Université Constantine 2
– Cours 5 et 6 –
Chapitre 3 : Technologie Blockchain et consensus distribués
Algorithmes distribués avancés (ALDA)
2018/2019. Semestre 1
Dr. BOUKHARROU R.
Faculté des nouvelles technologies
radja.boukharrou@univ-constantine2.dz

Université Constantine 2
Etudiants concernés
Faculté/Institut Département Niveau Spécialité
RSD Master 2 Nouvelles technologies IFA
2018/2019. Semestre 1
Dr. BOUKHARROU R.
Faculté des nouvelles technologies
radja.boukharrou@univ-constantine2.dz
Algorithmes distribués avancés (ALDA)
– Cours 5 et 6 –
Chapitre 3 : Technologie Blockchain et consensus distribués

Université Constantine 2 4 © Dr. Boukharrou R.
Blockchain
Bitcoin
Smart-contracts
Blockchain semi-publique et privée

Université Constantine 2 5
Blockchain
(Chaine de blocs)
© Dr. Boukharrou R.
Bitcoin

Université Constantine 2 6
Dans un contexte de crise économique (2008-2009), de scandales
financiers et monétaires, de perte de confiance en les institutions
bancaires,
Un groupe de hackers a crée une crypto-monnaie émise par un système peer-
to-peer et indépendant de tout système de contrôle centralisé
C’est ainsi que Satoshi Nakamato pose les principes fondateurs de Bitcoin en
2008, en publiant « Bitcoin: A Peer-to-Peer Electronic Cash System »
L’idée est devenue une réalité après le développement du logiciel open-source
du bitcoin en 2009
Contexte
© Dr. Boukharrou R.

Université Constantine 2 7
Problématique
Comment résoudre le problème cryptographique du double paiement (ou
problème des généraux Byzantins) ?
Comment deux utilisateurs peuvent s’échanger des biens (monnaies, …), sans
passer par un tiers de confiance ?
Comment garantir une monnaie sans autorité centrale ?
Solution : Naissance du Bitcoin
Bitcoin est une crypto-monnaie supportée par une technologie décentralisée
appelée la Blockchain (la chaine de blocs)
Echange peer-to-peer des transactions  Désintermédiation (Sans passer par des
banques)
Stockage des transactions dans un registre complet
Vérification décentralisée des transactions à tout moment
La blockchain est présentée comme une révolution impactant les mondes
industriel, économique et citoyen
Problématique
© Dr. Boukharrou R.
Consensus distribué et sécurisé

Université Constantine 2 8
Une technologie de stockage et de transmission d'informations sans organe de
contrôle
Les informations envoyées par les utilisateurs et les liens internes à la base
sont groupés en blocs et vérifiés à intervalles de temps réguliers
Les blocs sont sécurisés contre la falsification ou la modification par des
techniques cryptographiques,
Les blocs sont liés entre eux, formant une chaîne de blocs, qui est vue
comme une BD distribuée et sécurisé de toutes les transactions effectuées
depuis le démarrage du système réparti.
Blockchain (Chaine de bloc)
© Dr. Boukharrou R.
Bloc 49
Transaction 102
Transaction 103
Transaction 104
Transaction 105
Bloc 48
Transaction 99
Transaction 100
Transaction 101
Bloc 47
Transaction 96
Transaction 97
Transaction 98
Bloc 46
Transaction 92
Transaction 93
Transaction 94
Transaction 95

Université Constantine 2 9
La première étude sur les chaînes de blocs cryptographiquement sécurisées a
été décrite en 1991 (par Bayer, Haber et Stornetta)
Les documents horodatés ne pourraient pas être falsifiés ou antidatés
En 1992, ils ont incorporé le concept d'arbre de Merkle pour améliorer
l’efficacité du système
Plusieurs documents sont assemblés en un seul bloc
En 2008, la 1
ère
chaîne de blocs a été conceptualisée (par Satoshi Nakamoto)
La blockchain du Bitcoin a été implémentée (3 Janvier 2009 à 18h15 UTC) où
elle sert de registre publique à toutes les transactions sur le réseau
Le 1
er
bloc est appelé bloc de genèse. La 1
er
transaction bitcoin est une
transaction unique de paiement de 50 nouveaux bitcoins à son créateur
Actuellement (oct 2018), la Blockchain du Bitcoin enregistre 547 416 blocs avec
environ 150 blocs/jour comportant en moy. 1700 transactions chacun (Lien)
+1000 crypto-monnaies sur le marché : Litecoin (2011), Ethereum (2015),
Zcash (2016), Bitcoin Cash (2017), …
Blockchain
Historique
© Dr. Boukharrou R.

