

Αναλύσεις Προγραμμάτων και Ψηφιακά Νομίσματα

Γιάννης Σμαραγδάκης, ΕΚΠΑ

Κρυπτονομίσματα/ Ψηφιακά Νομίσματα



Κρυπτονομίσματα

- Κάτι σαν “νομίσματα” σε μεγάλο online βιντεοπαιχνίδι;
- Με πολύ κόσμο να πληρώνει για να πάρει αυτά τα νομίσματα
 - δηλαδή τη συμφωνία των άλλων παικτών ότι έχει αυτά τα νομίσματα στο παιχνίδι

Κρυπτονομίσματα

- Κάτι σαν “νομίσματα” σε μεγάλο online βιντεοπαιχνίδι;
- Με πολύ κόσμο να πληρώνει για να πάρει αυτά τα νομίσματα
 - δηλαδή τη συμφωνία των άλλων παικτών ότι έχει αυτά τα νομίσματα στο παιχνίδι
- Ακόμα χειρότερο: το “παιχνίδι” δεν έχει καν πλοκή
 - μόνος λόγος ύπαρξής του να κρατάει το πόσα νομίσματα έχει ο κάθε παίκτης

CRYPTOCURRENCY

[FX](#) | [AMERICAS FX](#) | [ASIA FX](#) | [EU FX](#) | **[CRYPTOCURRENCY](#)**

Ethereum hits a fresh record high and is up over 13,000% in a year

- The price of ethereum hit an all-time high of \$1,417.38 on Wednesday, according to CoinDesk
- The cryptocurrency's price is up around 60 percent in the last week
- Steven Nerayoff, a co-creator of ethereum, said it could "easily" double or triple this year

Arjun Kharpal | [@ArjunKharpal](#)

Published 3:16 AM ET Wed, 10 Jan 2018 | Updated 9:56 AM ET Wed, 10 Jan 2018



Ethereum just hit
a fresh record high

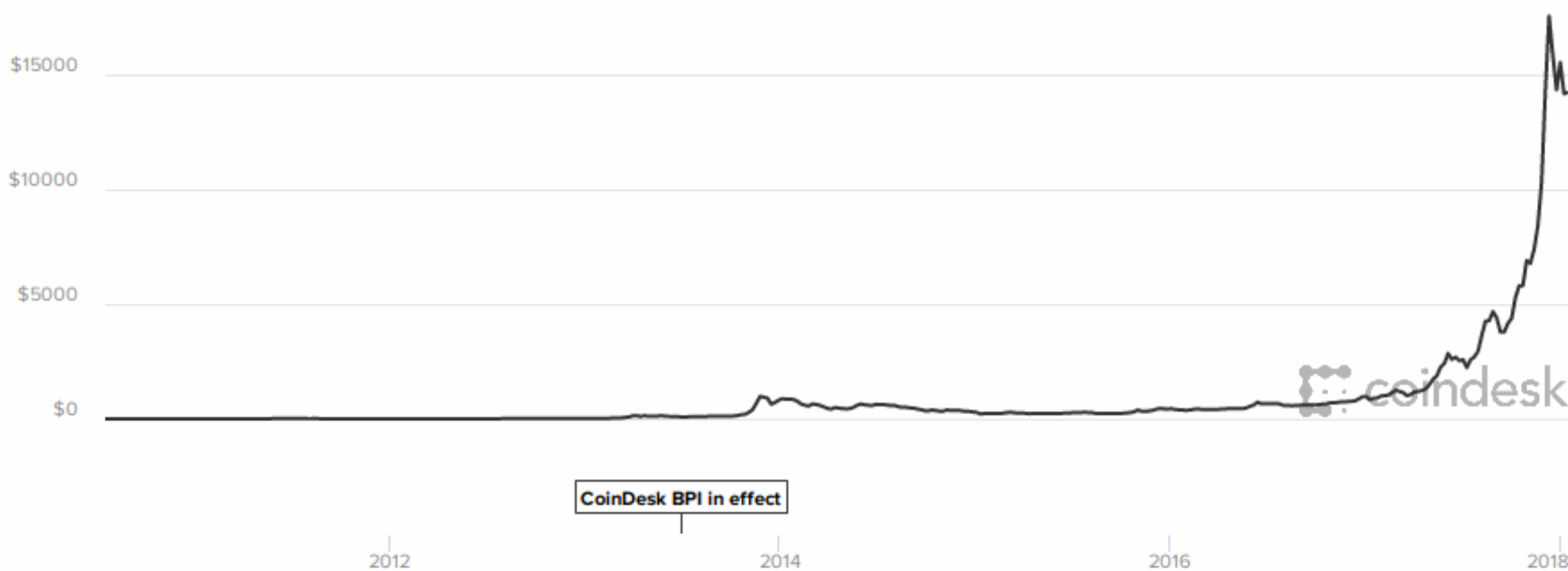


Bitcoin (USD) Price

Closing Price ☐ OHLC

1h 12h 1d 1w 1m 3m 1y **All**

Jul 18, 2010 to Jan 15, 2018 [Export](#)



