Τεχνολογίες Blockchain και Αποκεντρωμένες Εφαρμογές

Ι. Μαυρίδης, Π. Φουληράς
MSN Lab (http://msnlab.uom.gr)

Διάλεξη #06

Πώς λειτουργεί το Ethereum

Περιεχόμενα

- Από το BTC στο Ethereum
- Επισκόπηση του Blockchain στο Ethereum
- Έξυπνα Συμβόλαια στο Ethereum
- Το Οικοσύστημα του Ethereum

Από το BTC στο Ethereum (ETH)

- Το BTC εμφανίσθηκε το 2009 και μαζί του η τεχνολογία Blockchain
- Επειδή άντεξε στον χρόνο, οι άνθρωποι εμπιστεύθηκαν τις δυνατότητές του
- Το BTC είναι κρυπτονόμισμα μόνον για μεταφορά BTC από μία δνση σε μία άλλη
- Δημιουργήθηκαν και άλλα κρυπτονομίσματα

Το Ethereum ως Blockchain Νέας Γενιάς

- Σύντομα υπήρξαν σκέψεις και για άλλες εφαρμογές εκτός από απλές πληρωμές σε κρυπτονομίσματα
- Αρχικά έγιναν προσπάθειες:
  - είτε με διαφορετικό κώδικα BTC που να επιτρέπει κάτι τέτοιο,
  - είτε με χρήση νέας αλυσίδας από μπλοκ (blockchain)
- Τελικά πήγαμε σε νέα πλατφόρμα blockchain, γενικής χρήσεως, που ήταν το Ethereum

Σημαντική Σχέση Ethereum και ETH

- Κάθε εφαρμογή που χρησιμοποιεί την Δημόσια πλατφόρμα του Ethereum πρέπει να πληρώνει αμοιβή (σε ETH) για συναλλαγές σε αυτήν
- ETH είναι το αντίστοιχο κρυπτονόμισμα (Ether)
  - Ð: Με Λατινικό σύμβολο
  - Ξ: Με Ελληνικό σύμβολο
- Έτσι, η πλατφόρμα αυτή βγάζει τα έξοδά της (για τους ~~miners~~/validators) και είναι αυτάρκης

Θυμηθείτε…

- Κύρια Συστατικά Ανοικτής & Δημόσιας Πλατφόρμας Blockchain:
  1. Ένα δίκτυο P2P που συνδέει τους μετέχοντες και διαδίδει συναλλαγές και μπλοκ επιβεβαιωμένων συναλλαγών, βασιζόμενο σε ένα τυποποιημένο πρωτόκολλο “κουτσομπολιού”
  2. Μηνύματα, υπό μορφή Συναλλαγών (Transactions), που αναπαριστούν μεταβολές κατάστασης (State Transition – **S.T.**)
  3. Ένα σύνολο από Λογαριασμούς που περιέχουν την βασική μονάδα ανταλλαγής (Κρυπτονόμισμα) αξιών μεταξύ των συμμετεχόντων, καθώς και αμοιβών σε κόμβους για το προσφερόμενο έργο τους

Θυμηθείτε… (συνέχεια)

…συνέχεια:

5. Ένα Σύνολο κανόνων Συναίνεσης (Consensus): καθορίζει τι αποτελεί συναλλαγή και ορθή μεταβολή κατάστασης, συμπεριλαμβανομένων των περιπτώσεων διαφορετικών (προσωρινά) αποτελεσμάτων από τους μετέχοντες
6. Αλυσίδα μπλοκ, που αποτυπώνει με ασφαλή τρόπο το καθολικό όλων των επιβεβαιωμένων & αποδεκτών μεταβολών κατάστασης
7. Ένα σχέδιο παροχής κινήτρων, στέρεο από πλευράς Θεωρίας Παιγνίων (π.χ., κόστη μηχανισμού συναίνεσης PoW ☠ / PoS συν αμοιβές μπλοκ) για οικονομική διασφάλιση της κατάστασης μηχανής σε ανοικτό περιβάλλον
8. Μία ή περισσότερες υλοποιήσεις των παραπάνω σε λογισμικό ανοικτού κώδικα για τους κόμβους του συστήματος (“δίκτυο”)

