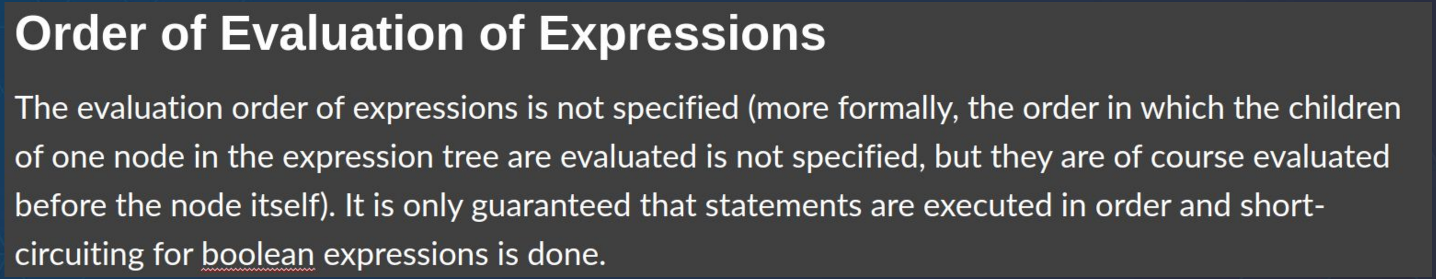
Underhanded Solidity '22

Evaluation Order in Solidity

Dominic Brütsch

Lead Engineer (Founding Partner) | Chainsecurity

Evaluation Order in Solidity



Order of Evaluation of Expressions

The evaluation order of expressions is not specified (more formally, the order in which the children of one node in the expression tree are evaluated is not specified, but they are of course evaluated before the node itself). It is only guaranteed that statements are executed in order and short-circuiting for boolean expressions is done.

f(g(...), h(...)) -> Unclear if g or h is evaluated first

Evaluation Order

```
function fun(uint a) returns (uint) {
    return a + a++;
}
```

- What is the result of fun(2)?
- In this case, we will get 2 + 2 = 4
- But the compiler could give us (2+1) + 2 = 5
- Not specified, so we shouldn't rely on it

In Practice

- This only matters if we can get `unexpected` results
- (Un-)fortunately, there are three cases of unusual evaluation orders
- Found by analyzing the code generator

`addmod` and `mulmod`

```
addmod(a, b, N); // returns (a + b) mod N
mulmod(a, b, N); // returns (a * b) mod N
```

- Arguments evaluated right to left.
- This is documented in the IR-based Codegen Changes
- For example: `f(2)` is evaluated as `addmod(3, 2, 5) = 0`

```
function f(uint a) returns (uint) {
    return addmod(a, a++, 5);
}
```

Events

```
event Hello(uint indexed a, uint b, uint indexed c, uint d);
```

- The parameters of events are evaluated in a bizarre order
- First, the `indexed` params are evaluated right to left
- Then, the remaining params are evaluated left to right
- In the `Hello` event, the order is `c → a → b → d`
- For example: `g(2)` emits `Hello(2, 3, 2, 3)`

```
function g(uint a) {
    emit Hello(a++, a, a, a);
}
```

Underhanded Solidity `22

- Constant product DEX
- Each trade has a fee, which goes to liquidity pool
- Admin fee is proportional to the liquidity increase since the last claim
- Wait for liquidity to increase, raise fees, then steal profits

```
event AdminFeeChanged(uint256 indexed oldFee, uint256 indexed newFee);
function changeAdminFees(uint256 newAdminFee) external onlyAdmin nonReentrant {
    emit AdminFeeChanged(retireOldAdminFee(), setNewAdminFee(newAdminFee));
}
function retireOldAdminFee() internal returns (uint256) {
    // Claim admin fee before changing it
    _claimAdminFees();
    // Let people withdraw their funds if they don't like the new fee
    nextFeeClaimTimestamp = block.timestamp + 7 days;

    return adminFee;
}
function setNewAdminFee(uint256 newAdminFee) internal returns (uint256) {
    adminFee = newAdminFee;
    return newAdminFee;
}
```

About ChainSecurity

- We are focused on blockchain security
- Smart contract audits
- Some of our clients:
  - Maker
  - Curve.fi
  - Compound
  - Aave
  - Yearn
  - 1inch
  - Lido

Thank you!

Dominic Brütsch

Lead Engineer (Founding Partner) | Chainsecurity

dominic.bruetsch@chainsecurity.com

@chain_security

Section 1

Section 1 title here.

Section 1 title here.

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua.

- Sollicitudin
- Consectetur
    - Condimentum
        - **Magna**
        - **Ligula**

Section 1 details with an image. Enter title here.

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum.

Enter your main point / statement here.

Section 1 details with a main point. Enter title here.

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum.

Section 2

Section 2 title here.

Section 2 title here.

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua.

- Sollicitudin
- Consectetur
  - Condimentum
    - **Magna**
    - **Ligula**

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua.

- Sollicitudin
- Consectetur
  - Condimentum
    - **Magna**
    - **Ligula**

Section 2 details with an image. Enter title here.

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum.

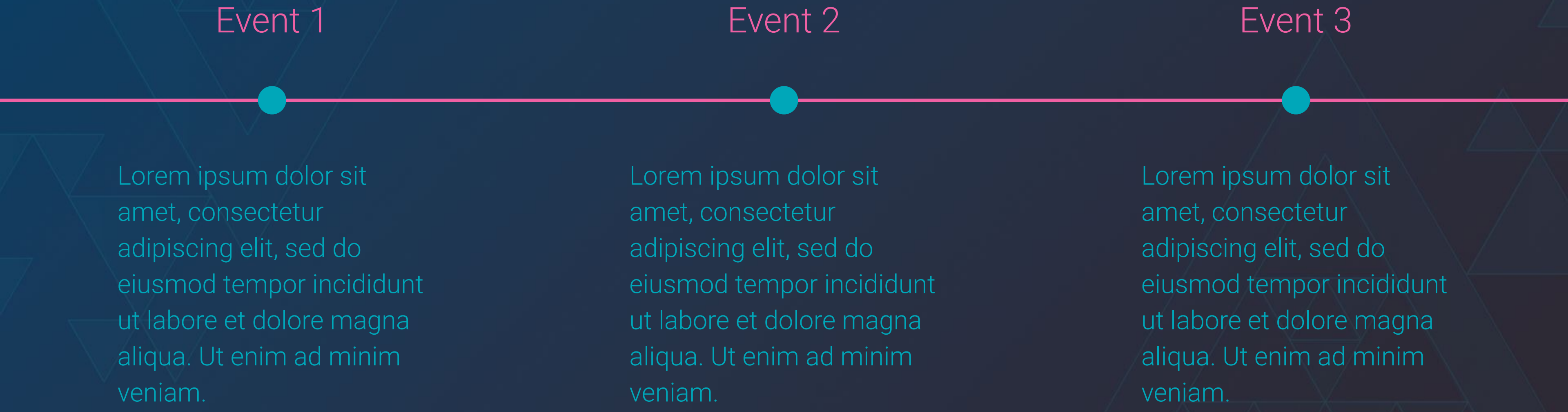
Section 2 details with a main point. Enter title here.

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum.

Enter your main point / statement here.

Enter your main point / statement here.

Here’s the timeline.



Event 1

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam.

Event 2

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam.

Event 3

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam.

Thank you!

Your Name

Your title, your organization

email@emailaddress.com

@twitterhandle