

BLOCKCHAIN ΚΑΙ CONSENSUS

μια σύντομη εισαγωγή

Άρης Παγουρτζής

Σχολή ΗΜΜΥ ΕΜΠ

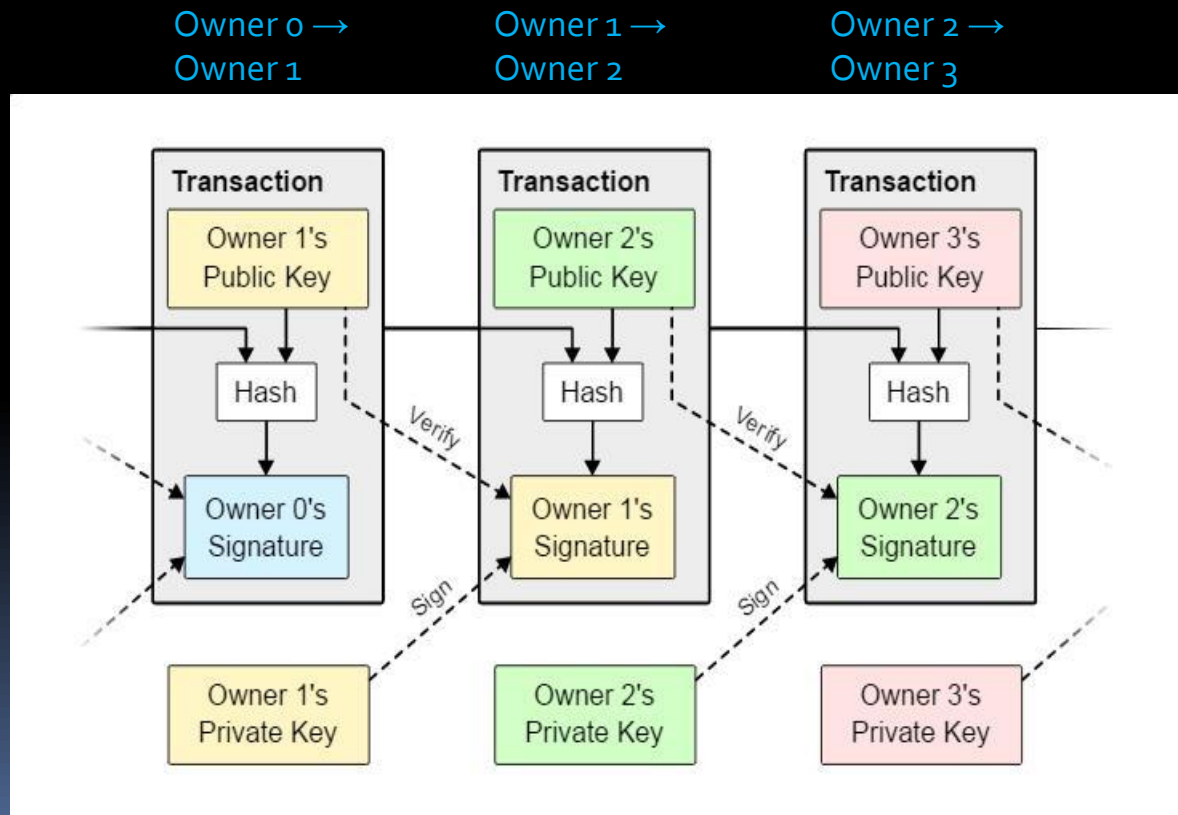
Υπολογιστική Κρυπτογραφία

(ΣΗΜΜΥ-ΣΕΜΦΕ-ΑΛΜΑ-ΕΜΕ)

Έν αρχῇ ἦν ... το Bitcoin

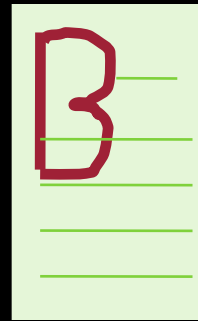
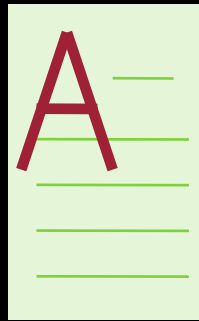


- ... και ο «ἀόρατος» δημιουργός αυτού:
Satoshi Nakamoto (2008)



