

FIGI Security Clinic

Towards new FS infrastructures

Anne-Sophie Cartray

4-5 December 2019
#financialinclusion

Sponsored by

BILL & MELINDA
GATES foundation

FIGI  FINANCIAL INCLUSION
GLOBAL INITIATIVE



Organized by

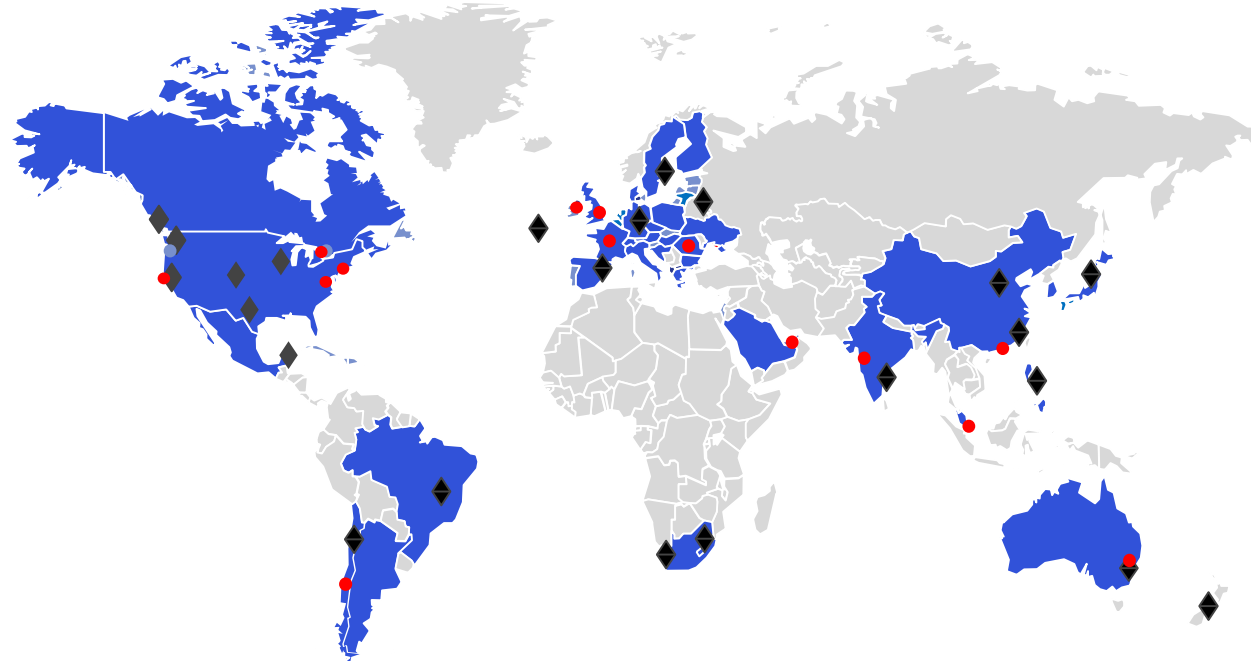


About ConsenSys

ConsenSys is the world's largest blockchain pure play tech company



We are 1,000+ blockchain experts, entrepreneurs, computer scientists, designers, engineers, consultants, and business leaders across 6 continents



- PROJECT DELIVERY LOCATIONS
- OFFICE LOCATIONS
- ◆ CONSENSYS PERSONNEL

Leader in all major industry associations and standardization bodies



OUR SERVICES

Infrastructure	Products	Education	Solutions	Capital
Help grow the ecosystem by building and maintaining core developer tools and clients	Incubate new companies developing decentralized applications on the Ethereum blockchain (current 50 +)	Educate developers and entrepreneurs about Ethereum through training programs	Consult and deliver production ready blockchain solutions for organizations and governments	Provides token services, crypto asset management and venture capital

Financial Services value drivers

Redesigning current financial services infrastructure and processes through simplicity, efficiency and disintermediation



