# Πρωτόκολλα κατανεμημένης συναίνεσης

Βελτιστοποίηση Δικτύων

24/2/2023

Εισαγωγή

Βυζαντινή συμφωνία
- Το πρόβλημα των Βυζαντινών στρατηγών
- Λύσεις
- Πρακτικοί αλγόριθμοι

Κατανεμημένα κατάστιχα
- Blockchain
- Κίνητρα τιμιότητας
- Εξόρυξη

Εφαρμογή του blockchain σε κατανεμημένα κατάστιχα

# Πρωτόκολλα σε κατανεμημένα συστήματα και δίκτυα, I

- Τα πρωτόκολλα είναι κανόνες με τους οποίους οντότητες που βρίσκονται σε διαφορετικά σημεία ενός δικτύου μπορούν να εκτελούν σε συνεργασία έναν αλγόριθμο.
- Για παράδειγμα, ο αλγόριθμος των Bellman Ford βασίζεται σε μετρήσεις που γίνονται με τη συνεργασία κάθε κόμβου με τους γειτονικούς του, ώστε να επικαιροποιεί ο κάθε κόμβος αυτόνομα τον πίνακα δρομολόγησης που διαθέτει.
- Στον αλγόριθμο Dijkstra, όπου χρειάζεται υπολογισμός με συγκεντρωτικά δεδομένα καθυστερήσεων και τοπολογιών, λειτουργούν πολύπλοκα πρωτόκολλα συλλογής και διαβίβασης δεδομένων.
- Τα πρωτόκολλα αυτά βασίζονται στο ότι οι κόμβοι είναι «τίμιοι», δηλαδή δεν αλλοιώνουν τα δεδομένα ή την συμπεριφορά τους.

# Πρωτόκολλα σε κατανεμημένα συστήματα και δίκτυα, II

- Ωστόσο σε ποικίλες περιπτώσεις παίκτες μπορεί να αποκομίσουν κέρδος με «μη τίμια» συμπεριφορά.
- Η συνεργασία μπορεί να επιβάλλεται είτε με συμβόλαια, κανόνες και ποινές, είτε με κίνητρα (είτε με συνδυασμό).
- Η συνεργασία είναι τόσο πιο δύσκολο να υλοποιηθεί όσο το κέρδος από την απόκλιση μεγαλώνει.

# Συνεργασία και θεωρία παιγνίων

- Στη μη συνεργατική θεωρία παιγνίων[1] (non-cooperative game theory) υπάρχει ένας πληθυσμός ανταγωνιστών παικτών. Η ισορροπία Nash είναι μια κατάσταση όπου κάθε παίκτης δεν έχει συμφέρον να αλλάξει την συμπεριφορά του.
- Η συνεργατική θεωρία παιγνίων[2] (cooperative game theory) αναλύει περιπτώσεις όπου οι παίκτες μπορούν να αποκομίσουν κέρδη σχηματίζοντας ομάδες.

[1] Fudenberg and Tirole 1991
[2] Curiel 2013

# Συγκεντρωτικά συστήματα

- Όταν η συμμόρφωση με κανόνες είναι απαραίτητη για τη λειτουργία ενός συστήματος, αυτή μπορεί να ελέγχεται κεντρικά με χρήση ενός συστήματος κινήτρων και τιμωριών.
- Για παράδειγμα, τα νομίσματα εκδίδονται από μια κεντρική κρατική τράπεζα. Η παραχάραξη και η εμπρόθετη χρήση πλαστών νομισμάτων είναι ποινικά αδικήματα.
- Σε ένα σύστημα καταχώρισης συμβολαίων για ναύλους (μεταφορές εμπορευμάτων με πλοίο) ο κεντρικός διαχειριστής εγγυάται ότι τα συμβόλαια συντάσσονται σωστά και περαιτέρω δεν αλλοιώνονται. Εν συνεχεία την τήρησή τους εγγυάται το δίκαιο (νόμοι, δικαστήρια, αστυνομία, φυλακές κ.λπ.).

