

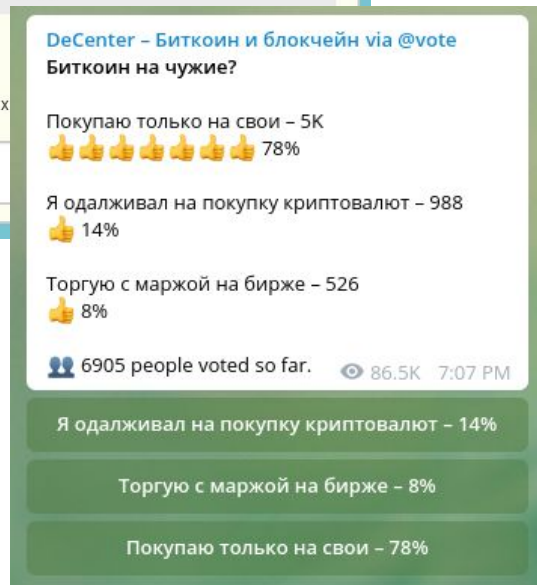
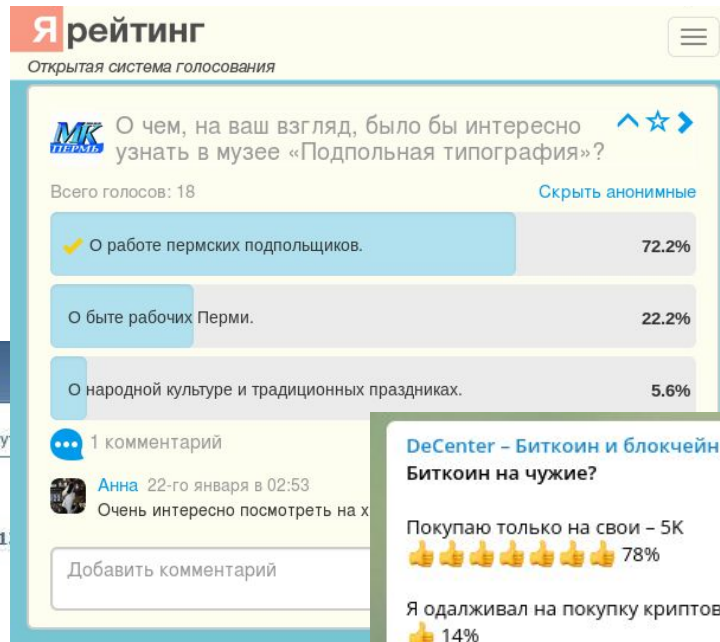
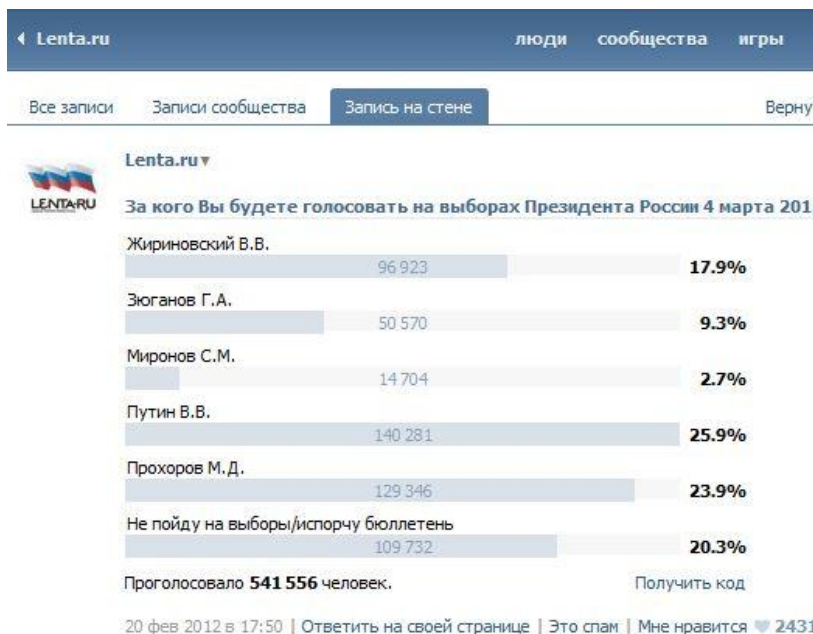
# Blockchain Voting

