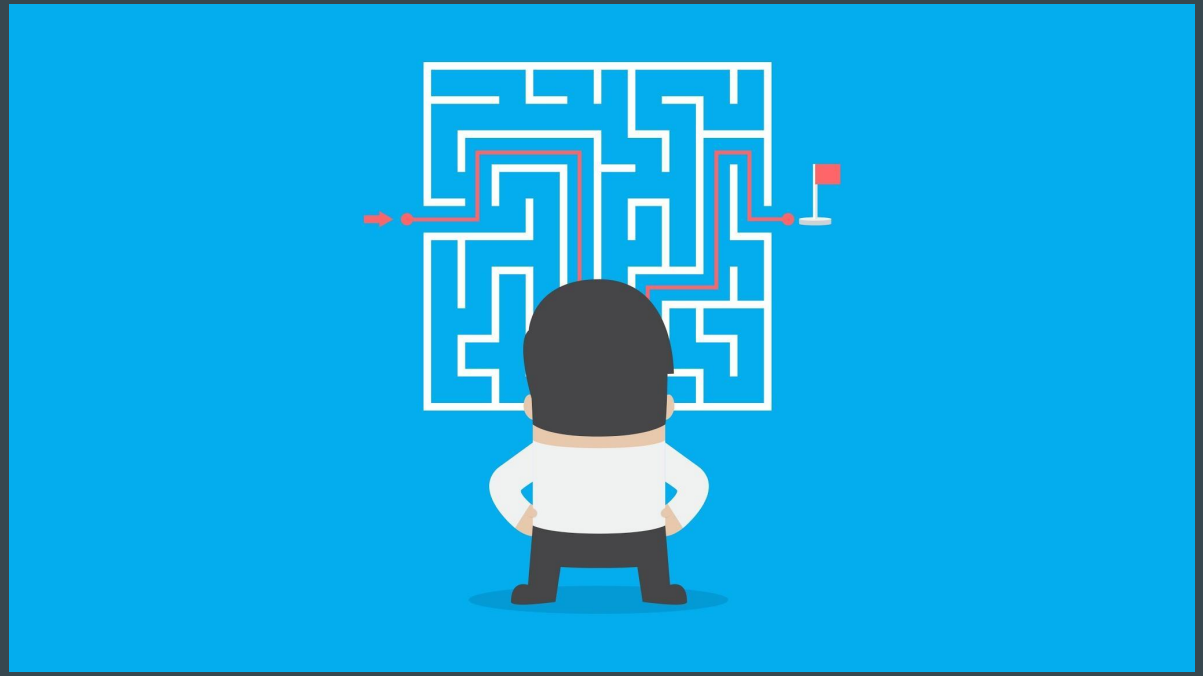
1	LLOYD. Thomas Edward Lloyd, Coedmore, in the County of Cardigan, Esquire.	
2	PUGH. Lewis Pugh Pugh, Abermaide, in the County of Cardigan, Esquire.	X

