

# Normes et monnaies virtuelles

Jonathan Unikowski

# Le droit est omniprésent dans le fonctionnement de la monnaie

Bitcoin est un exemple de monnaie qui fonctionne sans recours au droit Première partie: "Le droit est omniprésent dans le fonctionnement de la monnaie"











# Rareté et norme étatique







Or le droit fonctionne par emprise, aussi, il est inefficace pour réguler des réseaux non-centralisés



Deuxième partie: Bitcoin est un exemple de monnaie qui fonctionne sans recours au droit Paul Baran, "On Distributed Communications"



#### **Bitcoin: A Peer-to-Peer Electronic Cash System**

Satoshi Nakamoto satoshin@gmx.com www.bitcoin.org

Abstract. 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. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

#### 1. Introduction

Commerce on the Internet has come to rely almost exclusively on financial institutions serving as trusted third parties to process electronic payments. While the system works well enough for most transactions, it still suffers from the inherent weaknesses of the trust based model. Completely non-reversible transactions are not really possible, since financial institutions cannot avoid mediating disputes. The cost of mediation increases transaction costs, limiting the minimum practical transaction size and cutting off the possibility for small casual transactions, and there is a broader cost in the loss of ability to make non-reversible payments for non-reversible services. With the possibility of reversal, the need for trust spreads. Merchants must be wary of their customers, hassling them for more information than they would otherwise need. A certain percentage of fraud is accepted as unavoidable. These costs and payment uncertainties can be avoided in person by using physical currency, but no mechanism exists to make payments over a communications channel without a trusted party.

#### **Bitcoin: A Peer-to-Peer Electronic Cash System**

Satoshi Nakamoto satoshin@gmx.com www.bitcoin.org

**Abstract.** 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. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

#### 1. Introduction

Commerce on the Internet has come to rely almost exclusively on financial institutions serving as trusted third parties to process electronic payments. While the system works well enough for most transactions, it still suffers from the inherent weaknesses of the trust based model. Completely non-reversible transactions are not really possible, since financial institutions cannot avoid mediating disputes. The cost of mediation increases transaction costs, limiting the minimum practical transaction size and cutting off the possibility for small casual transactions, and there is a broader cost in the loss of ability to make non-reversible payments for non-reversible services. With the possibility of reversal, the need for trust spreads. Merchants must be wary of their customers, hassling them for more information than they would otherwise need. A certain percentage of fraud is accepted as unavoidable. These costs and payment uncertainties can be avoided in person by using physical currency, but no mechanism exists to make payments over a communications channel without a trusted party.

Comptes	
Henri	100
Paul	100
Pierre	100
Jean	100
Patrick	100
Benoît	100
Andrée	100
Xavier	100

Transaction	
Henri	-50
Paul	+50
Transaction	
Pierre	-10
Jean	+10
Transaction	
Patrick	-20
Benoît	+20

Comptes	
Henri	50
Paul	150
Pierre	90
Jean	110
Patrick	80
Benoît	120
Andrée	100
Xavier	100

Comptes	
Henri	100
Paul	100
Pierre	100
Jean	100
Patrick	100
Benoît	100
Andrée	100
Xavier	100

Transaction	
Henri	-50
Paul	+50
	_
Transaction	
Henri	-100
Jean	+100
Transaction	
Patrick	-20
Benoît	+20

Comptes	
Henri	???
Paul	???
Pierre	90
Jean	???
Patrick	80
Benoît	120
Andrée	100
Xavier	100

Un livre de compte décentralisé : la "blockchain"



## perelman

e5866ac795cde261edfa3d545f737398

### perelmanc

8c7f940c5f79815234d112697b81879e

## perelmanw

4ceacd732cd23d3c9b18dcb66f43083f

temps de calcul ~1 seconde

204 LIVRE I<sup>er</sup>. — INTRODUCTION. THÉORIE DES DROITS ET DES LOIS.

En d'autres mots, une loi désuète, sous peine de manquer son but, doit être rajeunie par celui qui est appelé à l'appliquer. Elle doit être *adaptée* aux idées, aux mœurs, aux conceptions nouvelles. C'est la seule manière d'en tirer encore quelque utilité. Ce système, qui aboutit à détacher la loi de la pensée de ceux qui l'ont faite et à lui donner une valeur propre *en fonction du temps et du milieu*, est, en période d'évolution sociale accélérée, le seul admissible.

3° Le règne de la justice est la seule raison d'être du droit et des lois. Il s'ensuit qu'une loi ne doit pas être interprétée pour elle-même, ni en elle-même, mais en fonction de l'idée de justice qui est à la base d'une civilisation donnée. Conséquemment, quand une disposition légale est susceptible d'être comprise comme décidant ce que la saine raison et le sentiment naturel du juste commandent de décider, elle doit être interprétée en ce sens (1).

Il s'ensuit que si le juge ne peut pas modifier une loi sous prétexte d'équité, il a cependant le devoir de s'inspirer de celle-ci quand les textes légaux prètent à des interprétations diverses (2).

4º Les lois qui dérogent aux principes supérieurs du juste, ou à l'exercice des droits naturels de l'homme doivent être interprétées restrictivement.

C'est l'application d'une vieille maxime : odiosa sunt restringenda. Si la distinction entre lois odieuses et lois favorables n'est actuellement plus fondée (3), l'idée n'en subsiste pas moins. C'est en fonction de cette idée qu'il a toujours été admis que le droit pénal ne pouvait être d'interprétation extensive ou analogique. Il en est de même des lois qui comminent des pénalités civiles, ou des déchéances. Le même principe s'applique lorsqu'une loi est déclarée rétroactive, et plus généralement pour toutes les lois dérogatoires au droit commun.