Blockchain: η «ραχοκοκαλιά» του Bitcoin

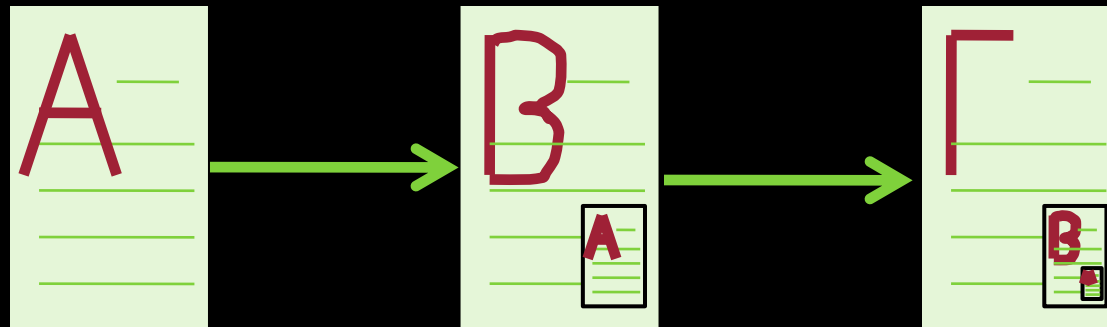
- Ας φανταστούμε: **κατάστιχο (ledger)** με ασύνδετα φύλλα



- Πώς ξέρουμε ότι δεν χάθηκε κάποιο φύλλο;
- Πώς ξέρουμε ότι κανείς δεν άλλαξε κάποιο φύλλο;
- **Συλλογικό** κατάστιχο: ποιος γράφει το επόμενο φύλλο;

Blockchain: η «μαγική» λύση!

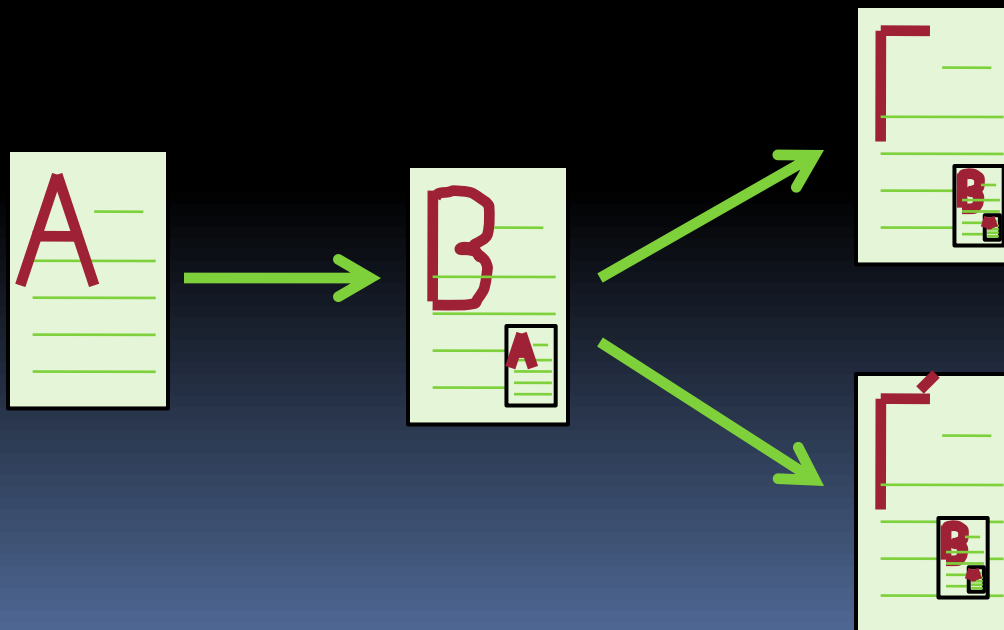
- Κάθε φύλλο περιέχει «αποτύπωμα» του προηγούμενου (π.χ. φωτογραφία σε σμίκρυνση)



- Κάθε φύλλο συνδέεται **ισχυρά** με το προηγούμενο και, μέσω αυτού, με **όλα τα προηγούμενα φύλλα**
- Πρακτικά αδύνατο να αλλοιωθεί μεμονωμένο φύλλο ή ενδιάμεση (ή αρχική) σειρά φύλλων
- Εγγύηση **ακεραιότητας** και **χρονικής αλληλουχίας**