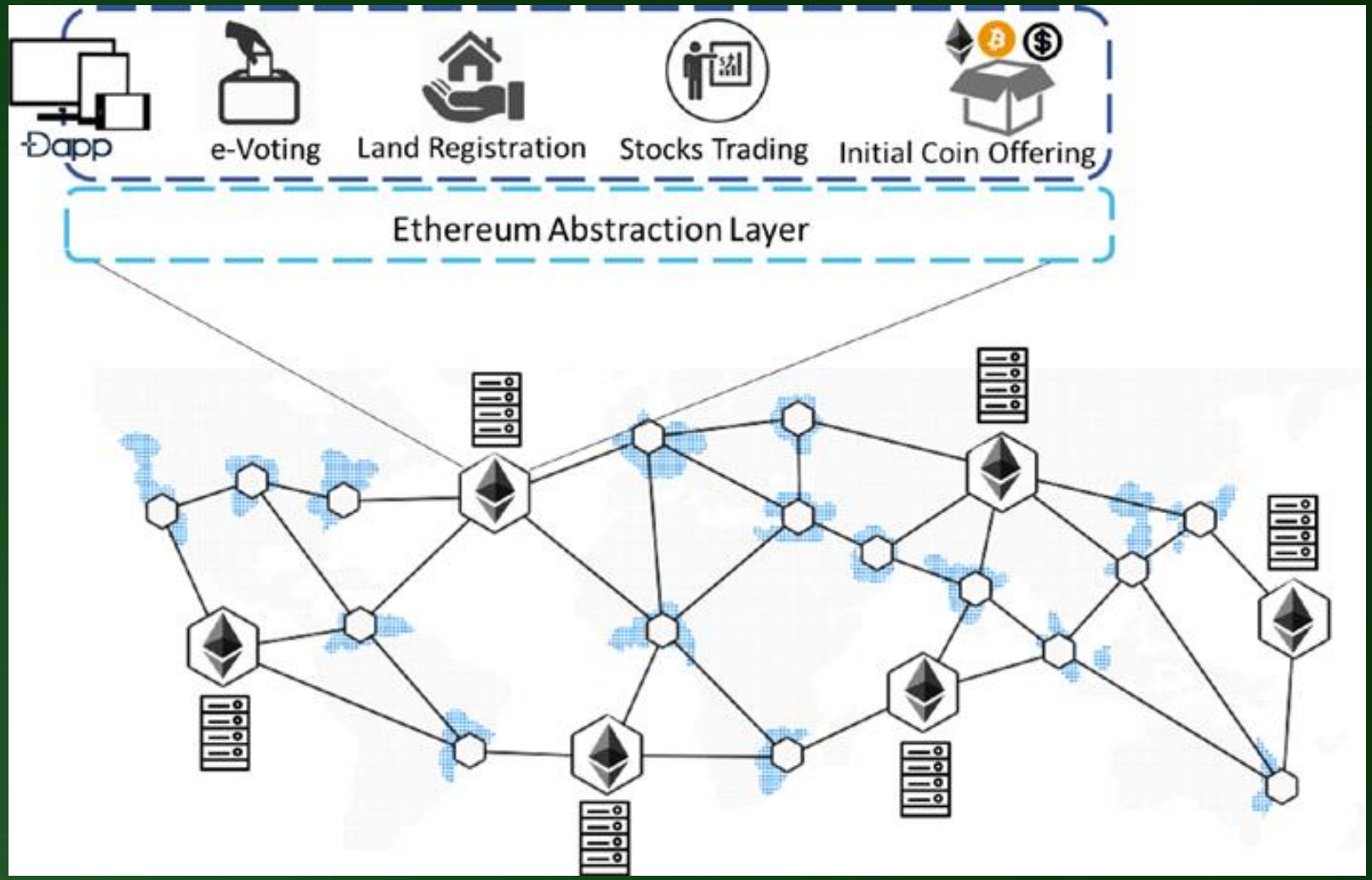
Φιλοσοφία Σχεδιασμού στο Ethereum

- Έχει δανεισθεί πολλά στοιχεία από BTC, αλλά σχεδιάσθηκε με διαφορετική φιλοσοφία, ακολουθώντας αρχές όπως:
  - Απλουστευμένος Σχεδιασμός
    - Αποκρύπτονται οι περισσότερες λεπτομέρειες υλοποίησης
  - Ελευθερία Ανάπτυξης
    - Κανένας περιορισμός ή προτίμηση σε εφαρμογές, εφόσον καταβάλουν αμοιβή συναλλαγής (*gas*)
  - Καμία Έννοια Ιδιαίτερων Χαρακτηριστικών
    - Απλά υποστηρίζει γλώσσες Turing-complete

Κάποια Ιστορικά Στοιχεία και Ορολογία

- Vitalik Buterin ο κύριος δημιουργός της πλατφόρμας Ethereum
- Το Ethereum ξεκίνησε την λειτουργία του στις 30 Ιουλίου 2015
- DApp = Decentralized Application (Αποκεντρωμένη Εφαρμογή)
- DeFi = Decentralized Financial System που υπάρχει στο Ethereum

Πολλαπλές DApp σε **Μία** Πλατφόρμα Ethereum



Κλειδιά στο Ethereum

- Υπάρχουν Ιδιωτικά Κλειδιά και Δημόσια Κλειδιά
- Μαζί με διευθύνσεις Ethernet και ψηφιακές υπογραφές συνθέτουν την ιδιοκτησία ενός λογαριασμού EOA
- Τα ιδιωτικά κλειδιά δεν χρησιμοποιούνται απ’ ευθείας στο Ethereum, ούτε καν αποθηκεύονται σε αυτό
- Πρόσβαση και έλεγχος πόρων επιτυγχάνεται μέσω ψηφιακών υπογραφών

Οδεύοντας προς το Web 3.0

- Σύμφωνα με τον Gavin Wood (συνιδρυτής Ethereum) έχουμε 3 φάσεις για τον Παγκόσμιο Ιστό (Web):
  - Web 1.0: Read-Only (1990-2004)
  - Web 2.0: Read-Write (2004-σήμερα)
    - Βασίζεται στην εμπιστοσύνη προς λίγες ιδιωτικές εταιρείες για ενέργειες που αποσκοπούν στο δημόσιο συμφέρον
  - Web 3.0: Read-Write-Own
    - Δεν εξαρτάται από τις εταιρείες παραπάνω (Web 2.0)

Βασικά Χαρακτηριστικά Web 3.0

- Αποκεντρωμένο: Ιδιοκτησία κατανέμεται μεταξύ των κατασκευαστών και των χρηστών του
- Χωρίς Άδεια: Κάθε ένας έχει ισότιμη πρόσβαση και κανείς δεν εξαιρείται
- Έχει ενσωματωμένες πληρωμές: Χρησιμοποιεί κρυπτονομίσματα για ξόδεμα και αποστολή χρημάτων online, αντί να βασίζεται στην παρωχημένη υποδομή τραπεζών και επεξεργαστών πληρωμών
- Χωρίς Εμπιστοσύνη: Λειτουργεί με κίνητρα και μηχανισμούς οικονομικών αντί να εξαρτάται από τρίτα μέρη κοινής εμπιστοσύνης

Άλλα Σημαντικά Στοιχεία

- web3.js: Βιβλιοθήκη JavaScript για διασύνδεση εφαρμογών JavaScript σε browsers με το Ethereum. Περιλαμβάνεται και διεπαφή με Swarm
- Swarm: Αποκεντρωμένο δίκτυο (P2P) αποθηκευτικού χώρου
  - Μαζί με Web3 χρησιμοποιείται συχνά για την δημιουργία DApp

ETH και Υποδιαιρέσεις

Τιμή (σε Wei)	Όνομα	Επίσημο Όνομα SI
1	Wei	Wei
10^3	Babbage	Kilowei ή femtoether
10^6	Lovelace	Megawei ή picoether
10^9	Shannon	Gigawei ή nanoether
10^{12}	Szabo	Microether ή micro
10^{15}	Finney	Milliether ή milli
10^{18}	Ether	Ether
10^{21}	Grand	Kiloether
10^{24}		Megaether

Από πού προέρχονται τα ETH;

- Αρχική διάθεση: 72 εκατομμύρια
- Mining: ~18 εκατομμύρια/έτος
- Δεν υπάρχει άνω όριο (σε αντίθεση με BTC που είναι 21 εκατομμύρια)

Τρέχουσα Κατάσταση

- "Ethereum in Numbers" (Προσπέλαση 25/11/2022):
  - Έργα κατασκευασμένα επάνω από Ethereum 2.970
  - Λογαριασμοί (πορτοφόλια) με περιεχόμενο > 71 εκατ.
  - Έξυπνα συμβόλαια επάνω από Ethereum 50,5 εκατ.
  - Αξία χρημάτων που διακινήθηκαν το 2021 $11,6 δισ.
  - Σύνολο αμοιβών από συναλλαγές το 2021 $9,92 δισ.

