IOTA: A Ledger for the Internet of Things

Michele Nati, PhD - Head of Telco and Infrastructure Development, MA Dept.
Luigi Vigneri, PhD - Senior Research Scientist - Research Dept.

Deep Dive into Blockchain
Summer school,
University of Zurich, July 12th

@iota
Outline

- Intro
- Why IOTA
- Tangle vs Blockchain
- IOTA Protocol
- Governance
- IOTA Adoption
- Exercise: TBD
Why a ledger for Internet of Things?

Trust in Data
Data is as important as services. Needs for data integrity and not only value transfer.

Real Time Transactions
Throughput and cost scalability.

Lightweight consensus
Any device can send and receive transactions for E2E trust and security.
The Blockchain Bottleneck

Blockchain is expensive and not for data
The Blockchain Bottleneck
Blockchain does not scale
How to realize a vision?
3 important Puzzle Pieces

Technology
Governance
Ecosystem
Tangle vs Blockchain
A DLT for the Internet of Things

The IOTA network is hosted by a collection of servers known as “nodes”
Nodes maintain a real-time database of the distributed ledgers
Nodes receive new transactions from users (wallets) and share them with their neighbors

Users contact nodes to:
- Send sensor data
- Issue payments
- Check ledger status

Nodes can:
- Perform PoW
- Choose tips
- Create messages
- Participate in voting

Smartphones, IoT devices
Any device

Users

Nodes
**Blockchain vs Tangle**

**Blockchain**
- Sets of transactions are cryptographically linked forming a **chain**
- Secured by Proof of Work
- Special nodes (miners)

**Tangle**
- Each transaction “approves” two (or more) existing transactions forming a **directed acyclic graph (DAG)**
- Secured by reputation
- No special nodes
What is a DAG?

A **DAG** is a finite directed graph with no cycles

- **Directed**: vertices connected by edges; edges have a direction
- **No cycles**: Vertices unable to be connected in a closed chain

**Partially-ordered set of messages**

- **Vertices**: are messages organized such that every edge is directed from earlier to later in the sequence
- **Edges**: are the references to existing messages

Each **vertex** represents a message (square)
Each **edge** represents a reference (line)
First transaction (DAG origin) is the genesis

More activity = more validation
Tangle benefits

- No dichotomy between miners and users
- Users validate the network without paying a fee
  - Validation of the ledger only requires CPU cycles and memory space
- Using a blockless DAG offers scalability
- With no payable fee, there is no minimum payment size: 1i sent is 1i received
- Low energy consumption

22,000 IOTA transactions = 1 cup of coffee
IOTA protocol
Protocol overview

**Consensus**
Determines which transactions can be considered valid

**Networking**
Prevents spam attacks and fairly shares network resources

**Peering**
Defines how to connect nodes with each other

**Data sharding**
Nodes process only a subset of all messages
IOTA protocol

Seeds, private keys and addresses

Tokens
- IOTA tokens are a finite amount, distributed with the genesis transaction
- New digital assets (colored tokens) can be created
- Tokens are held in an “account” or “wallet”

Seed
- The secret that controls the addresses holding tokens
- Knowing a seed is a Proof of Ownership. If you can control an address this means you own the tokens at it
- A private key is used to sign transaction (transfer of tokens between addresses)
## Message structure

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version</td>
<td>uint8</td>
<td>The message version. The schema specified in this specification is for version 1 only.</td>
</tr>
<tr>
<td>Parents count</td>
<td>uint8</td>
<td>The amount of parents preceding the current message.</td>
</tr>
<tr>
<td>Parents type</td>
<td>uint8</td>
<td>Bitwise encoding of parent type matching the order of preceding parents starting at least significant bit. 1 indicates a strong parent, while 0 signals a weak parent. At least MIN_STRONG_PARENTS parent type must be strong.</td>
</tr>
<tr>
<td>Issuer public key</td>
<td>ByteArray[32]</td>
<td>The public key of the node issuing the message.</td>
</tr>
<tr>
<td>(Ed25519)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Issuing timestamp</td>
<td>time</td>
<td>A value that shall represent the issuance time of the message.</td>
</tr>
<tr>
<td>Payload length</td>
<td>uint32</td>
<td>The length of the Payload in bytes. Since its type may be unknown to the node, it must be declared in advance. 0 length means no payload will be attached.</td>
</tr>
<tr>
<td>Payload</td>
<td></td>
<td>▶ Generic Payload</td>
</tr>
<tr>
<td>Nonce</td>
<td>uint64</td>
<td>The nonce which lets this message fulfill the Rate Control requirement.</td>
</tr>
<tr>
<td>Signature (Ed25519)</td>
<td>ByteArray[64]</td>
<td>Signature of the issuing node’s private key signing the BLAKE2b-256 hash of the entire message bytes.</td>
</tr>
</tbody>
</table>
Sybil protection

