PiTrust – A blockchain based trust network

CS6675 Advanced Internet Systems – Course Project

05 May 2022

Georgia Tech

PiTrust – A blockchain based trust network

- Use case
- Why blockchain?
- System description
- Preparation for Live Demo
- Guidance for Live Demo

Georgia Tech

PiTrust – Use Case

- Imagine being new in a company or at a location
- You need to know something about a particular topic
- Whom could you ask for assistance?

=> Database of people to find a knowledgeable person

PiTrust – Why blockcain?

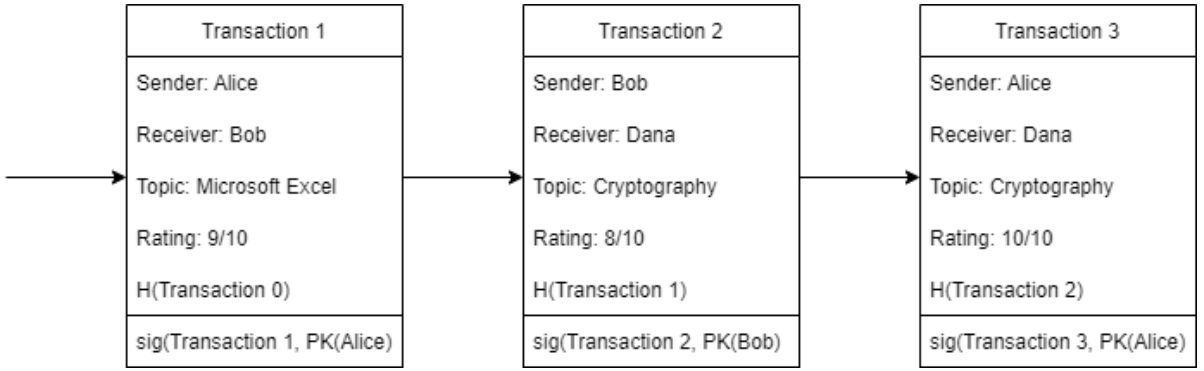
- Central database may be well-suited for a network of people trusting each other, but not for larger scale
  - Lack of transparency
  - Prone to manipulation
  - Scalability
- Blockchain solves these issues as it is publicly verifiable, non-revokable and highly scalable

Georgia Tech

System Description - General

- Transaction (rating) information will be stored on the Polygon blockchain
  - Polygon is compatible to the very well-known Ethereum blockchain, but comes with much lower transaction fees (~$0.10 compared to ~$30 on Ethereum)
- Each transaction will store information about the actual rating (on a scale between 1 and 10), topic and also who has rated whom:

  T = (Sender, Receiver, Topic, Rating)



Georgia Tech

System Description –Rating calculation

- Each transaction stores the most recent rating (for evidence) as well as the recalculated overall rating of a person's expertise based on all former and the most recent rating:

$$r_{new} = \frac{(r_{old} \times n) + r}{n + 1}$$

- The above-mentioned formula does not take into account that expert's ratings shall be weighted higher than novice's ones leading to a refined formla:

$$R_A = \frac{1}{11(n+1)} \sum_B R_A^B (R_B + 1)$$

with R_i being the (current) rating of person *i* and R_A^B being the (current) rating of person A for person B