Τρία “Ethereum”

- Ethereum Classic
  - Τηρεί την αρχική ιστορία του Ethereum αναλλοίωτη
  - ETC το σύμβολο του νομίσματος και αποπληθωριστικό όπως το BTC
- Ethereum
  - Χωρίσθηκε από το αρχικό στις 20/07/2016, διαγράφοντας την κλοπή DAO (Decentralized Autonomous Organization), ουσιαστικά μία εταιρεία Venture Capital Fund, όπου εκλάπη σχεδόν το 1/3 των κεφαλαίων
  - Αρχικά μηχανισμός συναίνεσης PoW, πλέον PoS, μετά από “The Merge”
- Ethereum PoW
  - Από Miners του Ethereum που παρέμειναν σε μηχανισμό συναίνεσης PoW
  - ETHW το σύμβολο του νομίσματος μετά από “The Merge”

Ιστορικό Αναβαθμίσεων Ethereum

Protocol layer	Code name	Release date	Block no./ Beacon Chain epoch
Execution	Frontier	30 July 2015	0
Execution	Ice Age	8 September 2015	200.000
Execution	Homestead	15 March 2016	1.150.000
Execution	DAO fork	20 July 2016	1.920.000
Execution	Tangerine Whistle	18 October 2016	2.463.000
Execution	Spurious Dragon	23 November 2016	2.675.000
Execution	Byzantium	16 October 2017	4.370.000
Execution	Constantinople	28 February 2019	7.280.000
Execution	St. Petersburg	28 February 2019	7.280.000
Execution	Istanbul	8 December 2019	9.069.000

Protocol layer	Code name	Release date	Block no./ Beacon Chain epoch
Consensus	Phase 0	1 December 2020	0 (epoch)
Execution	Muir Glacier	2 January 2020	9.200.000
Execution	Berlin	15 April 2021	12.244.000
Execution	London	5 August 2021	12.965.000
Consensus	Altair	27 October 2021	74.240 (epoch)
Execution	Arrow Glacier	8 December 2021	13.773.000
Execution	Gray Glacier	30 June 2022	15,050,000
Consensus	Bellatrix	6 September 2022	144.896 (epoch)
Execution	Paris	15 Sept. 2022	15.537.394
Execution	Shanghai	TBD	TBD
Consensus	Capella	TBD	TBD

Από πού μπορούμε να λάβουμε ETH;

- Minting (Νομισματοκοπή) – νέο ETH δημιουργείται ως αμοιβή για:
  - κάθε κόμβο που προτείνει μπλοκ συναλλαγών που επικυρώνεται (1/8 αμοιβής)
  - κάθε κόμβο-Επικυρωτή (Validator) που επικυρώνει μπλοκ. Στην πράξη τα 7/8 της αμοιβής μοιράζονται μεταξύ των validators, ανάλογα με το ποσό που έχουν ποντάρει
- Από ήδη υπάρχοντα ETH, όπως:
  - φιλοδωρήματα (tips) σε αμοιβές συναλλαγών (Transaction Fees)
  - λόγω MEV (Maximal Extractable Value – η μέγιστη αξία ενός μπλοκ από συμπερίληψη, αναδιάταξη ή διαγραφή συναλλαγών σε αυτό, επάνω από την ελάχιστη αξία εκτέλεσής τους)
  - από κάποιον άλλον λογαριασμό Ethereum

“Burning” ETH

- Εκτός από δημιουργία νέου ETH, ήδη υπάρχον ETH καταστρέφεται μέσω της διαδικασίας “καύσεως” (“burning”)
  - Για κάθε συναλλαγή προβλέπεται αμοιβή που καταβάλλει ο χρήστης
  - Ανάλογα με την ζήτηση για συναλλαγές, ορίζεται αυτόματα από το Ethereum μία αμοιβή βάσης (base gas fee) που καταστρέφεται, εξυπηρετώντας δύο στόχους:
    - Ο παραγωγός προτεινόμενου μπλοκ δεν αυξάνει την αμοιβή βάσης για τους άλλους, βάζοντας δικές του συναλλαγές δωρεάν στο μπλοκ
    - Εάν καταστρέφεται περισσότερο ETH από όσο δημιουργείται έχουμε αποπληθωρισμό

Validators (Επικυρωτές)

- Μέχρι το συμβάν "The Merge", το Ethereum χρησιμοποιούσε PoW
- Τώρα πλέον PoS, όπου μόνον όσοι κόμβοι είναι Validators (Επικυρωτές) μπορούν (διαφορετικά υποσύνολα):
  - Να προτείνουν μπλοκ συναλλαγών
  - Να επικυρώνουν προταθέντα μπλοκ συναλλαγών
- Γενικά, προϋπόθεση για τέτοιον χαρακτηρισμό κόμβου είναι η δέσμευση τουλάχιστον 32 ETH

Περιεχόμενα

- Από το BTC στο Ethereum
- Επισκόπηση του Blockchain στο Ethereum
  - Λογαριασμοί, Κλειδιά & Διευθύνσεις
  - Συναλλαγές
  - Μπλοκ Συναλλαγών, Tries & Σχετικές Δομές, EVM
  - Gas
  - Κόμβοι και Πελάτες
  - Δίκτυα
  - Μηχανισμοί Συναίνεσης
- Έξυπνα Συμβόλαια στο Ethereum
- Το Οικοσύστημα του Ethereum

Λογαριασμοί Ethereum – (1)

- Το Ethereum είναι Stateful (Καταστασιακό), με βασική μονάδα τον Λογαριασμό (Account)
- Κάθε λογαριασμός έχει μία κατάσταση που σχετίζεται με αυτόν και μία διεύθυνση 20-byte (160-bit) ως ταυτότητα, που εκφράζεται στο 16-δικό σύστημα (προσθήκη '0x' στην αρχή), π.χ.:

  `0x21C7656EC7ab88b098defB751B7401B5f6d8978F`

- Στόχος του Blockchain στο Ethereum είναι να παρακολουθεί τις μεταβολές των καταστάσεων, μέσω των λογαριασμών

Λογαριασμοί Ethereum – (2)

- Υπάρχουν δύο κατηγορίες λογαριασμών:
  1. Externally-Owned Account (EOA)
     - Συνηθισμένος λογαριασμός χρήστη που ελέγχεται μέσω του ιδιωτικού του κλειδιού
  2. Contract Account (CA)
     - Λογαριασμός όπου αναρτάται (deployed) ένα έξυπνο συμβόλαιο. Ελέγχεται από τον κώδικά του

Λογαριασμοί Ethereum – (3)

- Και για τις δύο κατηγορίες λογαριασμών ισχύει ότι:
  - Μπορούν να λαμβάνουν, κρατούν και στέλνουν ETH και tokens
  - Μπορούν να διαδρούν με ήδη αναρτημένα (στο Ethereum) έξυπνα συμβόλαια

Λογαριασμοί Ethereum – (4)

- Αλλά έχουν και βασικές διαφορές:
  - Λογαριασμοί EOA:
    - Δωρεάν δημιουργία λογαριασμού
    - Μπορεί να εκκινεί συναλλαγές
    - Συναλλαγές μεταξύ τους μόνον για μεταφορές ETH/Tokens
    - Αποτελούνται από κρυπτογραφικό ζεύγος κλειδιών (δημόσιο και ιδιωτικό)

(συνεχίζεται…) ☞

Λογαριασμοί Ethereum – (5)

(συνέχεια…)

- Λογαριασμοί CA:
  - Δημιουργία στοιχίζει επειδή γίνεται δέσμευση χώρου στο Ethereum
  - ***Δεν*** μπορούν να εκκινήσουν συναλλαγές. Αυτό μπορεί να γίνει μόνον από EOA προς λογαριασμούς CA και από εκεί σε άλλους λογαριασμούς CA ή/και EOA
  - ***Δεν*** έχουν *ιδιωτικό κλειδί*, αλλά ελέγχονται από τον κώδικα των αντίστοιχων συμβολαίων