Arsen Gasparyan

<http://yarating.ru>

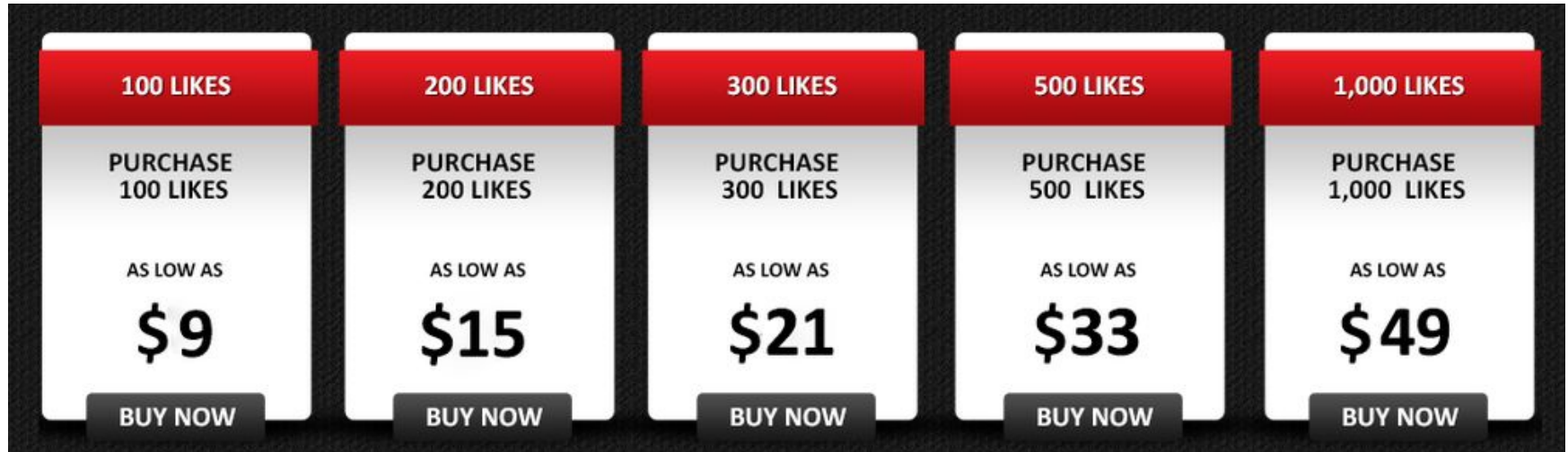
# Why Blockchain?

There are many voting solutions already



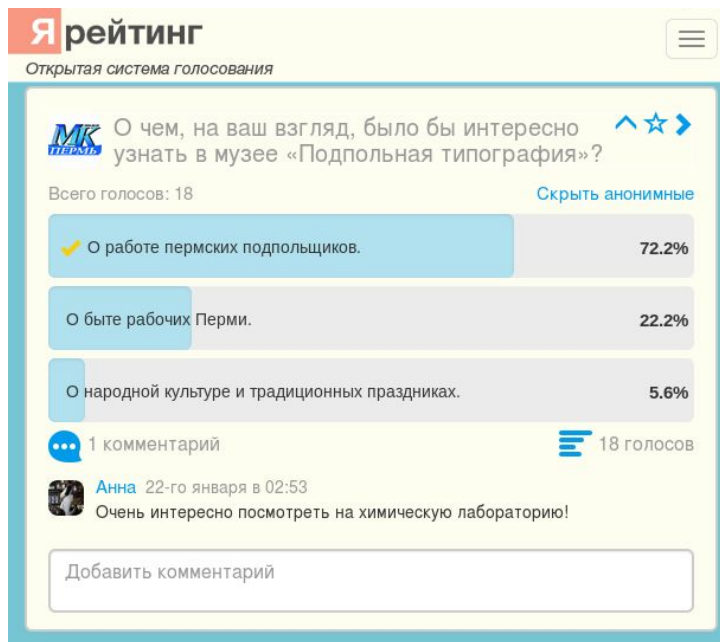
# Why Blockchain?