# Αποκεντρωμένα συστήματα

- Σε ένα αποκεντρωμένο σύστημα η τήρηση των κανόνων μπορεί να ελέγχεται από όλους, ή από μερικούς εξουσιοδοτημένους, ή ο έλεγχος να υπάρχει ως δυνατότητα, για όποιον θέλει να την χρησιμοποιήσει (π.χ. ένας κωδικός γνησιότητας προϊόντος).
- Ο έλεγχος βεβαίως δεν είναι αρκετός αν δεν λαμβάνονται περαιτέρω μέτρα, δηλ. αν ο παραβάτης δεν υφίσταται κάποια ζημία, ποινή κ.λπ.
- Σε *κατανεμημένα κατάστιχα* (distributed ledgers) και κρυπτονομίσματα γίνεται προσπάθεια να εμφανίζονται τα κίνητρα και να υλοποιούνται τα μέτρα «αυτόματα».

# Βυζαντινή συμφωνία

- Η λεγόμενη *βυζαντινή συμφωνία* αναφέρεται σε περιπτώσεις όπου ένα σύνολο οντοτήτων πρέπει να συμφωνήσουν πάνω σε ένα σύνολο δεδομένων (τιμές παραμέτρων), αλλά ορισμένες οντότητες δεν είναι αξιόπιστες, είτε κατά λάθος είτε σκόπιμα.
- Το *βυζαντινό σφάλμα* (byzantine fault) αναφέρεται στην περίπτωση όπου αφενός ορισμένες οντότητες βρίσκονται σε προβληματική κατάσταση, αφετέρου η διαθέσιμη πληροφορία για την κατάστασή τους είναι ανεπαρκής.
- Η ορολογία αυτή προέρχεται από το πρόβλημα των Βυζαντινών στρατηγών,[3] όπου $N$ στρατηγοί που βρίσκονται σε απόσταση και επικοινωνούν μέσω αγγελιαφόρων πρέπει να συντονιστούν σε μια κοινή απόφαση (π.χ. για ταυτόχρονη επίθεση).

[3] Lamport, Shostak, and Pease 1982

# Το πρόβλημα των Βυζαντινών στρατηγών

- Ένα σύνολο από τμήματα του βυζαντινού στρατού που καθένα διοικείται από διαφορετικό στρατηγό έχουν κατασκηνώσει έξω από μια πόλη, την οποία πολιορκούν.
- Οι στρατηγοί επικοινωνούν με αγγελιαφόρους και πρέπει να συμφωνήσουν σε ένα κοινό σχέδιο δράσης.
- Ωστόσο μερικοί από τους στρατηγούς μπορεί να είναι προδότες και να προσπαθούν να εμποδίσουν τους άλλους να φτάσουν σε συμφωνία.
- Το πρόβλημα είναι να βρεθεί ένας αλγόριθμος που
  A. θα επιτρέψει στους έντιμους στρατηγούς να υιοθετήσουν ένα κοινό σχέδιο και
  B. λίγοι προδότες στρατηγοί δεν μπορούν να παρασύρουν τους υπόλοιπους σε ένα κακό σχέδιο.

# Το πρόβλημα των Βυζαντινών στρατηγών

- Κάθε στρατηγός μπορεί να στείλει ένα μήνυμα σε άλλον στρατηγό σχετικά με τις προθέσεις του ή μεταφέροντας τις προθέσεις άλλων.
- Διαθέτει ένα τρόπο να αποφασίζει τι θα κάνει με βάση τα μηνύματα που παίρνει από τους άλλους (π.χ. να ταχθεί με την πλειοψηφία).
- Ο μη έντιμος στρατηγός μπορεί να δημιουργεί ή να μεταφέρει μηνύματα με σκοπό τη δημιουργία σύγχυσης.
- Για παράδειγμα, αν υπάρχουν 9 στρατηγοί που θέλουν να αποφασίσουν αν θα επιτεθούν ή όχι και ένας μη έντιμος στρατηγός δει ότι οι 4 είναι υπέρ της επίθεσης και οι άλλοι 4 υπέρ της μη επίθεσης, μπορεί να στείλει στους πρώτους 4 μηνύματα ότι είναι υπέρ της επίθεσης και στους άλλους 4 ότι είναι υπέρ της μη επίθεσης.