**Problem:** Sybil attacks
In distributed systems, attackers may try to build counterfeit identities (Sybil attacks) to harm the network.

**Solution:** Reward good behavior
To mitigate Sybil attacks, identities must be linked to a scarce resource. Unlike Bitcoin, which uses computational power, IOTA decouples nodes’ capabilities with their influence in the network, using a reputation-based mechanism to reward good behavior.

**How that works:** Mana
The basic component of the node’s reputation is mana. Each transaction carries an amount of mana equal to the value exchanged in the transaction itself. The transaction issuer decides which node should benefit from the mana (by default, it is the same node creating the message). You can think of mana as a form of delegated Proof of Stake.
What can one do with *mana*?

**Peer with other nodes**
A mana-based auto peering mechanism allows to search for peers, avoiding *eclipse attacks*.

**Write into the ledger**
Writing rights to the ledger are proportional to the mana owned by nodes to guarantee *fairness* among nodes.

**Participate in the consensus**
Conflict resolution is based on an iterative *voting* mechanism based on mana.
How to create a message?

1. Randomly choose from 2 to 8 existing recent unreferenced messages (tips)
2. Verify their correctness (valid signature, correct UTXO balances, etc.)
3. Sign the new message
4. Gossip it to the neighbors
5. Throughput is regulated by a sophisticated access control system ensuring fairness
IOTA protocol

Double spending resolution

**Attack:** Double spending
In IOTA, a double spending is detected when two messages are spending the same output.

**Solution:** Fast Probabilistic Consensus
- No Proof of Work to enable the IoT use case
- Iterative voting scheme

**Challenge:** Metastability
- Adversary can split opinions with simple majority rule
- Use randomness to break metastability

[Diagram of Random thresholds]
Approval weight

DAG ledger structure introduces additional challenges.

Finality criteria cannot be as simple as six block rule.

**Approval weight** counts the percentage of mana in the future cone of a message.
Hierarchical way to shard the Tangle for data
- Consensus is not required
- Easier than doing it for value transactions
A subset of nodes can create “subTangles”, called child Tangles
Child Tangles may be of two types
- **Leaf Tangle**: at the bottom of the tree of Tangles, include the actual data
- **Branch Tangle**: intermediate Tangle which sends references (hence, approvals) to the parent Tangle
About the IOTA Foundation

The IOTA Foundation was founded in 2017 to research, develop and grow the IOTA protocol and ecosystem.

Established as the first regulated DLT non-profit in Germany, we work together with partners in academia, government, and business to develop open source technologies that allow people to live freely, safely and securely in a digital world.

We are based in Berlin, Germany with operations worldwide.
A diverse and distributed team, the IOTA Foundation is one of the most experienced organizations in the DLT space.

150+ Colleagues

30+ Nationalities

1 Shared vision
Role of the IOTA Foundation
Open-source building blocks to accelerate product development and adoption

IOTA is the open-source protocol for standardized value exchange between machines

Utilise or extend the Tangle

Solve concrete business problems

Developer tools for software & hardware
- IoT-ready node software
- Open-source toolkits
- Deployment tools
- Active developer community
- Libraries for major platforms

Existing Products
- Certificates & audit trails
- Data & industry marketplaces
- Digital wallets
- Decentralized digital identity
- Secure data streams
- Access management

IOTA developer tools for software & hardware
- Active developer community
- Libraries for major platforms
- IoT-ready node software
- Open-source toolkits
- Deployment tools

IOTA is the open-source protocol for standardized value exchange between machines
IOTA Has One of the Largest and Most Vibrant DLT Ecosystems

More Companies are building on IOTA with and without the Foundation’s input.