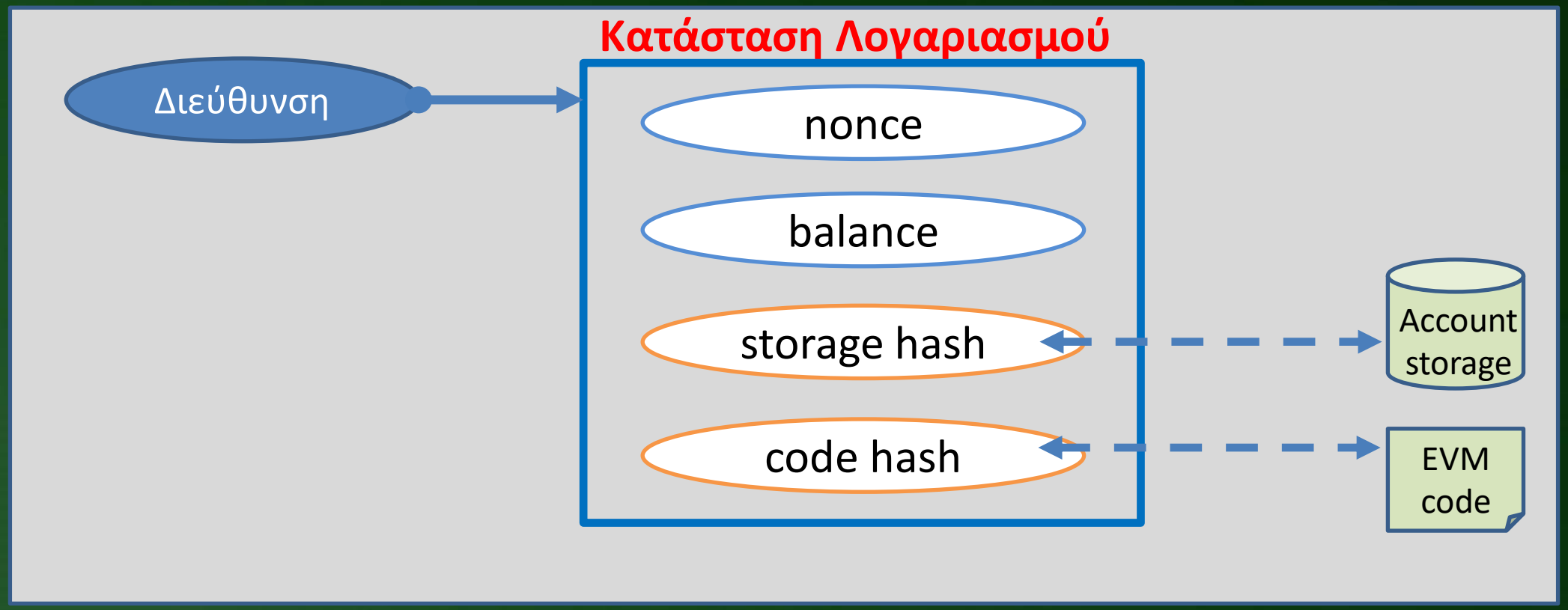
Προσοχή!

- Ένας λογαριασμός δεν είναι πορτοφόλι!
- Ένας λογαριασμός EOA είναι ουσιαστικά το ζεύγος κλειδιών του
- Ένα πορτοφόλι είναι μία διεπαφή ή εφαρμογή που επιτρέπει διάδραση με τον λογαριασμό μας Ethereum

Πεδία Λογαριασμού Ethereum

- **4 πεδία**, εκ των οποίων τα 2 τελευταία έχουν νόημα μόνον για CA:
  - nonce: Μετρητής
    1. Για EOA συναλλαγών που στάλθηκαν από τον λογαριασμό
    2. Για CA πλήθος συμβολαίων που δημιουργήθηκαν από τον λογαριασμό
  - balance: Υπόλοιπο λογαριασμού σε Wei (1 ETH = 10^{18} Wei)
  - codeHash: Hash για κώδικα EVM στο Ethereum Blockchain. Για EOA, η τιμή του πεδίου αυτού είναι το Hash της κενής συμβολοσειράς
  - storageRoot: Γνωστό και ως 'storage hash'. Είναι το Hash 256-bit του κόμβου root ενός Merkle Patricia Trie (MPT) που κωδικοποιεί τα περιεχόμενα του αποθηκευτικού χώρου του λογαριασμού. Εξ ορισμού, κενό

Πεδία Λογαριασμού Ethereum



Κλειδιά Λογαριασμών ΕΟΑ

- Κάθε λογαριασμός ΕΟΑ σχετίζεται με δύο κλειδιά:
  - Ένα ιδιωτικό, μήκους 32 byte, σχεδόν πάντα με τυχαίο τρόπο
  - Ένα δημόσιο, που προκύπτει από το ιδιωτικό με χρήση του αλγορίθμου ECDSA (Elliptic Curve Digital Signature Algorithm). Από 1 ιδιωτικό κλειδί μπορούν να προκύψουν πολλά δημόσια, αλλά όχι το αντίστροφο

Δημόσια Κλειδιά

- Στο Ethereum κάθε δημόσιο κλειδί μπορεί να δημιουργηθεί από ένα ιδιωτικό κλειδί (αλλά όχι το αντίστροφο), μέσω πολλαπλασιασμού σημείου ελλειπτικής καμπύλης (ουσιαστικά πρόσθεσης), σύμφωνα με το πρότυπο `secp256k1`
  - Δηλαδή, το λεγόμενο σημείο *G* (Generator point, 256-bit), που είναι το ίδιο για όλες τις υλοποιήσεις στο Ethereum, προστίθεται με τον εαυτό του τόσες φορές όση η τιμή του ιδιωτικού κλειδιού (τυχαίος αριθμός)
  - Αφού οι δύο αυτοί αριθμοί είναι 256 bit ή 32 byte ο κάθε ένας, το τελικό αποτέλεσμα θα είναι 512 bit ή 64 byte για το δημόσιο κλειδί
  - Στην πράξη, στο Ethereum, το Δημόσιο κλειδί είναι 65 byte γιατί τοποθετείται πρώτο (πιο σημαντικό) το byte 0x04

Λογαριασμοί CA

- Έχουν και αυτοί συνολικό μήκος 20 byte
- Αφού δεν έχουν ιδιωτικό κλειδί η διεύθυνσή τους προκύπτει από την διεύθυνση του δημιουργού τους και τον αριθμό συναλλαγών που έχουν σταλεί από αυτόν (τιμή πεδίου ‘nonce’ του δημιουργού)

Κλειδιά των Επικυρωτών

- Υπάρχουν πλέον οι κόμβοι-Επικυρωτές (Validators)

