



Money Revolution

Dimitris Lamprinos



Γιατί να σε ακούσω?



Γιατί να σε ακούσω?

Δεν είναι όλα τόσο ρόδινα στα fiat νομίσματα



Fiat Currency Problems

- ✗ Απαιτείται έμπιστη αρχή. Υπερβολικά μεγάλος έλεγχος
- ✗ Δεν υπάρχει ανωνυμία ή διαφάνεια
- ✗ Είναι εφικτή η πλαστογραφία τους
- ✗ Δεν υποστηρίζονται πολύ μικρά ποσά
- ✗ Αργές πληρωμές
- ✗ Κόστος για την χρήση σχεδόν οποιασδήποτε υπηρεσίας

1.

Κρυπτονομίσματα?

Τι είναι πάλι αυτά?



Μέσο ανταλλαγής όπως τα κανονικά νομίσματα

Όμως



Έχουν μόνο ψηφιακή μορφή

Πρωτόκολλα εξασφαλίζουν συγκεκριμένες ιδιότητες του
κρυπτονομίσματος

Αλγόριθμοι και κρυπτογραφικές μεθόδους για
συναλλαγές, ιδιοκτησία και δημιουργία νέων
μονάδων



Famous cryptocurrencies

- X Bitcoin
- X Litecoin
- X Dogecoin
- X Decred
- X Monero
- X Ethereum
- X Namecoin



Famous cryptocurrencies

- X Bitcoin
- X Litecoin
- X Dogecoin
- X Decred
- X Monero
- X Ethereum
- X Namecoin

- X ... > 300



Famous cryptocurrencies

- X Bitcoin
- X Litecoin
- X Dogecoin
- X Decred
- X Monero
- X Ethereum
- X Namecoin

- X ... > 300

?

Why bitcoin?

Το πρώτο που
Δημιουργήθηκε
(2009)

Το πιο γνωστό

Με το
μεγαλύτερο
market cap

Some Attributes

- X Peer to peer σύστημα πληρωμών - Πλήρως αποκεντροποιημένο
- X Συναλλαγές σε 1 second - Επιβεβαίωση εγκυρότητας σε 10 λεπτά
- X Μικρά ως μηδενικά κόστη σε κάθε συναλλαγή
- X Αδυναμία παραχάραξης

**WESTERN
UNION**

**Send warm
wishes today.**

FOR ONLY
\$5/\$50
TRANSFER FEE
SEND UP TO
FOR PICK UP WITHIN THE U.S.

[Find Agent Location »](#)

moving money for better

 **bitcoin**

**Send warm
satoshis today.**

FOR ONLY
\$0.01/\$ANY
TRANSFER FEE
SEND UP TO
AMOUNT
FOR PICK UP ANYWHERE ON EARTH

[Pick Your Wallet »](#)

moving money far better

Some More...

- ✗ Κάθε χρήστης έχει ένα πορτοφόλι ακριβώς όπως στα fiat νομίσματα, απλά είναι ηλεκτρονικό!
- ✗ Ανωνυμία → Οι διευθύνσεις δεν είναι συνδεδεμένες με κάποιο φυσικό πρόσωπο
- ✗ Διαφάνεια → Όλες οι συναλλαγές που γίνονται σε κάθε διεύθυνση είναι γνωστές σε όλους
- ✗ Δημιουργούνται μέσω της διαδικασίας του mining με κρυπτογραφικά ελεγχόμενο τρόπο

practically

- ✗ wallet στο υπολογιστή ή στο κινητό μέσω εφαρμογών (electrum, multibit)
- ✗ Ηλεκτρονική τράπεζα (coinbase, kraken, bittrex)
- ✗ Κάθε wallet μπορεί να έχει μια ή περισσότερες διευθύνσεις
E.x. 1BP8WwTRM96feFWnQEuKvn29JCyga33MfY
- ✗ Λογαριασμός τράπεζας \sim Διεύθυνση bitcoin

About keys

- ✗ Παραγωγή κλειδιών με ασύμμετρη κρυπτογραφία
- ✗ Κάθε χρήστης παράγει πανεύκολα ένα ζεύγος κλειδιών (Private Key - Public Key)

<https://www.bitaddress.org>

- ✗ Από το private key μπορεί να βρεθεί το public key ενώ το αντίθετο είναι ανέφικτο
- ✗ Το δημόσιο κλειδί κωδικοποιείται σε μια διεύθυνση.