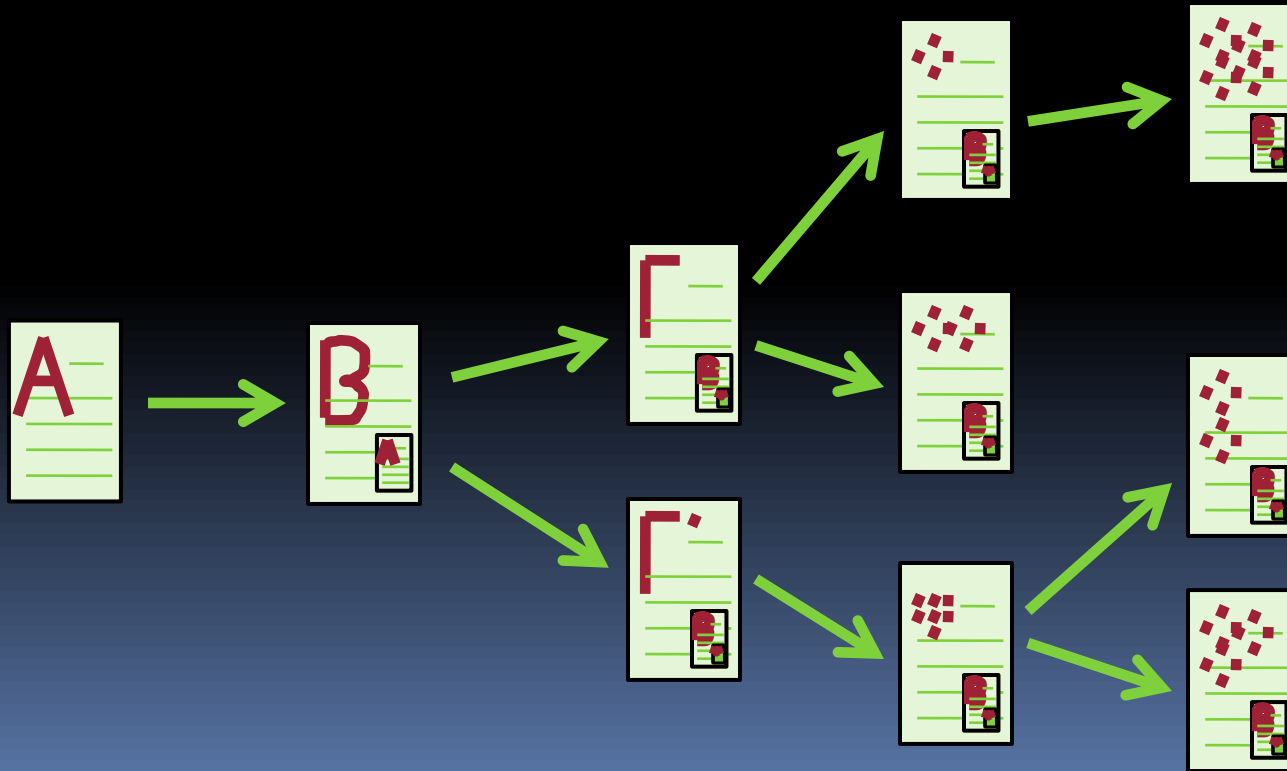
Blockchain: ανάγκη συμφωνίας!

- Συλλογικό κατάστιχο: ποιος φτιάχνει το επόμενο φύλλο;
- Τι θα συμβεί αν επιτρέψουμε πολλά έγκυρα επόμενα φύλλα;



Blockchain: ανάγκη συμφωνίας!

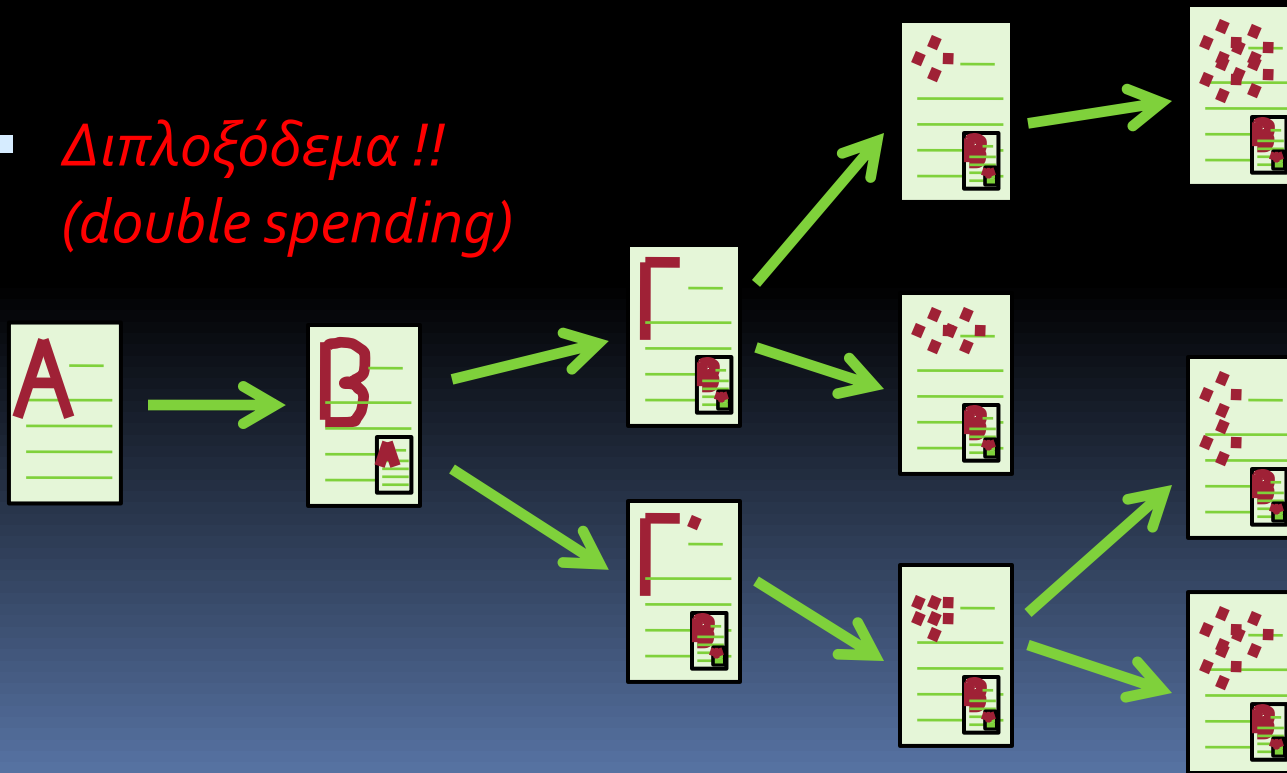
- Συλλογικό κατάστιχο: ποιος φτιάχνει το επόμενο φύλλο;
- Τι θα συμβεί αν επιτρέψουμε πολλά έγκυρα επόμενα φύλλα;



