

Decentralized Society and Bitcoin Contracts

Who we are

- Professional Lawyer and IT security guy
- Volunteers and freedom lovers
- Bitcoin enthusiasts



Centralized vs. decentralized law



Decentralized Internet

Decentralized Internet is a network of computers that are connected to each other in a way that no single point of control exists. This means that no single entity can control the network, and all participants have an equal say in how the network operates.



Decentralized currency

Decentralized currency is a type of digital currency that is not controlled by any central authority. It is created and managed by a network of participants, and it can be used to purchase goods and services. Decentralized currencies are often based on blockchain technology, which allows for secure and transparent transactions.

Contents

- Decentralized Legal system
- Decentralized Internet
- Decentralized Currency
- Decentralized Contracts
- Trade in decentralized world
- Decentralized future?

Decentralized Society and Bitcoin Contracts

Who we are

- Professional Lawyer and IT security guy
- Volunteers and freedom lovers
- Bitcoin enthusiasts



Centralized vs. decentralized law



Decentralized Internet

Decentralized Internet is a network of computers that are connected to each other in a way that no single point of control exists. This means that no single entity can control the network, and all participants have an equal say in the network's operation.



Decentralized currency

Decentralized currency is a type of digital currency that is not controlled by any central authority. It is created and distributed through a process called mining, which involves solving complex mathematical problems. Decentralized currencies like Bitcoin are designed to be secure, transparent, and resistant to censorship.

Contents

- Decentralized Legal system
- Decentralized Internet
- Decentralized Currency
- Decentralized Contracts
- Trade in decentralized world
- Decentralized future?

Who we are

- Professional lawyer and IT security guy
- Voluntaryists and freedom lovers
- Bitcoin enthusiasts



Welcome to the era of the central control - government crisis

**Law is not evil! =
it saves us from chaos**

Problem is WHO should create law and WHAT
should be regulated?

WHO: Law is basically created by a small
group of people

WHAT: Regulation in order to help society
reduces number of free choices, often it means
more regulation = over-regulation

If something does not work/or it is against our
economic interests, more regulation is created.



- Our current society is too complex to control /
manage centrally
- Law as a normative system
- Governments are trying to regulate complexity
through generally binding rules (laws)
- Over-regulation limits economic freedom and
therefore innovations and kills competition
- The solution is to respect mutually agreed
decentralized relations and embrace all
technologies that make it possible!

Friedrich Hayek (The Road to Serfdom): "The
economy is too complicated for politicians to avert
recessions and unemployment without unintended
consequences that may well be worse."

Law is not evil ! = it saves us from chaos

Problem is WHO should create law and WHAT should be regulated?

WHO: Law is basically created by a small group of people

WHAT: Regulation in order to help society reduces number of free choices, often it means more regulation = over-regulation

If something does not work/or it is against our economic interests, more regulation is created.

• Consumer over-protection limits innovations and always increases price
• Employee protection limits employees' mobility to find another better job
• Marriage regulation prevents long term relationships
• If the state does not have money, it simply creates new taxes and new regulations

- **Consumer over-protection limits innovations and always increases price**
- **Employee protection limits employees inability to find another better job**
- **Marriage regulation prevents long term relationships**
- **If the state does not have money, it simply creates new taxes and new regulations**


The state as a monopoly for economic regulations and laws

- Law is misused as a monopoly tool to achieve specific economic interests
- Law regulates situations where other normative systems would work more effectively
- This may result in corporatism



The state as a monopoly for economic regulations and laws

- Law is misused as a monopoly tool to achieve specific economic interests
- Law regulates situations where other normative systems would work more effectively
- This may result in corporativism

The background of the image is a deep space scene featuring a large, bright, yellowish-white nebula or galaxy on the right side, with various smaller stars and distant galaxies visible against a dark, star-filled sky. A large, thick white circle is superimposed over the center of the image, framing the text.

Friedrich Hayek (The Road to Serfdom): "The economy is too complicated for politicians to avert recessions and unemployment without unintended consequences that may well be worse."