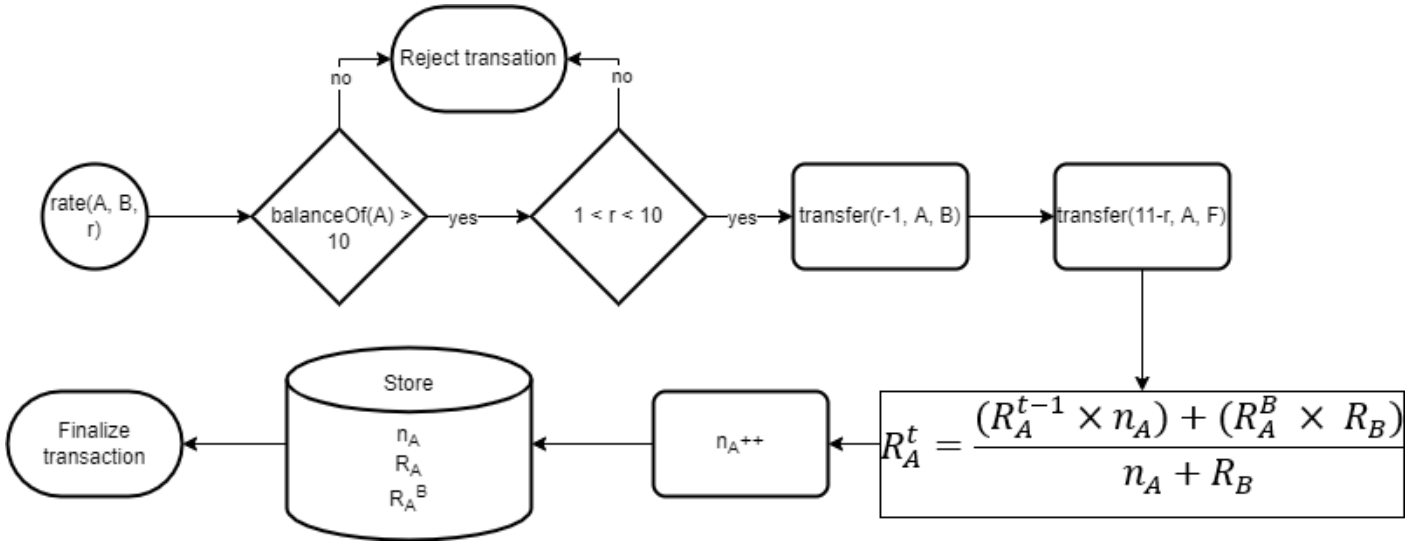
Georgia Tech

System Description – Tokenomics (1)

- The implementation the system as proposed would work, but also be prone to manipulation by creating large counts of fake-reviews, being positive or negative
- This may be mitigated by introducing a cryptocurrency token, which has a small, but real-world value as it can be exchanged against other cryptocurrencies such as Bitcoin and finally fiat money as well.
- Tokens can also be used as incentive for positive behavior (i.e., receiving, but also providing valuable feedback)

System Description – Tokenomics (2)

- Basic idea: Fixed supply with ability to buy tokens on (decentralized and/or centralized) exchanges
- Each rating costs 10 tokens, whereof *r-1* tokens will be transferred to the rated person and the rest being sent (back) to the contract wallet
  - Burning the tokens, i.e., sending them to an unusable address, was also considered



System Description – Tokenomics, additional thoughts

- *Spending* tokens for ratings currently does not provide any benefit for the users
  - Incentivation could be implemented by increasing voting power (social benefit) and/or provide some kind of interest on performed votings, comparable to *staking* tokens/coins
- Hoarding tokens for investment purposes does not fit its purpose
  - Rather high inflation (e.g. creating 20% additional tokens per year, currently implemented) or controlled burn of unmoved tokens (e.g. 10% per month) could mitigate that

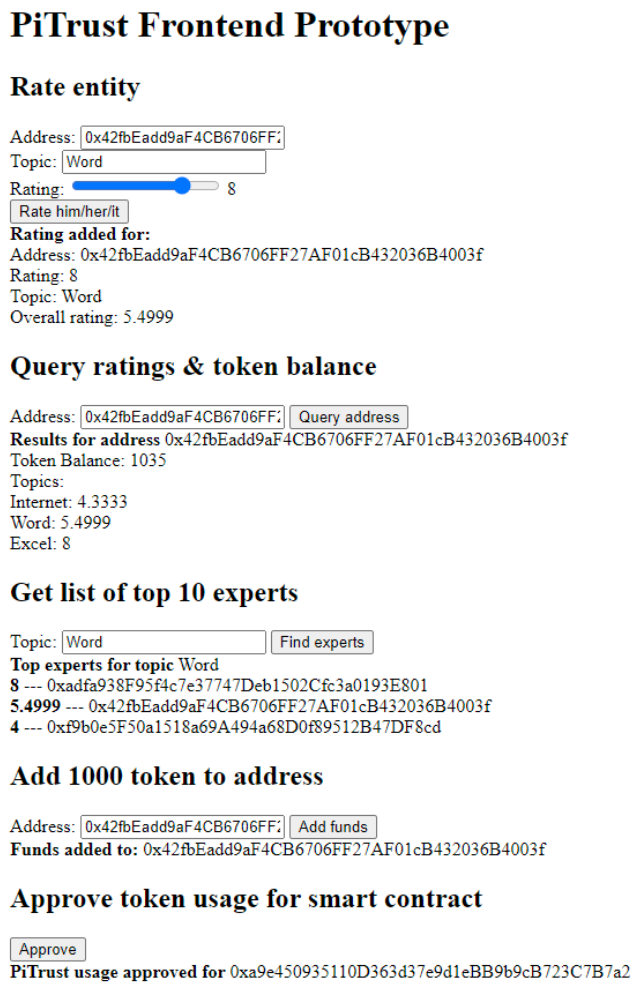
Georgia Tech

System Description – Frontend (1)