Blockchain: ανάγκη συμφωνίας!

- Συλλογικό κατάστιχο: ποιος φτιάχνει το επόμενο φύλλο;
- Τι θα συμβεί αν επιτρέψουμε πολλά έγκυρα επόμενα φύλλα;

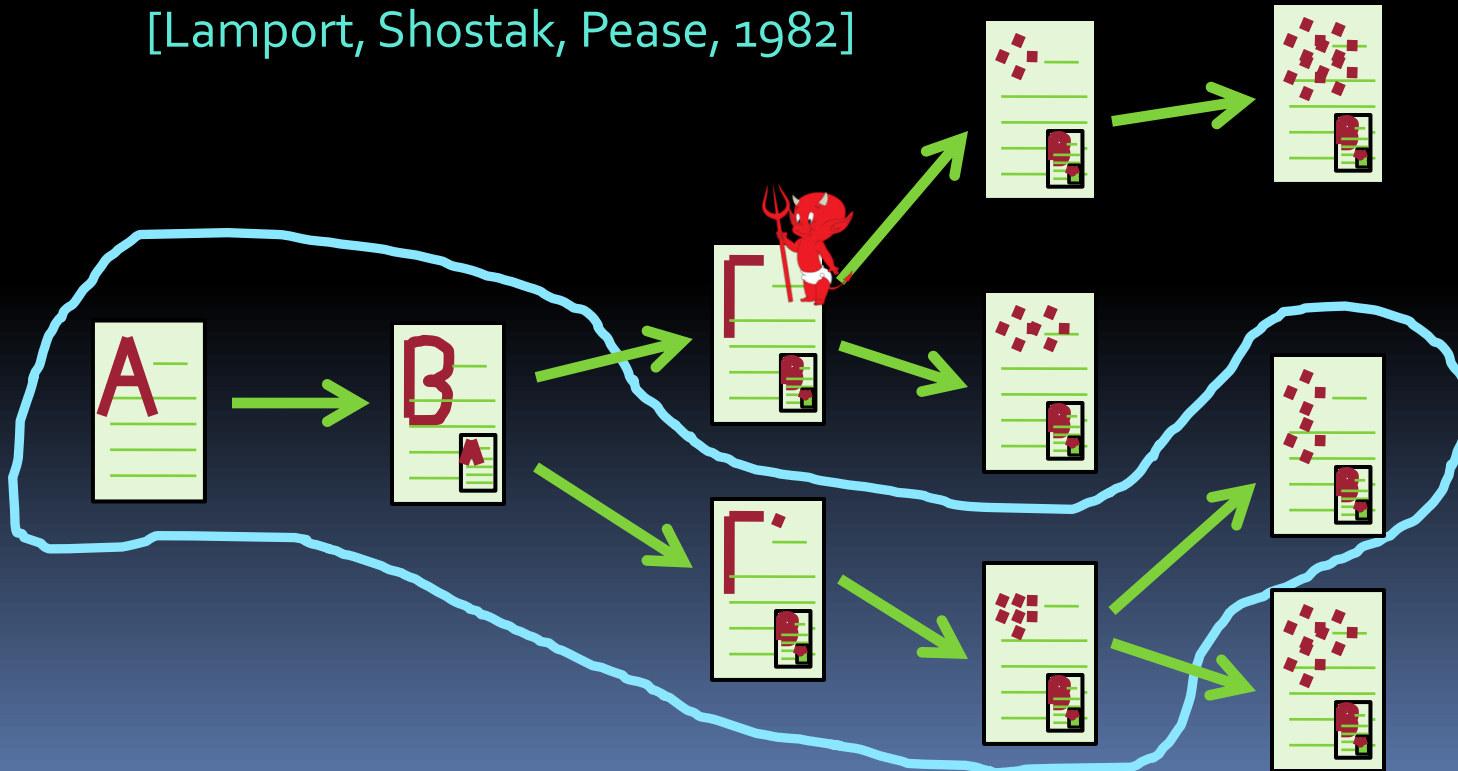
- *Διπλοξόδεμα !!
(double spending)*



Βυζαντινή συμφωνία

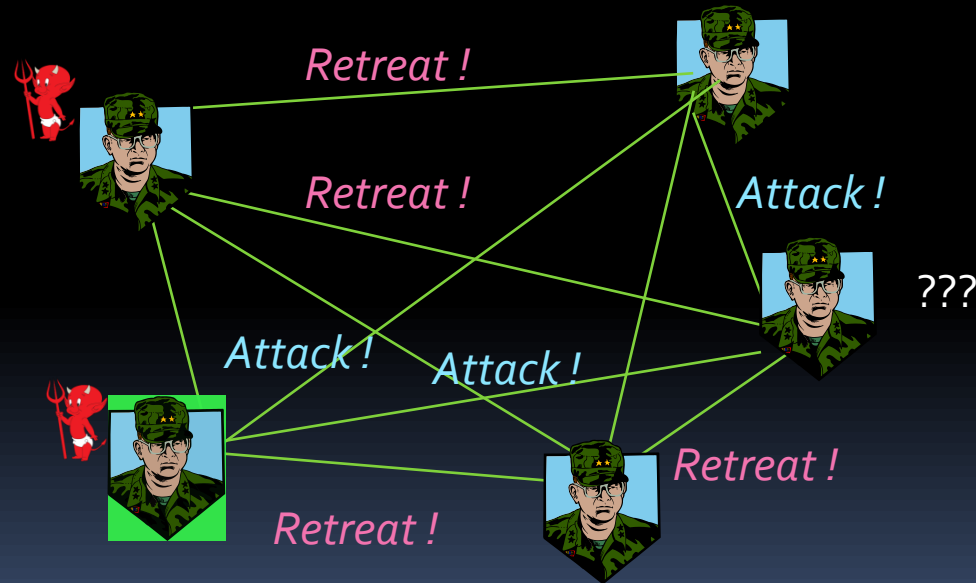
- Byzantine Agreement / Byzantine Fault Tolerance, γνωστό και ως Consensus: θέλουμε τα μέρη ενός κατακευματισμένου συστήματος να συμφωνήσουν σε ένα σύνολο δεδομένων ακόμη και υπό την παρουσία κακόβουλων (Βυζαντινών) αντιπάλων!

[Lamport, Shostak, Pease, 1982]