Centralized solutions are prone to manipulations



# Why Blockchain?

Central database is fine for polls



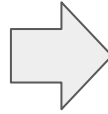
# Why Blockchain?

But collective decision making requires trust



# Registration

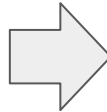
Online authentication to obtain voting power



# Ballot

Virtual ballot issued by a central authority gives a right to vote

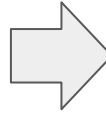
ИЗБИРАТЕЛЬНЫЙ БЮЛЕТЕНЬ для голосования на выборах Президента Российской Федерации 4 марта 2012 года	
<b>РАЗЪЯСНЕНИЕ О ПОРЯДКЕ ЗАПОЛНЕНИЯ ИЗБИРАТЕЛЬНОГО БЮЛЕТЕНЯ</b> Поставьте любой знак в пустом квадрате справа от фамилии только об одном зарегистрированном кандидате и только одного об одном кандидате. Идентификационный бюллетень, в котором не собраны отметки в квадратах, расположенных справа от сведений о зарегистрированных кандидатах, или знак (знаки) проставлен (проставлены) более чем в одном квадрате, считается недействительным. Избирательный бюллетень, не заверенный подписью двух членов районной избирательной комиссии с правом решающего голоса и печатью районной избирательной комиссии, без специального знака (знаки) проставленного бюллетенем неуставленной формы и при подбросе голоса не учитывается.	
<b>ЖИРИНОВСКИЙ Владимир Валентинович</b>	1946 года рождения, место жительства – город Москва, Государственная Дума Федерального Собрания Российской Федерации, депутат, руководитель фракции Политической партии «Либерально-демократическая партия России», член Комитета Государственной Думы по обороне; выдвинул Политической партией «Либерально-демократическая партия России», член Политической партии «Либерально-демократическая партия России», Председатель партии <input type="checkbox"/>
<b>ЗЮГАНОВ Геннадий Андреевич</b>	1944 года рождения, место жительства – город Москва, Государственная Дума Федерального Собрания Российской Федерации, депутат, руководитель фракции Политической партии «Коммунистическая партия Российской Федерации», член Комитета Государственной Думы по науке и научно-технической политике; выдвинул Политической партией «Коммунистическая партия Российской Федерации», член Политической партии «Коммунистическая партия Российской Федерации», Председатель Центрального Комитета партии <input type="checkbox"/>
<b>МИРОНОВ Сергей Махаилович</b>	1953 года рождения, место жительства – город Москва, Государственная Дума Федерального Собрания Российской Федерации, депутат, руководитель фракции Политической партии СПРАВЕДЛИВАЯ РОССИЯ, член Комитета Государственной Думы по жилищной политике и жилищно-коммунальному хозяйству; выдвинул Политической партией СПРАВЕДЛИВАЯ РОССИЯ, член Политической партии СПРАВЕДЛИВАЯ РОССИЯ, член Президиума Центрального Совета партии, Председатель Совета Партии депутатов партии <input type="checkbox"/>
<b>ПРОХОРОВ Махмуд Дмитриевич</b>	1965 года рождения, место жительства – Красноярский край, Северо-Енисейский район, ООО «Группа ОБСНСИМ», Президент; самовыдвиженец <input type="checkbox"/>
<b>ПУТИН Владимир Владимирович</b>	1952 года рождения, место жительства – город Москва, Правительство Российской Федерации, Председатель Правительства Российской Федерации; выдвинул Всероссийской политической партией «ЕДИНАЯ РОССИЯ» <input type="checkbox"/>



```
hQIOA9ZuNM597pYxEAgAz6X10D618TjeMgFV:  
cauG+p+c4pjFM9+Z3q14n2zj4wOdcHXUp5FB:  
wW8n8HHsIvptel5XzgpBhrmYp1HaxFuh6h9V1:  
Hmuy+KZINNwmpuTYmrGRdhfvw3a9Rpo0eRn:  
eS30os06bIvcA1+mJDHFhDGhFHI7pqR6p7dc:  
aULmY/KYi3G+bXNzk3AZaHS6WI+mL7UldvWZ:  
MHkY/QW22oY75uTM64LvswI/kMr6MjG6V40f:  
bEjpuPZvLMVNP1zHG4oyOaH6ZOGrfvHGoTsl:  
CndvvsDUNgHeGFhNiZ5qNnwka8ccHkZqgDFw:  
jMbb+DQ35mveZ6Gke+wiKKLaddB05vW4oAKG:  
p1G9rUqldUoI6d1pdUpkKdfo+HdFHKh+ Bd4/  
c4UCDgPmFSp+6RAVXBAH/2o691VM1OU9BJPv:  
TUCvCZCC5S2a2o01LGT1W/UvR3TJypbm2WSM
```

