BNDES

O banco nacional
do desenvolvimento

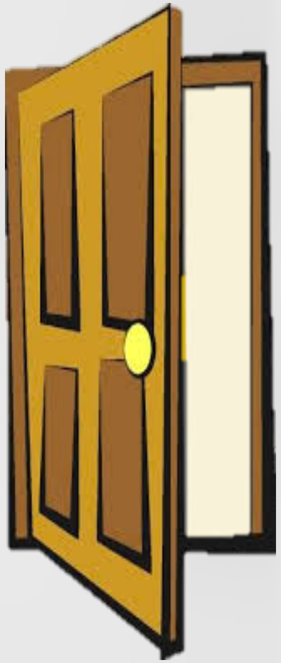
Requirements for Change Management in DLT-Based Decentralized Applications

April 2021

Classificação: Documento Ostensivo
Unidade Gestora: ATI

Trust and Applications

Centralized Apps



dApps + DLT

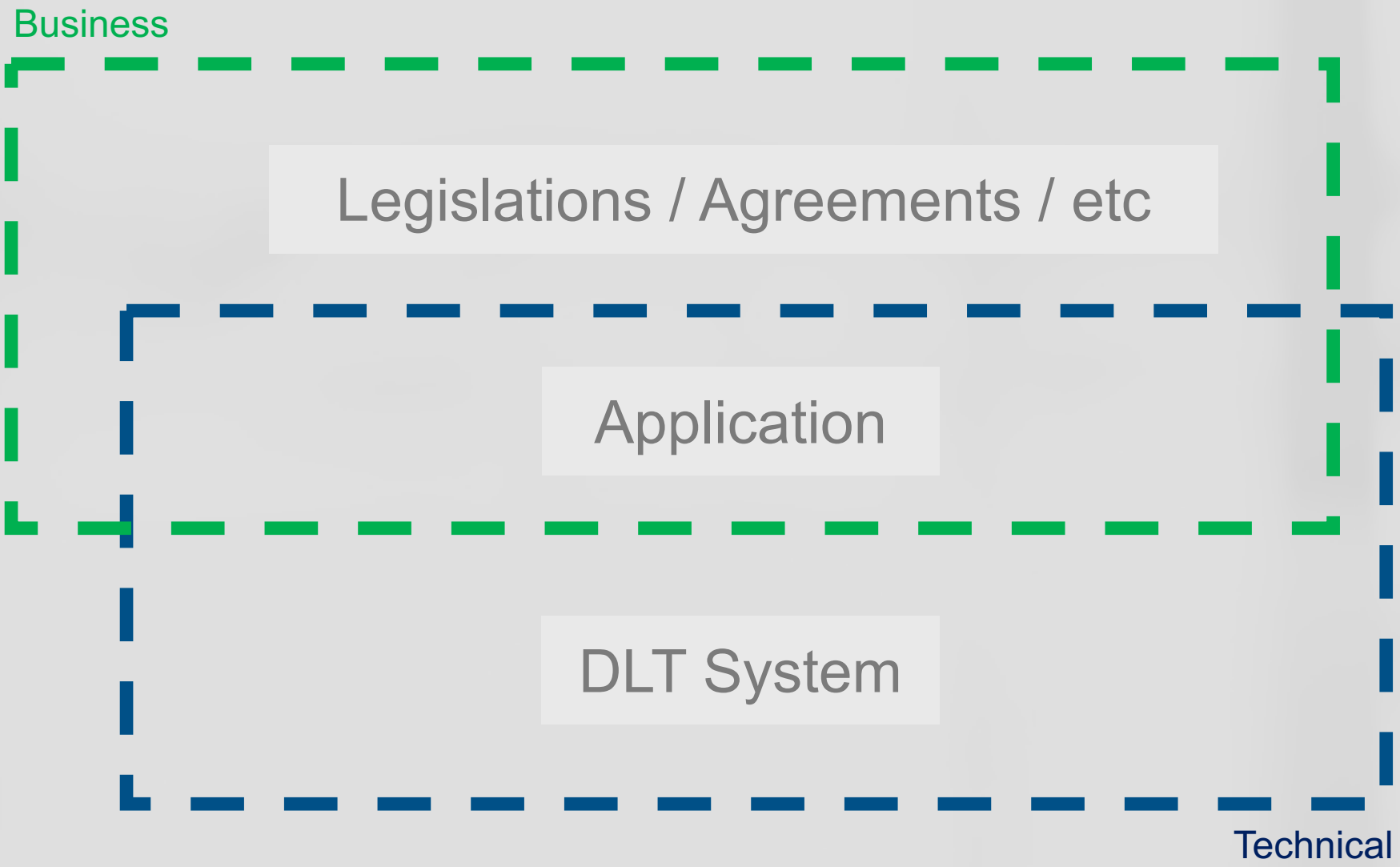
Simplified to one door

>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>

Trust in the immutability of an application (in general)

What Immutability?