Πρόβλημα Βυζαντινών στρατηγών

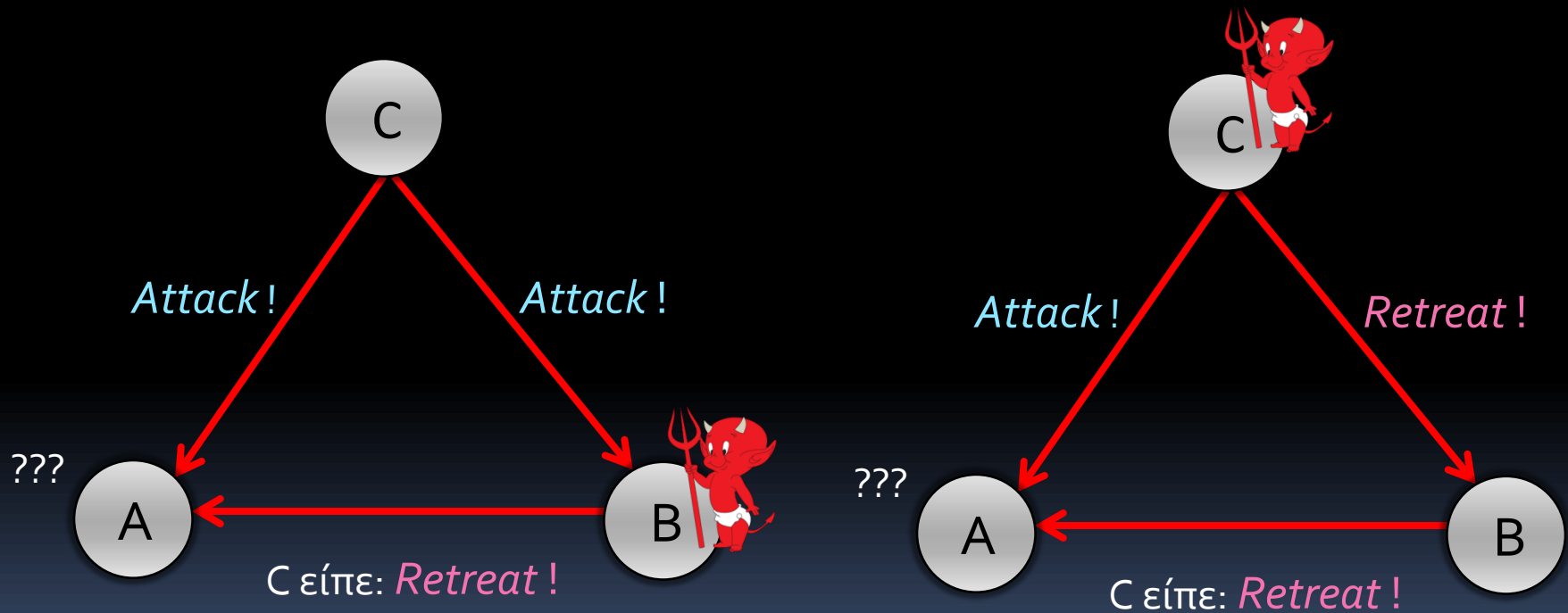
- Γνωστό και ως **Reliable broadcast**: θέλουμε ένας ηγέτης να μεταδώσει σωστά ένα μήνυμα (διαταγή) στα μέρη ενός κατανεμημένου συστήματος ακόμη και υπό την παρουσία κακόβουλων (**Βυζαντινών**) αντιπάλων!