# Το πρόβλημα των Βυζαντινών στρατηγών

- Ας υποτεθεί ότι ο στρατηγός $i$ ενός συνόλου $n$ στρατηγών παρατηρεί τον εχθρό και καταλήγει στην τιμή μιας παραμέτρου $v(i)$, την οποία κοινοποιεί στους άλλους στρατηγούς. Κάθε στρατηγός διαθέτει μια μέθοδο να αποφασίζει ένα σχέδιο δράσης όταν γνωρίζει το διάνυσμα $v = (v(1), v(2), \ldots, v(n))$.
- Η προηγ. συνθήκη Α μπορεί να ικανοποιηθεί αν η μέθοδος απόφασης είναι ίδια για όλους τους στρατηγούς.
- Για παράδειγμα, έστω ότι κάθε $v(i)$ είναι δυαδική παράμετρος (π.χ. επίθεση ή όχι). Έστω επίσης ότι η απόφαση λαμβάνεται με πλειοψηφία. Αν οι προδότες είναι πολύ λίγοι, αλλά η πλειοψηφία των εντίμων είναι ισχυρή, το αποτέλεσμα δεν θα αλλάξει.

# Λύσεις στο πρόβλημα των Βυζαντινών στρατηγών I

Οι Lamport, Shostak και Pease (1982) έδειξαν τα εξής:

- Αν υπάρχουν $m$ το πλήθος προδότες, δεν υπάρχει λύση για λιγότερους από $3m + 1$ στρατηγούς.
- Η ανεύρεση μιας προσεγγιστικής λύσης (π.χ. να συμφωνήσουν οι στρατηγοί σε μια δράση με ανοχή στο χρόνο της δράσης) είναι εξ ίσου δύσκολη, δηλαδή δεν επιτρέπει τη χαλάρωση της απαίτησης για το 1/3.
- Στην περίπτωση που τα μηνύματα που ανταλλάσσονται είναι *προφορικά* (αλλοιώσιμα κατά την προώθηση μεταξύ στρατηγών), αλλά τηρείται το 1/3, υπάρχει λύση.
- Η λύση βασίζεται στην ανταλλαγή μεγάλου αριθμού μηνυμάτων από όλους προς όλους ώστε να μπορεί να χρησιμοποιηθεί ένα κριτήριο πλειοψηφίας από κάθε στρατηγό.

# Λύσεις στο πρόβλημα των Βυζαντινών στρατηγών II

- Στην περίπτωση που όλα τα μηνύματα είναι μη αλλοιώσιμα (υπογράφονται από τον αποστολέα τους), το πρόβλημα είναι επιλύσιμο για πλήθος $m + 2$.
- Σε όλες τις περιπτώσεις έχει υποτεθεί πλήρης γράφος επικοινωνίας, δηλαδή ότι οποιοσδήποτε στρατηγός μπορεί να στείλει ένα μήνυμα απ' ευθείας σε οποιονδήποτε άλλον. Η λύση μπορεί να επεκταθεί σε ειδικές κατηγορίες γράφων.

# Practical Byzantine Fault Tolerance, I

Το 1999 οι Miguel Castro και Barbara Liskov[4] ανέπτυξαν τον αλγόριθμο *Practical Byzantine Fault Tolerance*, ο οποίος είναι πρακτικά εφαρμόσιμος σε ένα σύνολο μηχανών που επεξεργάζονται πολυάριθμα αιτήματα ανά μονάδα χρόνου και παρ΄ όλο που μπορούν να υποπέσουν σε βυζαντινά σφάλματα δίνουν απαντήσεις με αξιοπιστία στους πελάτες τους (clients).

- Υπάρχουν $n$ servers που εξυπηρετούν ένα πληθυσμό από clients.
- Οι απαντήσεις των servers προς τους clients είναι αξιόπιστες εφόσον οι προβληματικοί servers είναι το πολύ $\lfloor (n-1)/3 \rfloor$ το πλήθος.
- Οι αξιόπιστες μηχανές κατορθώνουν να παρέχουν μια υπηρεσία υπολογισμού σαν να εκτελούσε τους υπολογισμούς ένας και μοναδικός υπολογιστής (όλοι οι servers καταλήγουν στην ίδια σειρά εκτέλεσης των υπολογισμών - linearizability).

