

NEO & .NET Joint Meetup

Developing on the NEO Blockchain



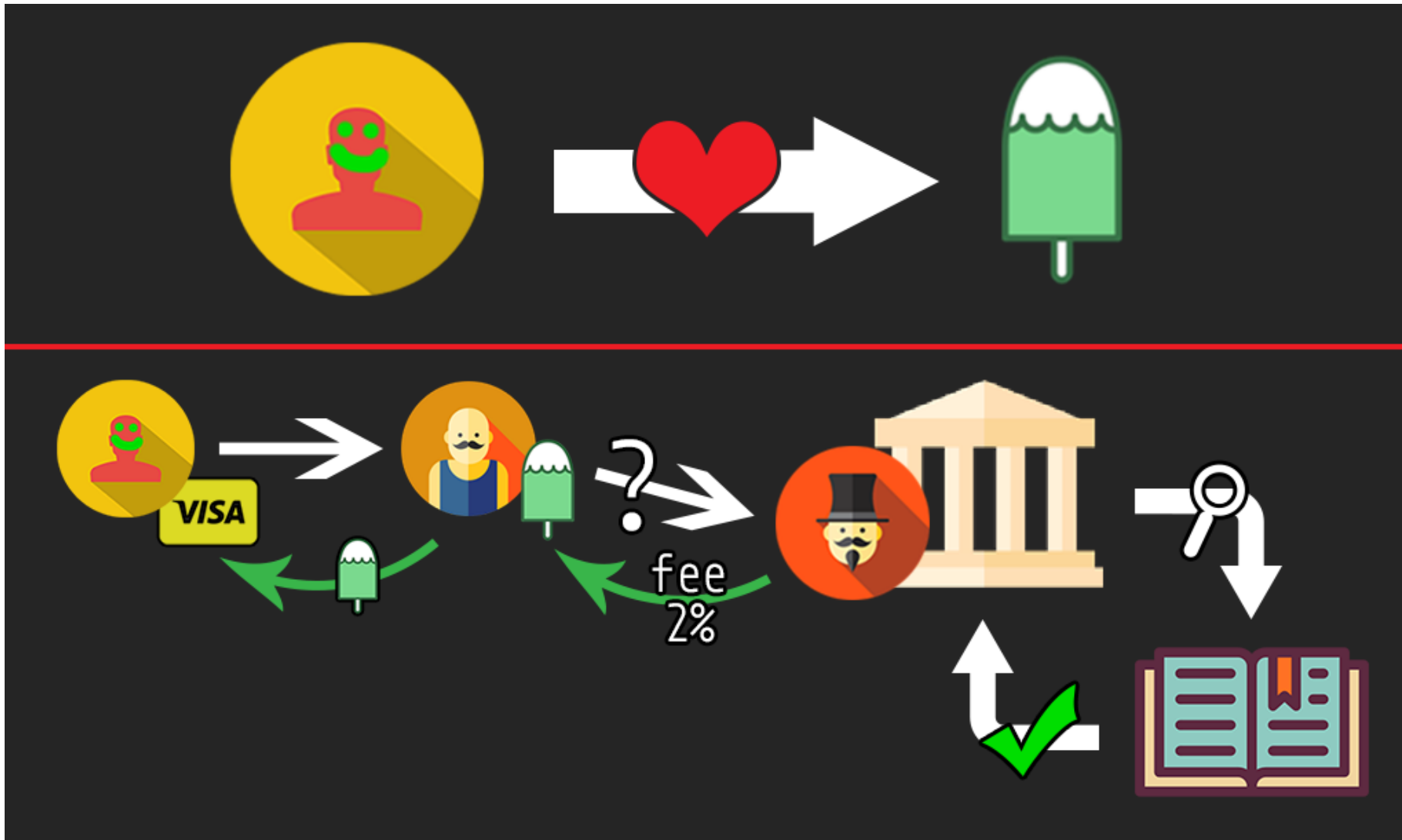
Presented by

D. Sfounis, S. Kourtzanidis, K. Karasavvas

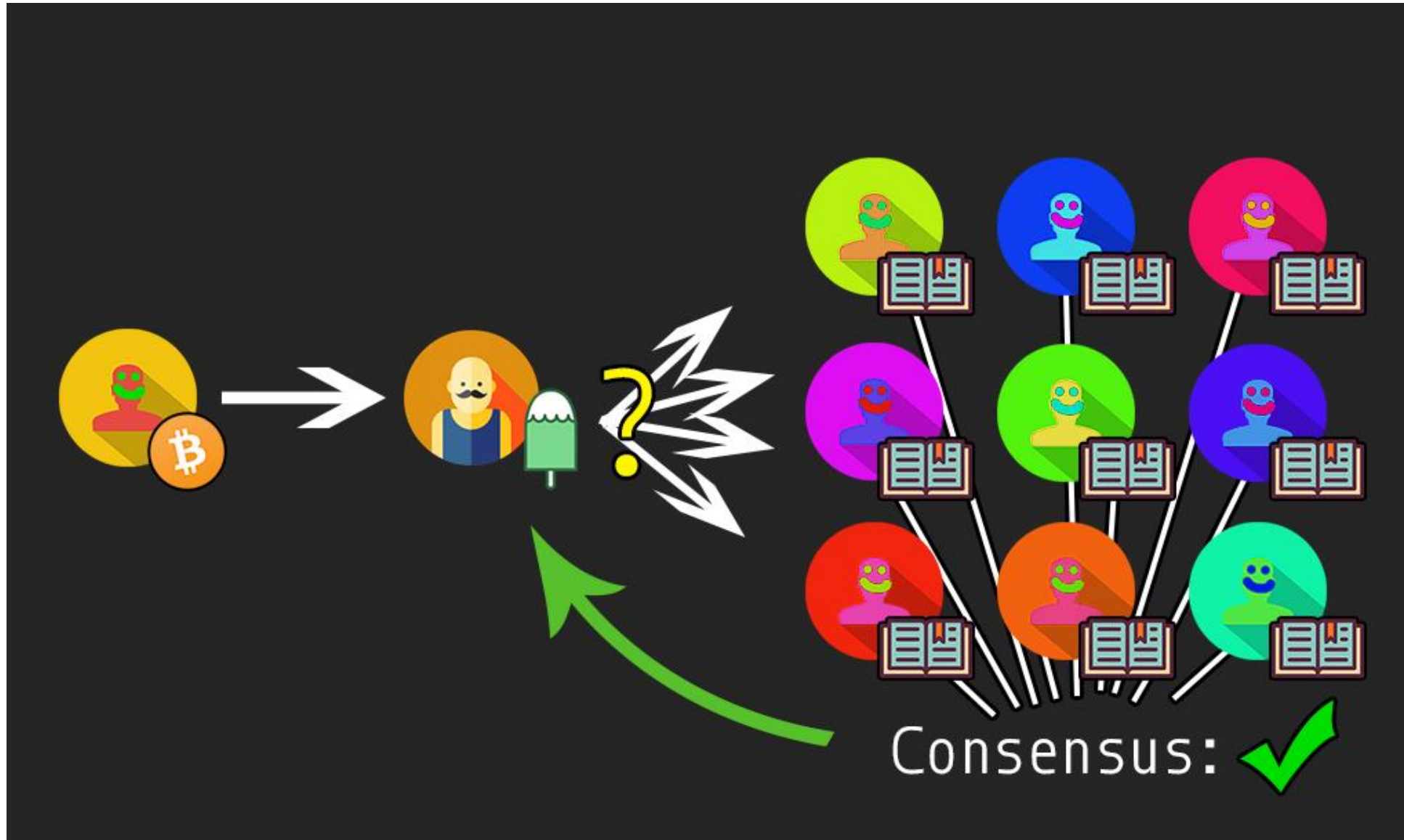
Μέρος 1^ο - Θεωρία

- Τι είναι blockchain, τι είναι το NEO.
 - Αρχιτεκτονική blockchain
 - Trustlessness και διαφορά από παραδοσιακά οικονομικά συστήματα
- Proof of Work & Proof of Stake
 - Επίλυση προβλήματος validation
 - Ασφάλεια & Mining
 - Scaling
- Η προσέγγιση του NEO
 - dBFT αντί για PoW/PoS
 - Open-source

Παράδειγμα ενός transaction σε παραδοσιακό οικονομικό σύστημα



Εξαφανίζοντας τον μεσάζοντα μέσω group consensus



Πως σιγουρεύεται το σωστό Consensus? Validation

- 2 πιο διάσημοι αλγόριθμοι για consensus:
 - Proof of Work (PoW)
 - Prove you worked to confirm the block, get a reward.
 - Proof of Stake (PoS)
 - Prove you want the block to be valid by having a lot to lose if it isn't.

Validity της αλυσίδας και Ασφάλεια

