



**ČVUT**  
ČESKÉ VYSOKÉ  
UČENÍ TECHNICKÉ  
V PRAZE

# Domain-Specific Languages for Off-chain UI in Decentralized Applications

Bc. Petr Ančinec

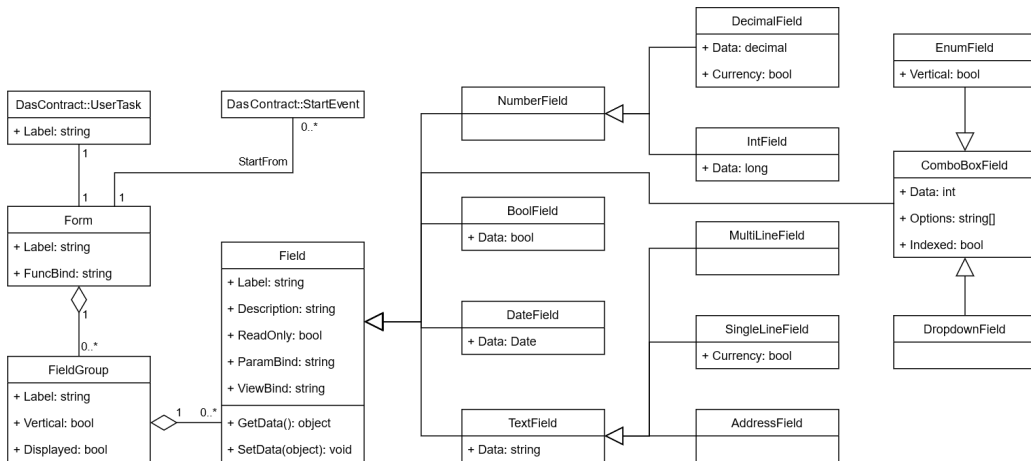


# Cíle práce

- Prozkoumat **technologie** spojené s **blockchainem** (decentralizované aplikace, chytré kontrakty, interakce, peněženky)
- Prozkoumat **standardy** a **přístupy** k deklarativnímu vývoji **uživatelského rozhraní**
- Navrhnout **doménově specifický jazyk** pro **uživatelské rozhraní** decentralizovaných aplikací vytvořených pomocí **Das Contractu**
- Vytvořit **webové aplikace** na podporu tohoto jazyka (editor, interpret)

# Nový doménově specifický jazyk

- Umožňuje **oboustrannou komunikaci** s chytrými kontrakty
- Používá k tomu **formuláře**
- Používá **ořezaný XML formát** k zápisu jazyka
- Inspirace z **XAML** od Microsoftu
- Podobný HTML/XAML, **jednoduchý na pochopení**



Metamodel nového jazyka

Form
+ Label: string
+ FuncBind: string

```
<Form Label="string" FuncBind="string">
  FieldGroup*
</Form>
```

FieldGroup
+ Label: string
+ Vertical: bool
+ Displayed: bool

```
<FieldGroup Label="string" Vertical="bool" Displayed="bool">
  Field*
</FieldGroup>
```

AddressField

```
<AddressField Label="string" Description="string" ReadOnly="bool" ParamBind="string" ViewBind="string" />
```

SingleLineField
+ Currency: bool

```
<SingleLineField Label="string" Description="string" ReadOnly="bool" ParamBind="string" ViewBind="string" Currency="bool" />
```

IntField

```
<IntField Label="string" Description="string" ReadOnly="bool" ParamBind="string" ViewBind="string" />
```

EnumField
+ Vertical: bool

```
<EnumField Label="string" Description="string" ReadOnly="bool" ParamBind="string" ViewBind="string" Indexed="bool" Vertical="bool">
  <Option>string</Option>*
</EnumField>
```

DropdownField

```
<DropdownField Label="string" Description="string" ReadOnly="bool" ParamBind="string" ViewBind="string" Indexed="bool">
  <Option>string</Option>*
</DropdownField>
```

Třídy bez XML  
reprezentace

Field
+ Label: string
+ Description: string
+ ReadOnly: bool
+ ParamBind: string
+ ViewBind: string