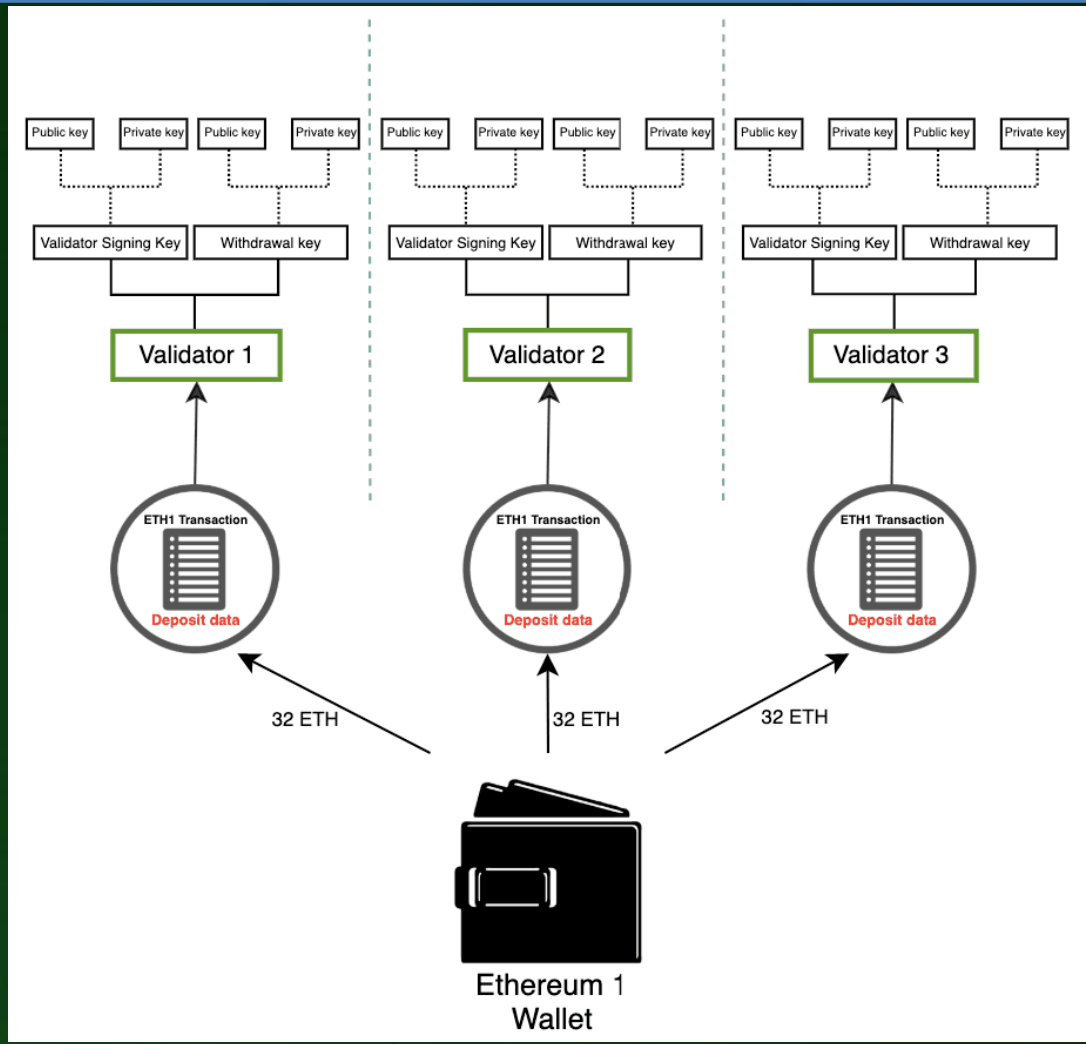
- Για να διακρίνονται από τους υπόλοιπους υπάρχουν ειδικά κλειδιά τύπου BLS (Boneh–Lynn–Shacham), δύο τύπων:
  - Κλειδιά Validator
  - Κλειδιά Withdrawal

Validator Key

- Στόχος ύπαρξης η υπογραφή προτεινόμενων μπλοκ και επικυρώσεων. Εδώ έχουμε:
  - Ιδιωτικό κλειδί Validator
  - Δημόσιο κλειδί Validator. Περιλαμβάνεται στην συναλλαγή μέσω της οποίας ο υποψήφιος Επικυρωτής καταθέτει ETH (deposit data) στο αντίστοιχο συμβόλαιο, επιτρέποντας στο Ethereum να τον αναγνωρίζει ως τέτοιον (Επικυρωτή)

Withdrawal Key

- Στόχος ύπαρξης η μετακίνηση υπολοίπου λογαριασμού του αντίστοιχου Επικυρωτή (Validator) στην μελλοντική αναβάθμιση “Shanghai” του Ethereum, ώστε ένας χρήστης να ελέγχει πολλαπλούς Επικυρωτές
- Εδώ έχουμε:
  - Ιδιωτικό κλειδί Withdrawal. Εάν χαθεί, μπορεί να συνεχίσει επικυρώσεις, αλλά δεν θα έχει κίνητρο να το κάνει
  - Δημόσιο κλειδί Withdrawal



Διευθύνσεις στο Ethereum – (1)

- Προσοχή: Άλλο Διεύθυνση Ethereum και άλλο Διεύθυνση/Ταυτότητα Κόμβου σε αυτό
- Κάθε Διεύθυνση Ethereum αποτελεί μοναδικό αναγνωριστικό (unique identifier) που προκύπτει από εφαρμογή Keccak-256 (`secp256k1`) Hash στο Δημόσιο Κλειδί του EOA ή του CA
- Κάθε Διεύθυνση Ethereum έχει μήκος 20 byte. *Πώς γίνεται αυτό;*

Διευθύνσεις στο Ethereum – (2)

- Keccak256 (Δημόσιο Κλειδί χωρίς το πρώτο byte 0x04) = Αποτέλεσμα

  64 byte 32 byte

- Από τα παραπάνω 32 byte κρατάμε τα τελευταία (λιγότερο σημαντικά) **20 byte** που είναι και η διεύθυνση Ethereum (συγκρίνετε με δνσεις IPv6 που έχουν μέγεθος 16 byte)

- Υπάρχουν και οι εναλλακτικές αναπαραστάσεις Διευθύνσεων Ethereum που χρησιμοποιούνται από πορτοφόλια σύμφωνα με τα πρότυπα ICAP, EIP-55

Περιεχόμενα

- Από το BTC στο Ethereum
- Επισκόπηση του Blockchain στο Ethereum
  - Λογαριασμοί, Κλειδιά & Διευθύνσεις
  - Συναλλαγές
  - Μπλοκ Συναλλαγών, Tries & Σχετικές Δομές, EVM
  - Gas
  - Κόμβοι και Πελάτες
  - Δίκτυα
  - Μηχανισμοί Συναίνεσης
- Έξυπνα Συμβόλαια στο Ethereum
- Το Οικοσύστημα του Ethereum

Συναλλαγές: Εισαγωγή – (1)