More Developers and researchers are developing new innovative solutions with IOTA.

More Grants are funded through the IOTA Ecosystem Development Fund (EDF) for open source development.

More Community members with an interest in IOTA and sharing its vision.

Companies
- 280+ patents reference IOTA from 121 unique entities

Research
- 410+ third-party peer reviewed research papers from 452 unique entities

IOTA Grants
- 27 grants (€1.4m+ funded by the Foundation to the Ecosystem)

Community
- 350,000+ individuals

*As of September 2020
Towards Production-Readiness in 2021

2020
IOTA 1.0
MAINNET

NOW
IOTA 1.5
CHRYSLASIS

2021 Q3
IOTA 2.0
COORDICIDE

IRI
Beta Version
1,500 Nodes

HORNET
Complete protocol upgrade
Smart Contracts
Tokenized Assets
10,000 Nodes

BEE
Production-ready
Fully decentralized
100,000+ Nodes
IOTA Networks

Mainnet

IOTA2.0

IOTA Communities

https://ecosystem.iota.org/

https://discord.iota.org/

https://iota.cafe/
IOTA Identity
Secure digital identities for humans, organizations and machines

An implementation based on the IOTA Tangle of W3C standards for Decentralized Identifiers and Verifiable Credentials (VC)

**IOTA Identity** establishes trust and interoperability across organizations, individuals and devices and enables the development of identity solutions in a production ready, open source environment.

It is the only decentralized identity solution that runs on the mainnet of a feeless, permissionless DLT.
IOTA Streams
A second layer protocol that enables encrypted data streams on the Tangle

**Brings together data from multiple sources**
Streams organizes the data from your devices into streams and combines them with complimentary data points.

**Access permissions to strengthen privacy and security**
Streams provides customizable access control configurations for sensitive data streams.

**Ensure the integrity and authenticity of data**
The data underpinning Streams is stored on the Tangle to guarantee data integrity at all times.
Smart Contracts
A second layer protocol that allows for scalable smart contracts on IOTA

Contract owner: consortium of companies
- define the contract
- size of committee
- consensus model

The committee:
# number of nodes running the identical code to yield a result

On-chain transactions
- Hash of contract
- Result of the committee
Tokenized Assets
A solution to deploy custom assets, stablecoins and new currencies on IOTA

Extends utility of IOTA Tokens
Tokenized assets are created ‘on top’ of IOTA Tokens, incentivizing participants to acquire more IOTA tokens as tokenization becomes popular

Regulated securitization and tokenization
IOTA is already working with partners to build fully compliant frameworks for asset tokenization on the network

Create digital twins, real estate and stablecoins
Use tokenization to create asset exchange between financial actors anywhere in the world with no transaction fees
IOTA Adoption
Together with our partners, we empower sustainable development and generate real-world impact.

Selected activities include:

- Digital MRV & Climate Data
- Electric Mobility & Smart Infrastructure
- Smart Cities & Positive Energy Districts
- Supporting Trade infrastructure
- Secure Digital Identities
Overview: Reduce cost of infrastructure while increasing use
Network Operators (CSPs) will face a huge CAPEX issue in the coming years. The challenge is thus to define efficient and straightforward solutions for moving away from the traditional costly “Make / Buy / Rent” models for infrastructure access. Instead of the long term commitment and shared procurement rules for infrastructure use, a more agile as a service/on-demand-based sourcing is needed.

The Solution: The Federated Marketplace
This can be achieved with the creation of a federated DLT-based CPSs Marketplace able to ensure trust and confidence, transparency, traceability and compliance with regulation and legislation, alongside with enabling new revenue opportunities.