Proof of Work

- Δύσκολο αλλά «τίμιο»
- Κοστοβόρο mining
 - 2018: 61 TWh, λίγο περισσότερο από την συνολική ετήσια κατανάλωση ρεύματος της Σερβίας (!)
 - Προσοχή στα extrapolations
- Verifiable από φυσικές μεθόδους
 - Νόμος του Bayes, νόμοι της Θερμοδυναμικής

Proof of Stake

- Ελαφρύ αλλά non-deterministic
- Δεν δίνει κίνητρο στους έχοντες να «κινήσουν» το νόμισμά
- Minting αντί για mining, ανοίγεσαι σε short-range + long-range attacks, Sybil attacks (περισσότερο από PoW)

PoS v2.0: delegated PoS και «Τεχνοκρατική Δημοκρατία»

- Οι χρήστες (διευθύνσεις {wallets}) ψηφίζουν μεγάλους stakers να πάρουν μέρος στη συναλλαγή (ως Witnesses) και να την κάνουν confirm/validate.
- Όσο περισσότερο stake έχουν οι χρήστες αντίστοιχα, τόσο περισσότερα votes μπορούν να δώσουν
- Οι top-20 **Witnessing nodes** παίρνουν δώρο network fees, οπότε όλοι θέλουν να γίνουν witnesses

How NEO does it: delegated Byzantine Fault Tolerance (dBFT)



Βυζαντινοί στρατηγοί?