TextField

NumberField

ComboBoxField
+ Options: string[]
+ Indexed: bool

```
<Form Label="Apply for a mortgage" FuncBind="ApplyForaMortgagePayable">
  <FieldGroup Label="My details">
    <AddressField Label="My ETH Address" ReadOnly="true" ViewBind="const:myAccountAddress" />
    <AddressField Label="Contract ETH Address" ReadOnly="true" ViewBind="const:myContractAddress" />
  </FieldGroup>
  <FieldGroup Label="Submit mortgage application">
    <IntField Label="Property ID" ParamBind="propertyId" Description="ID of an ERC721 HouseToken." />
    <SingleLineField Label="Property price (Ether)" Currency="true" ParamBind="propertyPrice" />
    <DecimalField Label="Mortgage duration (months)" ParamBind="mortgageDurationMonths" ReadOnly="true" ViewBind="const:60" />
    <SingleLineField Label="Mortgage downpayment (Ether)" Currency="true" ParamBind="const:payValue" Description="Upfront payment." />
    <DateField Label="Mortgage starting date" ParamBind="startDate" />
    <BoolField Label="Terms and Conditions" ParamBind="tosAgree" />
  </FieldGroup>
</Form>
```

**Ukázka kódu formuláře pro decentralizovanou hypotéku**

### Apply for a mortgage

**My details**

My ETH Address

Contract ETH Address

**Submit mortgage application**

Property ID

Property price (Ether)

Mortgage duration (months)

Mortgage downpayment (Ether)

**Mortgage starting date**

5/8/2021 12:10:00 PM

☐ Terms and Conditions

**SUBMIT**

# Aplikace pro podporu jazyka

- Komponenta pro **zobrazování formulářů**
- **Validace XML a převod** do tříd metamodelu
- **Renderování** metamodelu do HTML



# Aplikace pro podporu jazyka

- **Editor formulářů**
- Založený na **Monaco editoru** (VS Code)
- Většina funkcionalit jako ve **VS Code** včetně našeptávání
- Ověření správnosti formuláře
- Náhled formuláře

NEW UPLOAD SAVE RENDER MODEL VALID: 

```

34 </Form>
35
36 <!-- BORROWER -->
37 <form Label="Apply for a mortgage" FuncBind="ApplyForMortgagePayable">
38   <FieldGroup Label="My details">
39     <AddressField Label="My ETH Address" ReadOnly="true" ViewBind="const:myAccountAddress" />
40     <AddressField Label="Contract ETH Address" ReadOnly="true" ViewBind="const:myContractAddress" />
41   </FieldGroup>
42
43   <FieldGroup Label="Submit mortgage application">
44     <IntField Label="Property ID" ParamBind="propertyId" Description="ID of an ERC721 HouseToken that" />
45     <SingleLineField Label="Property price (Ether)" Currency="true" ParamBind="propertyPrice" />
46     <IntField Label="Mortgage rate (K)" ParamBind="rate" />
47     <IntField Label="Mortgage duration (months)" ParamBind="mortgageDurationMonths" />
48     <SingleLineField Label="Mortgage downpayment (Ether)" Currency="true" ParamBind="const:payValue" />
49   </FieldGroup>
50 </Form>
51
52 <form Label="Cancel mortgage application" FuncBind="CancelApplication">
53   <FieldGroup Label="My details">
54     <AddressField Label="My ETH Address" ReadOnly="true" ViewBind="const:myAccountAddress" />
55     <AddressField Label="Contract ETH Address" ReadOnly="true" ViewBind="const:myContractAddress" />
56   </FieldGroup>
57
58   <FieldGroup Label="Cancellation details">
59     <MultilineField Label="Cancellation reason" ParamBind="reason" />
60   </FieldGroup>
61 </Form>
62
63 <form Label="Pay mortgage fee" FuncBind="PayMortgageFeePayable">
64   <FieldGroup Label="My details">
65     <AddressField Label="My ETH Address" ReadOnly="true" ViewBind="const:myAccountAddress" />
66     <AddressField Label="Contract ETH Address" ReadOnly="true" ViewBind="const:myContractAddress" />
67   </FieldGroup>
68
69   <FieldGroup Label="Payment">
70     <SingleLineField Label="Amount (Ether)" Currency="true" ParamBind="const:payValue" Description="Ye" />
71   </FieldGroup>
72 </Form>
73
74 <!-- LENDER -->
75 <form Label="Escrow money" FuncBind="EscrowMoneyPayable">
76   <FieldGroup Label="My details">
77     <AddressField Label="My ETH Address" ReadOnly="true" ViewBind="const:myAccountAddress" />
78     <AddressField Label="Contract ETH Address" ReadOnly="true" ViewBind="const:myContractAddress" />
79   </FieldGroup>
80
81   <FieldGroup Label="Escrow">
82     <SingleLineField Label="Amount (Ether)" Currency="true" ParamBind="const:payValue" />
83   </FieldGroup>
84 </Form>
85
86 <form Label="Request default" FuncBind="RequestDefault">