- Ισοδύναμο με Consensus !*

Επίδραση Βυζαντινών αντιπάλων

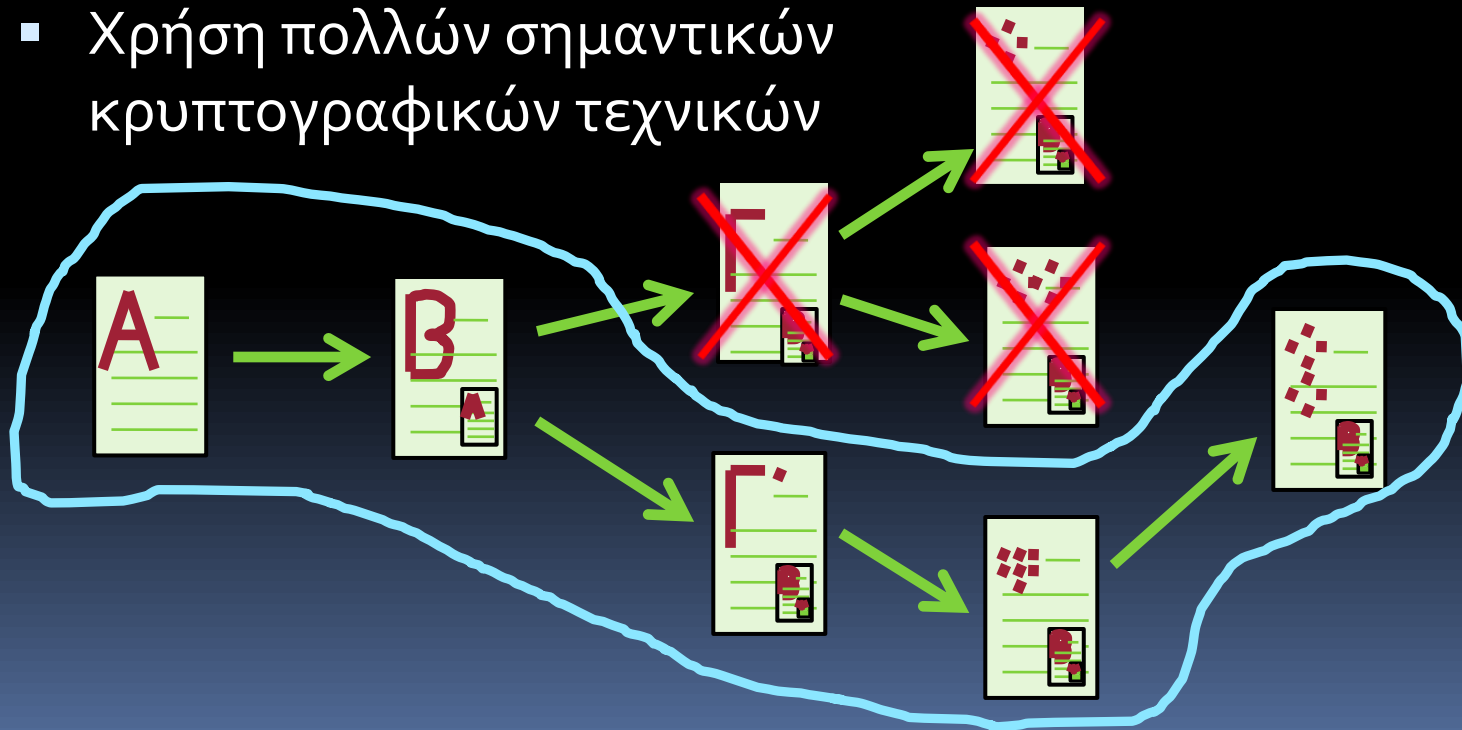
- Αν μπορούν να επηρεάσουν το $\frac{1}{3}$ των συμμετεχόντων μπορούν να εμποδίσουν την επίτευξη συμφωνίας!