- Ethereum/Polygon smart contract alone is not usable by even technically versed people without prior knowledge of and tools for blockchain development
- Frontend could be developed as a “classic” executable application, but modern Web (3.0) applications rather make use of general-purpose web servers using HTML & JavaScript
  - More sophisticated frameworks such as React add even more value to the usability but have not been evaluated in-depth or used for the prototype
- Main interface between the frontend and the smart contract is provided by Metamask (or any other Web3 crypto wallet)

System Description – Frontend (2)

- Frontend was tested purely local, but will be provided on a publicly accessible webserver for the live demo
- Consists of 5 actions:
  - Rate an entity/person (i.e. a wallet address)
  - Query ratings & balance of one address
  - Get a list of experts for a given topic
  - Add 1000 token to an address (admin only)
  - Approve token usage (prerequisite for any action)



Georgia Tech

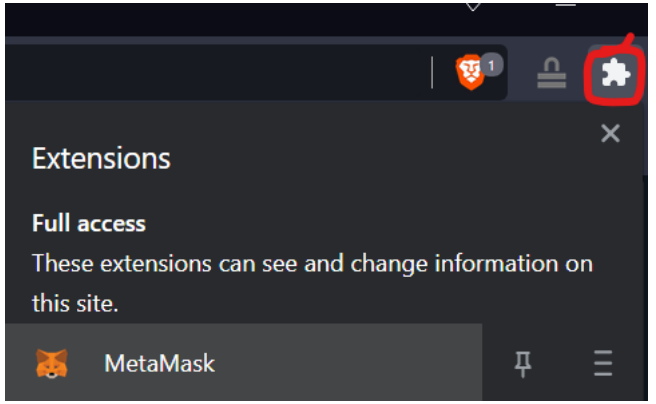
Preparation for Live Demo (1) - Prerequisites

- Browser capable to use Metamask extension (Chrome, Brave, Firefox, Edge)
  - Mobile browsers & other Web3 wallets (e.g. Wallet Connect) shall also work but are not covered by the project's scope
- Installation of Metamask extension
- Configuration of Metamask for Polygon Mumbai testnet
- Import of (test-)wallet

Georgia Tech

Preparation for Live Demo (1) – Metamask installation

- Go to https://metamask.io/download/
- Click on “Install Metamask for <your browser>
- Install from the Chrome (or other browser’s) web store
- After installation, you will find the MetaMask icon (a fox) after clicking on the puzzle tile in the upper right corner
- After clicking on the Metamask symbol click on Get Started



Georgia Tech

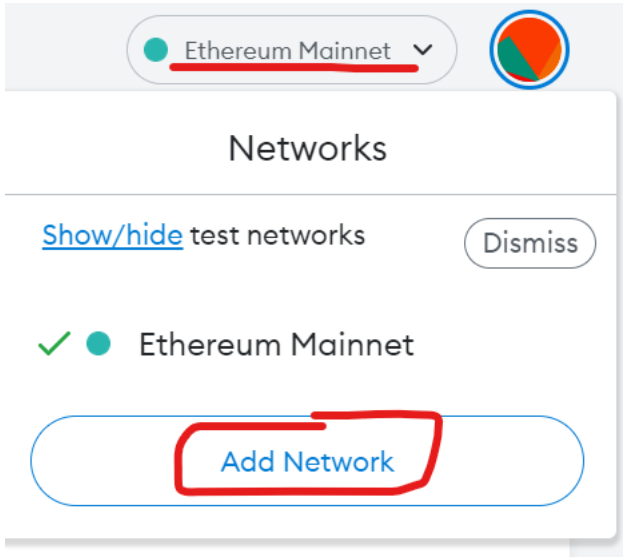
Preparation for Live Demo (2) – Metamask configuration

- Click on “Create a wallet”
- Then “I agree”
- Chose a password you like and accept the terms of use
- Click on “Next” and “Remind me later”
  - You won’t use the wallet you created at all, but Metamask does not allow to start with importing a private key, which we will use (next slide)