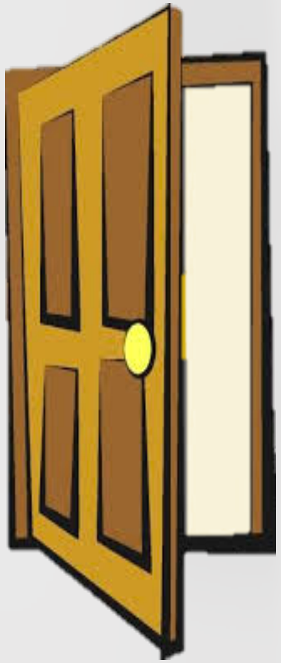
BNDES



Trust and Applications

Centralized Apps

Apps with
“Managed Mutability”



dApps + DLT

>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>

Trust in the immutability of an application (in general)

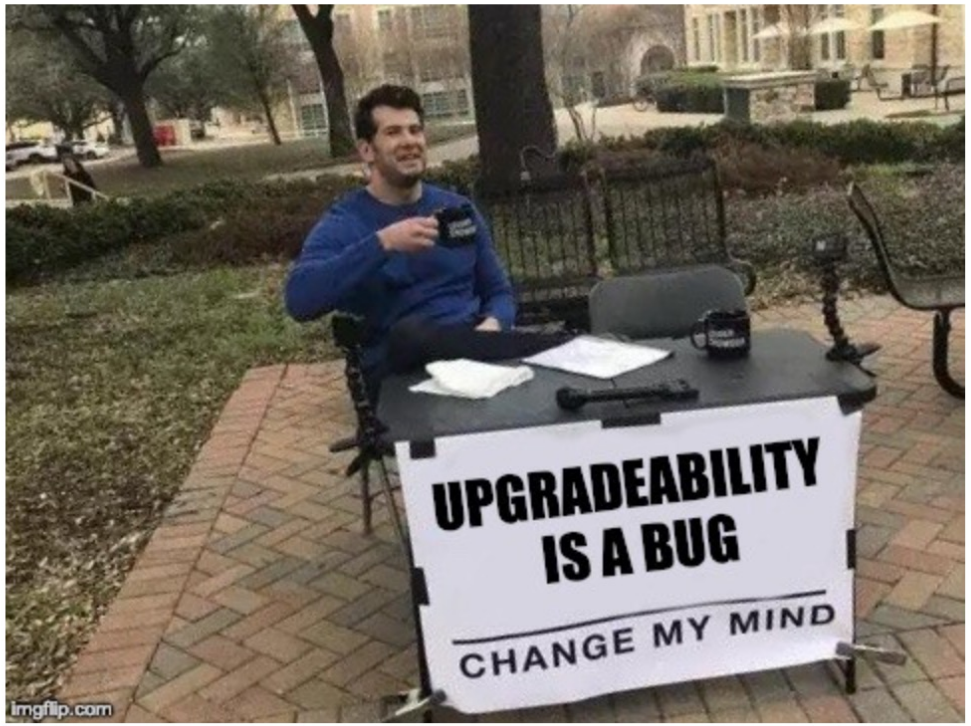
Bug or Feature?

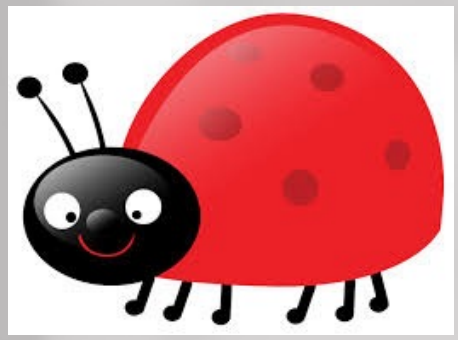
BNDES

Upgradeability Is a Bug

Steve Marx Follow

Feb 5, 2019 · 5 min read





Example – Changing a Bank Contract

```
function changeBankFee(uint256 percentual, string memory description) public onlyOwner {
        require (percentual < 100, "Fee > 100%");
        bankFee = percentual;
        emit ManualIntervention_Fee(percentual, description);
}
```

