



Secure Development and Operations

using OpenZeppelin Contracts & Defender

Jonathan Alexander

jonathan@openzeppelin.com

 @jalex206

Santiago Palladino

santiago@openzeppelin.com

 @smpalladino



Our mission is to protect
the open economy

OpenZeppelin is a software company that
provides **security audits** and **products** for
decentralized systems.

Projects from any size -from new startups to
established organizations- trust OpenZeppelin to
build, inspect and connect to the open economy.



Security, Reliability and Risk Management

OpenZeppelin provides a complete suite of **security and reliability products** to build, manage, and inspect all aspects of software development and operations for decentralized projects.



OpenZeppelin Contracts

Secure building blocks for Solidity

What's in OpenZeppelin Contracts

IERC1155
IERC1155Receiver
ERC1155Receiver
ERC1155Holder
ERC1155
ERC1155Burnable
ERC1155Supply
IERC1155MetadataURI
ERC1155Pausable
ERC1155PresetMinterPauser
IERC777Sender
IERC777
IERC777Recipient
ERC777PresetFixedSupply
ERC777
IERC20
ERC20
TokenTimelock
SafeERC20
ERC20VotesComp
IERC20Metadata
ERC20Wrapper
ERC20Votes
ERC20Burnable
IERC20Permit
ERC20Pausable
ERC20FlashMint

ERC20Permit
ERC20Capped
ERC20Snapshot
ERC20PresetMinterPauser
ERC20PresetFixedSupply
ERC721
ERC721Holder
ERC721Pausable
ERC721Burnable
IERC721Metadata
ERC721Enumerable
ERC721URIStorage
IERC721Enumerable
IERC721Receiver
IERC721
ERC721MinterPauserAutoId
TransparentUpgradeableProxy
ProxyAdmin
IBeacon
UpgradeableBeacon
BeaconProxy
Clones
UUPSUpgradeable
Initializable
ERC1967Proxy
ERC1967Upgrade
Proxy

GovernorCompatibilityBravo
IGovernorCompatibilityBravo
TimelockController
GovernorCountingSimple
GovernorVotes
GovernorTimelockCompound
GovernorTimelockControl
GovernorVotesComp
IGovernorTimelock
GovernorVotesQuorumFraction
Governor
IGovernor
Ownable
AccessControl
AccessControlEnumerable
Pausable
PullPayment
ReentrancyGuard
Create2
Strings
Timers
Counters
Address
SignatureChecker
MerkleProof
ECDSA

EIP712
Context
Multicall
Arrays
IERC1820Registry
IERC165
ERC165Checker
ERC1820Implementer
IERC1820Implementer
ERC165Storage
ERC165
Escrow
ConditionalEscrow
RefundEscrow
SafeCast
Math
SignedSafeMath
SafeMath
StorageSlot
EnumerableMap
EnumerableSet
BitMaps
PaymentSplitter
ERC2771Context
MinimalForwarder
IERC3156
IERC1271

What's in OpenZeppelin Contracts

- **Token standards** (ERCs 20, 721, 777, 1155)
- **Access control** (Ownable, RBAC, Timelock)
- **Proxies** (Minimal, Transparent, UUPS)
- **Meta-transactions** (ERC2771)
- **Utilities** (ECDSA, Merkle proofs, EIP712, ERC165)
- **Security** (Reentrancy guard, Pausable, PullPayment)
- **Governance** (coming soon!)

Bootstrap Contracts

wizard.openzeppelin.com

Deploying upgradeable contracts

- Code an upgradeable ERC721 with the **Wizard**
- Download the code into a **Hardhat** or **Truffle** project
- Deploy an upgradeable instance using an **Upgrade plugin**

OpenZeppelin Defender

Secure operations platform for smart contract systems

Manage our contract, **monitor** token activity,
and **automate** the **minting** of new tokens