Contents

- **Decentralized Legal system**
- **Decentralized Internet**
- **Decentralized Currency**
- **Decentralized Contracts**
- **Decentralized Registers**
- **Trade in decentralized world**
- **Decentralized future?!**

Centralized vs. decentralized law

Government's legal systems

Current legal systems problems

- No risk of reputation loss
- No risk of bankruptcy
- Funding is involuntary and enforced by coercion
- No terrestrial competition
- Laws are enforced by majority against minority

Decentralized freemarket legal systems

Legal protection in the decentralized society

- People vs Legal agencies vs. Courts
- Completely based on mutual contracts and legal agency / court reputation

People vs. Legal agencies

- People prefer legal agencies with good reputation and history that protect their rights
- Any case of corruption / bribe can cause a significant loss of their reputation and possible bankruptcy

Being fair makes economic sense

- Fair legal decisions can be a powerful signal of reputation and history that protect their rights
- Any case of corruption / bribe can cause a significant loss of their reputation and possible bankruptcy

Legal agencies dispute process

- Legal agencies are motivated to solve most conflicts without lawsuits if it is possible, otherwise they have to pay court costs
- Legal agencies prefer courts with good reputation and history (because their direct customers also require fair decisions)
- They can decide on arbitrary number of courts, but this can be a very expensive and time-consuming process (and can lead to loss of reputation)

Decentralized courts

- The most critical business value of courts is its fairness, otherwise they can lose their reputation and all customers -> legal agencies that require fair decisions

What does the current industry use to solve disputes? Legal agency or private decentralized court?

There is much more likely in the current legal system which is the result of reputation loss and bankruptcy and no competition at all. Example: "Nadine's legal system in Sweden. Why did courts disappear, when you can buy cheap courts?"

Government's legal systems

Current legal systems problems

- No risk of reputation loss
- No risk of bankruptcy
- Funding is involuntary and enforced by coercion
- No terrestrial competition
- Laws are enforced by majority against minority

David Friedman: "Thinking less is not as easy as it seems. The government is not a good provider of justice, and it is not a good provider of law. Why do you expect it to do a good job of providing the legal system unless you are thinking to provide the law and the courts?"

Decentralized freemarket legal systems

Legal protection in the decentralized society

- People vs Legal agencies vs. Courts
- Completely based on mutual contracts and legal-agency / court reputation

People vs. Legal agencies

- People prefer legal agencies with good reputation and history that protects their rights
- Any case of corruption / bribe can cause a significant loss of their reputation and possible bankruptcy

Being fair makes economic sense

For legal agencies:

- have to protect rights of their customers otherwise they would lose them
- but also have to be able to cooperate with other legal agencies and accept decisions of chosen courts, otherwise they lose their reputation (and consequently customers)

For courts:

- they have to do fair decisions, otherwise they lose their customers (=legal agencies)

Legal agencies dispute process

- Legal agencies are motivated to solve most conflicts without courts if it is possible, otherwise they have to pay court costs
- Legal agencies prefer courts with good reputation and history (because their direct customers also require fair decisions)
- They can decide on arbitrary number of courts, but this can be a very expensive and time-consuming process (and can lead to loss of reputation)

Decentralized courts

- The most critical business value of courts is its fairness, otherwise they can lose their reputation and all customers -> legal agencies that require fair decisions

And what about now?
Every legal agency will have to be on
side of rules derived from legal history
"common-law" decisions.
Legal decisions will be a matter of up and
downside of both collected justice / trial
legal agencies

Wait! But in this system anybody can easily corrupt private legal agency or private decentralized court!

This is much more likely in the current legal system where is no risk of reputation loss and bankruptcy and no competition at all!
(example "Harabin's legal system in Slovakia: Why pay expensive lawyers, when you can buy cheap courts?")

Current legal systems problems

- No risk of reputation loss
- No risk of bankruptcy
- Funding is involuntary and enforced by coercion
- No terrestrial competition
- Laws are enforced by majority against minority

David Friedman: "Producing laws is not an easier problem than producing cars or food, so if the government's incompetent to produce cars or food, why do you expect it to do a good job producing the legal system within which you are then going to produce the cars and the food?"

st minority

David Friedman: "Producing laws is not an easier problem than producing cars or food, so if the government's incompetent to produce cars or food, why do you expect it to do a good job producing the legal system within which you are then going to produce the cars and the food?"