\$14,216.94 ▲ 4.39%

Today's Open	\$13,619.03	Change	▲ \$597.91
Today's High	\$14,307.53	Market Cap	\$0.239T
Today's Low	\$13,401.24	Supply	16,804,188

Ιδέες;

Νόμισμα/Χρήμα

- Χρήμα = κάτι που πιστεύω ότι έχει αξία, επειδή πιστεύω ότι άλλοι πιστεύουν ότι έχει αξία
 - δεν υπάρχει εγγενής αξία, μόνο ανταλλαξιμότητα
- Συνήθως αυτή η ομαδική παράκρουση (“ευρεία συμφωνία”) ξεκινά από κάποια *έμπιστη αρχή*
 - π.χ. το κράτος τυπώνει νόμισμα
- Κρυπτονομίσματα/ψηφιακά νομίσματα: αυθαίρετη απόδοση αξίας σε ακολουθίες από bit
- Βάση κρυπτονομισμάτων: είναι δυνατή η ευρεία συμφωνία χωρίς να υπάρχει έμπιστη αρχή

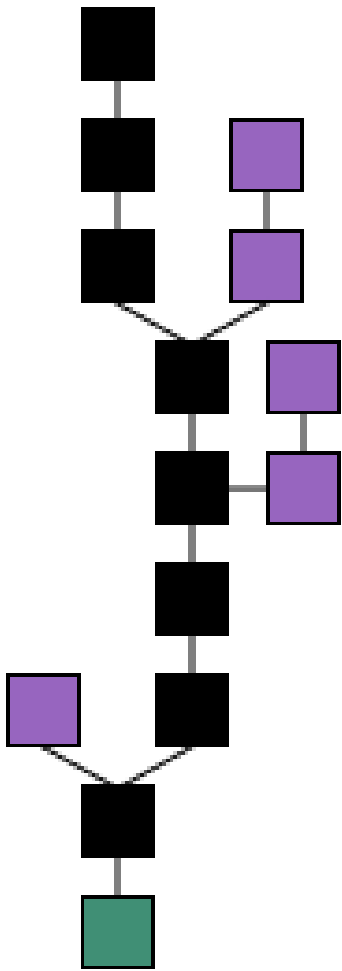
Κρυπτογραφία

- Δύσκολο να κατανοηθεί πώς δουλεύει, εύκολο να κατανοηθεί τι πετυχαίνει
- Δυνατότητες αντίστοιχες καθημερινών, αλλά στον υπερθετικό βαθμό:
 - υπογραφή/ταυτοποίηση χωρίς δυνατότητα παραχάραξης
 - δημοσίευση άπειρων κουτιών (οποιοιδήποτε μεγέθους) με λουκέτα που μόνο εγώ ξεκλειδώνω
- Για κρυπτονομίσματα: «Έχω» = «Ξέρω»

Blockchain

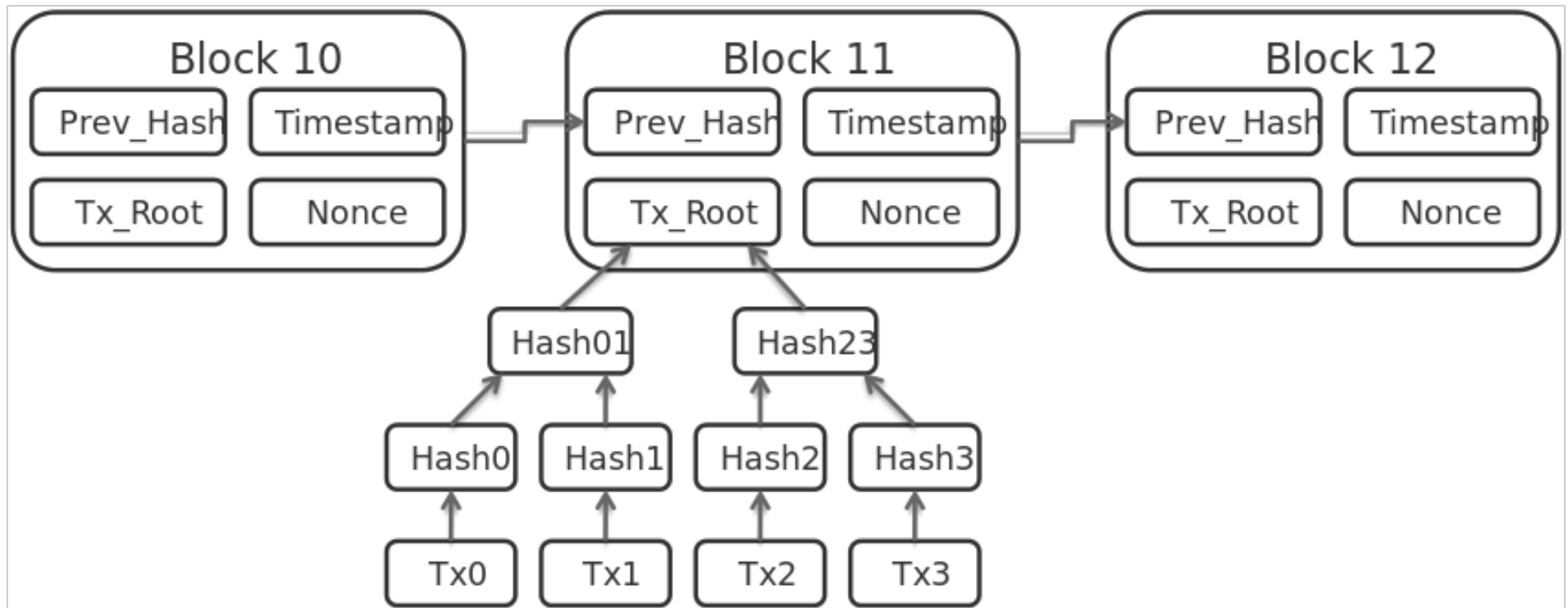
- *“Η τεχνολογία Blockchain έχει την ικανότητα να δημιουργήσει νέα θεμέλια για τα οικονομικά και κοινωνικά συστήματα.”*

