



PROFESSEURS:

Didier DONSEZ

Georges-Pierre BONNEAU

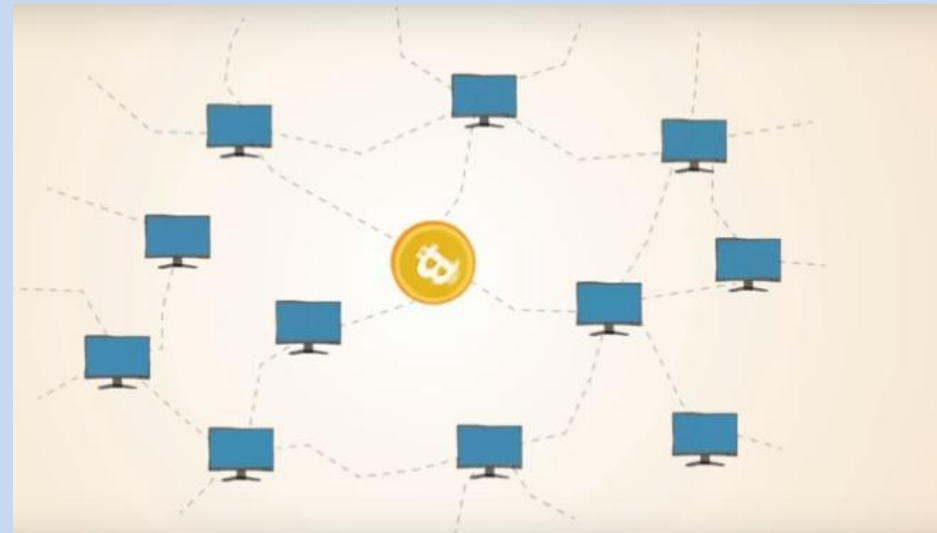
ÉTUDIANT: Longfei YAO

Sommaire

- Introduction
- Utilisation
- Principe
- Conclusion
- Démonstration

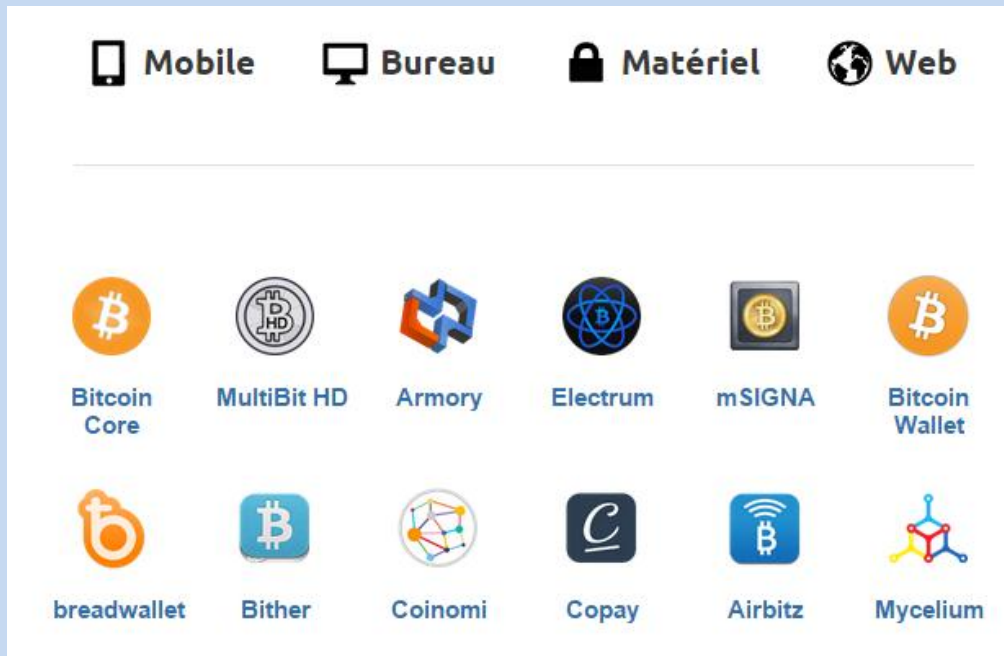
Introduction

- Première monnaie électronique décentralisé
- Se transmette de particulier à particulier à travers le réseau sans passer par les banques (P2P)
- Créé par **Satoshi Nakamoto**(?)