Legal protection in the decentralized society

- **People vs Legal agencies vs. Courts**
- **Completely based on mutual contracts and legal-agency / court reputation**

People vs. Legal agencies

- **People prefer legal agencies with good reputation and history that protects their rights**
- **Any case of corruption / bribe can cause a significant loss of their reputation and possible bankruptcy**

Legal agencies dispute process

- Legal agencies are motivated to solve most conflicts without courts if it is possible, otherwise they have to pay court costs
- Legal agencies prefer courts with good reputation and history (because their direct customers also require fair decisions)
- They can decide on arbitrary number of courts, but this can be a very expensive and time-consuming process (and can lead to loss of reputation)

• Any case of co
can cause a si
their reputati
bankruptcy

Decentralized courts

- The most critical business value of courts is its fairness, otherwise they can lose their reputation and all customers
-> legal agencies that require fair decisions

Being fair makes economic sense

For legal agencies:

- have to protect rights of their customers otherwise they would lose them
- but also have to be able to cooperate with other legal agencies and accept decisions of chosen courts, otherwise they lose their reputation (and consequently customers)

For courts:

- they have to do fair decisions, otherwise they lose their customers (=legal agencies)

Wait! But in this system anybody can easily corrupt private legal agency or private decentralized court!

This is much more likely in the current legal system where is no risk of reputation loss and bankruptcy and no competition at all!

(example "Harabin's legal system in Slovakia: Why pay expensive lawyers, when you can buy cheap courts?")

And what about laws?

- Every legal agency will have their own subset of rules derived from legal industry "best practice" standards
- Legal decision will be a mutually agreed compromise of both affected parties / their legal agencies

Decentralized Internet

- **FunkFeuer - wifi-based mesh decentralized network**
- **The Serval Mesh - mobile mesh decentralized network**
- **Anonymization networks (like I2P)**
- **IPv6 based decentralized network (cjdns)**
- **Decentralized DNS system (namecoin, ODDNS)**

Decentralized currency

- **Bitcoin is the first example of massively used decentralized currency**
- **But there are a lot of other alternatives**
Namecoin, Litecoin, Tonal Bitcoin, lxCoin, Devcoin, PPCoin, Freicoin, l0coin, Terracoin, Liquidcoin...
- **We are just at the beginning of a completely new decentralized bank system!**
- **Be prepared for more secure and better implementations!**

Bitcoin contracts

- Providing a deposit
- Escrow and dispute mediation
- Assurance contracts
- Using external state
- Trading accross chains
- Micropayments

Bitcoin as a fully decentralized register

- Estate Wadsworth can be used as a decontrolled ledger or any property (cars, houses, phones, ...)
- It can include references to / pointers to another established decontrolled database with a lot of data (e.g. children)
- Sale is done using two connected transactions:
 - the first one moves money from the buyer to seller, the second one moves the ownership from the seller to the buyer

Car trade in the decentralized world

Directions:

1. Car is produced at a newly formed assembly plant with depend of 5 cables (C1, C2, C3, C4, C5) in a sequence / parallel / random / sequential order.
2. The longer assembly and parallel / random / sequential to the order to be the valid / correct / wrong / false.
3. The car is made a single depend (C1) car is the valid / correct / wrong / false.
4. The car is made a parallel / random / sequential order, of which the car is the valid / correct / wrong / false.
5. The car is made a parallel / random / sequential order, of which the car is the valid / correct / wrong / false.
6. The car is made a parallel / random / sequential order, of which the car is the valid / correct / wrong / false.
7. The car is made a parallel / random / sequential order, of which the car is the valid / correct / wrong / false.
8. The car is made a parallel / random / sequential order, of which the car is the valid / correct / wrong / false.
9. The car is made a parallel / random / sequential order, of which the car is the valid / correct / wrong / false.
10. The car is made a parallel / random / sequential order, of which the car is the valid / correct / wrong / false.

Escrow and dispute mediation

- Bitcoin blockchain supports escrow, so it is not necessary to use 3rd-party web application (like Silk Road market)
- Escrow is voluntarily chosen by both parties
- No dispute: buyer and seller signs
- Dispute: buyer/mediator signs and the seller loses
- Dispute: seller/mediator signs and the seller wins
- Mediator can't steal or move money by themselves

Bitcoin contracts

- Providing a deposit
- Escrow and dispute mediation
- Assurance contracts
- Using external state
- Trading accross chains
- Micropayments

Bitcoin as a fully decentralized register

Bitcoin blockchain can be used as a decentralized register of any property: cars, houses, shares, ...
It can include information / pointers to further distributed decentralized databases with a lot of data (big databases)
Side is more using how connected to computers
Side is also more connected from the ledger to other side and makes the contract to have the order in the ledger

Car trade in the decentralized world

1. Car is represented with a number (unique identifier) in the ledger of the decentralized world
2. The car is sold by the seller to the buyer
3. The buyer pays the seller with a number (unique identifier) in the ledger of the decentralized world
4. The seller transfers the car to the buyer
5. The buyer transfers the car to the seller
6. The seller transfers the car to the buyer
7. The buyer transfers the car to the seller
8. The seller transfers the car to the buyer
9. The buyer transfers the car to the seller
10. The seller transfers the car to the buyer