# Voting

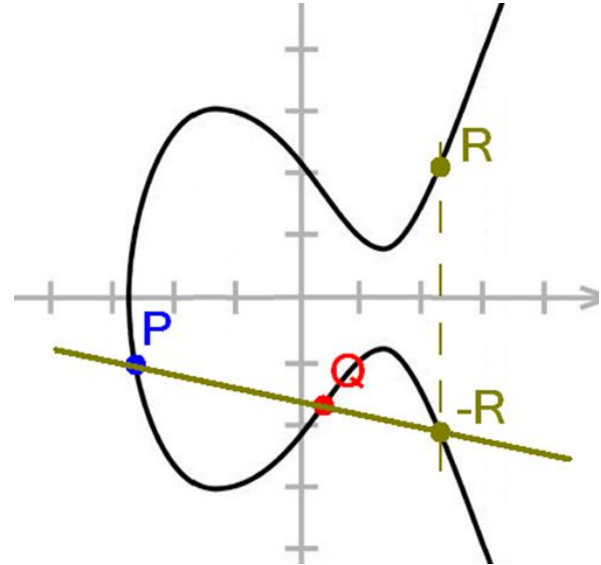
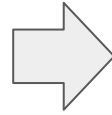
No physical presence is required





# Privacy

Cryptography (math) ensures anonymity



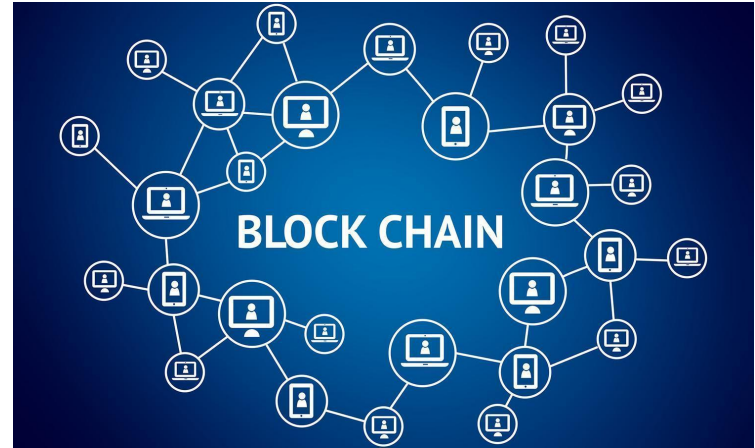
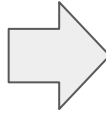
# Privacy vs Transparency

There are cryptographic methods which make it possible to achieve anonymity and verifiability at the same time.

- Blind signatures
- Ring signatures
- Zero-knowledge proofs

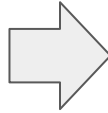
# Ballot box

Global transparency and immutability



# Tallying

Independently verifiable results



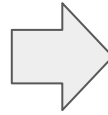
```
GroupDesc* item = el->FirstChildElement();  
GroupDesc* elDesc;  
  
std::string sp_name = item->Attribute("sp_name");  
std::string spritename = item->Attribute("spritename");  
  
float x = boost::lexical_cast<float>(item->Attribute("x"));  
float y = boost::lexical_cast<float>(item->Attribute("y"));  
float offset = boost::lexical_cast<float>(item->Attribute("offset"));  
unsigned layer = 50; // default  
if ( item->Attribute("layer") != NULL )  
{  
    layer = boost::lexical_cast<unsigned>(item->Attribute("layer"));  
}  
  
elDesc->name_ = sp_name;  
elDesc->spriteName_ = spritename;  
elDesc->x_ = x;
```