```

## Apply for a mortgage

### My details

My ETH Address

Contract ETH Address

### Submit mortgage application

Property ID

0

Property price (Ether)

Mortgage rate (%)

0

Mortgage duration (months)

0

Mortgage downpayment (Ether)

SUBMIT

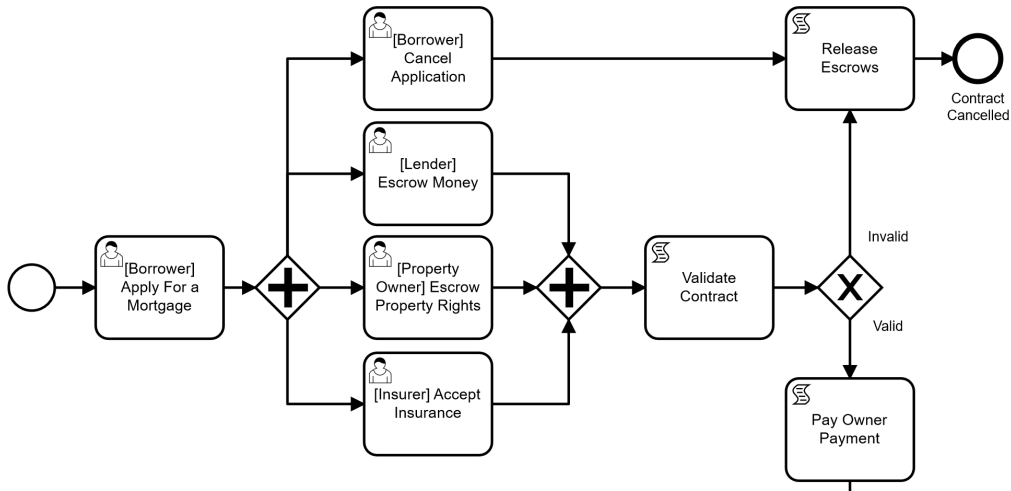
## Cancel mortgage application


### My details


My ETH Address


# Aplikace pro podporu jazyka

- **Interpret formulářů** pro Ethereum
- Integrace s doplňkem MetaMask
- **Nasazení i sledování** existujícího chytrého kontraktu
- Práce s chytrými kontrakty (Das Contract i obyčejné)
- Podpora **rolí a návaznosti akcí** u Das Contractu




 DASHBOARD

 NEW CONTRACT


 JOIN EXISTING

Contract list

Mortgage contract
 

Mortgage details
 

Apply for a mortgage

Manage properties
 

Create property token
   
 Give property token access

## Apply for a mortgage

My details

My ETH Address  
 0x317534725794dfbcd52b6993d8eedfc79598a80f

Contract ETH Address  
 0x6e76ddb4c4e2c01DaF48c2C97F8E718068FE2A908

Submit mortgage application

Property ID  
 0

Property price (Ether)  
 10


Mortgage rate (%)  
 5

Mortgage duration (months)  
 60


Mortgage downpayment (Ether)  
 1.1

SUBMIT

Extension: (MetaMask) - MetaMask

 Borrower

https://localhost:44309  
 CONTRACT INTERACTION

 1.1

DETAILS

DATA

GAS FEE  
 No Conversion Rate Available  
 0.042


Gas Price (GWEI)  
 20  
 Gas Limit  
 2100000

TOTAL  
 No Conversion Rate Available  
 1.142


Reject

Confirm


Interpret formulářů - decentralizovaná hypotéka Das Contract



DASHBOARD



NEW CONTRACT



JOIN EXISTING

Contract list

- Manage properties
  - Create property token
  - Give property token access
- Mortgage contract
  - Mortgage details
  - Pay mortgage fee