Scenario: Infrastructure and assets management - Value: CAPEX reduction
IOTA Solution: Threat sharing and SSI Bridge

**Overview:** Prevent risks and increase security of e-commerce
Prevention of frauds and other cyber-physical threats in e-commerce requires a combination of secure verifiable identities of involved actors as well as the ability to monitor and securely communicate and process threats and incidents information.

**The Solution:** Audit GW and SSI Bridge
The Audit Trail based on IOTA Streams offers a multi-stakeholders channel for fast communication among e-commerce systems.

The Bridge allows e-commerce ecosystem actors including sellers, buyers and payment providers (banks) to register decentralized identities and issue verifiable credentials. Identities and credentials can be created and verified for both individuals and products.

**Scenario:** e-commerce; logistics - **Value:** Security; authenticity
IOTA Solution: P2P Energy Trading

**Overview: Empower sustainable districts**
Use of renewable energy sources (such as solar panels and windmills) can help neighborhoods to be less dependent on microgrid energy and the microgrid to optimise planning. This requires to measure and share information in a trusted way and efficiently settle granular trades.

**The Solution: IOTA Energy tracking and Settlement Layer**
Certified and verified energy sources can share available surplus or request for additional energy. Settlements are recorded onto the IOTA Tangle for future auditability and fast P2P payments.

**Scenario: Smart energy; smart cities; IoT - Value: Data Integrity; Settlement; Monetisation**
Trusted Digital Twins and Edge Computing
Creating new privacy-preserving monitoring and alerting systems

Increasing safety of workers requires monitoring data from trusted devices and generation and sharing of information in a privacy preserving way.

Why IOTA identity
IOTA Identity for wearables allows for tamper-proof credential validation and immutable registration of key events in the lifespan of a worker. This improves the person health and safety monitoring, while improving control and data management.

Sensors IDs can be combined with the owner’s personal ID to enable personalised incident responses in case of emergency.

Scenario: Smart infrastructure; IoT - Value: Data Integrity

- Smart garment: Reports information in real time
- Edge Digital Twin: Analyses behavior and generates credentials locally. Using ZKP information can be shared without revealing secrets
- Employee and HSE: Takes decisions and produce privacy-preserving audits
Digital Monitoring, Reporting & Verification (DMRV)

Overview: GHG data is hard to assess
Current GHG monitoring, reporting and verification (MRV) systems are inefficient and require manual auditing. Amd MRV efforts to digitize data for climate actions lack security, trust, and common standards reducing utility of the data. Data cannot be accessed in real-time and often lacks granularity to enable more informed decision making at a portfolio or asset level.

The Solution: Secure, reliable source data
DMRV leverages IOTA Streams for encrypted data exchange and high availability and levels of assurance. DMRV automates data collection and enables near real-time MRV with reduced need for on-site visits and offers direct integration with standards development. This allows for virtual auditing of facilities and their energy usage and production. It also reduces time and cost while improving the trustworthiness and utility of the data for decision makers.
Case Study: Energy Provenance

Overview: Sustainable Energy Traceability
A lot of energy today, particularly renewables, is difficult to trace back to a point of origin. The ability to trace the origin opens up many business opportunities including carbon credit tokenization and dynamic pricing based on origins.

The Solution: Immutable Energy Production Ledger
A joint project developed by IOTA, JLR, and Engie Labs at the energy-positive Powerhouse building in Trondheim Norway uses IOTA’s immutable DLT to create a tamper-proof record of all energy transactions and sources at the building. This information is then shown in the dashboard of the I-Pace vehicle so the user can see the origin of the energy being used to charge their car.

This was done as part of an EU Horizon 2020 grant where IOTA is working together with 32 partners and across 11 testbeds in Europe to develop localized districts that are a net positive for energy production rather than consumption.

Source: [www.youtube.com/watch?v=9pzd4MPy1AI](https://www.youtube.com/watch?v=9pzd4MPy1AI)
Overview: Enabling new means of transparency
Today's trade is still based on paper documents and outdated processes often involving many actors (public and private). IOTA supports tomorrow’s supply chain where original documents and events are reported in real time and made available to authorized actors. It provides transparency to the process and allows everyone to piggy-back on the original data.