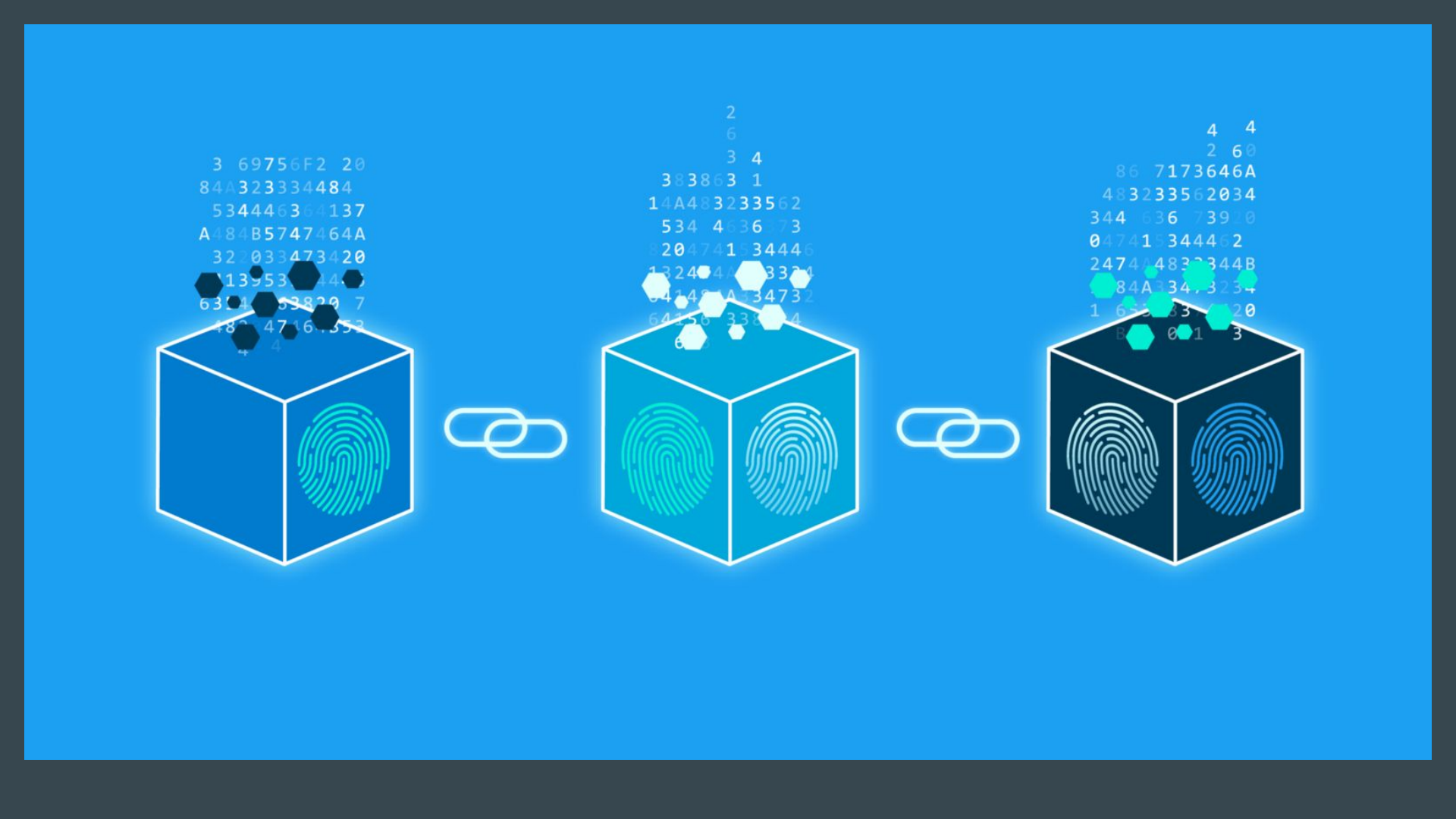
Under the Ballot it is absolutely impossible for any one to tell which way any Voter has Voted, unless informed by the Voter himself; and Mr. David Davies, M.P., has offered £1,000 to any one who can prove how any individual Voter has Voted.

Please Turn Over.

Имало едно време ... същото като сега?