Assurance contracts

- **Kickstarter style funding model where supporters pledge money that is only taken if enough pledges are gathered**
- **Can be combined with dispute mediation**
- **Suitable for provision of ANY public goods (e.g. building bridges, localization of web/tools, etc)**

Bitcoin contracts

- Providing a deposit
- Escrow and dispute mediation
- Assurance contracts
- Using external state
- Trading accross chains
- Micropayments

Bitcoin as a fully decentralized register

Bitcoin blockchain can be used as a decentralized register of any property: cars, houses, shares, ...
It can include information / pointers to further distributed decentralized databases with a lot of data (big databases)
Side is more using how connected to computers
Side is also more connected from the ledger to other side and makes the contract to have the order in the ledger

Car trade in the decentralized world

1. Car is represented with a number (unique identifier) in the ledger of the decentralized world (the ledger is a distributed database)
2. The car is sold (the seller is the owner of the car) and the car is represented with a number (unique identifier) in the ledger of the decentralized world (the ledger is a distributed database)
3. The car is sold (the seller is the owner of the car) and the car is represented with a number (unique identifier) in the ledger of the decentralized world (the ledger is a distributed database)
4. The car is sold (the seller is the owner of the car) and the car is represented with a number (unique identifier) in the ledger of the decentralized world (the ledger is a distributed database)
5. The car is sold (the seller is the owner of the car) and the car is represented with a number (unique identifier) in the ledger of the decentralized world (the ledger is a distributed database)
6. The car is sold (the seller is the owner of the car) and the car is represented with a number (unique identifier) in the ledger of the decentralized world (the ledger is a distributed database)
7. The car is sold (the seller is the owner of the car) and the car is represented with a number (unique identifier) in the ledger of the decentralized world (the ledger is a distributed database)
8. The car is sold (the seller is the owner of the car) and the car is represented with a number (unique identifier) in the ledger of the decentralized world (the ledger is a distributed database)
9. The car is sold (the seller is the owner of the car) and the car is represented with a number (unique identifier) in the ledger of the decentralized world (the ledger is a distributed database)
10. The car is sold (the seller is the owner of the car) and the car is represented with a number (unique identifier) in the ledger of the decentralized world (the ledger is a distributed database)

External agents

- **"Oracles" to lock money - a special program to run external agents (programs) and then sign or not sign**
- **Suitable for bets, heritage agreements, some insurance against loss of business due to your website getting hacked -> special conditions have to be met to release money**

Bitcoin contracts

- Providing a deposit
- Escrow and dispute mediation
- Assurance contracts
- Using external state
- Trading accross chains
- Micropayments

Bitcoin as a fully decentralized register

Bitcoin blockchain can be used as a decentralized register of any property: cars, houses, shares, ...
It can include information / pointers to further distributed decentralized databases with a lot of data (big databases)
Side is more using how connected to neighbors
Side also means transfers from the ledger to other side and means the transfer is from the ledger to the ledger

Car trade in the decentralized world

1. Car is represented with a number (unique identifier) in the ledger of the decentralized world (the ledger is a distributed database)
2. The car is sold (the seller is the owner of the car)
3. The buyer is looking for a car (the buyer is the owner of the car)
4. The car is sold (the seller is the owner of the car)
5. The car is sold (the seller is the owner of the car)
6. The car is sold (the seller is the owner of the car)
7. The car is sold (the seller is the owner of the car)
8. The car is sold (the seller is the owner of the car)
9. The car is sold (the seller is the owner of the car)
10. The car is sold (the seller is the owner of the car)

Bitcoin as a framework for multiple, independent currencies

- "Coloured satoshi" - multiple currency issuers with their reputations, history and reserves (e.g. backed up currency)
- Bitcoin is used as a transaction medium, suitable for regional / local currencies
- Implementation of the free banking system (people can freely and voluntarily choose what currency is the best one for them)

Bitcoin contracts

- Providing a deposit
- Escrow and dispute mediation
- Assurance contracts
- Using external state
- Trading accross chains
- Micropayments

Bitcoin as a fully decentralized register

- Estate Wadsworth can be used as a decontrolled ledger or any property (cars, houses, phones, ...)
- It can include references to / pointers to another established decontrolled database with a lot of data (e.g. children)
- Sale is done using two connected transactions:
 - the first one moves money from the buyer to seller, the second one moves the ownership from the seller to the buyer