- Συναλλαγές στο Ethereum είναι ψηφιακά υπογεγραμμένα μηνύματα που:
  1. Ξεκινούν πάντοτε από έναν λογαριασμό EOA
  2. Μεταδίδονται στο δίκτυο του Ethereum
  3. Καταγράφονται στο Ethereum blockchain

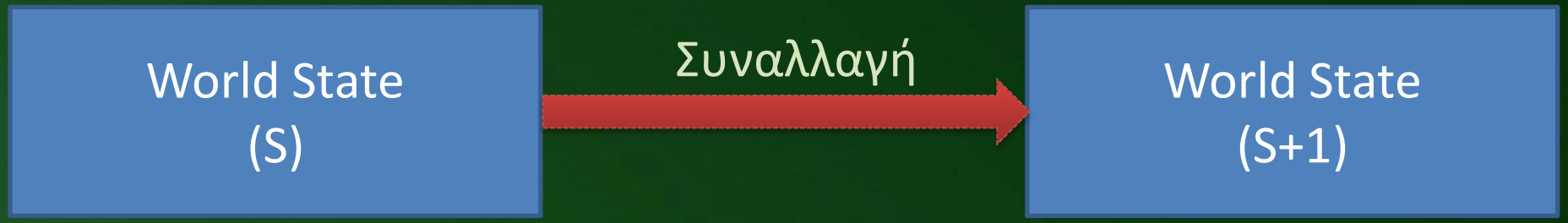
- Προσοχή όμως:
  - Η καταγραφή δεν είναι κρυπτογραφημένη ώστε όλοι οι κόμβοι-Επικυρωτές (Validators) να μπορούν να επικυρώσουν την κάθε συναλλαγή
  - Τα Συμβόλαια δεν εκτελούνται από μόνα τους. Μόνον μετά από κατάλληλη συναλλαγή προς αυτά

Συναλλαγές: Εισαγωγή – (2)

- Συναλλαγές που μεταβάλλουν την κατάσταση της EVM, χρειάζεται να εκπέμπονται σε όλο το δίκτυο
- Οιοσδήποτε κόμβος μπορεί να ζητήσει την εκτέλεση κάποιας συναλλαγής
- Όμως μόνον ένας κόμβος-Επικυρωτής εκτελεί την συναλλαγή και διαδίδει την μεταβληθείσα κατάσταση σε όλο το υπόλοιπο δίκτυο
- Κάθε συναλλαγή απαιτεί και την αντίστοιχη αμοιβή που πρέπει να περιλαμβάνεται στο αντίστοιχο επικυρωμένο μπλοκ (συναλλαγών)

Τι είναι μία Συναλλαγή;

- Μία συναλλαγή (transaction) ξεκινά με ένα μήνυμα από αποστολέα, αλλά δεν ολοκληρώνεται εάν δεν επικυρωθεί, εγγραφόμενη οριστικά στο κατανεμημένο καθολικό (άρα από όλους τους κόμβους)
  - Τότε έχουμε ουσιαστικά μεταβολή στην World (Global) State του Ethereum



- Μέχρι τότε είναι σαν να έχουμε ζητήσει να γίνει μία συναλλαγή δεσμεύοντας το αντίστοιχο ποσό από πλευράς μας, αλλά εάν δεν ολοκληρωθεί (με οριστική επικύρωση), είναι ακόμα εκκρεμής

Πεδία Συναλλαγής – (1)

- Κάθε συναλλαγή πρέπει να περιλαμβάνει τα παρακάτω πεδία:
  - to (recipient) – η δνση παραλήπτη. Εάν EOA, η συναλλαγή μεταφέρει κάποιο ποσό. Εάν CA, η συναλλαγή εκτελεί τον κώδικα του συμβολαίου
  - signature – η ταυτότητα του αποστολέα. Γεννάται όταν το ιδιωτικό κλειδί του υπογράφει συναλλαγή, επιβεβαιώνοντας εξουσιοδότησή του
  - nonce – ακέραιος (αυξανόμενος) μετρητής του πλήθους συναλλαγών από τον συγκεκριμένο αποστολέα
  - value – ποσό μεταφοράς ETH από αποστολέα → παραλήπτη (σε WEI)

Πεδία Συναλλαγής – (2)

…συνέχεια:

- data – προαιρετικό πεδίο για συμπερίληψη οιωνδήποτε δεδομένων (για συμβόλαια). Όταν ζητείται δημιουργία νέου CA, παραμένει κενό
- gasLimit – μέγιστο ποσό σε μονάδες gas για την συγκεκριμένη συναλλαγή που θέλει να καταβάλει ο χρήστης
- maxPriorityFeePerGas – μέγιστο ποσό gas ως φιλοδώρημα στον Validator
- maxFeePerGas – μέγιστο ποσό gas που είναι διατεθειμένος ο αποστολέας να πληρώσει για την συναλλαγή (συμπεριλαμβανομένων των baseFeePerGas και maxPriorityFeePerGas)

Παράδειγμα Αντικειμένου Συναλλαγής

```
{
   from:              "0xEA674fdDe714fd979de3EdF0F56AA9716B898ec8",
   to:                "0xac03bb73b6a9e108530aff4df5077c2b3d481e5a",
   gasLimit:          "21000",
   maxFeePerGas:                  "300",
   maxPriorityFeePerGas:          "10",
   nonce:                         "0",
   value:                         "10000000000"
}
```

Παράδειγμα Αντικειμένου Υπογεγραμμένης Συναλλαγής


```
{
  "jsonrpc": "2.0",
  "id": 2,
  "result": {
    "raw":
"0xf883800182033394 07a565b7ed
2885bedbb695fe080a44401a6e400
0000000000000000000000000000
0001226a0223a7c9bcf5531c99be5
0cfe0bbc322e97cc5c7f71ab8b20ea
bb15bc42d9c09de4a6754e7000908
71491663",
  }
} ΣΥΝΕΧΕΙΑ →
```

```
"tx": {
      "nonce": "0x0",
      "maxFeePerGas": "0x1234",
      "maxPriorityFeePerGas": "0x1234",
      "gas": "0x55555",
      "to": "0x07a565b7ed7d7a678680a4c162885bedbb695fe0",
      "value": "0x1234",
      "input": "0xabcd",
      "v": "0x26",
      "r": "0x223a7c9bcf5531c99be5ea7082183816eb20cfe0bbc322e97cc5c7f71ab8b20e",
      "s": "0x2aadee6b34b45bb15bc42d9c09de4a6754e7000908da72d48cc7704971491663",
      "hash": "0xeba2df809e7a612a0a0d444ccfa5c839624bdc00dd29e3340d46df3870f8a30e"
    }
  }
}
```

Μερικές Λεπτομέρειες – (1)

- tx – η υπογεγραμμένη συναλλαγή σε μορφή JSON
- hash – το Hash της υπογραφής, μέσω του οποίου μπορεί να αποδειχθεί κρυπτογραφικά ότι προήλθε από τον συγκεκριμένο αποστολέα

Μερικές Λεπτομέρειες – (2)