PROBLEMS
AHEAD
NEXT
14 MILES






VOTE

Станция А

Станция В

Станция Б

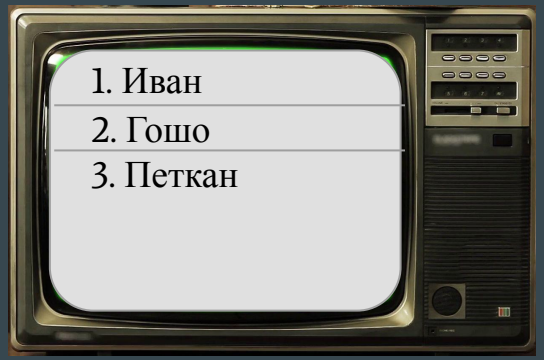
Станция А

Станция А

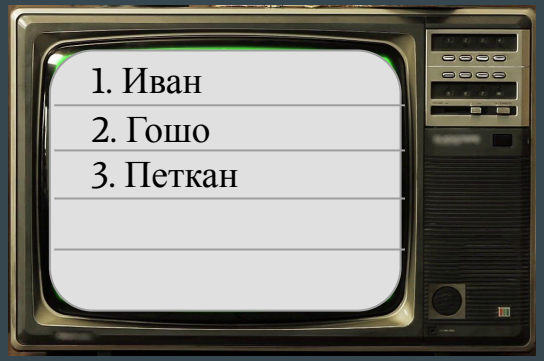
PIN: 9881

Станция А

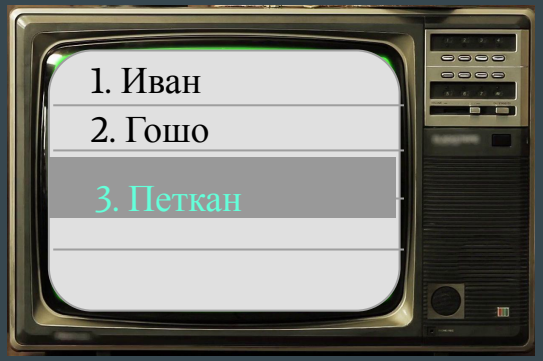
PIN: 9881



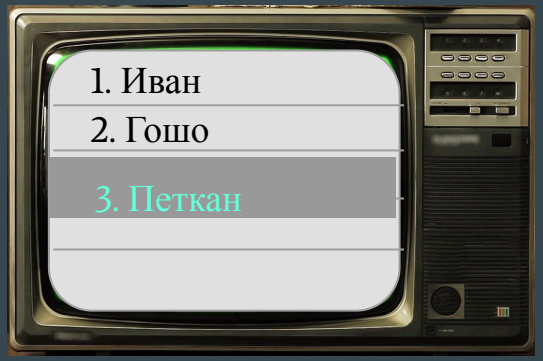
Станция А

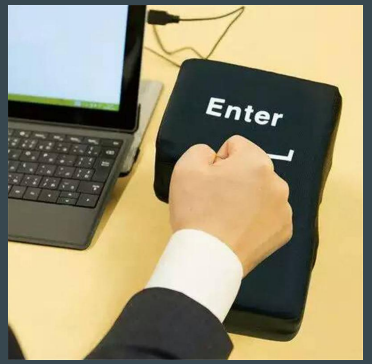


Станция А

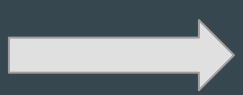


Станция А





Нов глас



Станция А

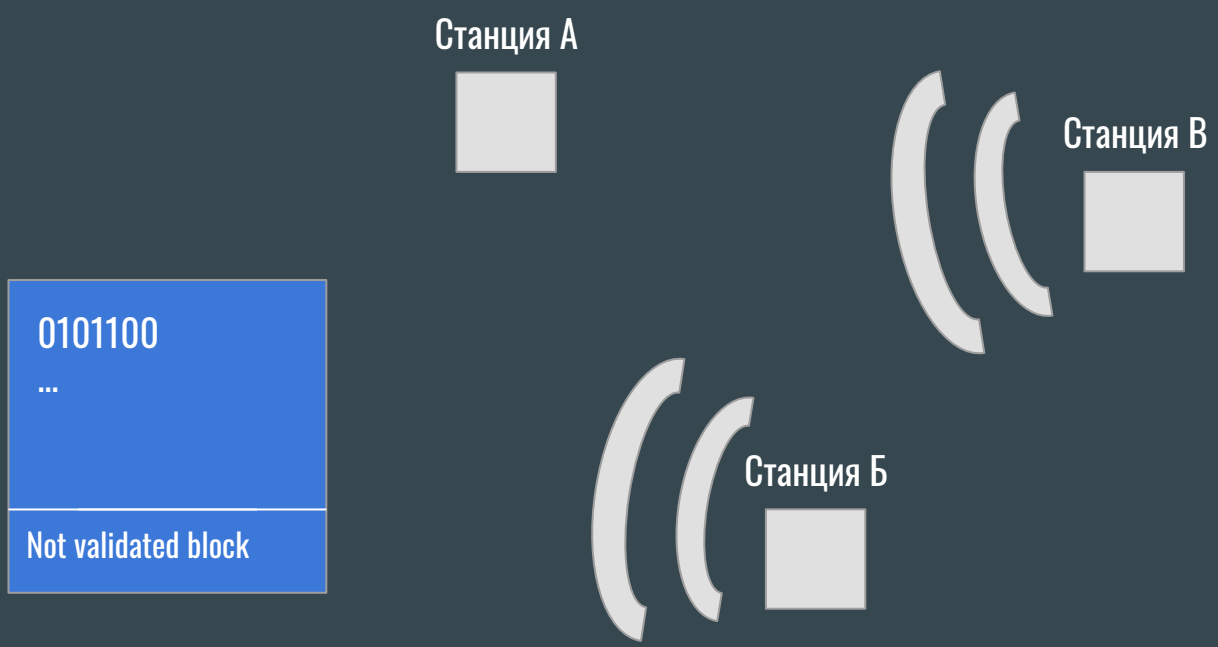
1	Signature	10:03:24
2	Signature	10:05:41
2	Signature	10:08:04