The Solution: Trade and logistics information pipeline
TradeMark East Africa and IOTA are piloting a system that will connect border agencies with overseas customs and local traders for a smarter and more efficient experience.

Early indications suggest that such a system can add more than 5% to the region's GDP with economic opportunities and job creation as results.
Provenance, ethical sourcing, proof of origin, supply chain status, GS1, inventory status, product authenticity etc are all based on “best effort”

No live and fully trusted data are ready available from the source to all / selected supply chain actors or consumers

**THE MISSING PIECES:**
- Physical to digital link
- Fully traceable data back to its source (data accountability)
- Data immutability
Michele Nati
Head of Telco & Infrastructure Development
IOTA Foundation

Michele is responsible to drive IOTA-based innovation and adoption in the Telco & Infrastructure sector. He manages business and technical relations with partners, establish solutions' architecture and manages governance of collaborations. Michele also leads EU projects and IOTA international research collaborations. To date, he matured almost 20 years of research and development in Wireless Sensor Networks and Internet of Things, both in Academia and SMEs.

@michelenati
https://www.linkedin.com/in/michelenati/
Luigi Vigneri
Senior Research Scientist
IOTA Foundation

Luigi is leading the networking team at IOTA Foundation since 2018. His current research interests concern network optimization and scalability in the context of distributed ledger technologies. Prior to IOTA, Luigi joined Huawei Research Lab in Paris as a postdoctoral researcher working on 5G networks, online machine learning and artificial intelligence. In 2017, he obtained his Ph.D. in Mobile Communications from EURECOM, France, with a thesis on caching popular content in vehicular networks.

https://www.linkedin.com/in/luigivigneri/
Questions?

Michele Nati
@iotafoundation
Exercise: Verifiable Credentials for University Grades
Verifiable Credentials for Grades

Story:

- You are coming to an exam in your university
- The professor asks you to authenticate yourself using your passport
- After the exam is done and assessed the professor issues a grade for the exam
- An employer wants to verify the grade

Technical Solution:

- You create an identity which identifies yourself
- Having your passport information the professor is able to assign a trusted verifiable credential to your identity
- After the exam is rated, the professor issues a second verifiable credential with your grade for this exam to your identity
- Using the credentials the employer is able to verify that the grade and personal information are assigned to your identity and issued by the professor/university
Do it yourself - Setup

Supported language: TypeScript

Prerequisite:

- Node.js 8, or Node.js 10 or higher. We recommend the latest LTS.
- A code editor such as Visual Studio Code
- Access to a command-line interface (Optional: Postman)

Checkout the repository or download it as zip at:
https://github.com/iotaledger/e-commerce-tools/

Use the folder: ./clients/summer-school-client

Install dependencies: npm install
Do it yourself - Setup

(As described in the ./clients/summer-school-client/README.md)

1. Create .env file

2. Add following content into the .env file:

   BASE_URL=https://ensuresec.solutions.iota.org/api/v0.1
   API_KEY=94F5BA49-12B6-4E45-A487-BF91C442276D
1. Create and identity

1.0. Run the script inside a command line: `npm run create-identity`
   (Use the folder: `./clients/summer-school-client` to run it)

> An identity will be created and stored on the ledger. In addition, the identity is stored in the
  `./clients/summer-school/src/create-identity/Student.json` file with the private key.

> You can request your identity via GET at the following api in a browser or via Postman by replacing
  `INSERT_IDENTITY_ID` with your identity id (doc.id) to receive information about your identity at the api.

https://ensuresec.solutions.iota.org/api/v0.1/identities/identity/INSERT_IDENTITY_ID?api-key=94F5BA49-12B6-4E45-A487-BF91C442276D

Example GET request for the identity of the professor:

https://ensuresec.solutions.iota.org/api/v0.1/identities/identity/did:iota:7Ub2g1fvWfH5pzE6QECwpXPdiVfv3bXaWBDwJFXM8aGs2?
api-key=94F5BA49-12B6-4E45-A487-BF91C442276D
Do it yourself - Credentials

2. Create verifiable credentials

2.0. Open the index.ts file in the create-credentials folder

2.1. Set your newly created identity id from the Student.json->doc.id as the identityId variable

2.2. Set your claim for the identity like your name and birthDate as the identityClaim variable

2.3. Before creating the credentials you are able to adjust your grade for the exam
   (This will become the signed grade of the professor)

2.4. Save the file and run the script inside a command line: npm run create-credentials
   (Two files are created containing a credential in the folder ./clients/summer-school-client/create-credentials)

> Two credentials will be issued. One for the student containing personal information
  (BasicIdentityCredential.json) and one for the result of the exam (ExamRatingCredential.json).