# Costs

~ 10.3B RUB (\$330M) spent on  
Russian Presidential Elections  
in 2012

~ 110M people voted

~ 94 RUB (\$3) per vote



\*Probably less

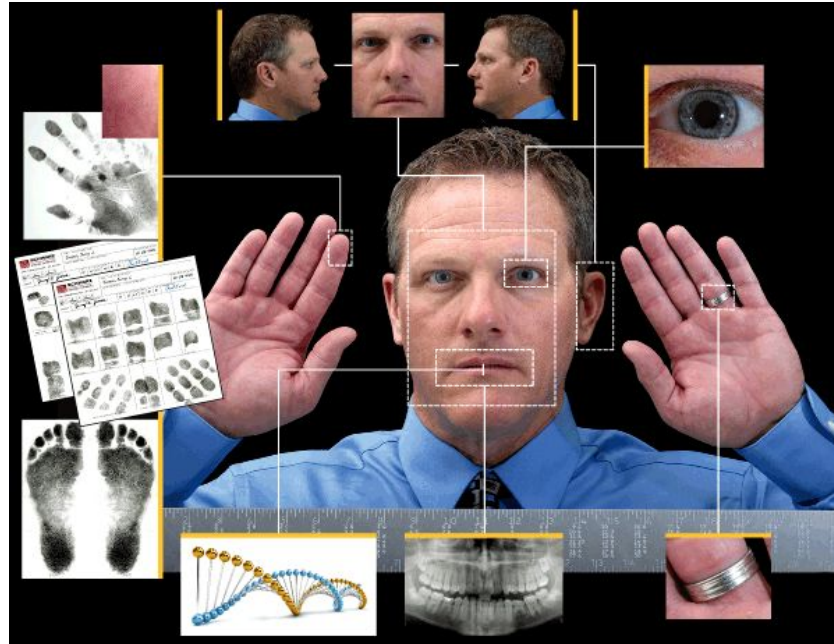


# Problems

- Organizational
- Security
- Technical

# Voter identification

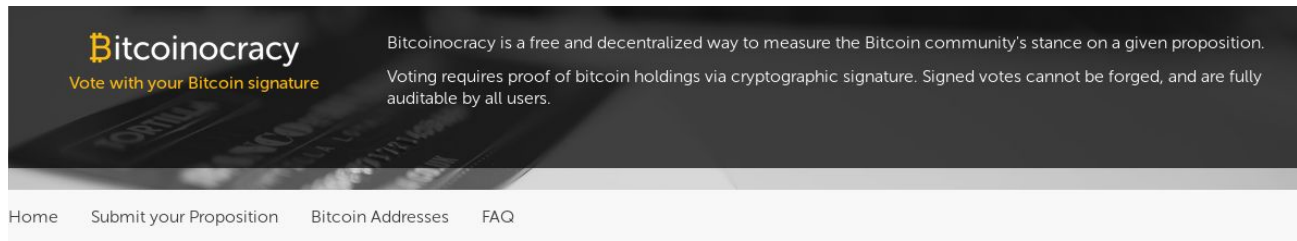
- Identification centers will link digital identities to real people



# Sometimes anonymous key-pair is enough

PoS  
(Proof-of-Stake) /  
shareholder voting

a-la  
[vote.bitcoin.com](https://vote.bitcoin.com)



**Bitcoinocracy**  
Vote with your Bitcoin signature

Bitcoinocracy is a free and decentralized way to measure the Bitcoin community's stance on a given proposition. Voting requires proof of bitcoin holdings via cryptographic signature. Signed votes cannot be forged, and are fully auditable by all users.

Home   Submit your Proposition   Bitcoin Addresses   FAQ

Active	Popular	Controversial	Decided	Valid	Invalid	Newest	Hidden

Micropayment channels and other tools can help Bitcoin reach all applications for money, without compromising Bitcoin's most valuable properties. Updated about 1 hour ago	-\$233,945,777
Block size limit should be increased to 8 mb as soon as possible Updated about 1 hour ago	\$233,920,363
In the event of a fork, I will sell RBF BlockStream Core Coins and buy Classic Bitcoins Updated about 1 hour ago	\$187,694,918

Submit

Latest Bitcoin News Stories

BTC/USD **11120.14** ▼

- Hong Kong Fund Acquires Chinese Mining ...
- The 2018 Satoshi's Vision Conference Hea...
- AIER Researchers: Bitcoin's Price Moves wi...
- PR: Propy Launches the First Pilot in the U...
- Us Government Scientists: "Bitcoin is a For...
- PR: LiveTree Adept and the 21 Million Proje...
- Japanese Crypto Exchanges Strengthen S...
- Russia Developing System to Identify Cryp...



