Crypto@Cracow #1
Cryptocurrencies
&
Blockchain

A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution.

Satoshi Nakamoto

Agenda

1. What is the motivation behind the technology?
2. How does it work?
3. What are the practical use cases?
4. Is it legal?
5. Q & A session

What is the motivation behind the technology?

Why Blockchain is Hard to Understand:

At the crossroad of

1. Game theory (*Nash equilibrium*)
2. Cryptography
3. Computer networking and data transmission
4. Economic and monetary theory

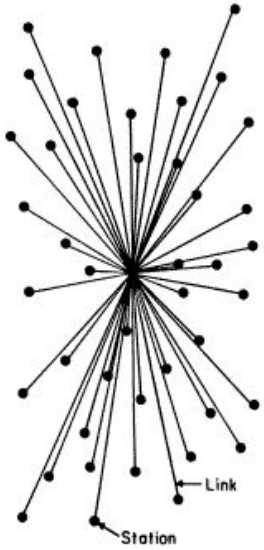
Mainly not a technology, a cultural paradigm shift instead

“Privacy is necessary for an open society in the electronic age. We cannot expect governments, corporations, or other large, faceless organizations to grant us privacy. We must defend our own privacy if we expect to have any. Cypherpunks write code. We know that someone has to write software to defend privacy, and we're going to write it..”

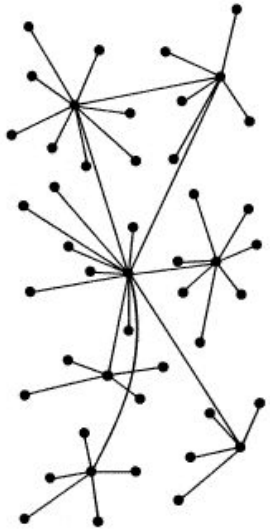
“What is needed is an electronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other”