Georgia Tech

Preparation for Live Demo (3) – Adding Polygon Testnet

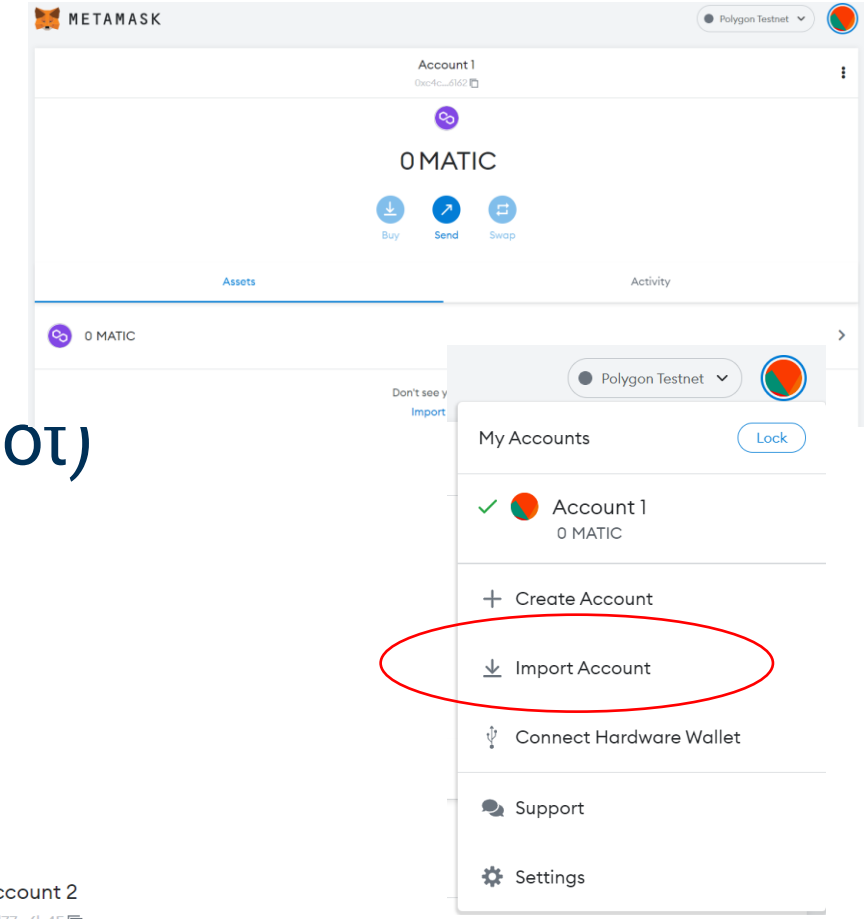
- Next, we will add the Polygon (Mumbai) testnet to Metamask (which is by default only configured for Ethereum Mainnet)
- Click on “Ethereum Mainnet” at the top of the Metamask site, then on “Add Network”
- Enter following network data:
  - Network Name: Polygon Testnet (does not matter)
  - New RPC URL: *https://rpc-mumbai.maticvigil.com*
  - Chain ID: 80001
  - Currency symbol: MATIC
  - Block explorer URL: *https://polygonscan.com/*

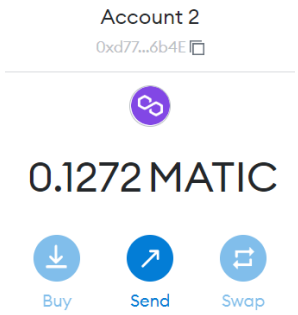


Georgia Tech

Preparation for Live Demo (4) – Adding Test account

- The screen shall now look like this:
- Next, we will add a “public” test account to Metamask.
- Click on the colorful “ball” in the top-right corner (colors may differ from the screenshot)
- Then click on “Import Account”
- Enter the (not-so-) private key string:
  7790309415a34c7019b60fa9cb4e03e027acb6174067b8901cf7e144f54612f1
- *And click on “Import”*
- *Now you shall see a (small) amount of MATIC available*

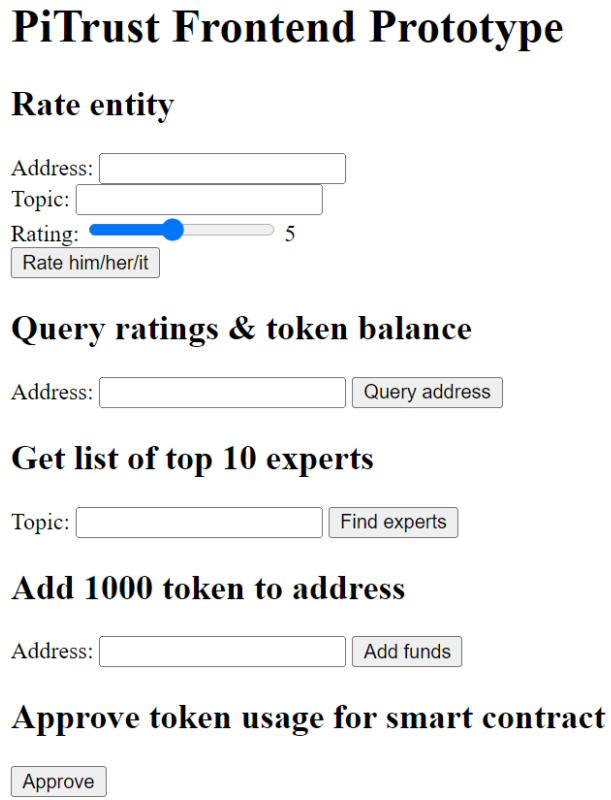




Georgia Tech

Live Demo

- After setting up Metamask, you are ready to interact with the smart contract
- Call http://pitrust.pidabbelju.de
- No need to “approve” token usage (was already done by me)
- Adding tokens to addresses will not work (admin only), but if you need some for additional addresses please just drop a message in the Ed Discussion forum