# Practical Byzantine Fault Tolerance, II

- Ο αλγόριθμος βασίζεται σε κρυπτογραφική προστασία των μηνυμάτων, ώστε να μην αλλοιώνονται κατά την επικοινωνία.
- Διατάσσει τα αιτήματα προκειμένουν να διασφαλίσει τη σειρά των υπολογισμών, βασίζεται σε πλειοψηφικές αποφάσεις και απαρτίες, και εφαρμόζει την πολλαπλή διάχυση των μηνυμάτων σε διατεταγμένα βήματα.

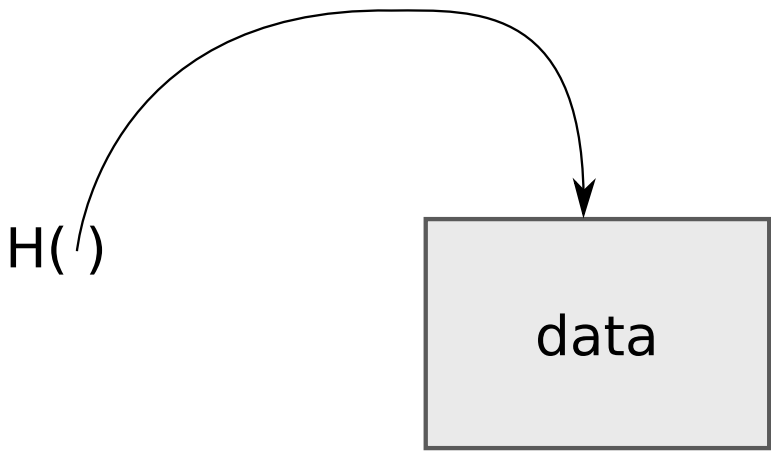
[4] Castro and Liskov 2002

# Συνάρτηση κατακερματισμού I

- Συνάρτηση κατακερματισμού (ή κατατεμαχισμού - hash function) είναι μια συνάρτηση που απεικονίζει μια σειρά συμβόλων (string) αυθαιρέτου μήκους σε μια σειρά με σταθερό μήκος (όχι απαραίτητα από το ίδιο σύνολο συμβόλων). Συνήθως η δεύτερη σειρά είναι μικρού και σταθερού μήκους.
- Αν κάποιος θέλει να προστατεύσει ένα κείμενο ή αρχείο από αλλοιώσεις μπορεί να αποθηκεύσει (με ασφαλή τρόπο) μια τιμή κατακερματισμού και κάθε φορά που εγείρεται αμφιβολία για την ακεραιότητα του κειμένου να επανυπολογίζεται η τιμή και να συγκρίνεται με την αποθηκευμένη.
- Μια συνάρτηση κατακερματισμού πρέπει να είναι μη αναστρέψιμη, δηλαδή αν δοθεί το $y = h(x)$: (α) να μη μπορεί να βρεθεί το $x$, (β) ένα $x'$ τέτοιο ώστε $y = h(x')$, (γ) ένα ζεύγος οιωνδήποτε διαφορετικών $x, y$ τέτοιων ώστε $h(x) = h(y)$.

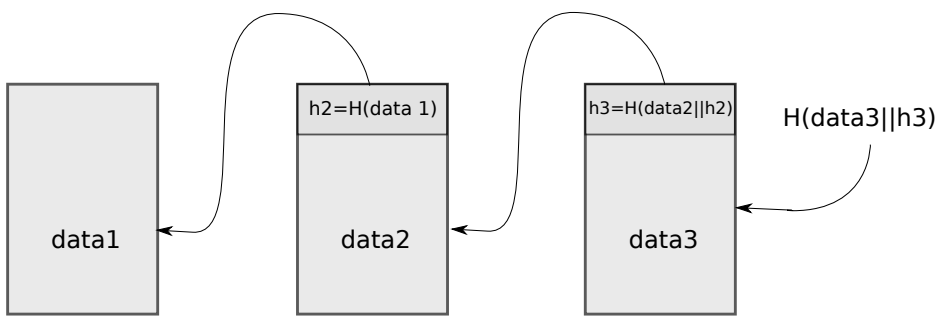
# Δείκτης κατακερματισμού

- Ο δείκτης κατακερματισμού είναι ένας δείκτης που δείχνει μια θέση στην οποία είναι αποθηκευμένες πληροφορίες, αλλά περιλαμβάνει επίσης ένα κωδικό κατακερματισμού για τις ίδιες πληροφορίες.
- Κατά συνέπεια ο δείκτης κατακερματισμού δίνει επί πλέον τη δυνατότητα επαλήθευσης της ακεραιότητας των πληροφοριών.