Satoshi Nakamoto

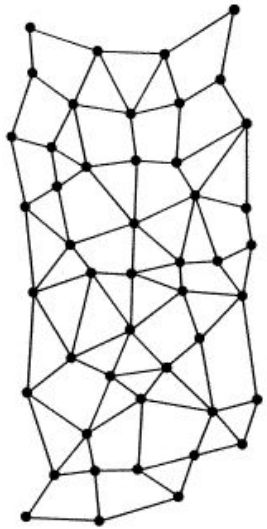
Network models



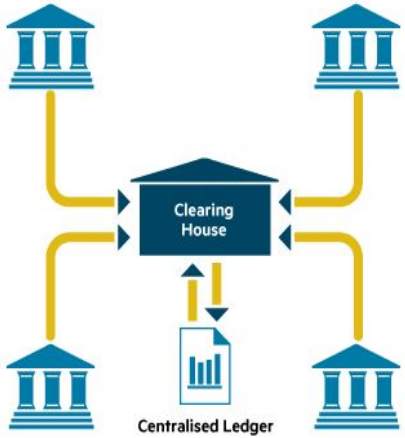
CENTRALIZED

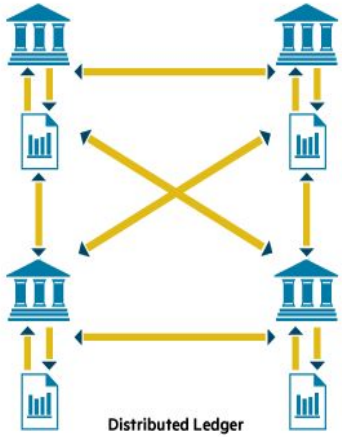


DECENTRALIZED

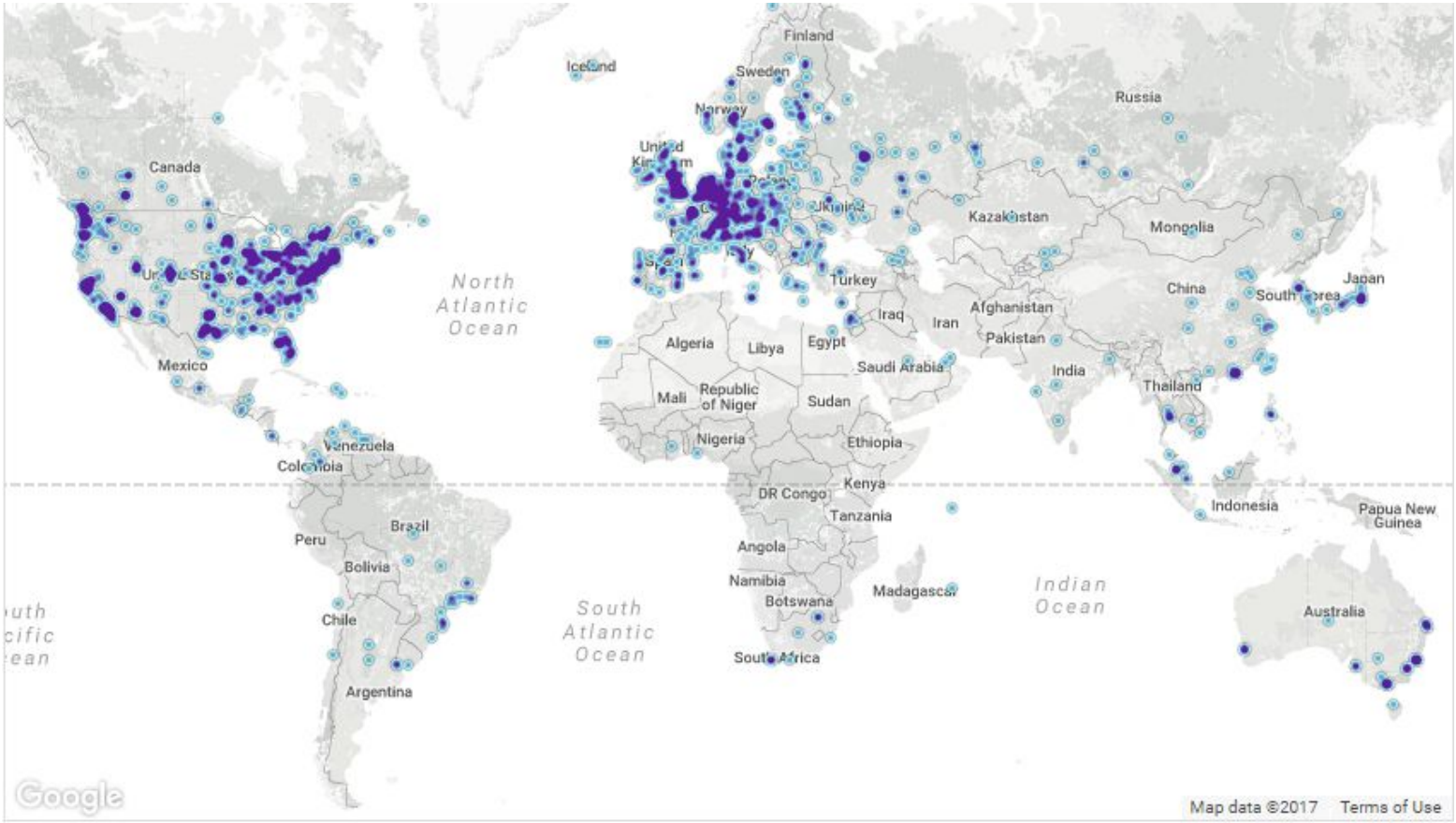


DISTRIBUTED





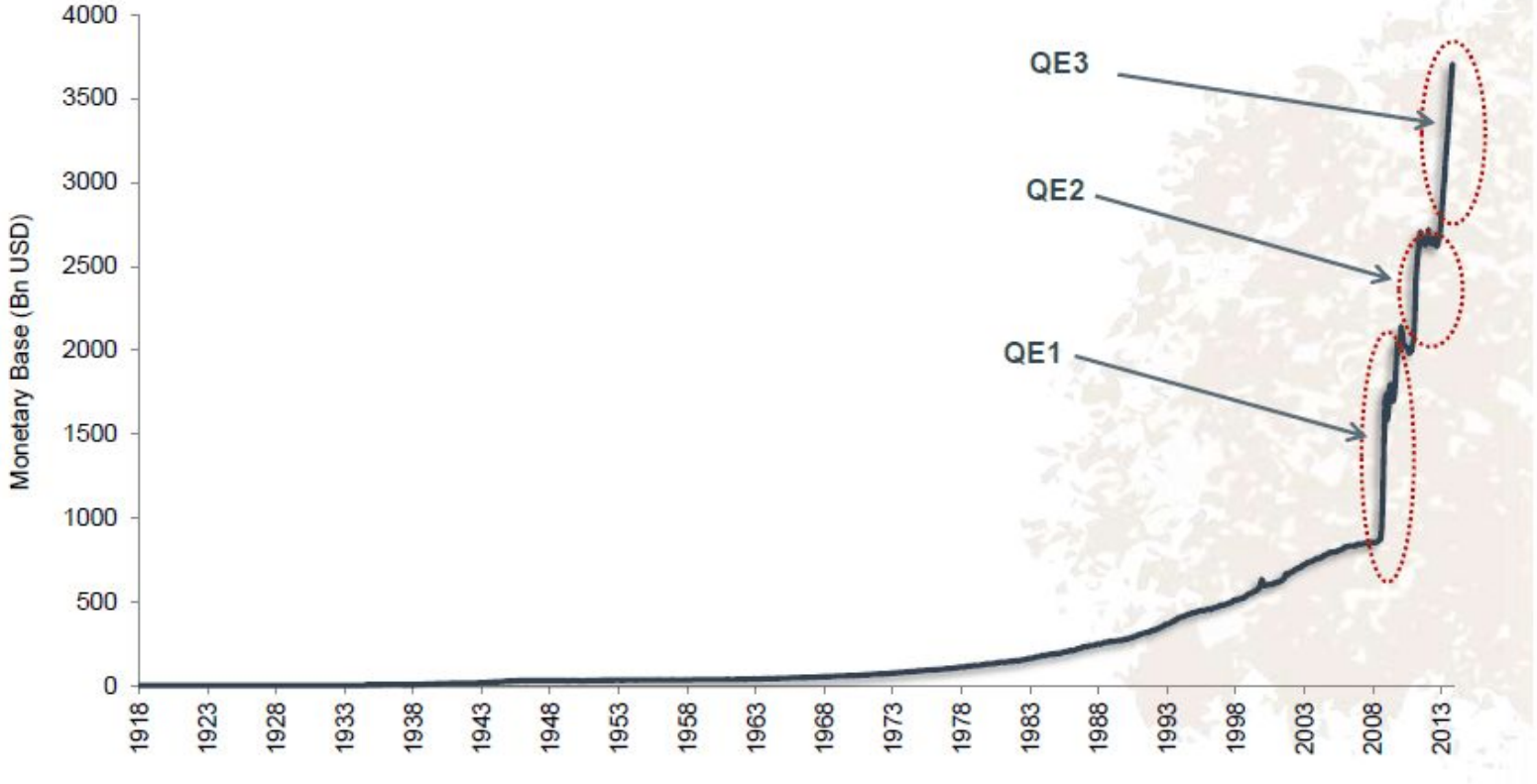
Bitcoin nodes distribution