## Mortgage details

**My details**

My ETH Address  
0x317534725794dfbcd52b6993d8eedfc79598a80f

Contract ETH Address  
0xe76ddbC4E2C01DaF48c2C97fBE718068FEZA908

Contract balance (Ether)  
0

**Mortgage details (view only)**

Property ID  
0

Property price (Ether)  
10

Mortgage rate (%)  
5

Mortgage downpayment (Ether)  
1.1

Mortgage duration (months)  
60

Total paid on mortgage (Ether)  
0

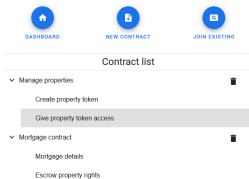
**Insurance details (view only)**

☒ Insurance active

Additional information  
I accept

**Additional info (view only)**

☐ Mortgage contract completed



### Give property token access

**My details**

My ETH Address  
0x0bd3bdf1d8b6a88b6d49f83f2acd120c7395e

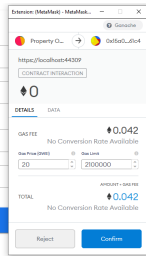
Contract ETH Address  
0x15a0876600A6C2A93c2ab6EECF94e25484461c4

**Give token rights to a contract**

Contract address  
0x6e76ddbC4E2C01DaF48c2C97F8E71806BFE2A908

Token ID  
0

**SUBMIT**



Interpret formulářů - práce s ERC721 tokenem

# Nasazení a decentralizace

- Blazor WebAssembly (C#)
- GitHub (MIT licence): <https://github.com/ancinpet>
- Microsoft Azure
- **Editor:** <https://yellow-beach-0c4abc503.azurestaticapps.net>
- **Interpret:** <https://witty-bay-09186f103.azurestaticapps.net>



# Závěr

- Průzkum **standardních přístupů** k deklarativnímu **uživatelskému rozhraní**
- Návrh nového **doménově specifického jazyka** pro **uživatelské rozhraní** decentralizovaných aplikací vytvořených pomocí **Das Contractu**
- Editor formulářů
- Interpret formulářů pro Ethereum
- Nasazení a dostupnost

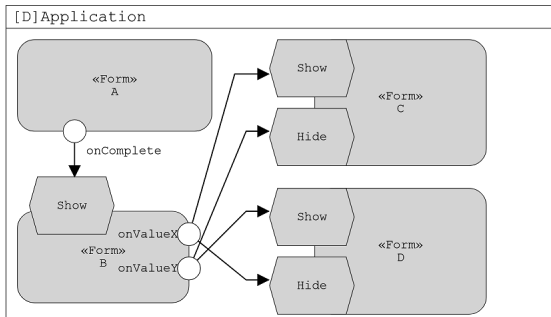
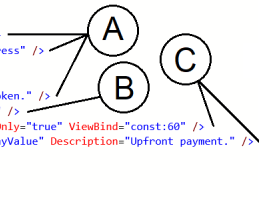
**Děkuji za pozornost!**

**V závěru zmiňujete, že budoucí rozšíření by mohlo zahrnovat více různé interaktivity ve formulářích. Tím se ale zřejmě podstatně zesložití DSL, není možné, že v takovém případě se ukáže, že IFML zavržený mimojiné z důvodu složitosti by býval byl lepší volbou?**

```

<Form Label="Apply for a mortgage" FuncBind="ApplyForaMortgagePayable">
  <FieldGroup Label="My details">
    <AddressField Label="My ETH Address" ReadOnly="true" ViewBind="const:myAccountAddress" />
    <AddressField Label="Contract ETH Address" ReadOnly="true" ViewBind="const:myContractAddress" />
  </FieldGroup>
  <FieldGroup Label="Submit mortgage application">
    <IntField Label="Property ID" ParamBind="propertyId" Description="ID of an ERC721 HouseToken." />
    <SingleLineField Label="Property price (Ether)" Currency="true" ParamBind="propertyPrice" />
    <DecimalField Label="Mortgage duration (months)" ParamBind="mortgageDurationMonths" ReadOnly="true" ViewBind="const:60" />
    <SingleLineField Label="Mortgage downpayment (Ether)" Currency="true" ParamBind="const:payValue" Description="Upfront payment." />
    <DateField Label="Mortgage starting date" ParamBind="startDate" />
    <BoolField Label="Terms and Conditions" ParamBind="tosAgree" />
  </FieldGroup>
</Form>

```



\* Pouze ukázka,  
neodpovídá IFML standardu