- Είμαστε στρατηγοί στο Βυζάντιο, και **θέλουμε να πάρουμε το Κάστρο** (να κάνουμε validate ένα block).
- Ο καθένας από μας (peers/nodes ενός blockchain) μπορεί να **επιτεθεί** ή να **οπισθοχωρήσει** (να πιστοποιήσει ως valid ή όχι ένα block).
- Αν όλοι επιτεθούμε ή όλοι οπισθοχωρήσουμε, το αποτέλεσμα είναι βέλτιστο. Αν εμείς προσωπικά επιτεθούμε (ή οπισθοχωρήσουμε) ενώ η πλειοψηφία των υπολοίπων στρατηγών οπισθοχωρεί (ή επιτίθεται), **το προσωπικό μας στράτευμα ζημιώνεται** (η αξιοπιστία μας ως validator).
- Όλα καλά όταν όλοι μας είμαστε ειλικρινείς και καλοπροέραιτοι.
- Τι συμβαίνει όταν τα μηνύματα μεταξύ στρατηγών αλλοιώνονται από τους αγγελιοφόρους?
 - **Machine errors, SSL & HTTP errors**
- Τί γίνεται όταν μερικοί στρατηγοί προσπαθούν επίτηδες να χιάσουν τη φάση?
 - **Κακόβουλες επιθέσεις στο blockchain, hijacking attempts**
- Παράδειγμα 9^{ου} στρατηγού

Τι είναι τελικά το NEO?

- Εισάγει ακαδημαϊκά πιο αποδοτικό και γρήγορο αλγόριθμο για blockchain consensus (10,000 tx/s ως θεωρητικό όριο – VISA: 1,700 tx/s avg).
- Είναι πλήρως open-source και διάφανο στις διαδικασίες του (NEPs).
- Ευκολότερο για νέους developers, μπορείς να γράψεις Smart Contracts που επιδρούν και δρουν με το chain σε C#, Python, Java, Javascript, Ruby.
- Προσπαθεί να ηλεκτρονικοποιήσει υλικά, real-world assets και τις ανταλλαγές τους πάνω σε blockchain, με αποκεντρωμένο και ελευθεριακό τρόπο.
- Scammer-unfriendly λόγω κόστους.

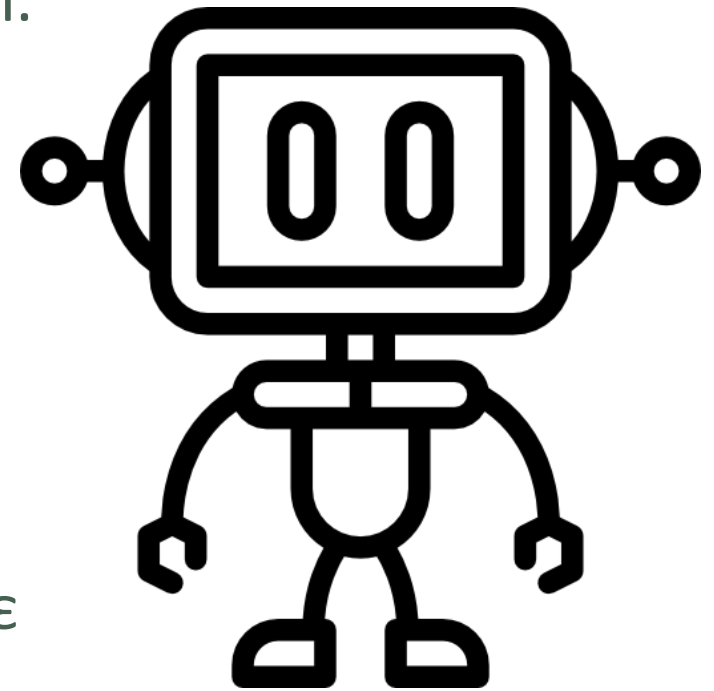
Part 2:

Writing Smart Contracts on NEO

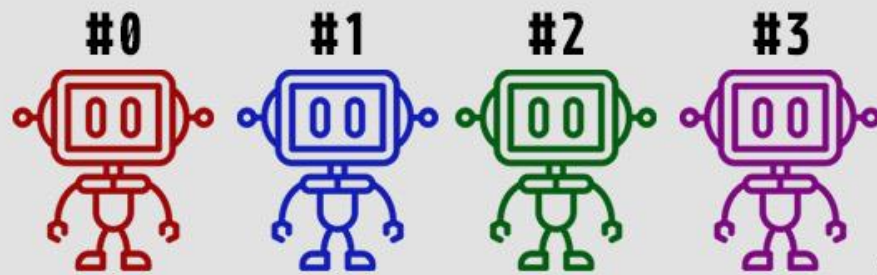


Τι είναι ένα Smart Contract?

- Μία σακούλα κώδικα αφημένη πάνω στο blockchain.
- Αυτοματοποιημένος πράκτορας, δαίμονας (dApp)
 - Επιδρά πάνω στο blockchain βάσει των προγραμματισμένων λειτουργιών του (είναι ανοικτές αφού όλα τα smart contracts σε open-source chains είναι διαφανή by design)
- Accept, reject, execute logic πάνω σε transactions και γενικά πληροφορίες του blockchain.
- “Ζει” αυτόνομα πάνω στο chain και δεν υπακούει σε κανέναν, ούτε στον δημιουργό του, αφού φάει deploy.

