22. Internationales Rechtsinformatik Symposion
IRIS 2019, Rechtsvisualisierung II
February 22nd 2019, Salzburg

A Comparison of Approaches for Visualizing Blockchains and Smart Contracts

Felix Härer and Hans-Georg Fill

A Comparison of Approaches for Visualizing Blockchains and Smart Contracts

UNIVERSITÉ DE FRIBOURG / UNIVERSITÄT FREIBURG | FACULTÉ DES SCIENCES ECONOMIQUES ET SOCIALES / WIRTSCHAFTS- UND SOZIALWISSENSCHAFTLICHE FAKULTÄT
Digitalization and Information Systems Group | Felix Härer | Hans-Georg Fill

1. Introduction

The Digitalization of Contracts

Today, any individual, legal entity or software may engage in blockchain transactions.

Preconditions:

1. Digitalization of Documents

   Written Documents → Digital Documents *Representational Change*

2. Digitalization of Transactions

   Transaction Records → Blockchain Transactions *Operational Change*

How can Effects be Understood, Evaluated and Shaped?

3. Digitalization in the form of a "Crypto-Law System"?

   Blockchain Transactions → Algorithmic Enforcement? *Systemic Change?*

1. Introduction

Blockchain-based Enforcement of

- Transactions, e.g. in Bitcoin
- Smart Contracts, e.g. in Ethereum

⟷

Legal Implications of

- Monetary Transactions
- Actual Contracts

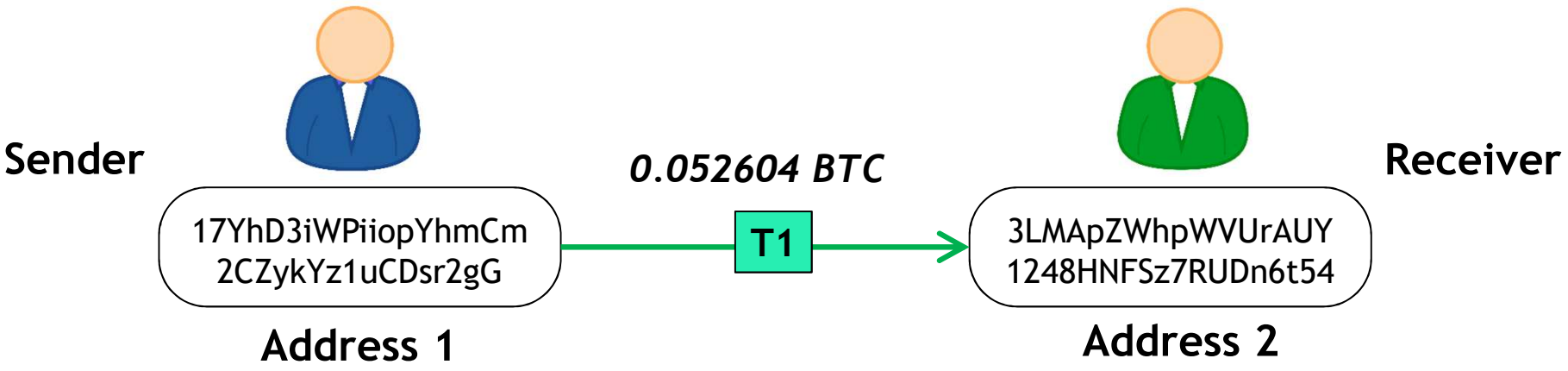
How to Interact with Blockchains from a legal and not necessarily technical point of view?

1. **Analysis:** ***How can Transactions and Smart Contracts be analysed?***
2. **Design:** ***How can Legal Applications and Smart Contracts be designed?***