Georgia Tech

Live Demo

- You can create ratings for arbitrary Polygon addresses and topics
  - Some exemplary addresses:
    0xc4ca55d47915A8f19F5e153bc2606739CEF36162 (your wallet)
    0xd77Ba78904Cf1cDa9D243C33E844317B95d46b4E (admin wallet)
    0xD5D02341C1163957a3a5f85c84cE27a7ee12C3F4 (contract address)
- You can search for already rated addresse, for example the above-mentioned ones or any other
- You can search for “experts”; at the time of writing, only the topic “Word” was used

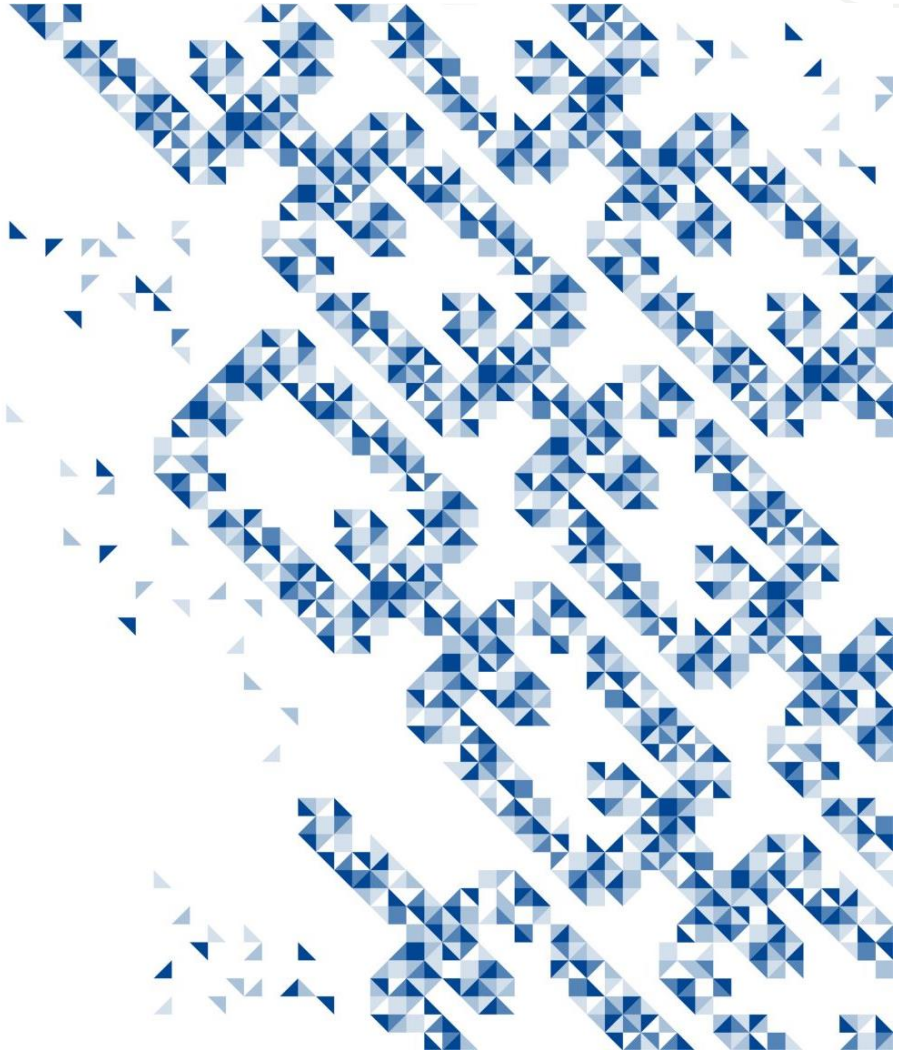
Georgia Tech

Thanks for clicking through this presentation!

Any comments, questions, recommendations and discussions are heavily appreciated!

Please just post in the dedicated Ed discussion thread – or via mail at

pwissmann3@gatech.edu



Georgia Tech