Operational efficiency

Reduction of reconciliations and disputes



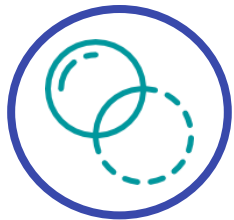
Risk reduction

Trustless execution and lower counterparty risk



Transaction efficiency

Fast and cost-effective execution and settlement



Transparency

Full asset provenance and transaction history



Capital efficiency

Reduction of capital lock-in during transactions

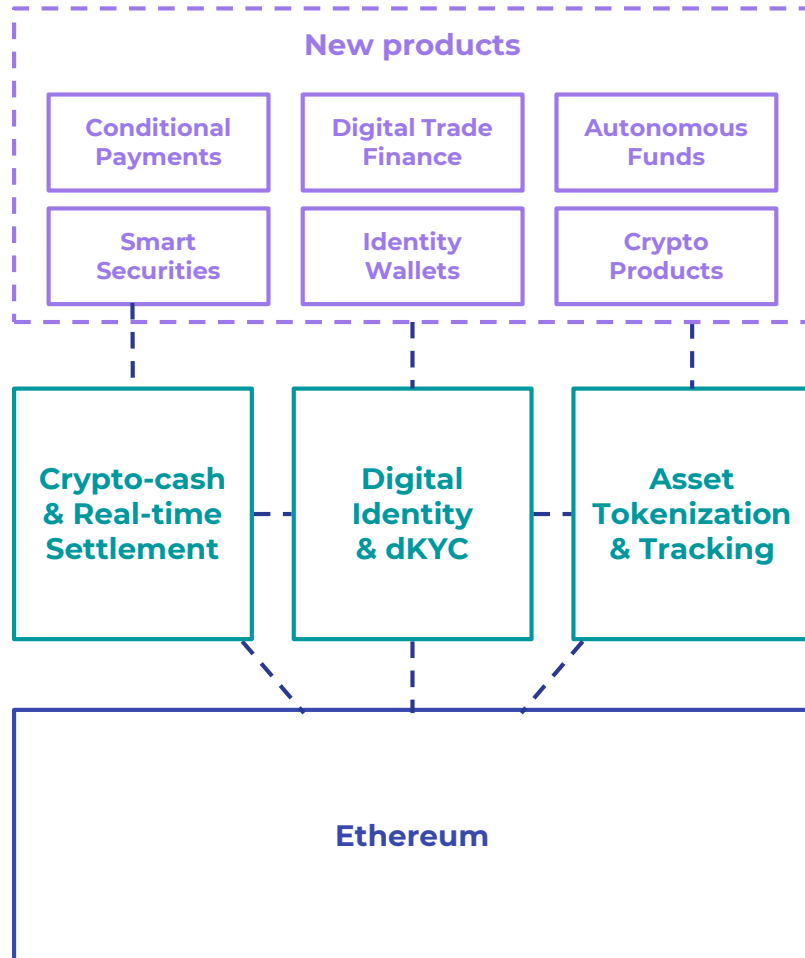


Regulatory inclusion

Compliance and monitoring as transaction by-product

A new foundational financial infrastructure

Developing the market infrastructure and the key enablers for tomorrow's greenfield financial products



Greenfield products can be developed on-top of the new market infrastructure:

- Real-time cross-border payments: Instantaneous and cost effective P2P FX
- Smart securities: Self-executing and self-servicing DVP securities contracts
- Digital trade finance: Digitized and secure trade financing transactions
- Identity wallets: Digital wallets for identity management and passporting
- Crypto products: Crypto as a new asset class with dedicated investment and services

New foundational services can be built on top of Ethereum establishing a shared and more efficient market infrastructure:

- Crypto-cash: Asset-backed tokens allow for real-time settlement of payments and trades
- Digital Identity: Self-sovereign identity and decentralized identity verification
- Asset Tokenization: A unique source of truth for asset provenance and transaction history

Ethereum's core components provide fundamental capabilities:

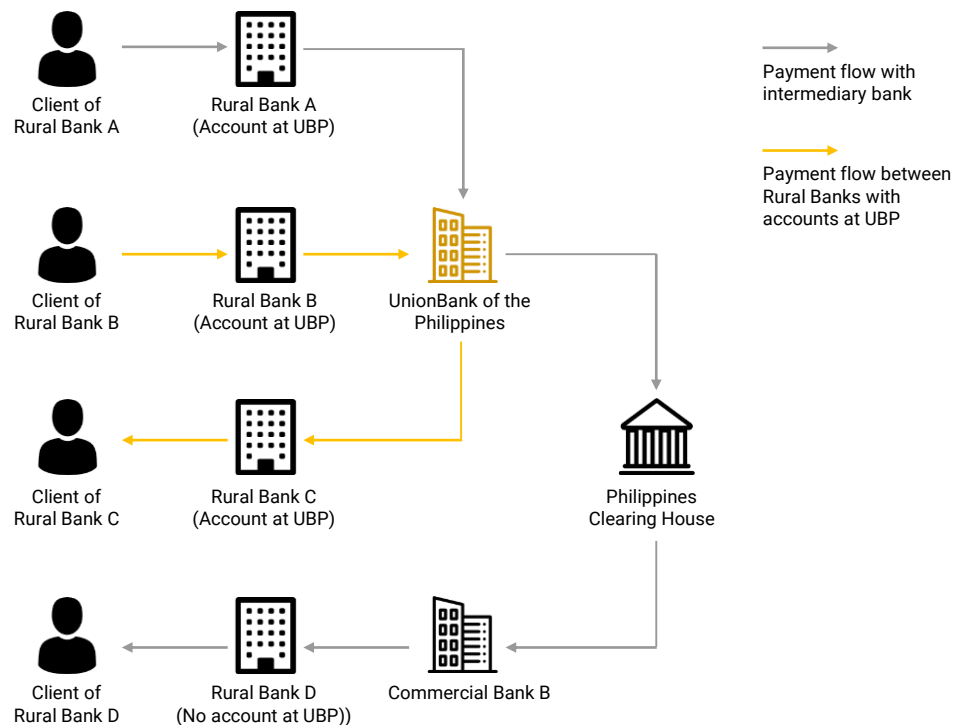
- Decentralized network: Peer-to-peer transactions and disintermediation
- Distributed ledger: Immutable digital records
- Cryptographic signatures: Proof of ownership and security
- Consensus: Trustless execution and "automated" reconciliation
- Smart contracts: Programmable and deterministic business logic