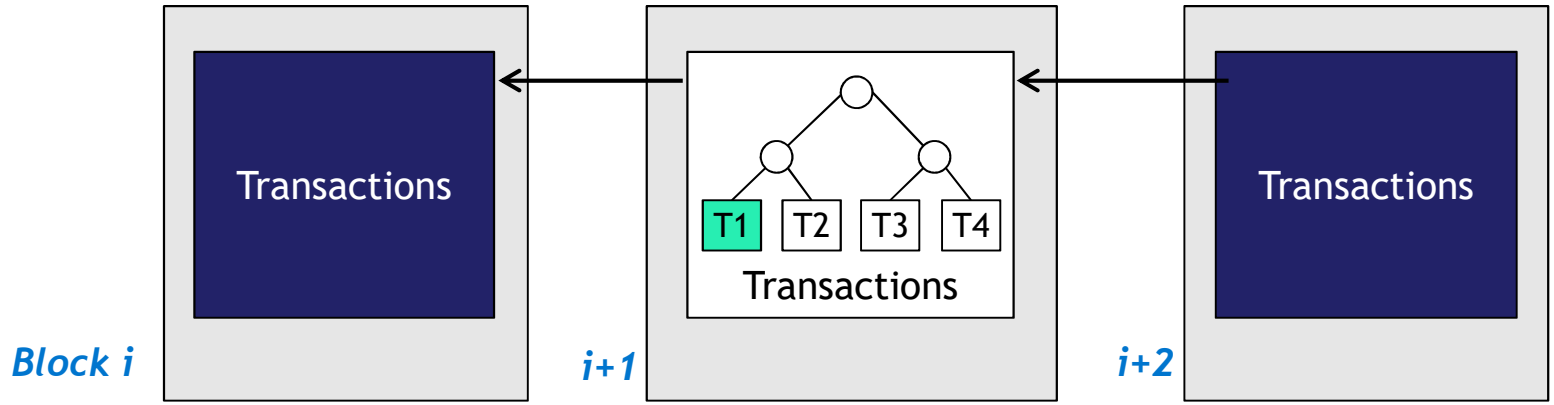
A Comparison of Approaches for Visualizing Blockchains and Smart Contracts