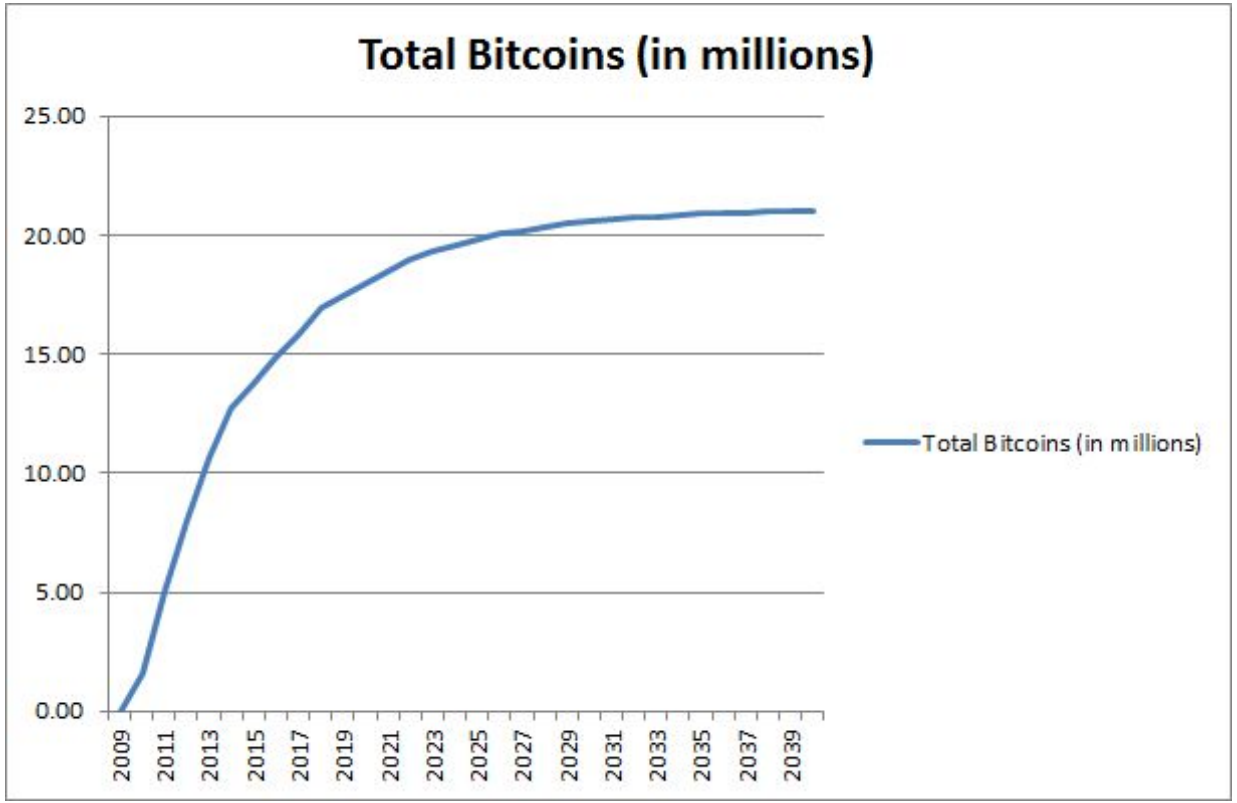
The 7 Characteristics of Money

1. **Scarcity:** limited, predictable supply
2. **Durability:** won't decay
3. **Divisibility:** easy to subdivide
4. **Recognizability:** units are recognized
5. **Fungibility:** units are exchangeable
6. **Transportability:** easy to move
7. **Difficulty of counterfeiting:** ability to make a copy to steal the value

Monetary base (USD) since 1918



Bitcoin supply



How it works?

How it works?

Bitcoin crypto building blocks

Public-key cryptography (asymmetric cryptography)

- ECDSA - Elliptic Curve Digital Signature Algorithm

Cryptographic hash functions

- SHA-256
- RIPMD-160

How it works?