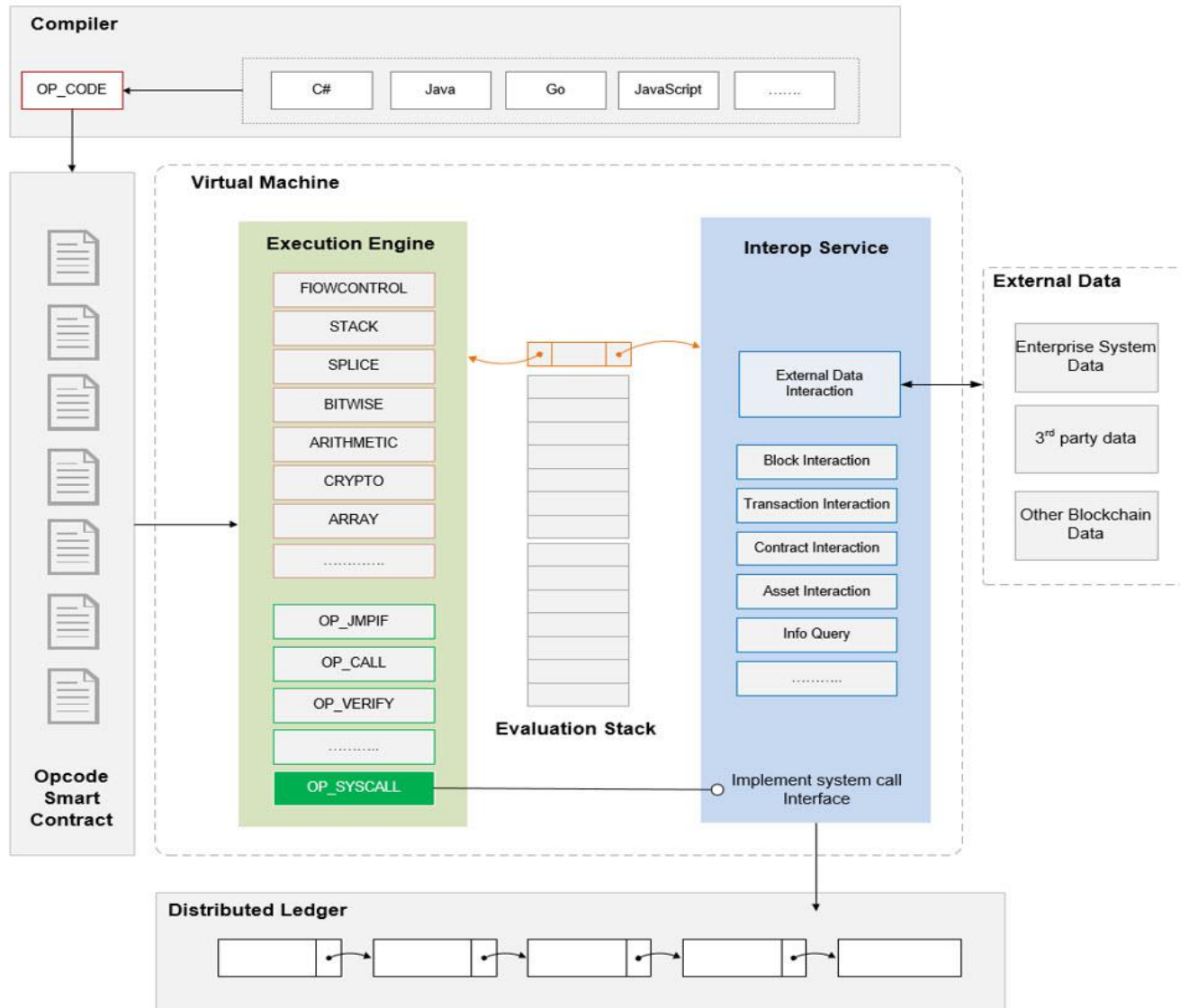


Smart Contracts



NEO Blockchain

NEO Virtual Machine



Η εργαλειοθήκη μας

Που ξεκινάω?

docs.neo.org is your friend

NEO Discord is your friend

neo.stackexchange.com is your friend

Πως γράφω Smart Contracts?

C#: Visual Studio + NEO Framework (neon.exe compiler)

Άλλες επιλογές: Java NEO Libraries, neo-python, neon-js

Πως κάνω deploy το Smart Contract μου στο blockchain?