2. Blockchain Foundations – Distributed Ledger Blockchains

Key Concept:
Transaction for the Transfer of Value

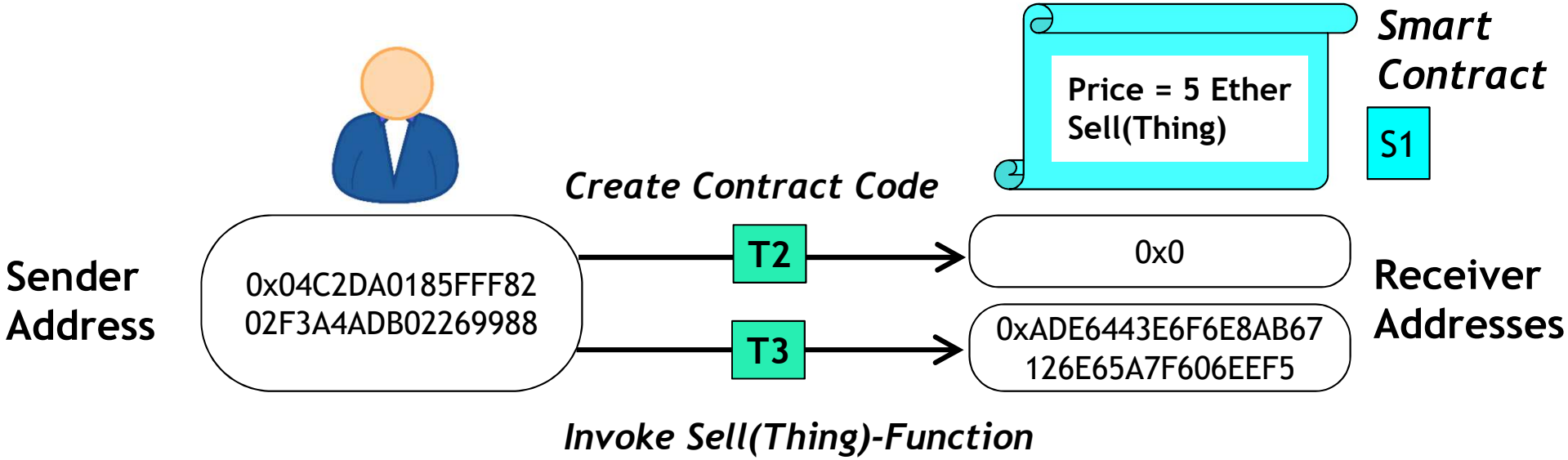


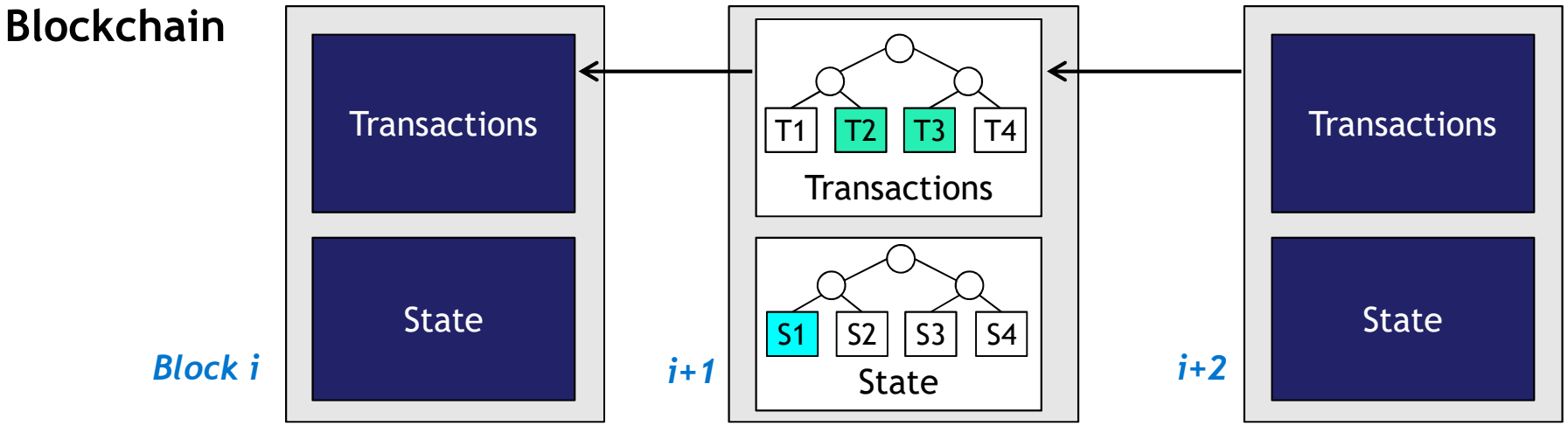
Blockchain



2. Blockchain Foundations – Smart Contract Blockchains

Transactions: Transfer OR Create OR Invoke

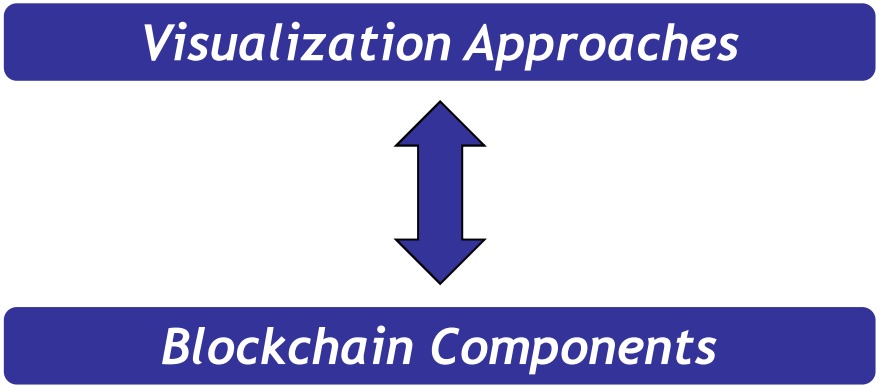




A Comparison of Approaches for Visualizing Blockchains and Smart Contracts

3.1. Classification Framework

Distributed Ledger		Smart Contract	
Design	Analyis	Design	Analysis
3	6	3	4



3.2. DISTRIBUTED LEDGER · DESIGN · MODEL DRIVEN DESIGN

Gaur et al. 2018

Model File
models/org.example.loc.cto

Script File

```
async function initialApplication(application) { // eslint-disable-line no-unused-vars
  const factory = getFactory();
  const namespace = 'org.example.loc';

  const letter = factory.newResource(namespace, 'LetterOfCredit', application.letterId);
  letter.applicant = factory.newRelationship(namespace, 'Customer', application.applicant.getIdentifier());
  letter.beneficiary = factory.newRelationship(namespace, 'Customer', application.beneficiary.getIdentifier());
  letter.issuingBank = factory.newRelationship(namespace, 'Bank', application.applicant.bank.getIdentifier());