Bitcoin key pairs and addresses

Bitcoin address: 17wPSXDDo9b1KDdXAMV3a1WJcsmRoKpY6t

RIPMD-160, SHA-256, Base58Check

Public key:

0450863AD64A87AE8A2FE83C1AF1A8403CB53F53E486D8511DAD8A04887E5B23522CD470243453A299FA9E77
237716103ABC11A1DF38855ED6F2EE187E9C582BA6

Elliptic Curve Cryptography

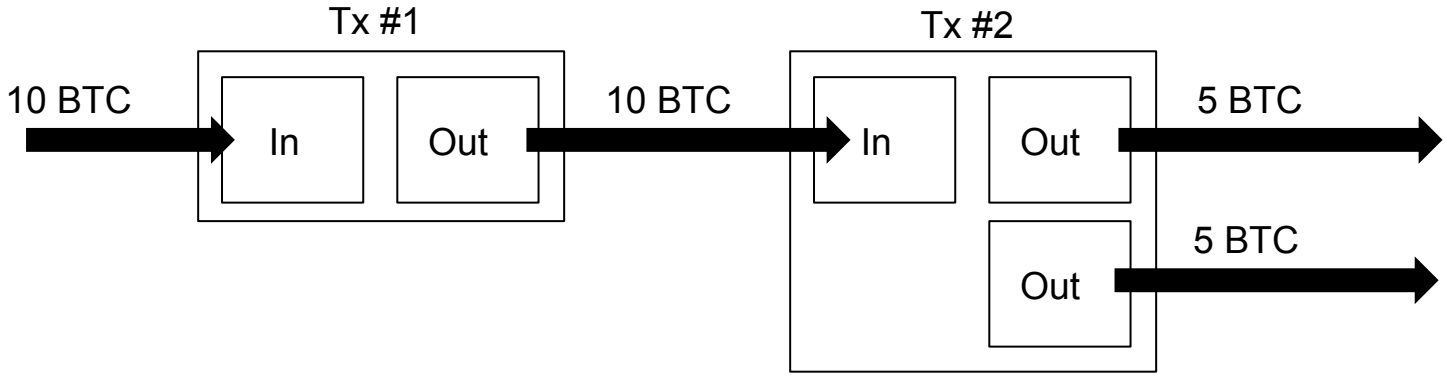
Private key: 18E14A7B6A307F426A94F8114701E7C8E774E7F9A47E2C2035DB29A206321725

How it works?

UTXOs - Unspent Transaction Outputs

An UTXO can be spent as an input in a new transaction

- No balances
- No accounts



How it works?

UTXO

Unspent outpus of the **18cBEMRxXHqzWWCxZNtU91F5sbUNKhL5PX** Bitcoin address:

[{
"**tx_hash**":"ff9bf8a9398bda843d90d189db616d113cd3390199e6e78bfb33f646168002ca",
"**script**":"76a914536ffa992491508dca0354e52f32a3a7a679a53a88ac",
"**value**": **1129370611** (Satoshi)
},
{
"**tx_hash**":"ffba26a369ac1ed6b81c68c2aa2dbe78497790bbd916611c7e395c581b440e9d",
"**script**":"76a914536ffa992491508dca0354e52f32a3a7a679a53a88ac",
"**value**": **1306498238** (Satoshi)
}, (...)]

Final balance = sum of **values** in unspent outputs

How it works?

Transaction scripts

Bitcoin uses **stack-based scripting** system.

Transaction is valid when the script execution returns TRUE.

- Supports **about 80 OP_CODE**s:
  - **Flow control**: OP_IF, OP_ELSE, ...
  - **Arithmetic**: OP_ADD, OP_SUB, ...
  - **Crypto**: OP_RIPEMD160, OP_SHA256, OP_CHECKSIG, ...
  - **Bitwise logic**: OP_EQUAL, ...

- It is **not Turing-complete** (no loops)

How it works?

Transaction scripts

Bitcoin transaction script is build from two parts: <**scriptSig**> <**scriptPubKey**>

scriptPubKey - **Locking** script (in a transaction output)

scriptSig - **Unlocking** script

How it works?