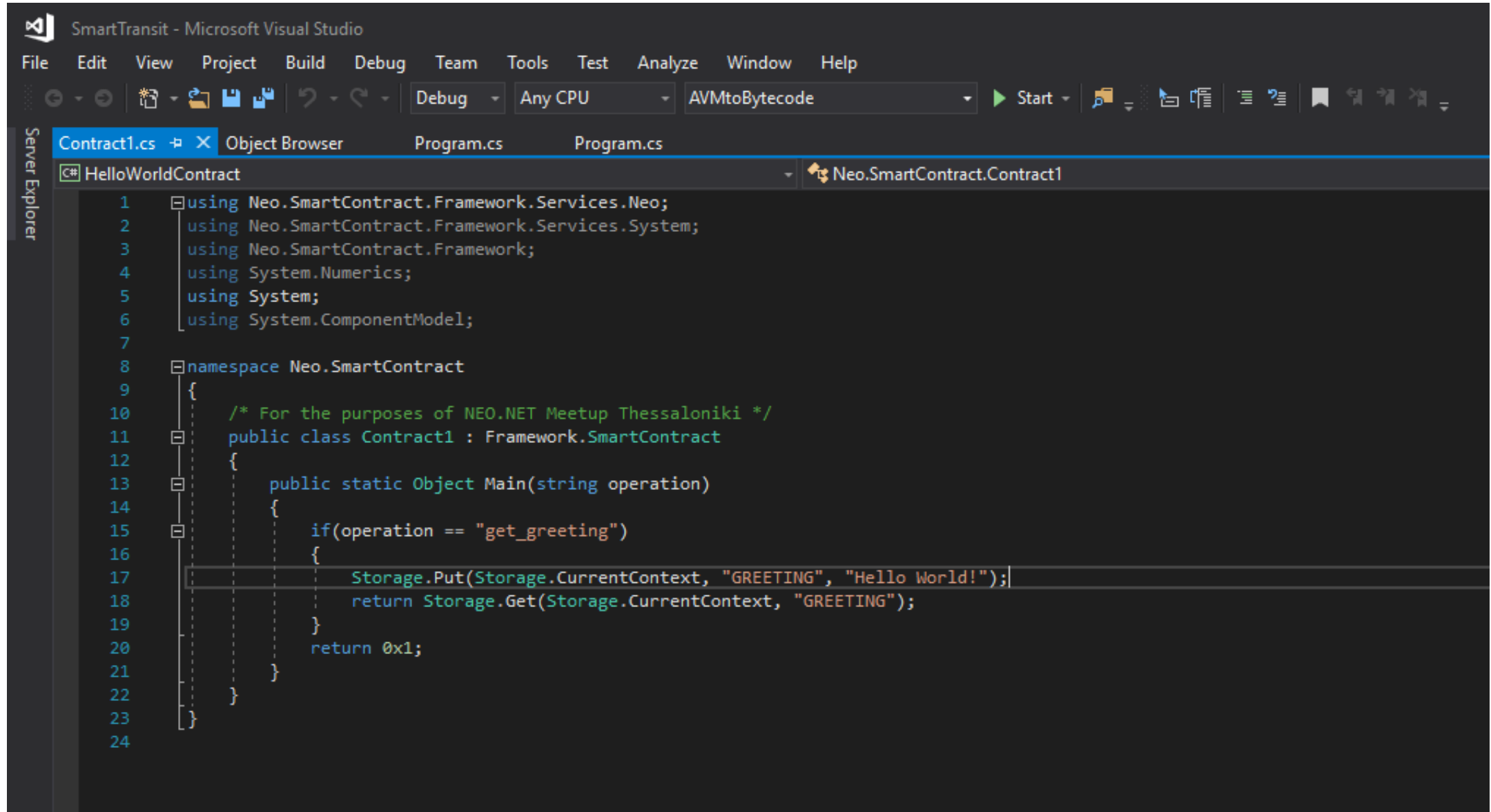
neo-gui (Windows client for NEO) -> Deploy contract (κόστος: 500 GAS)

Πως το χρησιμοποιώ, αφ'ότου το βάλω στο blockchain?

Βασικές χρήσεις: neo-gui -> Invoke contract

Πιο advanced invocations: neo-python, neon-js και τα υπόλοιπα APIs.

HelloWorld.cs



SmartTransit - Microsoft Visual Studio

File Edit View Project Build Debug Team Tools Test Analyze Window Help

Debug Any CPU AVMtoBytecode Start

Contract1.cs Object Browser Program.cs Program.cs

Server Explorer

Contract1 HelloWorldContract Neo.SmartContract.Contract1

```
1 using Neo.SmartContract.Framework.Services.Neo;
2 using Neo.SmartContract.Framework.Services.System;
3 using Neo.SmartContract.Framework;
4 using System.Numerics;
5 using System;
6 using System.ComponentModel;
7
8 namespace Neo.SmartContract
9 {
10     /* For the purposes of NEO.NET Meetup Thessaloniki */
11     public class Contract1 : Framework.SmartContract
12     {
13         public static Object Main(string operation)
14         {
15             if(operation == "get_greeting")
16             {
17                 Storage.Put(Storage.CurrentContext, "GREETING", "Hello World!");
18                 return Storage.Get(Storage.CurrentContext, "GREETING");
19             }
20             return 0x1;
21         }
22     }
23 }
24
```

Deploying HelloWorld.avm

The screenshot displays the neo-gui ChainTestNet application. In the background, the main window shows the 'Account' tab with 'Standard Account' and 'Contract Address' sections. The 'Contract Address' section lists two addresses: 'AbQy4rYsd4wzTHgqHPYPNRRBc4XCcW28St' and 'AL5DvcD3GnVdXPFRt9jztM624v3vuD7sx2'. Overlaid on this is a 'Deploy' dialog box. The dialog has three main sections: 'Information', 'Metadata', and 'Code'. The 'Information' section contains fields for 'Name' (HelloWorldContract), 'Version' (1.0), 'Author' (dsfounis), and 'Email' (itris@gmail.com). The 'Description' field contains the text: 'Will return "Hello World!" if you send it string argument "get_greeting", otherwise 0x1. It's literally 4 lines of code, don't overthing it.' The 'Metadata' section has a 'Parameter' field with the value '07'. The 'Code' section contains a large text area with the following hexadecimal code: '53c56b6c766b00527ac4616c766b00c30c6765745f6772656574696e67876c766b51527ac46c766b51c3648700616168164e656f2e53746f726167652e476574436f6e74657874084752454554494e470c48656c6c6f20576f726c6421615272680f4e656f2e53746f726167652e507574616168164e656f2e53746f726167652e476574436f6e74657874084752454554494e47617c680f4e656f2e53746f726167652e4765746c766b52527ac4620e00516c766b52527ac46203006c766b52c3616c7566'. At the bottom of the dialog, there are two checkboxes: 'Need' (unchecked) and 'Need Dyncall' (unchecked), followed by a text field containing '18e04b19fbb64c3ef64e8c6526da-'. The 'Deploy' button is highlighted in blue. The status bar at the bottom of the application shows 'Height: 1391747/1391747/1391747 Connected: 10' and 'Waiting for next block: [green progress bar]'.