Université Constantine 2 10
Bitcoin est une crypto-monnaie dédié aux paiements électroniques peer-
to-peer, fonctionnelle depuis 2009
La Blockchain du Bitcoin permet de stocker des données des transactions
depuis la création du Bitcoin, qui sont :
Pérennes (durent très longtemps)
Infalsifiables (non modifiables, ni supprimables)
Distribués (sur plusieurs nœuds)
Blockchain - Implémentation
Monnaie virtuelle - Bitcoin
© Dr. Boukharrou R.
Bloc 49
Transaction 102
Transaction 103
Transaction 104
Transaction 105
Bloc 48
Transaction 99
Transaction 100
Transaction 101
Bloc 47
Transaction 96
Transaction 97
Transaction 98
Bloc 1
Transaction 1
Transaction 2
Transaction 3

Université Constantine 2 11
Bitcoin
White paper
© Dr. Boukharrou R.
Bitcoin: A Peer-to-Peer Electronic Cash System (2009)
Cité 229 fois
Auteurs :
• Satoshi Nakamoto (Unknown affiliation)
Lien :
• https://bitcoin.org/bitcoin.pdf
Mots clés :
Transactions  Blockchain  peer-to-peer 
Monnaie électronique  Cryptographie 
Consensus distribué

Université Constantine 2 12
Bitcoin
Principe de fonctionnement
© Dr. Boukharrou R.
Nœud 6
Nœud 1
Nœud 2
Nœud 5
Nœud 4
Nœud 3

Université Constantine 2 13
Bitcoin
Principe de fonctionnement
© Dr. Boukharrou R.
Nœud 6
Nœud 1
Nœud 2
Nœud 5
Nœud 4
Nœud 3

Université Constantine 2 14
Bitcoin
Principe de fonctionnement
© Dr. Boukharrou R.
Banque 1
Banque 2
Systèmes bancaires
Une requête est
envoyée à la banque

Université Constantine 2 15
Bitcoin
Principe de fonctionnement
© Dr. Boukharrou R.
Banque 1
Banque 2
Systèmes bancaires
Vérification centralisée
puis exécution de la
transaction
-10 $ 
+10 $ 

Université Constantine 2 16
Bitcoin
Principe de fonctionnement
© Dr. Boukharrou R.
Banque 1
Banque 2
Systèmes bancaires
Consultation
du compte

Université Constantine 2 17
Bitcoin
Principe de fonctionnement
© Dr. Boukharrou R.
Blockchain
La trans. est envoyée à
tous les nœuds du réseau

Université Constantine 2 18
Bitcoin
Principe de fonctionnement
© Dr. Boukharrou R.
Blockchain
Bloc
La trans. est mise
dans un bloc

Université Constantine 2 19
Bitcoin
Principe de fonctionnement
© Dr. Boukharrou R.
Blockchain
Bloc
Après plusieurs
itérations

Université Constantine 2 20
Bitcoin
Principe de fonctionnement
© Dr. Boukharrou R.
Blockchain
Vérification distribuée
des blocs (Minage)

Université Constantine 2 21
Bitcoin
Principe de fonctionnement
© Dr. Boukharrou R.
Blockchain
Bloc miné en premier

Université Constantine 2 22
Bitcoin
Principe de fonctionnement
© Dr. Boukharrou R.
Blockchain
Envoi du bloc miné

Université Constantine 2 23
Bitcoin
Principe de fonctionnement
© Dr. Boukharrou R.
Blockchain
Les transactions non-
traitées sont isolées

Université Constantine 2 24
Bitcoin
Principe de fonctionnement
© Dr. Boukharrou R.
Blockchain
Envoi des transactions
non-traitées

Université Constantine 2 25
Bitcoin
Principe de fonctionnement
© Dr. Boukharrou R.
Blockchain
Hachage et
chainage des blocs

Université Constantine 2 26
Désintermédiation :
Pas d’autorité centrale
Données partagées dans tous les nœuds du réseau
Architecture décentralisée
Autonomie :
Blocs horodatés (time-stamped) et hachés
Émission de crypto-monnaies (ex: Bitcoin)
Sécurité :
Blocs chainés cryptographiquement
Minage et preuve de travail
Protection cryptographique
Propriétés de la Blockchain
© Dr. Boukharrou R.
Centralisé
Décentralisé