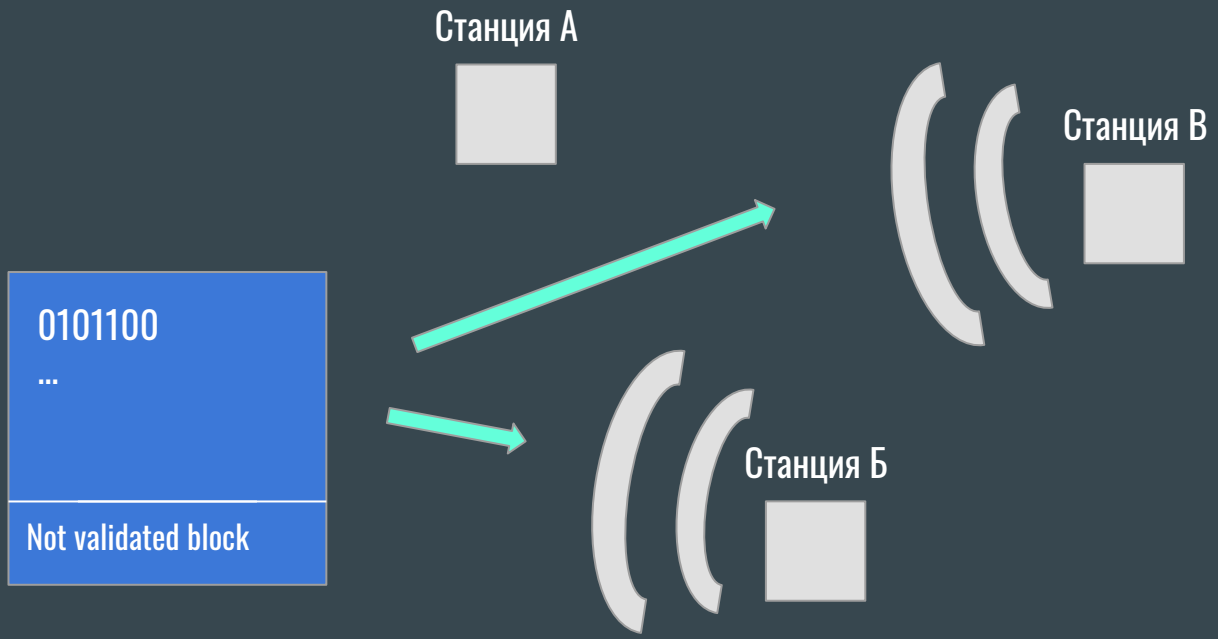
Нов глас

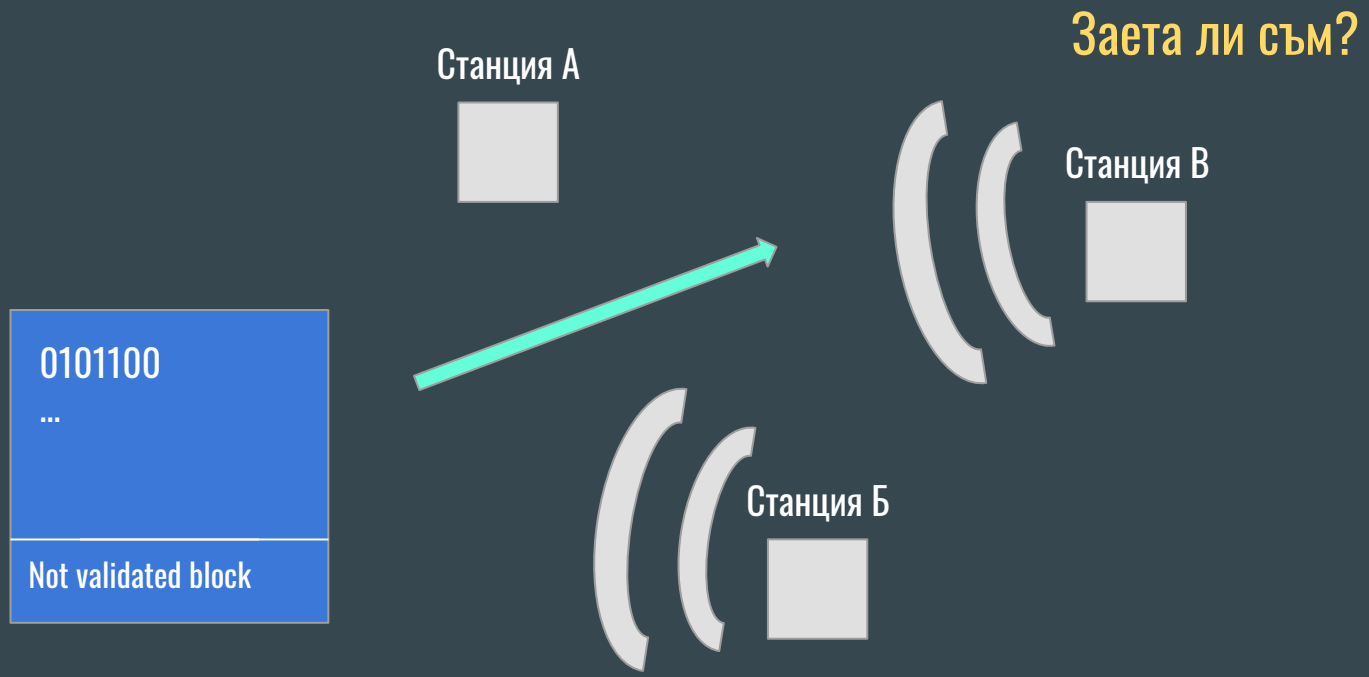
Станция A

1	Signature	10:03:24
2	Signature	10:05:41
2	Signature	10:08:04
3	Signature	10:24:19

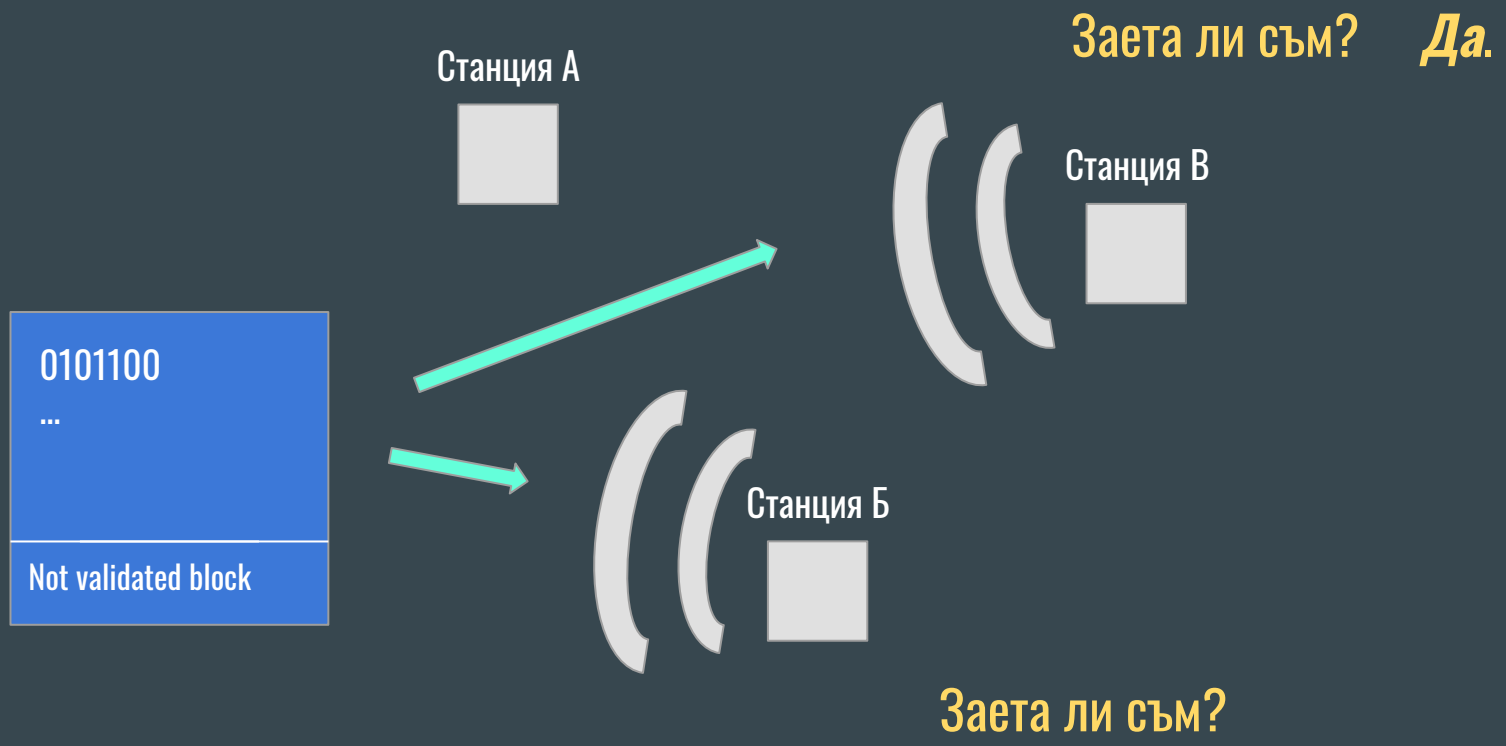