Enables a change to fixed fee ✓

Enables unexpected changes ✗

https://blog.coinbase.com/usdc-v2-upgrading-a-multi-billion-dollar-erc-20-token-b57cd9437096

Change Management in DLT-based dApp

BNDES

OpenZeppelin | docs

A smart contract upgrade is an action that can arbitrarily change the code executed in an address while preserving storage and balance.

https://blog.openzeppelin.com/the-state-of-smart-contract-upgrades/

Change Management Requirements

BNDES

(3) **Governance**
Ensuring that the application governance works appropriately

(2) **Transparency**
Providing stakeholders with trust in the change management process

(1) **Upgradeability**
Facilitating the evolution of an application that uses smart contracts

Change Management Requirements

BNDES

(1) Upgradeability

Facilitating the evolution of an application that uses smart contracts

a) preserve the access to the data originally used by the current smart contracts to the future smart contracts, as a way to minimize data migration;
b) in the context of a change, make it feasible to alter data used by the current smart contracts in a way that is not possible without a change;
c) in the context of a change, make it feasible to alter the data structure used by the current smart contracts in a way that is not possible without a change;
d) expose an immutable way of finding the current version of the smart contracts (sometimes called “proxy contract”);
e) preserve some parts of the code from the current smart contracts as non-upgradeable;
f) preserve the quality of the smart contracts codes throughout time, even after various evolutions;
g) In the context of a change, enable or not the choice for application users to opt between stay managed by the current smart contracts, migrate to the future smart contracts or even finish the relationship with the smart contracts (if the user can choose, it is known as “you-are-free-to-opt-out” principle);

Change Management Requirements

BNDES

(2)

Transparency

Providing stakeholders with trust in the change management process

a) establish that changes go through a life cycle, which includes proposal, approval, execution, and conclusion or canceling;
b) associate the change with off-chain information that spells out its motivation and the rationale adopted for the solution;
c) guarantee that every change is executed through an automatized change script;
d) make change proposal (including change script) available for analysis of the application governance before the change approval;
e) avoid the execution of changes that do not go through the change process;
f) provide transparency regarding which changes were proposed and what happened to these propositions;
g) work out a system to monitor the changes in progress;
h) enable the introduction of a time gap between the approval and the execution of the change, which would allow the users to take some time to decide what to do regarding the imminent application change as well as allow the development team to create an additional safety mechanism.

Change Management Requirements

BNDES

(3)

Governance

Ensuring that the application governance works appropriately

(a) include a mechanism to aid the group's decision-making process;
(b) provide a mechanism for the creation of subgroups to decide on specific changes;
(c) support the classification of changes in different levels of formality regarding deployment, which will depend on how high the change impact will be and how urgent it needs to be implemented;
(d) support the definition of rules concerning the inclusion or elimination of members of the application governance;
(e) enable the participation of the governance structure since the very first deployment of the smart contracts.

Change Management Requirements

BNDES

Application deployed in the context of a change management process to maximize trust of stakeholders
(discussions off-chain + formalities on-chain)

(3) **Governance**
Ensuring that the application governance works appropriately

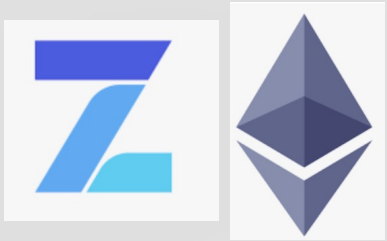
(2) **Transparency**
Providing stakeholders with trust in the change management process

(1) **Upgradeability**
Facilitating the evolution of an application that uses smart contracts

What do we have today?

Examples:

EOS



Ethrereum + OpenZeppelin

Xuperchain

Hyperledger Fabric v2.x

Enables a new class of apps to be deployed on DLT

Additional concerns in real life: Complexity / Execution cost / Existing smart contract standards

Obrigada!

Portal BNDES
www.bndes.gov.br

Atendimento Empresarial
0800 702 6337
Chamadas internacionais
+55 21 2052 6337

Ouvidoria
0800 702 6307
www.bndes.gov.br/ouvidoria

Fale Conosco
www.bndes.gov.br/faleconosco

facebook.com/bndes.imprensa

twitter.com/bndes_imprensa

youtube.com/bndesgovbr

slideshare.net/bndes

BNDES O banco nacional do desenvolvimento

MINISTÉRIO DA ECONOMIA

PÁTRIA AMADA BRASIL GOVERNO FEDERAL