- nonce: Εάν κάποιος κόμβος λάβει συναλλαγή από αποστολέα-λογαριασμό με τιμή nonce *k*+1, θα την αγνοήσει έως ότου λάβει την συναλλαγή από τον ίδιο με nonce *k*. Επίσης αποτρέπει *Replay Attacks*

- Ερώτηση: Εάν σταλούν 2 συναλλαγές με ίδιο nonce, αλλά διαφορετικό ποσό;
- Απάντηση: Αποδεκτή θα γίνει από κόμβο-παραλήπτη όποια ληφθεί πρώτη

Μερικές Λεπτομέρειες – (3)

- raw: Πριν αποσταλεί ένα μήνυμα συναλλαγής, πρώτα υπογράφεται ψηφιακά, και μαζί με την υπογραφή γίνεται serialization, χρησιμοποιώντας την μέθοδο κωδικοποίησης RLP (Recursive Length Prefix)
- Στην αρχή κάθε πεδίου εισάγεται ως πρόθεμα το μήκος του κάθε πεδίου
- Κάθε αριθμός αναπαρίσταται σε μορφή Big Endian

Μερικές Λεπτομέρειες – (4)

- *v, r, s*: Τιμές που αντιστοιχούν στην ψηφιακή υπογραφή ECDSA (Elliptic Curve Digital Signature Algorithm) της συναλλαγής
- Ερώτηση: Μήπως ξεχάσαμε το πεδίο from; Πώς ξέρει ο παραλήπτης της συναλλαγής, ποιος είναι ο αποστολέας;
- Απάντηση: Όχι! Από τα στοιχεία *v*, *r*, *s* της ψηφιακής υπογραφής ECDSA μπορεί ο παραλήπτης να εξάγει το *Δημόσιο Κλειδί* του αποστολέα και από αυτό την *Διεύθυνση* του αποστολέα

Μερικές Λεπτομέρειες – (5)

- Ερώτηση: Εάν ο παραλήπτης λογαριασμός είναι τύπου CA, τότε πώς γνωρίζει ο αποστολέας μέχρι πόσα ETH θα χρειασθεί να πληρώσει;
- Απάντηση: Η χρέωση του λογαριασμού αποστολέα γίνεται μετά από την επικύρωση (εκτέλεση) της συναλλαγής. Εάν η συναλλαγή έχει να κάνει με CA, τότε χρεώνεται όσο χρειάζεται, π.χ.:
  - Κώδικας συμβολαίου καλείται 9 φορές με χρέωση α, αλλά την $10^{η}$ η χρέωση είναι μεγαλύτερη. Θα χρεωθεί ο λογαριασμός αποστολέα για τις 9 συναλλαγές, αλλά εάν δεν φθάνει το υπόλοιπό του για την $10^{η}$ συναλλαγή, η $10^{η}$ δεν θα εκτελεσθεί (αρά και δεν θα επικυρωθεί)

Μερικές Λεπτομέρειες – (6)

- Εάν στείλουμε ETH σε μία δνση λογαριασμού (θυμηθείτε 20 byte), κατά λάθος, και δεν την κατέχει κανείς, το ποσό αυτό «καίγεται»

- Πεδία value και data:
  - Συναλλαγή με μόνον το πεδίο value, θεωρείται πληρωμή (μεταφορά στον λογαριασμό-παραλήπτη)
  - Συναλλαγή με μόνον το πεδίο data, θεωρείται κλήση σε συμβόλαιο
  - Συναλλαγή και με τα δύο πεδία, θεωρείται και πληρωμή (μεταφορά στον λογαριασμό-παραλήπτη) και κλήση σε συμβόλαιο
  - Συναλλαγή με κανένα από τα δύο πεδία, σπατάλη gas!

Μερικές Λεπτομέρειες – (7)

- Εάν στείλουμε συναλλαγή σε διεύθυνση κάποιου CA, η EVM θα εκτελέσει το συμβόλαιο καλώντας την συνάρτηση που ονομάσαμε στο πεδίο data
- Ερώτηση: Εάν δεν υπάρχει πεδίο data στην συναλλαγή μας;
  - Απάντηση: Τότε η EVM θα καλέσει μία συνάρτηση *fallback*. Εάν η συνάρτηση αυτή είναι χρεώσιμη (για τον αποστολέα), θα την εκτελέσει. Εάν τέτοια συνάρτηση δεν υπάρχει, απλά θα αυξήσει το υπόλοιπο ETH που διαθέτει το συμβόλαιο με το ποσό που απεστάλη από την συναλλαγή μας
- Ερώτηση: Μπορεί ένα συμβόλαιο να απορρίψει εισερχόμενες πληρωμές;
  - Απάντηση: Εάν έτσι ορίζουν οι όροι του, φυσικά και μπορεί

Τύποι Συναλλαγών

- Κανονικές: συναλλαγή από έναν λογαριασμό σε άλλον
- Ανάπτυξης Συμβολαίου (contract deployment): συναλλαγή χωρίς δνση στο πεδίο to, όπου το πεδίο data χρησιμοποιείται για τον λογαριασμό συμβολαίου
- Εκτέλεσης συμβολαίου: συναλλαγή που διαδρά με ήδη αναπτυγμένο (deployed) έξυπνο συμβόλαιο, οπότε η δνση στο πεδίο to είναι η δνση του συμβολαίου αυτού

Τι είναι το Gas

- Κάθε συναλλαγή έχει κόστος που αποτιμάται σε “Gas”
  - Η λογική είναι ίδια π.χ. κάποιο αυτοκίνητο καταναλώνει 10 lt βενζίνης για να διανύσει 100 km
- Έτσι μπορούν να είναι σταθερές οι ποσότητες gas για κάθε ενέργεια και να μεταβάλλεται η τιμή του gas (σε ETH)
- Απλές συναλλαγές μεταφοράς απαιτούν 21.000 μονάδες gas

Παράδειγμα Απλής Συναλλαγής

- Για να στείλει ο Bob στην Alice 1 ETH, εάν baseFeePerGas = 190 gwei και maxPriorityFeePerGas = 10 gwei, πρέπει να ξοδέψει επιπρόσθετα για αμοιβές: (190 + 10) * 21.000 = 4.200.000 gwei ή 0,0042 ETH
- Άρα θα έχουμε:
  - Ο λογαριασμός του Bob θα χρεωθεί (-1,0042 ETH)
  - Ο λογαριασμός της Alice θα πιστωθεί (+1,0 ETH)
  - Η αμοιβή βάσης (base fee) θα “καεί” (-0,00399 ETH)
  - Ο Validator θα λάβει φιλοδώρημα (+0,000210 ETH)
- Ό,τι δεν ξοδεύεται επιστρέφεται στον αποστολέα (συχνό για CA)