# Bitcoinocracy

“ I believe that Block size limit should be increased to 8 mb as soon as possible ”

Agree Doubt

Please copy the above statement, sign it with your bitcoin address, and paste signature here

Place signature here ?

Submit

Warning: [Bitcoin signatures expose your public keys](#) (that shouldn't be a problem until [ECDSA](#) is broken). Moreover address reuse with a faulty random number generator [may leak your private keys](#).

# Bitcoinocracy

“ I doubt that Block size limit should be increased to 8 mb as soon as possible ”

Agree Doubt

Please copy the above statement, sign it with your bitcoin address, and paste signature here

Place signature here ?

Submit

Warning: [Bitcoin signatures expose your public keys](#) (that shouldn't be a problem until [ECDSA](#) is broken). Moreover address reuse with a faulty random number generator [may leak your private keys](#).

# Bitcoinocracy

Signatures are downloadable and verifiable

21524.39227201 BTC (97.73%) Believe		499.22241000 BTC (2.27%) Doubt	
<a href="#">1KwA4fS4uVuCNjCtMi...</a>	20539.98688563 BTC	<a href="#">1M1RdcicqSA93SAtPHb...</a>	403.81141000 BTC
<a href="#">1BMjmWXy7hnYnJwCY...</a>	673.86081200 BTC	<a href="#">1LGXUxGntKfA6sE6hZ3...</a>	95.41000000 BTC
<a href="#">1Hz96kJKF2HLPGY15J...</a>	217.18690430 BTC	<a href="#">1HwAjL8p3RfpdzA2cnn...</a>	0.00100000 BTC
<a href="#">1KZS9h672dMDJAiTsy...</a>	50.00812788 BTC	<a href="#">1L7pKQwnOKsauuN4p...</a>	0.00000000 BTC
<a href="#">1Mwcdn9NZ9LedHZdl...</a>	25.00000000 BTC	<a href="#">17ecfpkYSKugWVB8uv...</a>	0.00000000 BTC
<a href="#">1G7...78551198M...</a>	0.96161600 BTC	<a href="#">1B...7...82688VF-C-</a>	0.00000000 BTC

[All signatures as JSON](#)

# Scalability

- Naive on-chain voting is too expensive to be practical using general purpose blockchain
- E. g. it would take ~200 days and enormous expenses on transaction fees to conduct Russian presidential elections on Bitcoin blockchain
  - 260 bytes per transaction \* 110M voters / 144 mb per day

# Related Projects

- Follow My Vote
  - an open-source platform for blockchain voting
  - <http://followmyvote.com>
- Open Vote Network
  - Ethereum contract which utilizes non-interactive zero-knowledge proofs for voting
  - <https://github.com/stonecoldpat/anonymousvoting>
- Polys
  - a potentially open-source platform for blockchain voting powered by Kaspersky Lab
  - <https://polys.me/>
- HyperLedger Indy (by Sovrin Foundation)
  - decentralized identity and tools for permissioned-validation blockchains
  - [http://www.windley.com/archives/2017/05/hyperledger\\_welcomes\\_project\\_indy.shtml](http://www.windley.com/archives/2017/05/hyperledger_welcomes_project_indy.shtml)

# Conclusions

- Small scale anonymous yet verifiable blockchain voting is already a reality
- Global elections via public general-purpose blockchain are too expensive due to high costs and scalability issues
- An established platform for global votings on the blockchain is probably a matter of time since there are already tools and approaches which make it possible

# Thank you!



Also thanks to

- Lykke competition participants  
(<https://streams.lykke.com/Project/ProjectDetails/blockchain-voting>)
- Google, Wikipedia, Roger Ver, Satoshi Nakamoto and the whole Internet