LAB 2 Shared Wallet

* 1. Project Shared Wallet
     1. Kegunaan Dunia Nyata untuk Proyek ini

Tunjangan dana untuk anak per hari/minggu/bulan yang dapat di gunakan

Pegawai memberi tunjangan ke pewawai lainnya untu keperluan biaya perjalanan mereka

Bisnis memberikan kontraktor keperluan dana yang dapat di keluar untuk menggunakan anggaran

* + 1. Pencapaian Dalam Pembuatan

Memiliki sebuah “on-chain wallet smart contract”. Contract wallet dapat menyimpan saldo dan mengizinkan user untuk mengambil dana. Dapat memberikan tunjangan ke orang lain atau pada spesifik user berdasarkan alamat si user. Menggunakan Kembali smart contract yang telah di buat sebelumnya

* 1. Mendifinisikan Smart Contract

Dibawah ini adalah bentuk sederhana smartcontract. Ini dapat menerima ether dan memungkinkan untuk menarik Ether. Tetapi fungsi dari smart contract ini masih belum cukup berguna

Sharedwallet.sol

Text

Description automatically generated

* 1. Pemissions: Mengizinkan

Pada Langkah ini kita akan membatasi pengeluaran saldo ke pemilik wallet itu sendiri. Bagaimana kita menetukan dari pemiliki?

Text

Description automatically generated

Pada code diatas kita juga dapat menambahkan fungsi “onlyOwner” untuk merubah ke fungsi “withdrawMoney”

* 1. Menggukan Kembali kontrak dari OpenZeppllin

Mempunyai logika “owner-logic” langsung didalam smart contract bukan lah hal yang mudah untuk di audit. Maka dari itu cobalah untuk memecah menjadi bagian-bagian kecil dan menggunakan smart contract yang telah di audit dari OpenZeppelin. Pada build OpenZepplin yang terbaru sudah tidak memiliki fungsi “isOwner” maka dari itu kita menambahkannya sendiri.

Text

Description automatically generated

* 1. Permission: Menambahkan Pengeluaran untuk Roles Luar

Pada Langkah ini kita menambahkan mapping, jadi kita dapat menyimpan address => uint amounts. Ini akan seperti array Ketika disimpan

Text

Description automatically generated

Jika kita jeli pada smart contract yang kita buat ini masih ada bug, yaitu bug double spending

* 1. Improve/Fix Pengeluaran Guna Menghindari Double Spending

Dengan tidak mengurangi dana pada transaksi, seseorang adapat bertransaksi secara terus menerus dengan jumlah yang sama terus menerus. Pada kode dibawah ini kita mencoba membuat smart contract dengan mengurangi saldo untuk semuanya selain pemiliki.

Text

Description automatically generated

* 1. Improve Struktur Smart Contract

Hingga disini kita sudah mengetahui fungsi basic dari structure smart contract. Untuk dapat mudah dibaca oleh developer lainnya, ada baiknya kita memecah dari fungsi smart contractnya

Text

Description automatically generated

* 1. Menambahkan Event di Dalam Allowance Smart Contract

Disini kita akan menambahkan contract tetapi biarkan kosong terlebih dahulu

Text

Description automatically generated

* 1. Menambahkan Event didalam kontrak shared wallet

Text

Description automatically generated

* 1. Menambahkan Library SafeMath untuk Operasi Aritmatik

Berdasarkan dari source code SafeMath Library operasi aritmatik pada solidity dibungkus didalam overlow. Ini dapat menghasilkan bug, karena programmer biasanya mengasumsi terjadi error overflow, yang dimana adalah prilaku standard di dalam high level programming languages. SafeMath mengembalikan pemikiran ini dengan mengembalikan transaksi jika operasi terjadi overflow. Pada update solidity terbaru tipe variable interger sudah tidak bisa overflow lagi, ini berlaku dari solidity versi diatas 0.8.

Jika anda masih menggunakan solidity versi dibawah 0.8 maka tambahkan kode dibawah ini

Text

Description automatically generated

Tetapi karena kita menggunakan solidity versi 0.8 keatas maka ini tidak perlu ditambahkan pada kode smart contract kita

* 1. Menghapus dari fungsi “Renounce Ownership”

Langkah selanjutnya hilangkan fungsi untuk menghapus pemilik. Kita hanya menghentikan ini dengan pengembalian. Tambahkan fungsi berikut ke Shared Wallet:

Text

Description automatically generated

* 1. Memindahkan Smart Contract Menjadi File yang Terpisah

Pada tahapan ini kita akan memisahkan file dan menggunakan fungsi import

SharedWallet.sol

Text

Description automatically generated

Allowance.sol

Text

Description automatically generated