About keys

X Private key:

5JXesisRRU2Z7HMmwMpNtoiYk1QDMVjV3HLoYMd1PTKEkJhJT1z

X Public key:

045a5f526dfe5d5995bf95f1229e70e21818190883c40ab3590458476ad34aaae59bc772b9
8a587035b452638b59238e2a39e954b43ab7a4f32408664d36ec1575

X Address

133GT5661q8RuSKrrv8q2Pb4RwSpUTQU1Z

About keys

X Private key:

5JXesisRRU2Z7HMmwMpNtoiYk1QDMVjV3HLoYMd1PTKEkJhJT1z

X Public key:

045a5f526dfe5d5995bf95f1229e70e21818190883c40ab3590458476ad34aaae59bc772b9
8a587035b452638b59238e2a39e954b43ab7a4f32408664d36ec1575

X Address

133GT5661q8RuSKrrv8q2Pb4RwSpUTQU1Z

Key generation demo

About addresses

✗ Μπορούμε να τις θεωρούμε παρόμοιες με τις διευθύνσεις τραπεζικών λογαριασμών.

✗ Συχνά τις αναπαριστούμε με QR codes.



✗ Μπορούμε να τις δημοσιεύουμε χωρίς φόβο.

Ωραία ακούγονται... Από πού προέκυψε?

1998: Wei Dai, “bmoney”: Πρώτες αποκεντρωμένες ιδέες

2005: Nick Szabo, “bit gold”: Πλήρης θεωρητική περιγραφή του bitcoin

2008: Satoshi Nakamoto, “Bitcoin: A peer-to-peer electronic cash system”

2009: Δημοσίευση του bitcoin software

Ωραία ακούγονται... Από πού προέκυψε?

1998: Wei Dai, “bmoney”: Πρώτες αποκεντρωμένες ιδέες

2005: Nick Szabo, “bit gold”: Πλήρης θεωρητική περιγραφή του bitcoin

2008: Satoshi Nakamoto, “Bitcoin: A peer-to-peer electronic cash system”

2009: Δημοσίευση του bitcoin software



Satoshi Nakamoto

Ιδρυτής του Bitcoin

Έγραψε το bitcoin paper

Έφτιαξε την πρώτη υλοποίηση

Συμμετείχε ενεργά σε forums

Κάποια στιγμή εξαφανίστηκε...

Και από τότε οι φήμες οργιάζουν





Πως μπορώ να αποκτήσω?

How to get

- X Από άμεση μεταφορά απο κάποιον που έχει BTC.
- X Από αγορά μέσω ηλεκτρονικού ανταλλακτηρίου
- X Μέσω bitcoin mining

How to get

- X Από άμεση μεταφορά απο κάποιον που έχει BTC.
- X Από αγορά μέσω ηλεκτρονικού ανταλλακτηρίου
- X Μέσω bitcoin mining
- X Από εμένα μετά την ομιλία



How to get

- ✗ Από άμεση μεταφορά απο κάποιον που έχει BTC.
- ✗ Από αγορά μέσω ηλεκτρονικού ανταλλακτηρίου
- ✗ Μέσω bitcoin mining
- ✗ Από εμένα μετά την ομιλία



Bitcoin Mining

- ✗ Διαδικασία επίλυσης ενός προβλήματος μέσω ειδικού λογισμικού
- ✗ Κάθε 10 λεπτά λύνεται ένα τέτοιο πρόβλημα και δημιουργείται ένα νέο block
- ✗ Επιτυγχάνεται με κρυπτογραφία σε κάθε block:
 - Η εγκυρότητα των συναλλαγών που έγιναν τα προηγούμενα 10 λεπτά
 - Η σειρά των συναλλαγών
- ✗ Οποιος/οι λύσουν το πρόβλημα: fees + κάποια ακόμα BTC

16,217,725 BTC

Υπάρχουν σήμερα συνολικά

>3,000,000 users

Έχουν στην κατοχή τους το bitcoin

1130€

Κοστίζει κάθε bitcoin **σήμερα**

Let's play

- X Blockchain (blockchain.info)
- X Bitcoin client (electrum, multibit)
- X Bitcoin exchange (bittrex, kraken)

Let's Buy with Bitcoin





Ευχαριστώ!

You can find me at
@pkakelas
<https://pkakelas.com>

GPG: 5456 5C0E 57FA 7A55 AB49 C0D1 65E3 D29D 92B4 1043