Transaction scripts

P2PKH (Pay-to-Public-Key-Hash) - most common Bitcoin transaction type

scriptPubKey: OP_DUP OP_HASH160 <pubKeyHash> OP_EQUALVERIFY OP_CHECKSIG

scriptSig: <sig> <pubKey>

Complete P2PKH script:

<**sig**> <**pubKey**> OP_DUP OP_HASH160 <**pubKeyHash**> OP_EQUALVERIFY OP_CHECKSIG

How it works?

Bitcoin mining

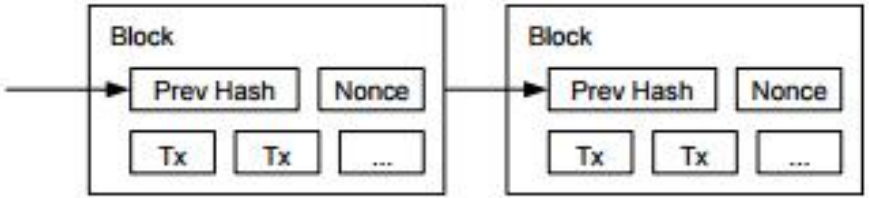
- Bitcoin mining is needed to prevent **double-spends**
- New transactions are added to the block (current block size: 1MB)
- Blockchain acts as a **distributed timestamp server**
- **Proof Of Work (POW)** is used as a consensus algorithm to choose which block to append to the blockchain
- Bitcoin nodes accept the **longest and “strongest” chain**
- Miner gets a reward for “finding” a new block (new coins are created)

How it works?

Bitcoin mining

Algorithm:

```
while(nonce < MAX):
  if sha256(sha256(blockHeader)) < target
    return nonce
  nonce += 1
```



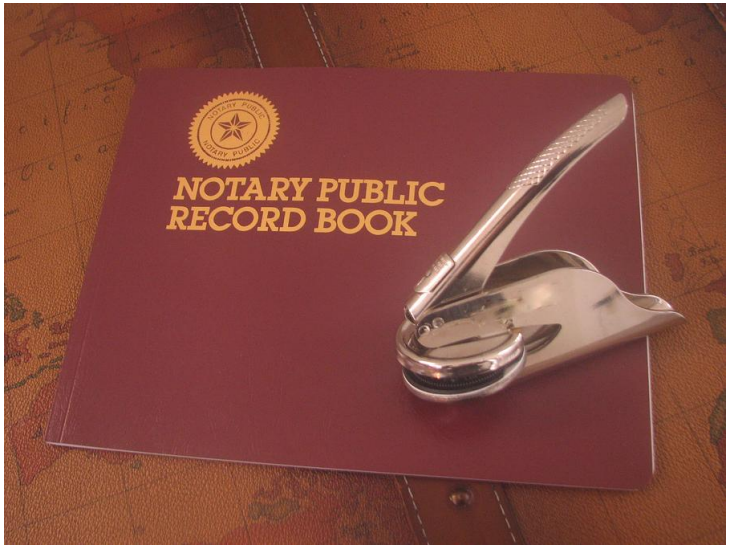
blockHeader contains:

- Hash of a prev block
- Hash based on all of the transactions in the block (Merkle tree root)
- Timestamp
- **Nonce** - usually starts at 0 and is incremented for each hash
- **Target** - current difficulty

What are the practical use cases of blockchain?

What are the practical use cases?

What if legal documents could be immutable?



Honduras property ownership case

„...Of the 7.3 billion people in the world, only two billion have a title that is legal and effective and public regarding their control over an asset”

What are the GovTech use cases?

Georgia

- First government Blockchain - a transparent, public and secure ledger — for managing land titles.

Estonia

- **Public Notary** - is an “electronic version” of a notary with remote access from anywhere globally. It was designed by developers of the e-Residency project, allowing foreign citizens to establish a business within Estonian jurisdiction.
- **The eHealth Foundation** - The system will secure citizen health data storage and allow to monitor patient conditions in real-time.
- **Blockchain based Voting for Exchanges** - Estonian subdivision of Nasdaq has successfully completed testing of the e-voting system designed for voting among shareholders of a company.