216. Considérations finales. — Les pouvoirs d'interprétation reconnus aux tribunaux, même compris dans l'esprit large et libéral qui est propre à notre époque, fonctionnent, en période normale, à la plus grande satisfaction de tous. Depuis la loi du 7 juillet 1865, c'est la Cour de cassation qui décide souverainement de la portée d'une loi. Les lois interprétatives sont, nous l'avons souligné, extrêmement rares de nos jours, et le Parlement est visiblement fort aise, dans des questions qui se révèlent toujours délicates, de céder la parole à des juristes spécialisés. Il est manifeste que de nos jours, on obtiendrait beaucoup moins facilement une rectification des lois par voie législative qu'il y a cent ans. Mais il faut reconna<u>ttra</u> aussi qu'en période

(2) Civ. Gand, 18 mars 1903, P. P., 1903, 1254.

#### 30 millions de signes

#### 17469a5e577aab94e4be249f9be5cd2a

#### 32 signes

<sup>(1)</sup> Concl. du ministère public sous cass., 15 mai 1930, Pas., 1930, I, 223. Voyez également cass., 23 juin 1932, Pas., 1932, I, 200, décision dont le sommaire publié par la Pasicrisie parle d' « interprétation anti-sociale ». Nous ne pouvons toutefois signaler ces deux décisions que comme tendance de la science juridique contemporaine, car ces deux points ne résultent pas des arrêts de la Cour de cassation, mais de la discussion qu'à leur occasion le Procureur général près cette Cour a instituée.

<sup>(3)</sup> DALLOZ, Rép. prat., vº Lois et décrets, nº 564.

204 LIVRE I<sup>er</sup>. — INTRODUCTION. THÉORIE DES DROITS ET DES LOIS.

En d'autres mots, une loi désuète, sous peine de manquer son but, doit être rajeunie par celui qui est appelé à l'appliquer. Elle doit être *adaptée* aux idées, aux mœurs, aux conceptions nouvelles. C'est la seule manière d'en tirer encore quelque utilité. Ce système, qui aboutit à détacher la loi de la pensée de ceux qui l'ont faite et à lui donner une valeur propre *en fonction du temps et du milieu*, est, en période d'évolution sociale accélérée, le seul admissible.

3° Le règne de la justice est la seule raison d'être du droit et des lois. Il s'ensuit qu'une loi ne doit pas être interprétée pour elle-même, ni en elle-même, mais en fonction de l'idée de justice qui est à la base d'une civilisation donnée. Conséquemment, quand une disposition légale est susceptible d'être comprise comme décidant ce que la *saine raison* et le *sentiment naturel du juste* commandent de décider, elle doit être interprétée en ce sens (1).

Il s'ensuit que si le juge ne peut pas modifier une loi sous prétexte d'équité, il a cependant le devoir de s'inspirer de celle-ci quand les textes légaux prètent à des interprétations diverses (2).

4º Les lois qui dérogent aux principes supérieurs du juste, ou à l'exercice des droits naturels de l'homme doivent être interprétées restrictivement.

C'est l'application d'une vieille maxime : odiosa sunt restringenda. Si la distinction entre lois odieuses et lois favorables n'est actuellement plus fondée (3), l'idée n'en subsiste pas moins. C'est en fonction de cette idée qu'il a toujours été admis que le droit pénal ne pouvait être d'interprétation extensive ou analogique. Il en est de même des lois qui comminent des pénalités civiles, ou des déchéances. Le même principe s'applique lorsqu'une loi est déclarée rétroactive, et plus généralement pour toutes les lois dérogatoires au droit commun.

#### a18e4cba1a3b3d42f1aa17a44b8d7356



#### 30 millions de signes

<sup>(1)</sup> Concl. du ministère public sous cass., 15 mai 1930, Pas., 1930, I, 223. Voyez également cass., 23 juin 1932, Pas., 1932, I, 200, décision dont le sommaire publié par la Pasicrisie parle d' « interprétation anti-sociale ». Nous ne pouvons toutefois signaler ces deux décisions que comme tendance de la science juridique contemporaine, car ces deux points ne résultent pas des arrêts de la Cour de cassation, mais de la discussion qu'à leur occasion le Procureur général près cette Cour a instituée.

<sup>(2)</sup> Civ. Gand, 18 mars 1903, P. P., 1903, 1254.

<sup>(3)</sup> DALLOZ, Rép. prat., vº Lois et décrets, nº 564.

### perelmanw

4ceacd732cd23d3c9b18dcb66f43083f

# perelman

@a3ceb71903bdfad654c8bf65003cb07

## perelmanne

00aff4fa0c83b182ede6025736cd78dd

temps de calcul ~1 seconde

### perelmanazmwoibm

### 00000000563959b79721c3f72f2f566

temps de calcul: 12 heures

### Bloc #1



### 3719a5607239c28de62ce2fb5be91cbe

temps de calcul ~1 seconde

### Bloc #1



### 00000000001e7df4efavd5cf9b57cb8

temps de calcul ~15 minutes

Un livre de compte décentralisé : la "blockchain"



### Bloc #1



### 00000000001e7df4efavd5cf9b57cb8

Bloc #2



temps de calcul ~15 minutes





temps de calcul ~45 minutes

Novembre 2013 – Novembre 2015

# ~500 exaFLOPS

(= 500 milliards de milliards de calculs par seconde)



### Valeur: 400 euros

### Nombre en activité: 404.268 unités Coût: 161 millions d'euros (+ frais opérationnels)

### Bloc





# Quels enseignements pour le juriste?

Le code comme norme

Décentralisation et automatisme

Applications



# Normes et monnaies virtuelles

Jonathan Unikowski