Utilisation

- Choisir une portefeuille



Utilisation

- Obtenir des bitcoins

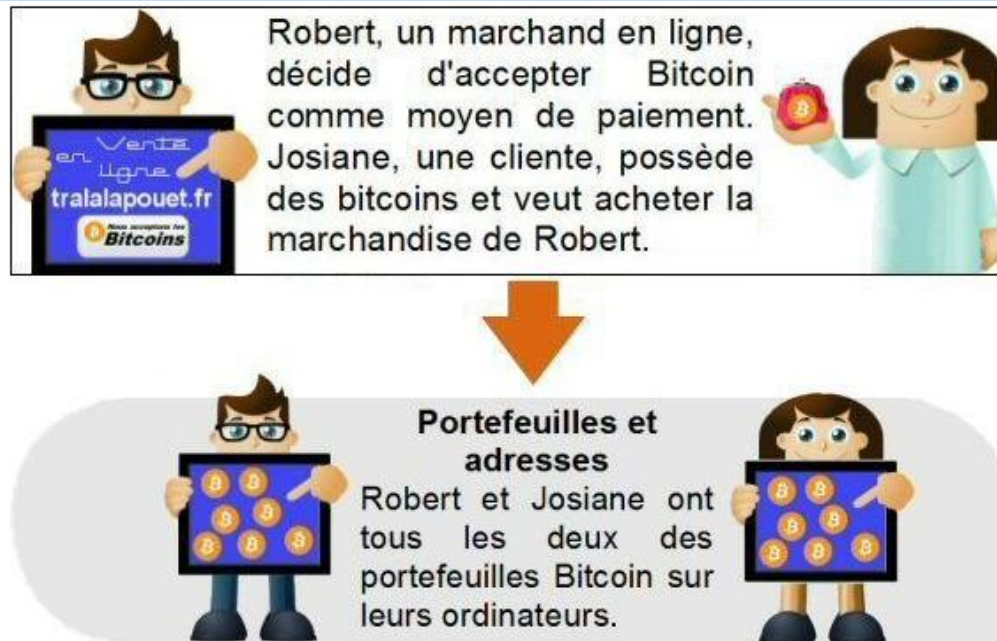
 How To Buy Bitcoins Twitter Facebook LinkedIn




ALL ARS AUD BGN BRL CAD CHF CLP CNY CZK DKK EUR GBP HKD HRK HUF IDR ILS INR JPY KES MXN
MYR NOK NGN NZD PHP PKR PLN RUR RSD SEK SGD THB TRY UAH USD VEF ZAR

Exchange	BID	ASK	Change	Unit
coinbase	331.39	331.40	0.00%	USD
QUOIN	41,198.55	41,258.72	0.00%	JPY
BTCChina	2,110.01	2,111.22	-0.14%	CNY
kraken	308.00	308.48	0.00%	EUR
BITFINEX	331.01	331.03	0.00%	USD
BITSTAMP	329.17	329.56	0.45%	USD
BTC e	329.59	329.88	-0.09%	USD
ANXBTC	329.68	332.99	-2.33%	USD
Bitcurex	326.89	504.60	0.00%	USD
ice³x	5,200.00	5,280.00	0.00%	ZAR
itBit	330.37	330.92	0.00%	USD
btcmarkets	465.26	469.89	0.00%	AUD

Utilisation

- Dépenser des bitcoins



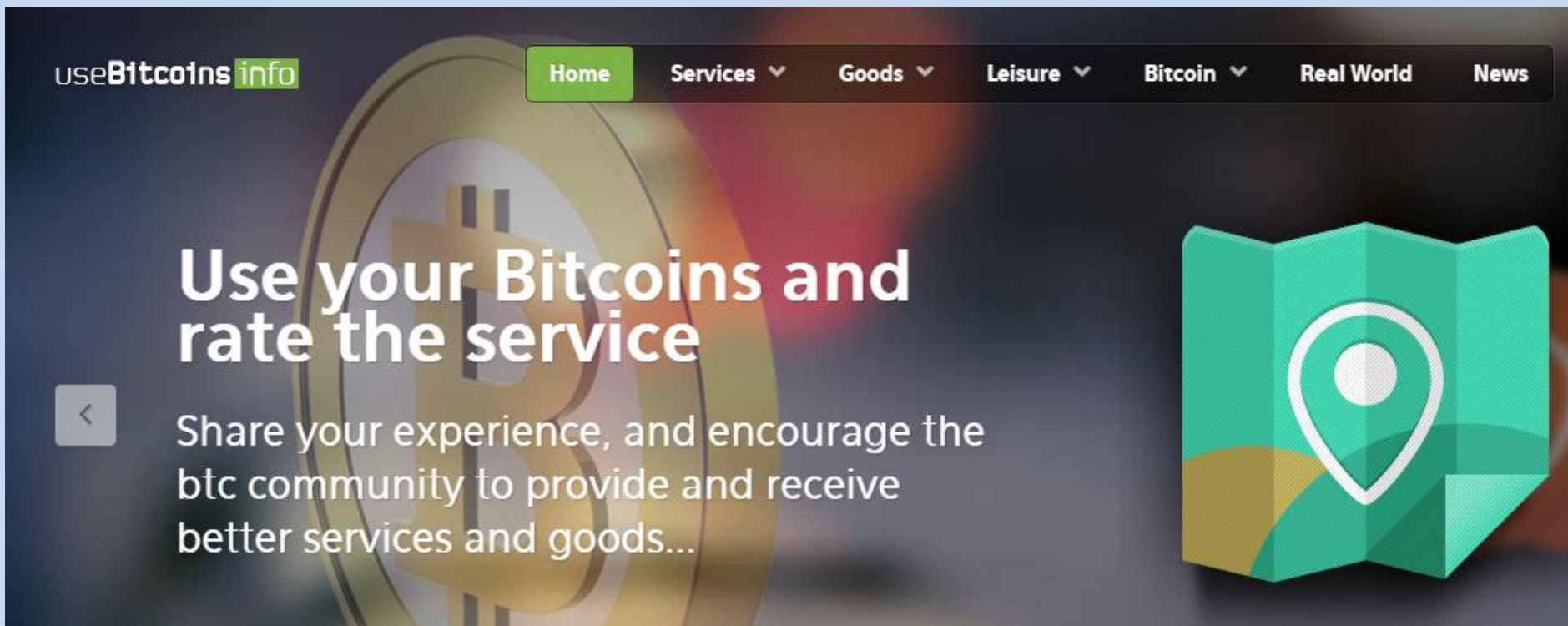
Pay To:   