Станция А

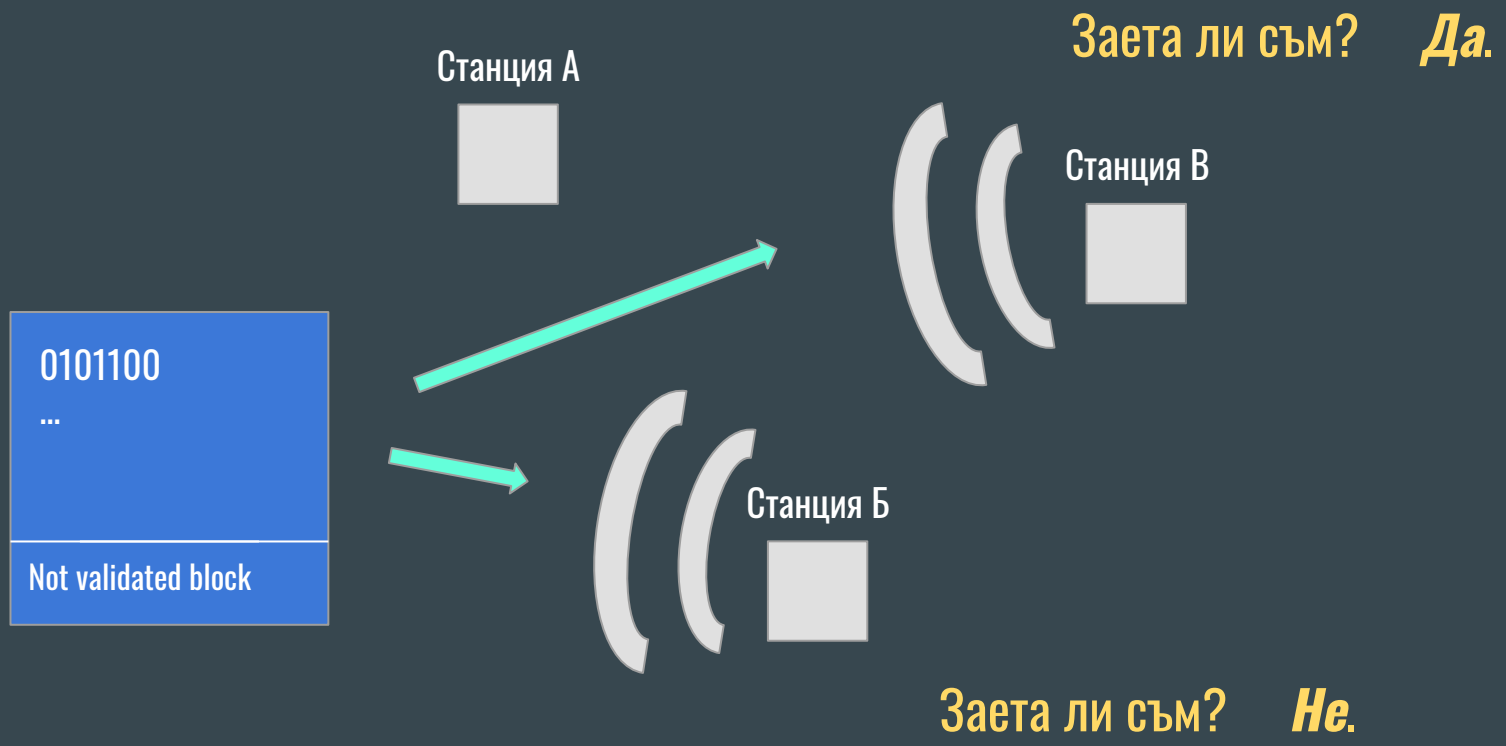

Станция А
Станция В
Станция Б
0101100
...
Not validated block

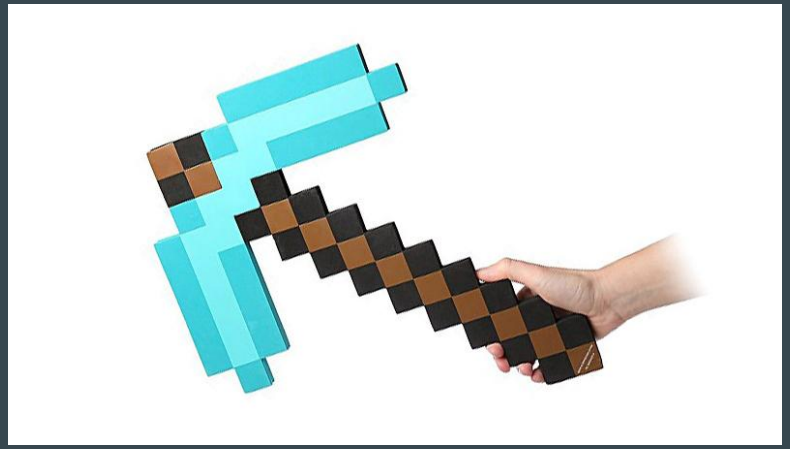

Станция А
Станция В
Станция Б
0101100
...