# blockchain

- Κατασκευάζουμε μια λίστα της οποίας το κάθε block περιέχει ένα δείκτη κατακερματισμού προς το προηγούμενο block.
- Άρα σε κάθε block υπάρχει επαλήθευση για το προηγ. block.
- Προϋπόθεση για τη διαφύλαξη της ακεραιότητας όλου του block chain είναι η ασφαλής φύλαξη του τελευταίου κάθε φορά κωδικού κατακερματισμού.
- Ένας επιτιθέμενος που θέλει να αλλάξει την πληροφορία σε ένα ενδιάμεσο block είναι υποχρεωμένος να αλλάξει τους κωδικούς σε όλα τα επόμενα, ως και τον τελικό κωδικό κατακερματισμού.



# Κατανεμημένο κατάστιχο και συμφωνία

- Όταν η Alice θέλει π.χ. να πληρώσει τον Bob, εκπέμπει προς το δίκτυο μια συναλλαγή

$$\texttt{pay to pk}_{Bob} : H(\,)$$

- Όλοι οι κόμβοι διαθέτουν ένα κατάστιχο, που περιλαμβάνει όλα τα blocks για τα οποία συμφωνούν.
- Επίσης, διαθέτουν ένα σύνολο από blocks, που έχουν φτάσει ως πληροφορία από άλλους κόμβους, αλλά δεν υπάρχει ακόμη συμφωνία. Το σύνολο αυτό μπορεί να διαφέρει από κόμβο σε κόμβο.
- Στη συνέχεια εκτελείται ένας αλγόριθμος που έχει σκοπό τη δημιουργία του επόμενου block από τις εκκρεμούσες συναλλαγές, για τις οποίες θα υπάρξει συμφωνία. Το block αυτό θα ενσωματωθεί στο κατάστιχο (blockchain ledger).

# Ο αλγόριθμος του Bitcoin

1. Οι νέες συναλλαγές εκπέμπονται προς όλους τους κόμβους.[5]
2. Κάθε κόμβος συλλέγει τις νέες συναλλαγές και τις συναρμολογεί σε ένα block.
3. Το νέο block περιέχει ένα δείκτη κατακερματισμού προς το προηγούμενο block, άρα συνεχίζει την αλυσίδα.
4. Σε κάθε γύρο επιλέγεται με τυχαίο τρόπο (*εξόρυξη*) ένας τυχαίος κόμβος που έχει το δικαίωμα να εκπέμψει το block του.
5. Οι άλλοι κόμβοι αποδέχονται το block μόνο εφόσον όλες οι συναλλαγές είναι νόμιμες, δηλαδή αντιστοιχούν σε ποσά που δεν έχουν δαπανηθεί και φέρουν νόμιμες υπογραφές.
6. Οι κόμβοι εκφράζουν την αποδοχή τους ως προς ένα block ενσωματώνοντας τον κωδικό κατακερματισμού του στο επόμενο block που θα δημιουργήσουν.

[5] Narayanan et al. 2016

# Ανταμοιβή σχηματισμού block

- Ο κόμβος που δημιουργεί ένα block έχει το δικαίωμα να προσθέσει μια ειδική συναλλαγή δημιουργίας νέων νομισμάτων πληρωτέων όπου νομίζει.
- Κατά συνέπεια έχει συμφέρον να θεωρηθεί το block του τίμιο, ώστε να παγιωθεί η ενσωμάτωσή του στο blockchain και να θεωρηθεί η αμοιβή του έγκυρη.
- Αυτός που προτείνει το νέο block θα μπορούσε να προσθέσει ψευδείς συναλλαγές (π.χ. πληρωμές από λογαριασμούς άλλων προς τον ίδιο).
- Τότε όμως διατρέχει τον κίνδυνο να απορριφθεί το block του, διότι οι άλλοι κόμβοι θα επιχειρήσουν να βάλουν ένα άλλο block πάνω στο τελευταίο και θα σχηματιστεί μια διχάλα.
- Μπορεί να επιβάλει την άποψή του μόνο αν διαθέτει πλειοψηφία (51% των κόμβων).