Label:

Amount: Subtract fee from amount

Utilisation

- Dépenser des bitcoins




The screenshot shows the top section of the useBitcoins.info website. The header is dark with a navigation menu containing: Home (highlighted in green), Services (with a dropdown arrow), Goods (with a dropdown arrow), Leisure (with a dropdown arrow), Bitcoin (with a dropdown arrow), Real World, and News. The main content area features a large, semi-transparent Bitcoin coin graphic on the left. To its right, the text reads: "Use your Bitcoins and rate the service". Below this, a smaller text block says: "Share your experience, and encourage the btc community to provide and receive better services and goods...". On the far left of this text block is a small grey button with a left-pointing arrow. On the right side of the main content area is a 3D-style teal and yellow map icon with a white location pin.

useBitcoins info

Home Services ▾ Goods ▾ Leisure ▾ Bitcoin ▾ Real World News

Use your Bitcoins and rate the service

Share your experience, and encourage the btc community to provide and receive better services and goods...



Principe

- Bitcoin Address

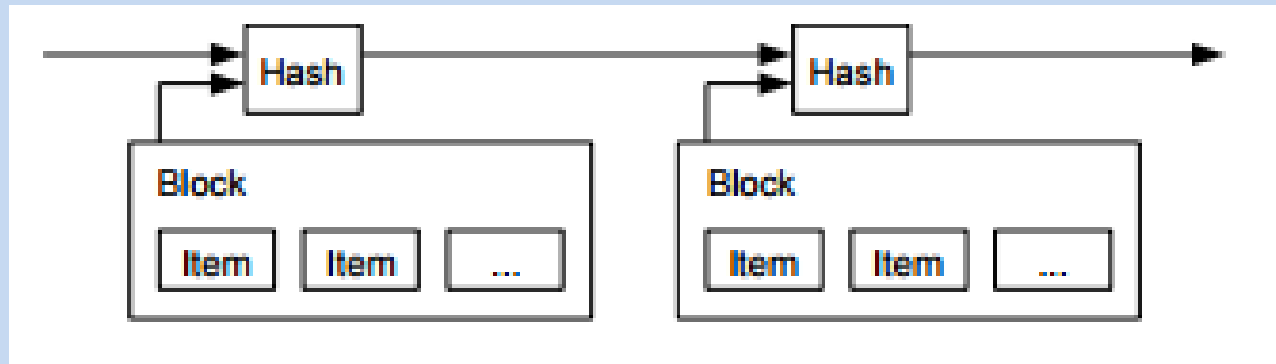
Clé privée et clé publique



Principe

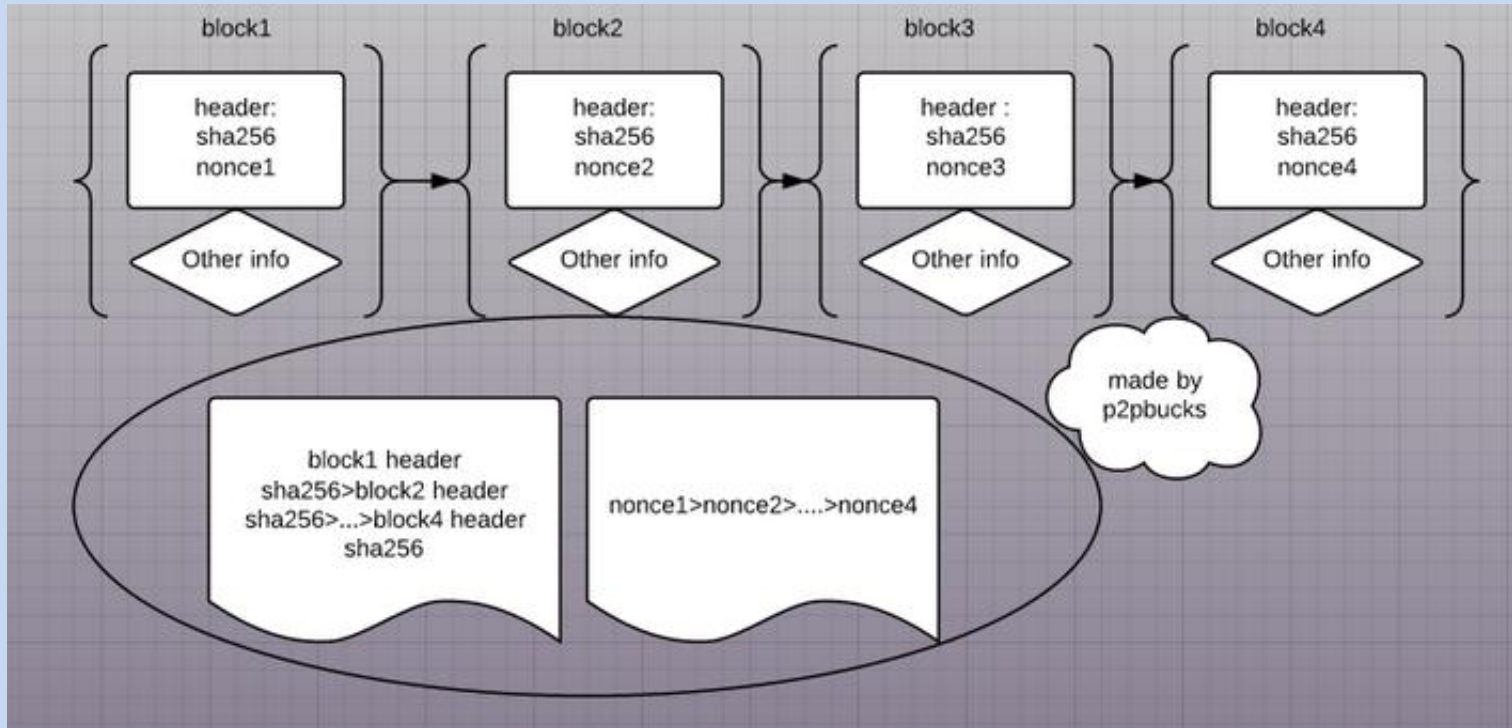
- Le format d'une transaction
 1. FROM(Vous)