- Γενικεύεται σε οσοδήποτε στρατηγούς!

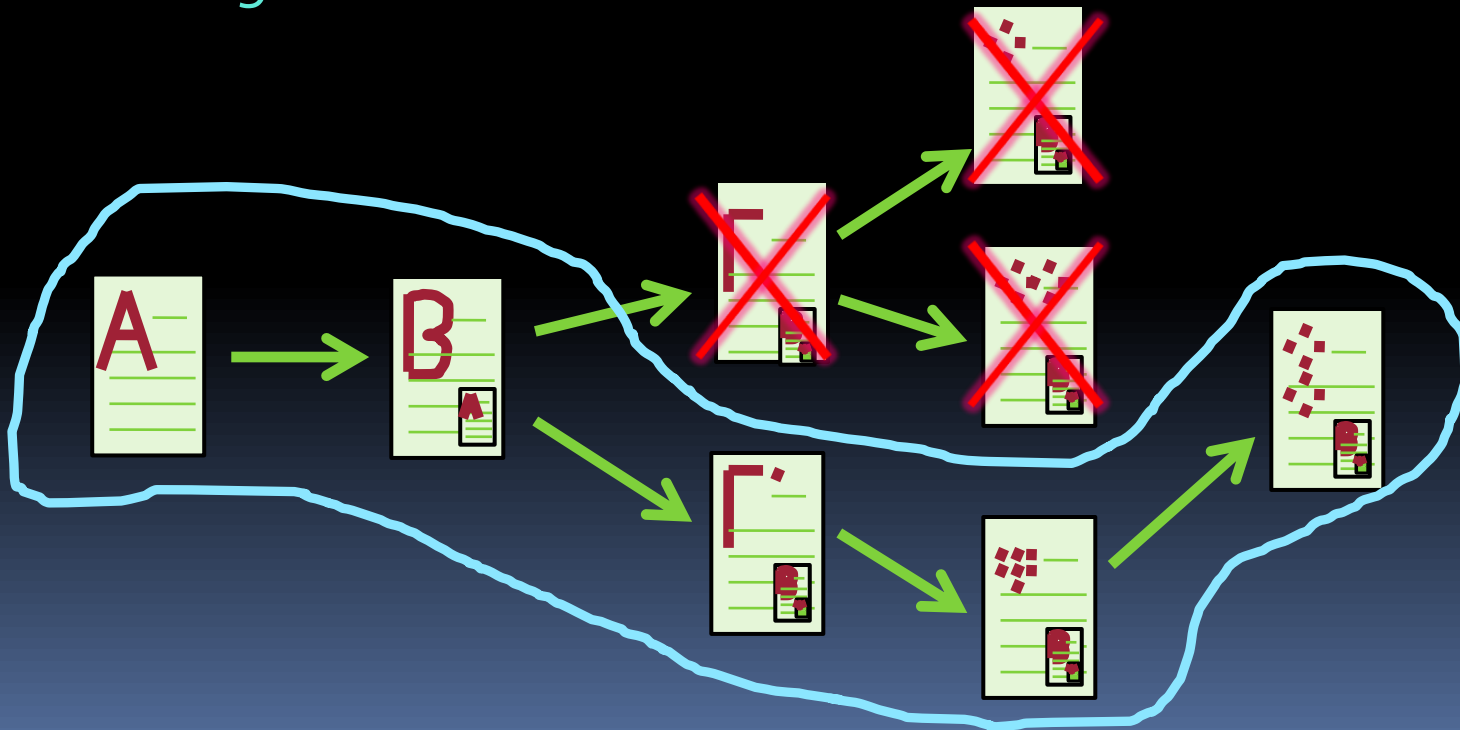
Η λύση του Bitcoin

- Επικρατεί η μεγαλύτερη αλυσίδα
- Αποδεδειγμένα ασφαλές υπό λογικές προϋποθέσεις [Garay, Kiayias, Leonardos 2015]
- Κρίσιμη τεχνική: απόδειξη έργου (Proof-of-Work, PoW)
- Χρήση πολλών σημαντικών κρυπτογραφικών τεχνικών