> These credentials are signed by the professor with the id: did:iota:7Ub2g1fVWfhH5pzE6QECwpXFdiVfV3bXaWBDwJFXM8aGs

> You can request the identity again and you will see the issued verifiable credentials.
Do it yourself - Verification

3. Check the verifiable credentials

3.0. Open the `index.ts` file in the `check-credentials` folder

3.1. Set the `identityCredential` variable to the content of `BasicIdentityCredential.json`

3.2. Set the `examCredential` variable to the content of `ExamRatingCredential.json`

3.3. Save the file and run the script inside a command line: `npm run check-credentials`

> The two credentials will now be checked for their content and validity. Furthermore if the credential is issued by a trusted identity like the professor.

(Optional)

> Try to change the content of the credentials, like the name or rating of the exam. It will then become invalid since it does not match with the hash of the credential!
Verifiable Credentials for Grades

- Learn more at: [https://www.w3.org/TR/did-core/](https://www.w3.org/TR/did-core/)
- You can also explore the identity of the professor or the student at the iota explorer!
- All identities can be accessed by their index which is following after `did:iota`:
  - For instance you can explore the identity with the id: `did:iota:GmJVcwQXeVMMZajxB4sGeQqXoM9FtbrwUzwHeBBUyYe`
  - By requesting the explorer at: [https://explorer.iota.org/mainnet/indexed/GmJVcwQXeVMMZajxB4sGeQqXoM9FtbrwUzwHeBBUyYe](https://explorer.iota.org/mainnet/indexed/GmJVcwQXeVMMZajxB4sGeQqXoM9FtbrwUzwHeBBUyYe)
- Have you noticed that the verifiable credentials are not stored on the tangle?
- What can verifiable credentials also be used for?
  - (You can also adjust the code to issue further credentials)
- For more information or follow up
  - Dominic Zettl, Software Engineer, dominic.zettl@iota.org
Students project: IOTA 2.0
IOTA Project

- **Objectives**
  - Install the IOTA GoShimmer DevNet
  - Build a dApp which uses the random number generator
  - Create and distribute colored tokens
  - TIP: build and test your own local network

- **Prerequisites**
  - Golang: [https://golang.org/](https://golang.org/)
  - Docker: [https://www.docker.com/](https://www.docker.com/)

- **Relevant links**
  - Where to start: [https://goshimmer.docs.iota.org](https://goshimmer.docs.iota.org)
  - GoShimmer repository: [https://github.com/iotaledger/goshimmer](https://github.com/iotaledger/goshimmer)
  - DevNet GUI wallet: [https://github.com/iotaledger/IOTA-2.0-DevNet-wallet/releases/tag/v0.7.0](https://github.com/iotaledger/IOTA-2.0-DevNet-wallet/releases/tag/v0.7.0)
  - How to set up a docker-network: [https://goshimmer.docs.iota.org/tooling/docker_private_network.html](https://goshimmer.docs.iota.org/tooling/docker_private_network.html)
  - How to write a dAPP (chat and network delay examples): [https://goshimmer.docs.iota.org/tutorials/dApp.html](https://goshimmer.docs.iota.org/tutorials/dApp.html)
  - Tokenomics framework: [https://goshimmer.docs.iota.org/protocol_specification/advanced_outputs.html](https://goshimmer.docs.iota.org/protocol_specification/advanced_outputs.html)
  - Wallet: [https://goshimmer.docs.iota.org/tutorials/wallet.html](https://goshimmer.docs.iota.org/tutorials/wallet.html)