Car trade in the decentralized world

Directions:

1. Car is produced at a newly formed company with the depend of 5 cables (Cable 1, Cable 2, Cable 3, Cable 4, Cable 5).
2. The larger quantity and greater number member to the order is the better the value of the order.
3. The car is made a single depend (cable 1) and 5 cables (Cable 2, Cable 3, Cable 4, Cable 5).
4. The first cable is the number of the cable, the cable value, of the order, the cable is the value of the cable order.
5. The larger quantity and greater number member to the order is the better the value of the order.
6. The first cable is the number of the cable, the cable value, of the order, the cable is the value of the cable order.
7. The larger quantity and greater number member to the order is the better the value of the order.
8. The first cable is the number of the cable, the cable value, of the order, the cable is the value of the cable order.
9. The larger quantity and greater number member to the order is the better the value of the order.
10. The first cable is the number of the cable, the cable value, of the order, the cable is the value of the cable order.

Micropayments using bitcoin micropayment channel

- Bitcoin transactions are cheap, but not free
- Bitcoin transactions are relatively slow
- Using micropayments it can be possible to pay e.g. for wifi access

Bitcoin as a fully decentralized register

- Bitcoin blockchain can be used as a decentralized register of any property (cars, houses, phones, ..)
- It can include references / pointers to another distributed decentralized databases with a lot of data (e.g. cadaster)
- Sale is done using two connected transactions - the first one moves money from the buyer to seller, the second one moves the ownership from the seller to the buyer

Car trade in the decentralized world

1. Car is produced with a newly created ownership key with deposit of T coins (e.g. 0.00001 BTC) - car computer / special immobilizer requires authentication using this ownership key
2. The buyer generates and sends a random number to the seller to obtain the valid car data
3. The car returns a digitally signed structure (by car's private key) that contains this random number, the cars public cert, all technical data, the public key of the current owner / ownership, so the buyer can verify properly what he wants to buy and if the seller really owns this car
4. The buyer creates a transaction with two inputs and two outputs. The first input signs for P coins (car price), the second input is connected to the output holding T coins for the ownership address. The first output sends P coins (car price) to the seller address and the second output sends T coins (ownership) to the buyer. This partially valid transaction is passed to the seller who signs the second input with the car's current ownership key and broadcasts this transaction
5. They wait for some confirmations, after that the car recognizes the new owner/ownership

**We already have
technologies to achieve fully
decentralized society.**

Decentralization can ...

- **cope with complex relations in our society much better**
- **be immune against misuse of the central control (SPOF)**
- **be economically effective**
- **means a bright future!**

References & credits

Decentralized law - David Friedman, Hans Hermann Hoppe, Stephen Kinsella

Bitcoin/contracts - Mike Hearn, Nick Szabo, Alexander Tabarok

Bitcoin friends & inspiration - Juraj Bednár, Marek Palatinus, Pavol Ruskák, Alex Howard, Frank Braun, Amir Taaki, Peter Šurda, Mike Gogulski and many others

The background of the slide is a cosmic scene featuring a nebula with warm orange and yellow hues. A large, semi-transparent rainbow arc is superimposed over the image, spanning from the left edge to the right. The text is centered and rendered in a bold, white, sans-serif font.

**We already have
technologies to achieve fully
decentralized society.**

Decentralization can ...

- cope with complex relations in our societies
much better**

We already have technologies to achieve fully decentralized society.

Decentralization can ...

- cope with complex relations in our society much better**
- be immune against misuse of the central control (SPOF)**
- be economically effective**
- means a bright future!**

References & credits

Decentralized law - David Friedman, Hans Hermann Hoppe, Stephen Kinsella

Bitcoin/contracts - Mike Hearn, Nick Szabó, Alexander Tabarrok

Bitcoin friends & inspiration - Juraj Bednár, Marek Palatinus, Pavol Rusnák, Alex Howard, Frank Braun, Amír Taaki, Peter

References & credits

Decentralized law - David Friedman, Hans Hermann Hoppe, Stephen Kinsella

Bitcoin/contracts - Mike Hearn, Nick Szabó, Alexander Tabarrok

Bitcoin friends & inspiration - Juraj Bednár, Marek Palatinus, Pavol Rusnák, Alex Howard, Frank Braun, Amir Taaki, Peter Šurda, Mike Gogulski and many others