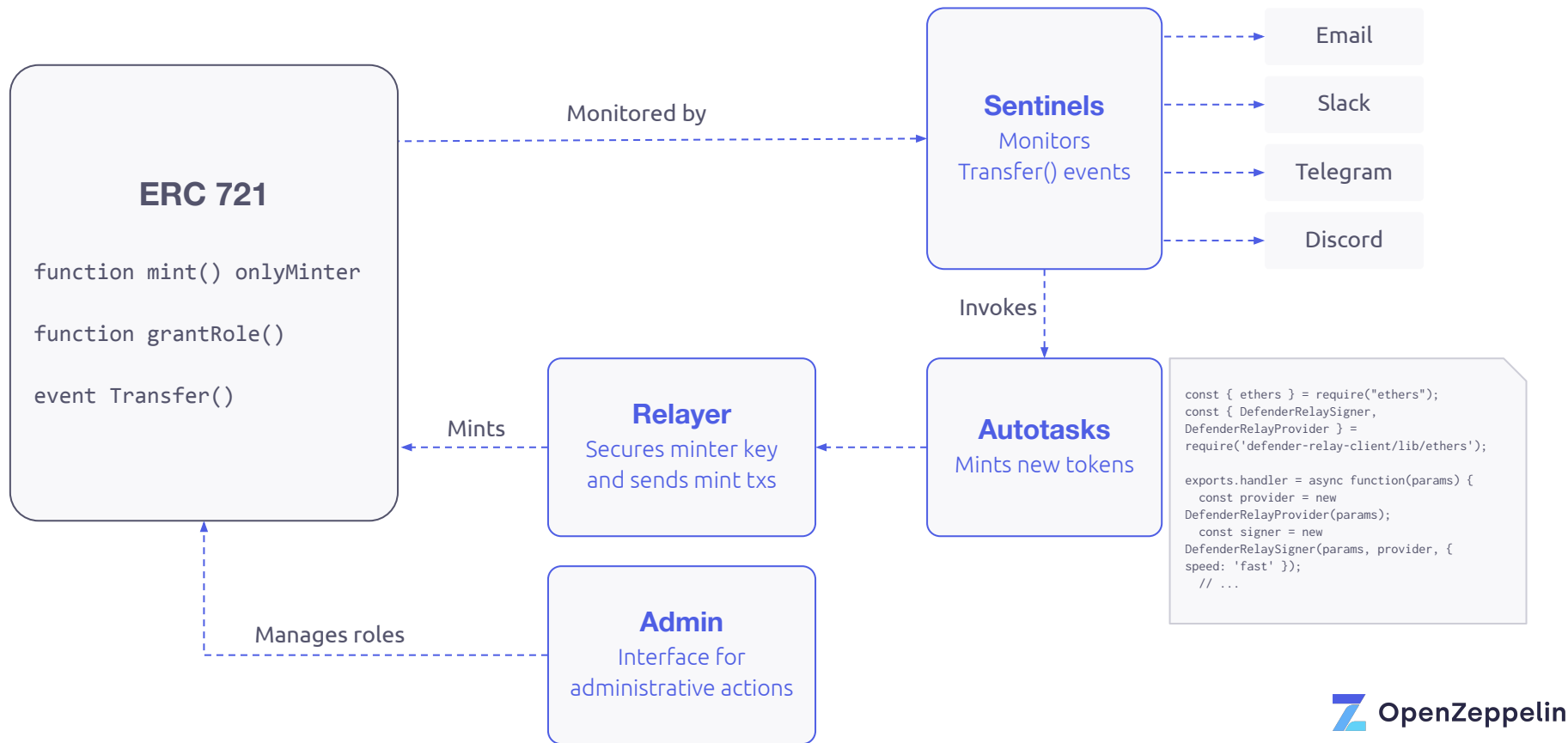
DevSecOps for Smart Contracts

defender.openzeppelin.com

Agenda

- Create a secure **hot wallet** for minting
- Assign the **minter role** to the wallet
- **Automate** the minting of new tokens
- **Monitor** our contract for transfers

Overview of our system



Learn security best practices

Defender **Advisor** 



Thank you!

Learn more

openzeppelin.com

forum.[openzeppelin.com](https://forum.openzeppelin.com)

docs.[openzeppelin.com](https://docs.openzeppelin.com)

Contact

 [@OpenZeppelin](https://twitter.com/OpenZeppelin)

contact@openzeppelin.com