Project i2i

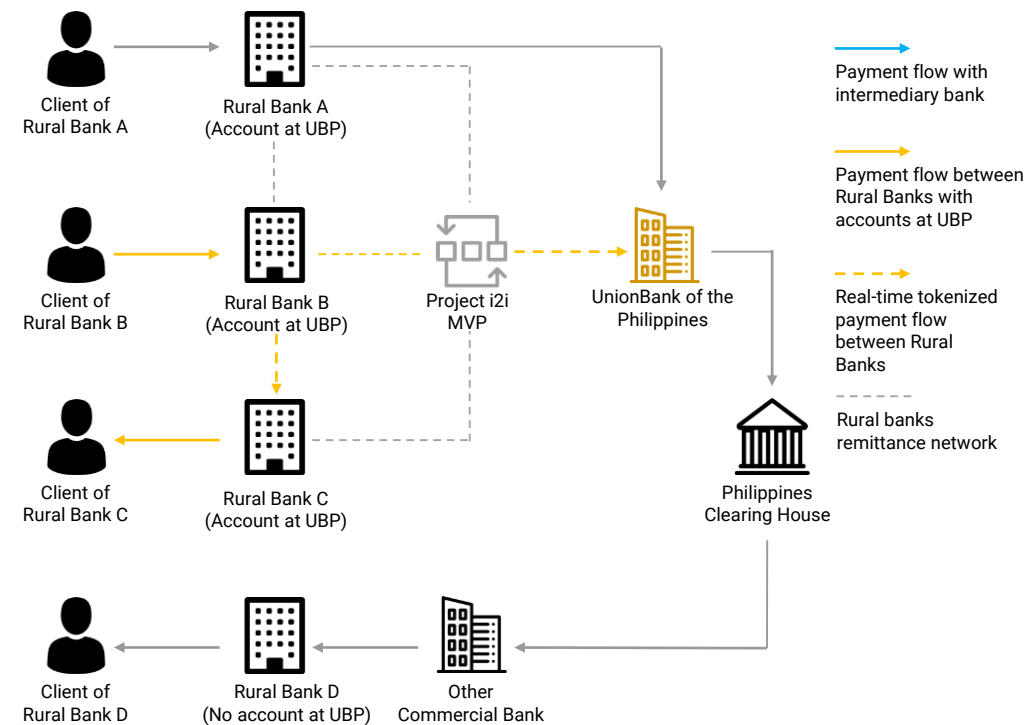
Private network for domestic remittances between Rural Banks



Traditional domestic remittance



Domestic remittance network on blockchain



- Complex process with multiple manual ops
- Complex reconciliations
- Long time to disburse to client
- Expensive (50 Pesos minimum fee)

- Simple digitized process
- Limited reconciliations
- Near real-time
- Cheaper (1 Peso flat fee endorsed by UnionBank)

The UnionBank logo consists of the word "UNIONBANK" in a bold, orange, sans-serif font, centered within a dark blue rectangular box with a thin orange border.

ConsenSys partnered with UnionBank to develop a closed-loop Tokenized cash solution in the Philippines to connecting rural banks to the main financial infrastructure.