neo-gui - ChainTestNet

Wallet Transaction Advanced Help

Account Asset Transaction History Event Log

Address

Standard Account

AHmV1mn1rkzhEuqS2twJGTvTukrk28wTq

AehieVzYk9zajxsUqM3vwXj2YtVPucZ1Xt

Contract Address

AbQy4rYsd4wzTHgqHPYPNRRBc4XCcW28St

AL5DvcD3GnVdXPFRt9jztM624v3vuD7sx2

Information

Name: HelloWorldContract

Version: 1.0

Author: dsfounis

Email: itris@gmail.com

Description: Will return "Hello World!" if you send it string argument "get_greeting", otherwise 0x1. It's literally 4 lines of code, don't overthing it.

Metadata

Parameter 07

Code

53c56b6c766b00527ac4616c766b00c30c6765745f6772656574696e67876c766b51527ac46c766b51c3648700616168164e656f2e53746f726167652e476574436f6e74657874084752454554494e470c48656c6c6f20576f726c6421615272680f4e656f2e53746f726167652e507574616168164e656f2e53746f726167652e476574436f6e74657874084752454554494e47617c680f4e656f2e53746f726167652e4765746c766b52527ac4620e00516c766b52527ac46203006c766b52c3616c7566

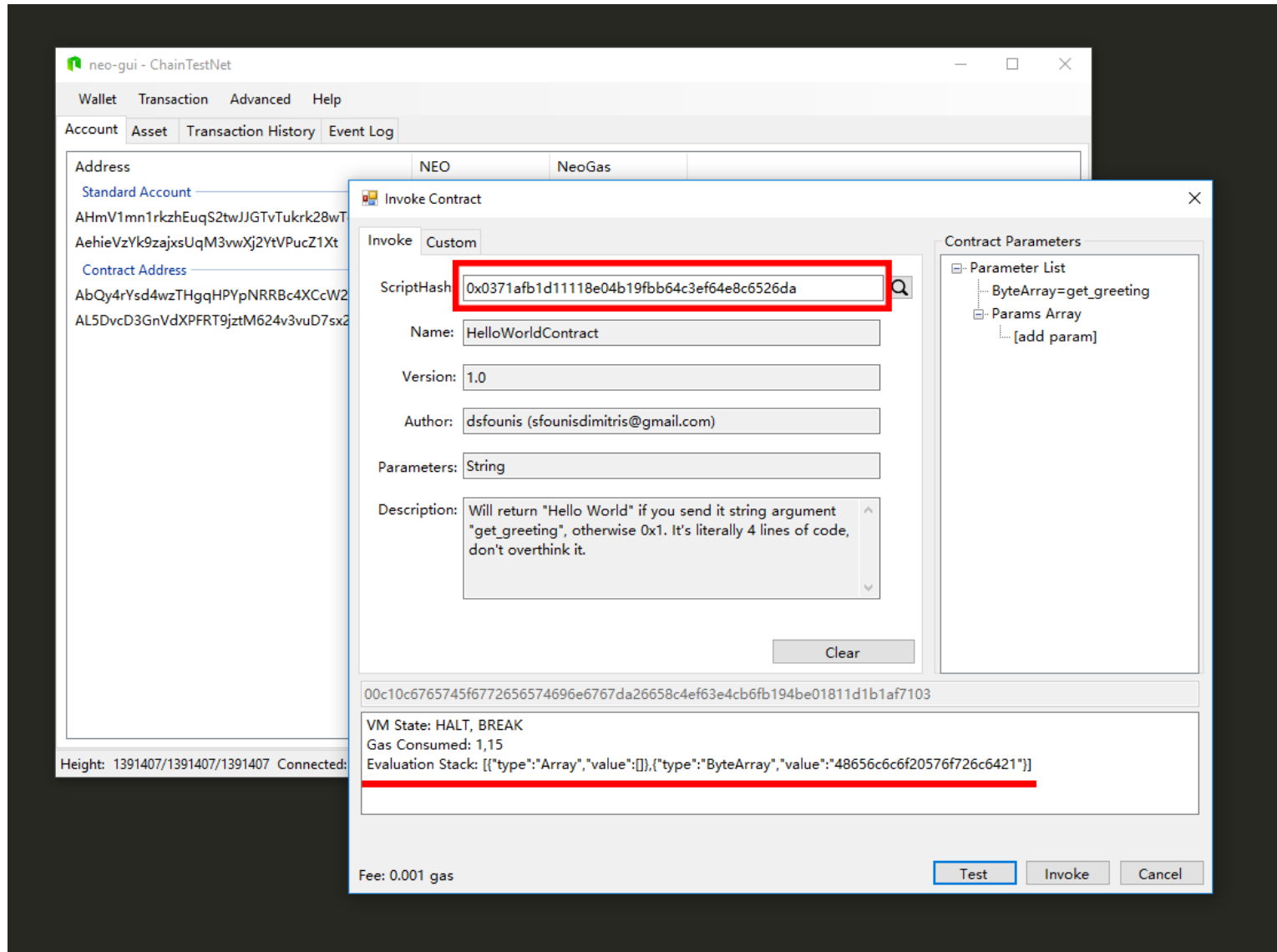
☐ Need ☐ Need Dyncall 18e04b19fbb64c3ef64e8c6526da-