Not validated block


Заета ли съм?
Станция А
Станция В
Станция Б
0101100
...
Not validated block


Заета ли съм? Да.
Станция А
Станция В
Станция Б
0101100
...
Not validated block


Заета ли съм? Да.
Станция А
Станция В
0101100
...
Not validated block
Станция Б
Заета ли съм?


Станция А
Заета ли съм? Да.
Станция В
0101100
...
Not validated block
Станция Б
Заета ли съм? Не.

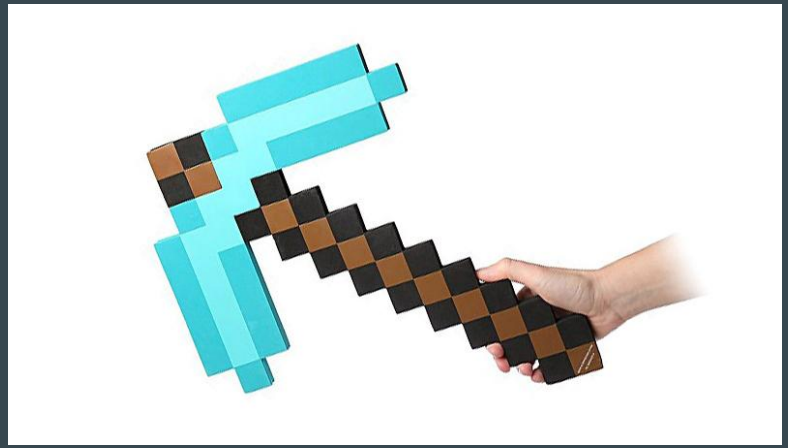


0101100

...