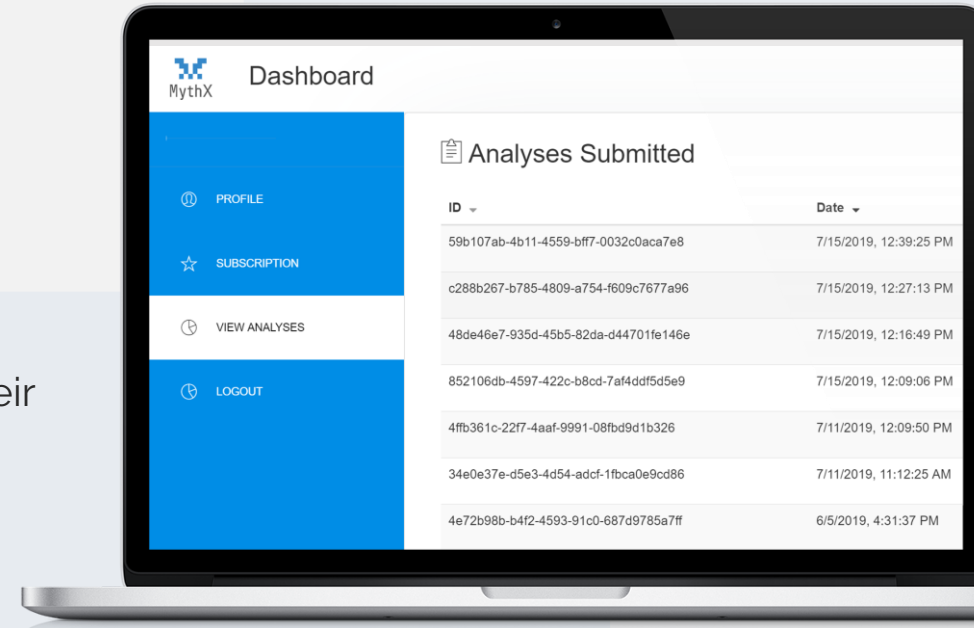
An aerial photograph of a coastal town. In the foreground, there is a large building with a red roof. To the left, a church with a blue roof and white facade is visible. The town extends to the water's edge, with many houses and buildings. In the background, there are mountains and a body of water. The sky is overcast.

PROJECT i2i

A PARTNERSHIP OF
UNIONBANK · KALEIDO · CONSENSYS

MythX automatically scans for security vulnerabilities throughout your project's lifecycle

Built by a team of security experts, MythX offers the most cutting-edge and exhaustive suite of analysis techniques that automatically detects security vulnerabilities in Ethereum smart contracts, giving developers confidence that their smart contracts are secure



POWERFUL

Industry-leading analysis techniques that accurately detects various security issues



INTEGRATED

Robust API that enables integration with tools and security products that smart contract developers rely on



SCALABLE

Scalable and performant security-as-a-service that runs multiple analysis processes in parallel

Explainer Video



Demo

The screenshot shows the MythX dashboard interface. At the top, the browser address bar displays the URL: `dashboard.mythx.io/#/console/analyses/c3b0425e-d23a-4b8b-9188-393fd732dede`. The dashboard header includes the MythX logo, the word "Dashboard", and a "Logout" button. On the left, a blue sidebar contains the user's email address `simanda.lee@consensys.net` and navigation links for "PROFILE", "SUBSCRIPTION", and "VIEW ANALYSES".

The main content area is titled "Detected Issues" and features a summary bar with three categories: "1 High", "0 Medium", and "1 Low". Below this is a table listing the detected issues:

ID	Severity	Name	File	Location
SWC-101	High	Integer Overflow and Underflow	external-lib.sol	L: 5 C: 12
SWC-103	Low	Floating Pragma	external-lib.sol	L: 1 C: 0

Below the table, the "Analysed Files" section shows a file named `browser/external-lib.sol` with a "Hide issues in code" button. The file content is displayed with two severity indicators: "1 High Severity" and "1 Low Severity".

The first issue shown is a "LOW SWC-103 | Floating Pragma" issue. The description states: "It is recommended to make a conscious choice on what version of Solidity is used for compilation. Currently multiple versions `^0.5.7` are allowed." The code snippet shows a pragma statement: `pragma solidity ^0.5.7;`

The second issue is a "HIGH SWC-101 | Integer Overflow and Underflow" issue. The description states: "The operands of the addition operation are not sufficiently constrained. The addition could therefore result in an integer overflow. Prevent the overflow by checking inputs or ensure sure that the overflow is caught by an assertion." A link to "See test cases" is provided. The code snippet shows a function definition: `function increment(uint256 _n) public pure returns (uint256) { return (n + 1); }`

At the bottom of the dashboard, there is an "Other info" section which is currently empty.