Nouveautés en cryptofinance

Segwit et le réseau Éclair (« Lightning Network »)

Cyril Grunspan
ESILV
de Vinci Finance Group
cyril.grunspan@devinci.fr

ESILV LÉONARD DE VINCI | ÉCOLE D'INGÉNIEURS PARIS-LA DÉFENSE

Au commencement était la loi fiscale…

- Roi d’Uruk Sin Kasid (-XIXe siècle)

« Un shekel d'argent vaut autant que :

- trois mesures d'orge,
- douze mines de laine,
- dix mines de cuivre
- et trois mesures d'huile de sésame »

- Unité de poids…

Crésus touche le pactole !

- Sardes, Lydie, -VIe siècle avant JC
- Temple d'Artémis, Ephèse
- 60% or, 40% argent
- Première manipulation de l'état !
- Napoléons

2008: année 0 de la « cryptofinance »

From: Satoshi Nakamoto <satoshi <at> vistomail.com>
Subject: Bitcoin P2P e-cash paper
Newsgroups: gmane.comp.encryption.general
Date: 2008-10-31 18:10:00 GMT

I've been working on a new electronic cash system that's fully peer-to-peer, with no trusted third party.

The paper is available at:

http://www.bitcoin.org/bitcoin.pdf

De multiples changements depuis 2008

- Version actuelle 0.12
- Bitcoin Core
- 152 BIP (Bitcoin Improvement Proposal
- BIP 112 : OP_CHECKSEQUENCEVERIFY
- Mark Friedenbach (Blockstream)
- Eric Lombrozo (Ciphrex)
- « Btcdrak » ?
- P2SH

Segregated Witness

- Résolution problèmes de malléabilité
- Réécriture et simplification
- Vérifications plus rapides
- Sécurité renforcée des MULTISIG
- Augmentation de la taille des blocs
- Désengorger la base des UTXO
- BIP 112, 143
- Ouvre la voie au réseau éclair !

Qu’est-ce qu’un « fork » ?

Nouvelles fonctionnalités apportées au protocole

- « Hard Fork » : les blocs minés par les « nouveaux » mineurs sont invalides pour les « anciens » (août 2010, mars 2013, version 0.8.1…)
- --> divergence de la blockchain
- « Soft fork » : les blocs minés par les « anciens » mineurs sont invalides pour les « nouveaux »
- Las de miner en vain, les « anciens » abandonnent…
- Mode P2SH (Pay to Script Hash), « soft fork », 2013
- BIP 66, juillet 2015, « soft fork »

Les Scripts du Bitcoin

- On ne « possède » pas réellement de l'argent !
- Argent utilisable associé à un problème de maths
- Script libérateur **scriptSig**
- Script bloquant **scriptPubKey**
- Langage Bitcoin = langage de pile très sommaire
- Non Turing-complet
- **scriptSig** + **scriptPubKey** → True ?

Les Scripts du Bitcoin (suite)

- Exemple **scriptSig :**

<Signature d'Alice>
<Adresse Publique d'Alice>

scriptPubKey rédigé par Eve :
OP_DUB
OP_HASH160
<Adresse_Publique_Alice>
OP_EQUALVERIFY
OP_CHECKSIG

Réseau Éclair (« Lightning Network »)

Exemple de canal de paiement à sens unique

Transaction initiale d'Alice **TX0** (10 BTC) déblocable si :

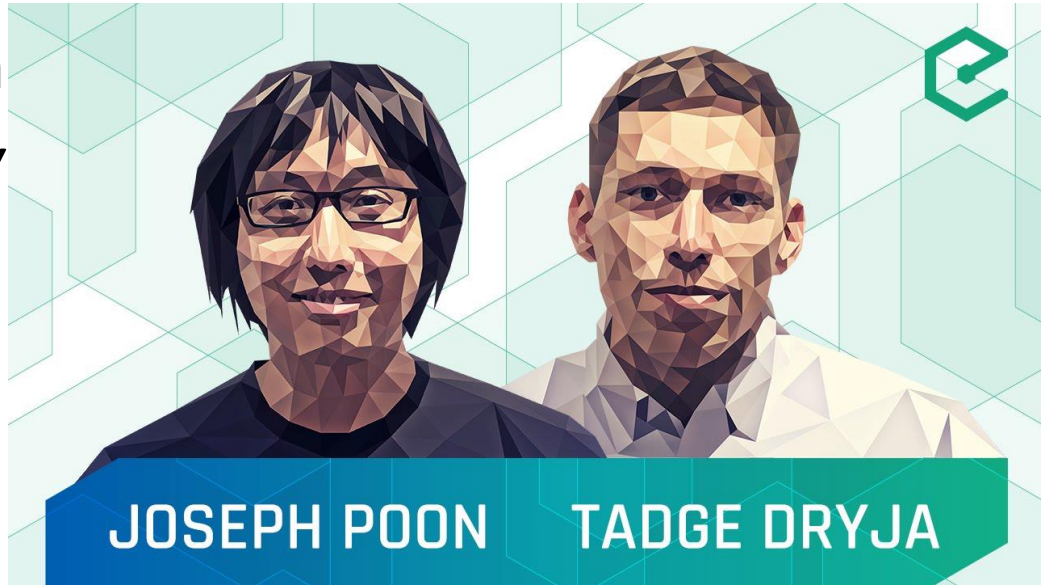
- Signatures d'Alice et de Bob réunies ensemble
- Ou signature d'Alice seule (mais après un certain délai)
- Propositions de transactions dans les mains de Bob
- 9,99 BTC pour Alice & 0,01 BTC pour Bob
- 9,98 BTC pour Alice & 0,02 BTC pour Bob
- Etc…

Réseau Éclair (suite)

- **Achat d'un secret ?**
- Trouver x tel que f(x) = 0 ? Bob, fort en maths…
- Tiers de confiance ou **UTX0** crée par Alice déblocable si **scriptSig** avec
- Signature de Bob et x tel que f(x)=0
- Ou signature d'Alice (mais après un certain délai)

Réseau Éclair (suite)

- Suite de canaux de paiements bidirectionnels
- Transactions totalement hors blockch
- OP code OP_CHECKSEQUENCEVERIFY
- Nœuds avec liquidité
- Problème de routage
- Résolution de tous les problèmes ?



Exemple canal de paiement bi-directionnel

- **UTXO** originale (fonds : 5BTC d'Alice & 5BTC de Bob) déblocable si 2x2 MULTISIG
- Rédactions de deux propositions de scripts (miroir)
- PTX1 : **UTXO** signée par Alice et versement de 6BTC à Alice + 4BTC à Bob (si attente de 500 blocs) ou Alice (si connaît secret S1 connu seul de Bob)
- PTX'1 : **UTXO** signée par Bob et versement de 4BTC à Bob + 6BTC à Alice (si attente de 500 blocs) ou Bob (si connaît secret S'1 connu seul d'Alice)
- Nouvelle proposition : rédactions de PTX2 et PTX'2 (nouveaux secrets) + révélations des secrets précédents
- … PTX_n, PTX'_n… →Transactions off-chain !