Όλα καλά επομένως;

- Όχι ακριβώς . . .
- PoW => Υπερβολική κατανάλωση ενέργειας
- PoW => Μικρός όγκος συναλλαγών
- *Rich get richer*



Εναλλακτικές λύσεις

- Proof of Stake (PoS) (Ethereum Casper, Cardano), Proof-of-Burn, Delegate systems, . . . έρευνα σε εξέλιξη !
- Χρησιμοποιούν διαφορετικούς μηχανισμούς Consensus
- Σημαντική η αξιόπιστη μετάδοση (reliable broadcast) για πολλές από τις παραπάνω λύσεις

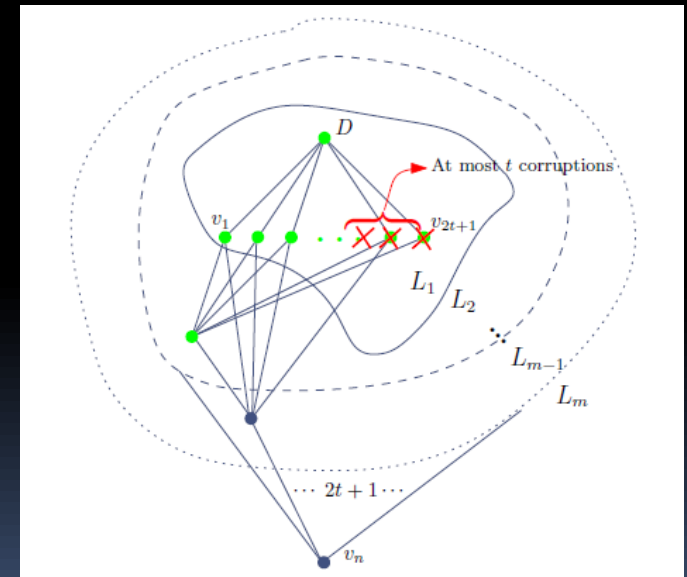
Reliable Broadcast

- Σημαντική λειτουργία, επιθυμητή η *χωρίς προϋποθέσεις ασφάλεια*
- Κλασικοί αλγόριθμοι υπέθεταν γνώση ενός *γενικού ορίου* στο πλήθος των διαφθορών
[Lamport, Shostak, Pease, 1982], [Garay, Moses, 1998]
- Πιο πρόσφατη θεώρηση: τοπικά φραγμένος αντίπαλος, εκτίμηση *τοπικού ορίου* διαφθορών, ανάμεσα στις γνωριμίες κάθε συμμετέχοντα
[Koo, 2004], [Pelc, Peleg, 2005], [P., Panagiotakos, Sakavalas, 2014]

Αλγόριθμος Αξιόπιστης Διάδοσης

- Certified Propagation Algorithm (CPA) [Koo, 2004]
- Εξαιρετικά απλή ιδέα: αν εκτιμάς t διαφθορές ανάμεσα στις γνωριμίες σου, περίμενε ώσπου να πάρεις $t+1$ ίδια μηνύματα

- Είναι προφανές ότι ο CPA είναι **ασφαλής** (αν έχουμε σωστή εκτίμηση). Αποδείξαμε ότι είναι και **βέλτιστος**!
[P., Panagiotakos, Sakavalas, 2014 & 2017]



Blockchain & Consensus

- **Blockchain**: μια επαναστατική τεχνολογία με ανεξάντλητες εφαρμογές (κρυπτονομίσματα, smart contracts, e-voting, reliable distributed databases, ψηφιακές ταυτότητες, . . .)
- **Consensus**: θεμελιώδης λειτουργία, κομβικής σημασίας για αποκεντρωμένα συστήματα και δίκτυα κάθε είδους.
- Το Blockchain είναι αλληλένδετο με το consensus. Στηρίζεται σε αυτό αλλά μπορεί και να το «παράγει».
- Οι μέθοδοι consensus ενισχύονται σημαντικά και εμπλουτίζονται μέσω της εντατικής έρευνας στο blockchain και τις εφαρμογές του και αντίστροφα.
- Πρόβλεψη: στο εξής θα συμβαδίζουν όλο και περισσότερο και θα προσφέρουν ακόμη πιο εντυπωσιακές εφαρμογές.