What are the commercial use cases?

- **Mycelia for Music -** Redefining the way we buy music - http://myceliaformusic.org/
- **Resonate -** Next generation of music streaming **-** https://resonate.is/
- **Slock -** Temporary access to all physical objects aka “the sharing economy” – (direct competition for Airbnb, Lyft,Uber, Trafficar) https://slock.it/
- **Followmyvote** - Blockchain based Online Voting platform https://followmyvote.com/
- **La Zooz** – New application for ride sharing; A Decentralized Transportation Platform owned by the community and utilizing vehicles unused space. By using cryptocurrency La Zooz works with a “Fair Share” rewarding mechanism for developers, users and backers. http://lazooz.org/
- **Steemit** - *Steem* is a blockchain-based social media platform where anyone can earn rewards (paid in Steemit cryptocurrency – exchangable for other cryptocurrencies) https://steemit.com/
- **Boardroom** - Boardroom is a Governance Framework and dApp made for Individuals and Companies to manage their Smart Contract Systems on the Public and Permissioned Ethereum Blockchains. http://boardroom.to/

What are the potential use cases?

- **Govtech - Vested Responsibility** - Smart contracts can ensure that electorates can be elected by the people for the people so that government is what it's meant to be. The contracts specify the electorate's expectations and electors will get paid only once they do what the electorate demanded rather than what funders desired.
- **Online Gambling Industry** – irreversible transactions, anti money laundering, know your customer, limiting fraud.
- **Birth, Wedding and Death Certificates** - Few things are more important than documents showing you're born, married, died which open your rights to all sorts of privileges (such as voting, working, citizenship), yet mismanagement is rife. Up to a third of children under the age of five have not been issued a birth certificate, the UNICEF reported in 2013.
- **Blockchain Based Personal Identification -** We carry a range of identifications: Our driver's license, computer password, identity cards, passports, keys, social security ID, and so forth. Blockchain ID is a digital form of ID that's engineered to replace all these forms of physical identification.
- **University Degrees and Diplomas** – Easy and error free way to confirm that a given document was issued by a legitimate institution.

Is it legal?

Is it legal?

What does it mean: to be legal?

Is using bitcoin punishable? (penalization)

Is using bitcoin a criminal act? (criminalization)

Is using bitcoin legally effective according to the private law?

Is using bitcoin regulated?

Is it legal?

Is using bitcoin taxed?

Is using bitcoin a violation of the personal data regulations?

Is consumer who's using bitcoin under the protection of the consumer law?

Is using bitcoin a subject to the administrative penalty?

Planned amendments:

1. Amendment of the Fourth Anti-Money Laundering Directive (European level)
2. Central Registry of Accounts Act - Ustawa o Centralnej Bazie Rachunków (National level)

Is it legal?

Summary:

According to the polish law, using cryptocurrencies isn’t punishable and criminalized. With some caution we could assumed that using cryptocurrencies as a mean of payment could effectively redeem pecuniary obligation. Using crypto-currencies is taxed, the customer remain under the protection of the customer law. Other administrative regulations apply to the service providers, not to the customers. Currently, there’s a lack of crypto-currencies’ definition in the polish legal system but it could change in a short time.

Disclaimer

Blockchain has a great potential to be a disruptive force in the many different sectors. It is already possible to see where it might have an impact, in areas ranging from payments and settlements to smart contracts, e-identity and commercial use.

When considering what technology to use to support your next-generation applications, do a careful analysis of your requirements whether a blockchain is the best possible solution. Don't let the arguments of proponents of any technology convince you that their approach is better.
For some, blockchain might seem as the silver bullet, however, bear in mind that not all glitter is gold. There is still long and bumpy way ahead.

Thank You For Your Attention!

Any questions?

You can find us at:

https://p2p.systems

contact@p2p.systems