Previous tx(L'identité de la transaction avant)
scriptSig(Votre clé privée)
 2. TO(bénéficiaire)
Value(Combien)
scriptPubKey(Clé publique de bénéficiaire)

Principe



- Chaque transaction ajoute un horodatage
- Les données d'une transaction sont mises dans un bloc
- Fonction de hachage($\text{Bloc}_2, \text{L'empreinte de bloc}_1$)
=> L'empreinte de bloc2
- Le premier bloc est créé par Satoshi Nakamoto

Principe



- SHA: Secure Hash Algorithm
- Calculer un sha256 qui est le plus petit dans la chaine => Créer un bloc
- Ajouter un nonce dans chaque bloc

Principe

Les transactions sur le réseau

- Toutes les transactions sont publique au réseau
- Chaque noeud recueille de nouvelles transactions dans un bloc
- Chaque noeud essayer de trouver un difficile preuve de travail pour son bloc
- Quand un nœud trouve une preuve de travail, il diffuse le bloc à tous les nœuds
- Tous les nœuds acceptent le bloc seulement si toutes les transactions en sont valides et non déjà passé
- Tous les nœuds expriment leur acceptation du bloc en travaillant sur la création du bloc suivant dans la chaîne, en utilisant le hachage du bloc accepté comme le hachage précédente

Conclusion

- De plus en plus adopté
- Ne dépendre pas des banques centrales
- Utilisé dans le monde entier
- Pas d'inflation
- Anonyme
- Risque de logiciel

Merci pour votre attention!

Des questions?