Deploy Cancel

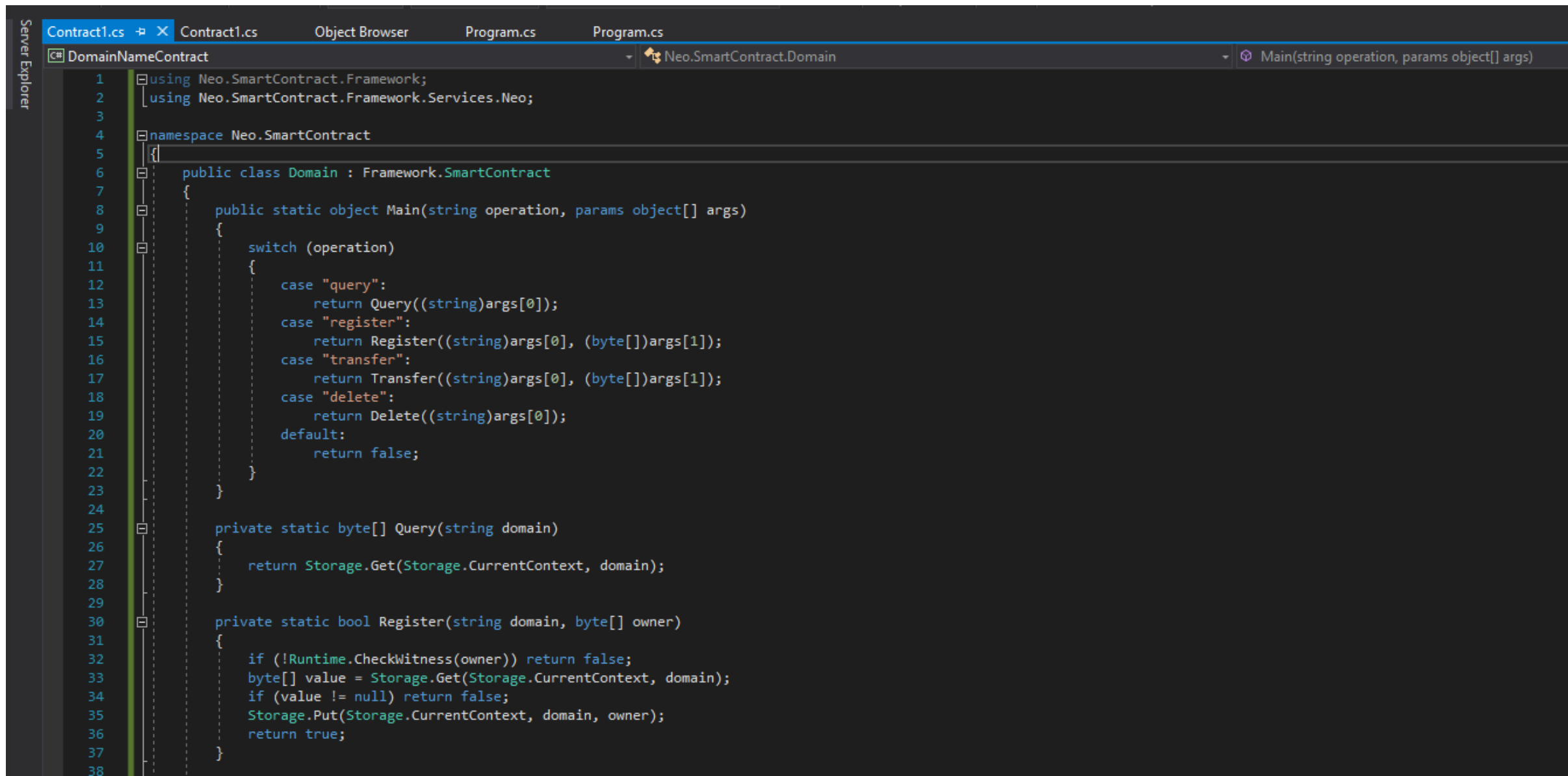
Height: 1391747/1391747/1391747 Connected: 10

Waiting for next block: [green progress bar]