# «Τυχαία» επιλογή κόμβου - εξόρυξη

- Κάθε κόμβος που επιθυμεί να προτείνει ένα νέο block οφείλει να βρει ένα nonce (τυχαίο αριθμό) τέτοιο ώστε

$$H(\texttt{nonce} \parallel \texttt{prev hash} \parallel \texttt{tx} \parallel \texttt{tx} \parallel \texttt{tx} \parallel \ldots) < \epsilon,$$

  όπου `prev hash` είναι ο κωδικός κατακερματισμού του προηγούμενο block, και $\epsilon$ είναι αρκετά μικρό σε σύγκριση με το μέγεθος του συνόλου τιμών της συνάρτησης κατακερματισμού.
- Πόσο μικρό; Για τη δημιουργία ενός block χρειάζεται να υπολογισθούν $2^{32} \times \delta$ κωδ. κατακερματισμού, όπου $\delta$ είναι η *δυσκολία* (difficulty).[6] Στις αρχές του 2019 ήταν $\delta \approx 6 \times 10^{12}$.
- Η *δυσκολία* επαναπροσδιορίζεται ώστε ο μέσος χρόνος ανάμεσα στη δημιουργία διαδοχικών block να είναι ίσος με δέκα λεπτά. Ο σκοπός είναι να μπαίνει σε κάθε block περίπου σταθερό πλήθος συναλλαγών.

[6] `https://bitcoinwisdom.com/bitcoin/difficulty`

# Εφαρμογή του blockchain πέρα από τα κρυπτονομίσματα

- Η τεχνική του blockchain επιτρέπει την υλοποίηση ενός κατανεμημένου κατάστιχου (βλ. π.χ. Hyperledger project [Androulaki et al. 2018]).
- Επιτρέπει σε άτομα και εταιρίες να κάνουν συναλλαγές χωρίς ενδιάμεσους.
- Ωστόσο παραμένουν ανοιχτά ζητήματα ιδιωτικότητας (πόση πληροφορία πρέπει να αποκαλυφθεί για να επαληθευτεί μια συναλλαγή), κλιμάκωσης και διαλειτουργικότητας [Underwood 2016].
- Παραδείγματα τέτοιων εφαρμογών είναι ναυλώσεις πλοίων, κτηματολόγιο, παρακολούθηση προϊόντων σε στάδια επεξεργασίας με σκοπό την επαλήθευση της αυθεντικότητας.

# Βιβλιογραφία I

Elli Androulaki et al. "Hyperledger fabric: a distributed operating system for permissioned blockchains." In: *Proceedings of the Thirteenth EuroSys Conference*. ACM. 2018, p. 30.

Miguel Castro and Barbara Liskov. "Practical Byzantine fault tolerance and proactive recovery." In: *ACM Transactions on Computer Systems (TOCS)* 20.4 (2002), pp. 398–461.

I. Curiel. *Cooperative Game Theory and Applications: Cooperative Games Arising from Combinatorial Optimization Problems*. Theory and Decision Library C. Springer US, 2013.

Drew Fudenberg and Jean Tirole. *Game Theory*. MIT Press, 1991.

# Βιβλιογραφία II

Leslie Lamport, Robert Shostak, and Marshall Pease. "The Byzantine generals problem." In: *ACM Transactions on Programming Languages and Systems* 4.3 (July 1982), pp. 382–401.

Arvind Narayanan et al. *Bitcoin and cryptocurrency technologies: a comprehensive introduction*. Princeton University Press, 2016.

Sarah Underwood. "Blockchain beyond bitcoin." In: *Communications of the ACM* 59.11 (2016), pp. 15–17.