Κύκλος Ζωής Συναλλαγής

- Τι συμβαίνει όταν υποβληθεί μία συναλλαγή:
  - Δημιουργείται το Hash της συναλλαγής (κρυπτογραφικά)
  - Η συναλλαγή εκπέμπεται (*flooding*) στο δίκτυο και περιλαμβάνεται σε ένα "pool" μαζί με άλλες (ανεπικύρωτες) συναλλαγές
  - Ένας Validator πρέπει να επιλέξει την συναλλαγή για συμπερίληψη σε ένα μπλοκ ώστε να επικυρωθεί και να θεωρηθεί επιτυχής. Ποτέ δεν επικυρώνεται μία συναλλαγή, αλλά μπλοκ συναλλαγών
  - Με το πέρασμα του χρόνου το παραπάνω μπλοκ αναβαθμίζεται σε "justified" και κατόπιν σε "finalized". Τότε δεν αλλάζει, εκτός από περίπτωση επίθεσης που θα στοίχιζε τεράστιο ποσό στον επιτιθέμενο

Ειδικές Συναλλαγές

- Για «κάψιμο» ETH από πρόθεση συνίσταται η αποστολή στην δνση:

  `0x000000000000000000000000000000000000dEaD`

- ΠΡΟΣΟΧΗ: Αυτά τα ETH δεν έχουν σχέση με τα ETH/Wei που πρέπει να στείλουμε ως gas για την συναλλαγή (αμοιβή δικτύου Ethereum)

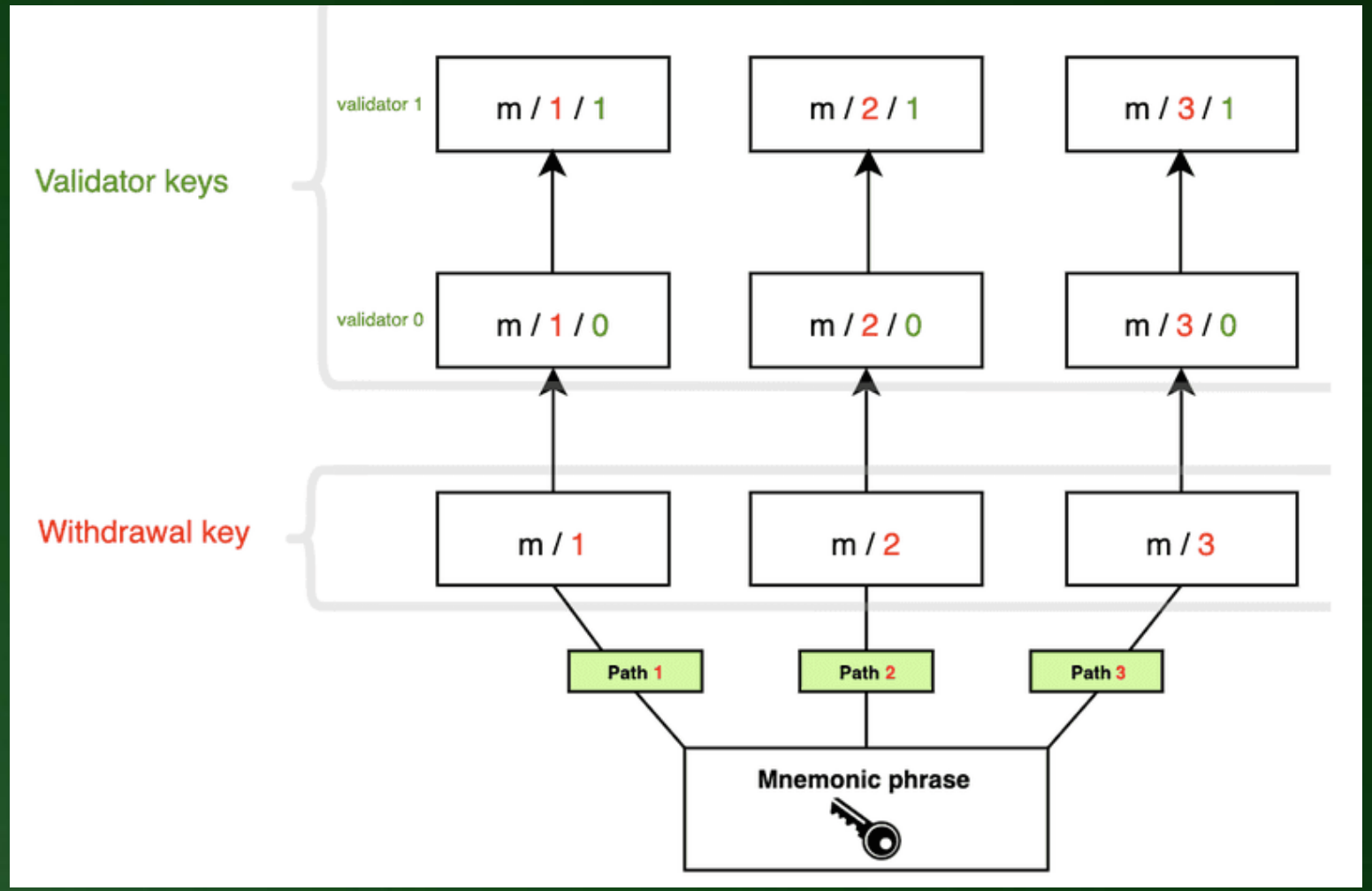
Λογαριασμοί, Κλειδιά & Πορτοφόλια

- Εάν έχουμε 10 λογαριασμούς, χρειαζόμαστε 10 ζεύγη κλειδιών
- Υπάρχουν 2 τύποι πορτοφολιών:
  - JBOK ("Just a Bunch Of Keyes") wallets
    - Nondeterministic (άσχετα μεταξύ τους κλειδιά)
  - Deterministic wallets
    - Υπάρχει ένα Master Key ("Seed") και από αυτό προκύπτουν τα υπόλοιπα
    - Η πιο διαδεδομένη μέθοδος (BIP-32/BIP-44) δημιουργεί μία δενδροειδή δομή εξαρτώμενων μεταξύ τους κλειδιών, ενώ το Seed κωδικοποιείται ως ένα υποσύνολο από Αγγλικές λέξεις που προέρχονται από ένα συγκεκριμένο μεγάλο τυποποιημένο σύνολο τέτοιων λέξεων (BIP-39)

Δημιουργώντας Κλειδιά από Φράση-“Φύτρα” (Seed) – (1)

- Για κάθε Validator θα χρειαζόταν 32 ETH, με νέο σετ από 2 πλήρως ανεξάρτητα κλειδιά $\Rightarrow$ μη κλιμακούμενο για μεγάλο πλήθος ελεγχόμενο από έναν χρήστη
  - Με μία μόνον μυστική φράση (mnemonic phrase) μπορούν να προκύψουν ένα ιδιωτικό κλειδί, που συνδυαζόμενο με πρόσθετα δεδομένα δημιουργείται ένα “master key”
  - Αυτό αποτελεί την ρίζα ενός λογικού δένδρου για την δημιουργία περαιτέρω κλειδιών, όπως έχουμε δει για πορτοφόλια σαν το MetaMask

Δημιουργώντας Κλειδιά από Φράση-“Φύτρα” (Seed) – (2)



Ερωτήσεις