Not validated block

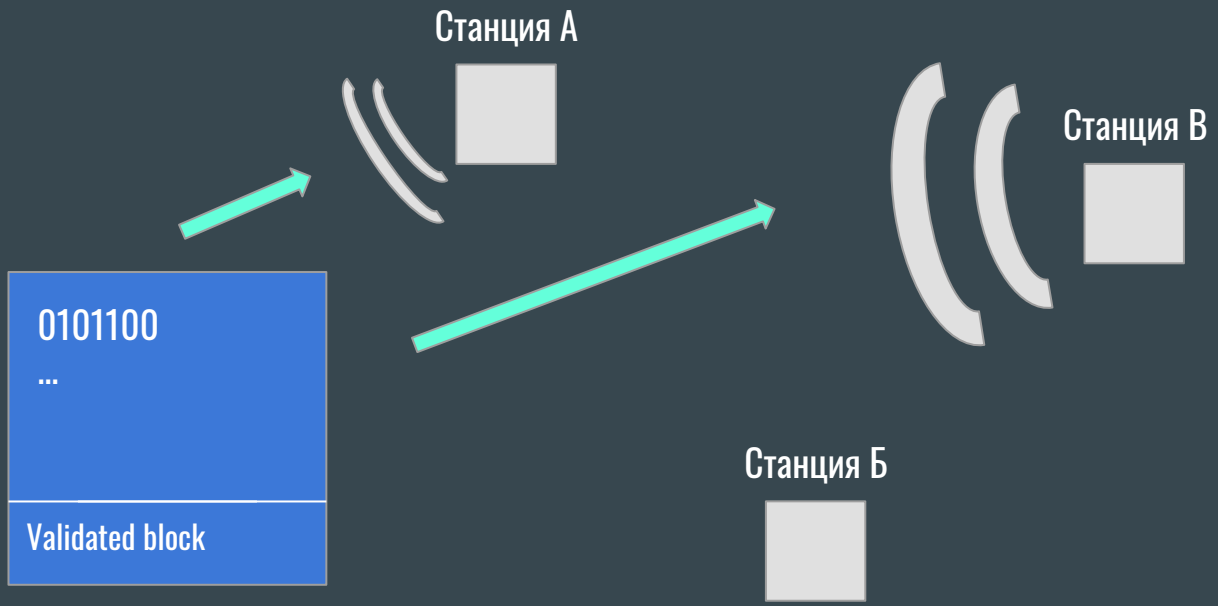
Станция Б



0101100
...

Validated block

Станция Б


Станция А
Станция В
Станция Б
0101100
...
Validated block


0101100
...
Validated block
0111100
...
Validated block
000100
...
Validated block

Във всяка станция

По Жицата у Вили

Стефан

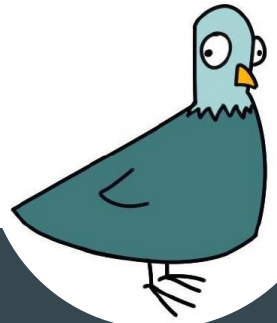
Криптография

Камен

P2P мрежа

Хари

Станции за гласуване



Крис

Структура на blockchain

Благодаря за вниманието!

Въпроси?

Сигурност

- Sha512 + Digital signature
- TCP с допълнителни checksum-и
- Пълна прозрачност
- На живо генерирани checksum-и за кода качен на станцията
  - Може да се сравни с този от хранилището от всеки желаещ

Proof-of-stake algorithm

- Невалиден блок не се добавя във веригата
- Не изчислява всяка станция
- За валидиране се избират само ненатоварени станции
- Решението се споделя с останалите

Гласуване по веднъж

- Временен PIN
- KeyPair (Private-Public) per vote

  $\Rightarrow$ Digital Signature per vote

- Без повторения
- Timestamp

Броене на гласове

- Всяка станция - всички гласове
- Всяка станция брои
- Сравнение
- Най-много еднакви отговори - верен отговор

Използвани алгоритми

- Хеширане (sha)
- Разширен алгоритъм на Евклид + идентичност на Безу
- Дигитален подпис (асиметрично криптиране)
- Blockchain + proof-of-stake

Благодарим на всички за вниманието

... и успех на всички участници.