Invoking the HelloWorld contract

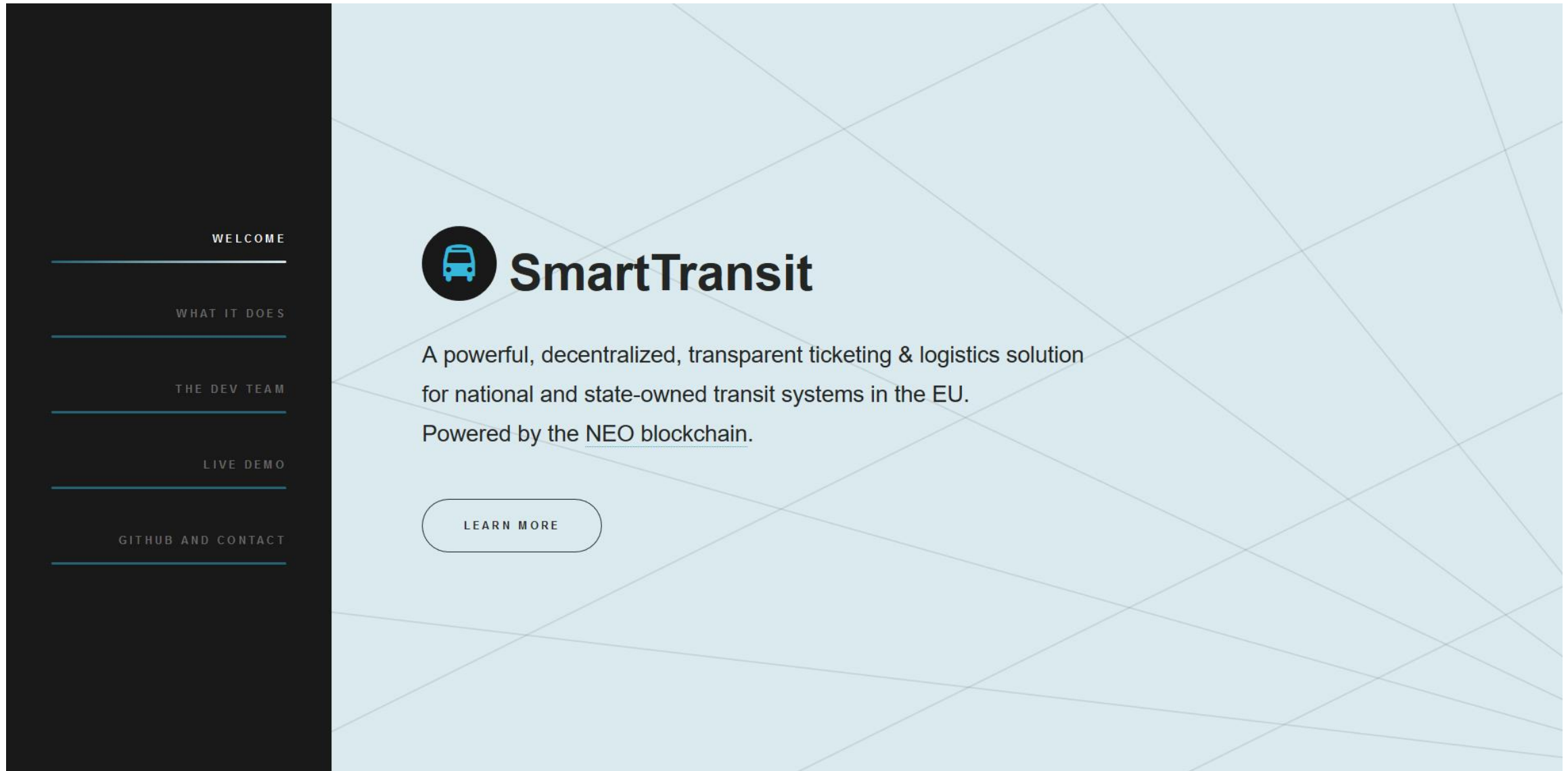


Κάτι καλύτερο: Domain Naming System



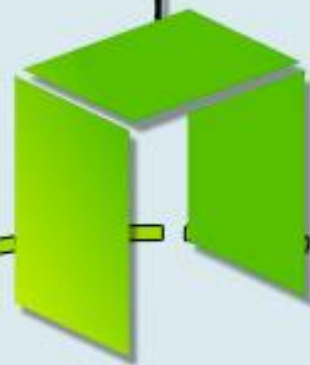
```
Contract1.cs Contract1.cs Object Browser Program.cs Program.cs
C# DomainNameContract Neo.SmartContract.Domain Main(string operation, params object[] args)
1 using Neo.SmartContract.Framework;
2 using Neo.SmartContract.Framework.Services.Neo;
3
4 namespace Neo.SmartContract
5 {
6     public class Domain : Framework.SmartContract
7     {
8         public static object Main(string operation, params object[] args)
9         {
10             switch (operation)
11             {
12                 case "query":
13                     return Query((string)args[0]);
14                 case "register":
15                     return Register((string)args[0], (byte[])args[1]);
16                 case "transfer":
17                     return Transfer((string)args[0], (byte[])args[1]);
18                 case "delete":
19                     return Delete((string)args[0]);
20                 default:
21                     return false;
22             }
23         }
24
25         private static byte[] Query(string domain)
26         {
27             return Storage.Get(Storage.CurrentContext, domain);
28         }
29
30         private static bool Register(string domain, byte[] owner)
31         {
32             if (!Runtime.CheckWitness(owner)) return false;
33             byte[] value = Storage.Get(Storage.CurrentContext, domain);
34             if (value != null) return false;
35             Storage.Put(Storage.CurrentContext, domain, owner);
36             return true;
37         }
38     }
39 }
```

To project μας: Smart Transit





Smart Transit
dApp



NEO Ecosystem

Ευχαριστούμε!

Χρήσιμα links:

- <https://neo.org>
- <https://docs.neo.org>
- <https://github.com/CityOfZion>
- <https://smarttransit.eu>
- Όλος ο κώδικας και τα examples/demos της παρουσίασης:
<https://github.com/dsfounis/SmartTransit>