Blockchain



- Κατανεμημένο “κατάστιχο” συναλλαγών χωρίς ανάγκη έμπιστης αρχής
- Ολοένα επιμηκυνόμενη σειρά block
 - η μεγαλύτερη σειρά θεωρείται έγκυρη
- Κάθε κόμβος μαζεύει συναλλαγές σε νέο block
- Κάθε κόμβος ψάχνει κρυπτογραφική λύση νέου block
 - δυσκολία (proof-of-work)
 - κίνητρο να προστεθούν block: πληρωμή αν βρεθεί λύση
- Κόμβοι δέχονται το νέο block αν οι συναλλαγές συνεπείς
- Δεκτά block: καθένα υπογράφει προηγούμενο
 - δεν αλλάζει block χωρίς να αλλάξει όλο το μέλλον
- Λύνει το θέμα του double spending

Παράδειγμα Blockchain



Ethereum: Smart Contracts

- Ethereum = ένα blockchain με τους λογαριασμούς να είναι έξυπνα συμβόλαια
- Έξυπνα συμβόλαια = προγράμματα, μόνιμα αποθηκευμένα στο blockchain
- Καλούνται από άλλα

Πρόβλημα: Λάθη, Ασφάλεια

Digital currency Ethereum is cratering because of a \$50 million hack



Rob Price

Jun. 17, 2016, 10:34 AM 30,040



The value of the digital currency Ethereum has dropped dramatically amid an apparent huge attack targeting an organisation with huge holdings of the currency.

The price per unit dropped to \$15 from record highs of \$21.50 in hours, with millions of units of the digital currency worth as much as \$50 million stolen at post-theft valuations.

At a pre-theft valuation, it works out as a staggering \$79.6 million.




Martin Hunter/Getty Images

Security

Parity's \$280m Ethereum wallet freeze was no accident: It was a HACK, claims angry upstart

And we have evidence to prove it, says biz stiffed out of \$1m

By [Iain Thomson](#) in [San Francisco](#) 10 Nov 2017 at 22:40

78  [SHARE](#) ▼



DAO Hack

```
contract SimpleDAO { ...  
    function withdraw(uint amount) {  
        if (credit[msg.sender] >= amount) {  
            msg.sender.call.value(amount)();  
            credit[msg.sender] -= amount;  
        }  
    }  
}
```


DAO Hack

```
contract SimpleDAO { ...  
    function withdraw(uint amount) {  
        if (credit[msg.sender] >= amount) {  
            msg.sender.call.value(amount)();  
            credit[msg.sender] -= amount;  
        }  
    }  
}
```

```
contract Attack {  
    ... function() { dao.withdraw(10); } ...  
}
```

(Στατική) Ανάλυση Προγραμμάτων

- Η μελέτη του τι κάνει ένα πρόγραμμα κάτω από *κάθε δυνατή συνθήκη*
 - άπειρες δυνατές συνθήκες (είσοδοι, περιβάλλον)
- Μαθηματικά αδύνατο σε πλήρη ακρίβεια
 - “αδύνατο να γράψουμε πρόγραμμα X που να εξετάζει άλλο πρόγραμμα Y και να λέει αν το Y πάντα θα ...”
- Ο βασικός μου τομέας έρευνας τα τελευταία 8-9 χρόνια

Έρευνα σε Ανάλυση Προγραμμάτων

- Εκφράζουμε αλγορίθμους σαν αναδρομικές προδιαγραφές σε μαθηματική λογική
- Εξαιρετικά ισχυρές βιβλιοθήκες για ανάλυση Java/C/C++
- Χιλιάδες λογικοί κανόνες!
 - ~5000 για Java (bytecode)
 - ~3000 για C/C++ (LLVM bitcode)
- Σκεφτείτε το σαν ένα σύστημα με εξισώσεις

Μελλοντική Έρευνα

- Ανάλυση έξυπνων συμβολαίων
- Εργαλείο για βοήθεια προγραμματιστών
 - εφαρμογή σε Facebook android app
- Όραμα: σύστημα που θα ξέρει περισσότερα για το πρόγραμμα από τον ίδιο τον προγραμματιστή!