  letter.exportingBank = factory.newRelationship(namespace, 'Bank', application.beneficiary.bank.getIdentifier());
  letter.rules = application.rules;
  letter.productDetails = application.productDetails;
  letter.evidence = [];
  letter.approval = [factory.newRelationship(namespace, 'Customer', application.applicant.getIdentifier())];
  letter.status = 'AWAITING_APPROVAL';
```

Model

Step 6
Shipment Accepted

Contract Details

Application Request	Supplier Request	Product Details
NAME	NAME	TYPE
Alice Hamilton	Bob Appleton	Computer
COMPANY NAME	COMPANY NAME	QUANTITY
QuickFix IT	Conga Computers	1250

Address Address

Contract Terms

However, this Contract is not „Smart“!

Terms of Letter of Credit

- The correct quantity of product has been delivered.
- The product was received within 30 days of the placement of the order.
- The product is not damaged and functions as expected.

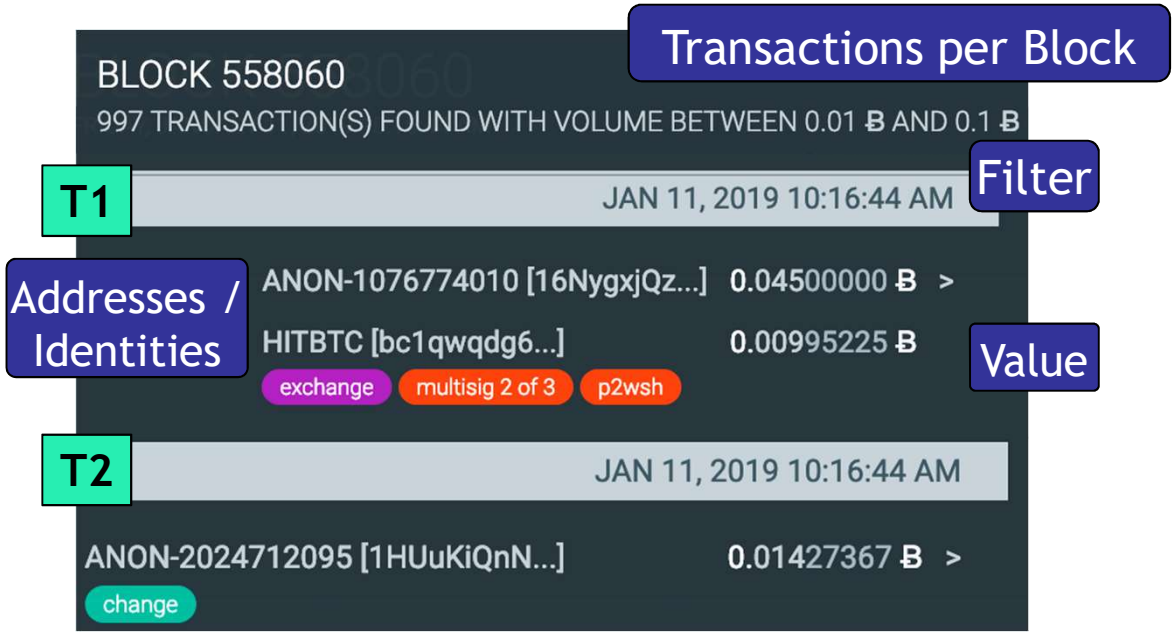
Edit

Transactions

2018-06-09, 07:43:19	Close	T4
2018-06-09, 07:42:35	ReadyForPayment	T3
2018-06-09, 07:41:31	ReceiveProduct	T2
2018-06-09, 07:38:37	ShipProduct	T1

3.2. DISTRIBUTED LEDGER · ANALYSIS · BLOCK/ADDRESS/TRANSACTION

Block Explorer Tools, e.g. OXT.me

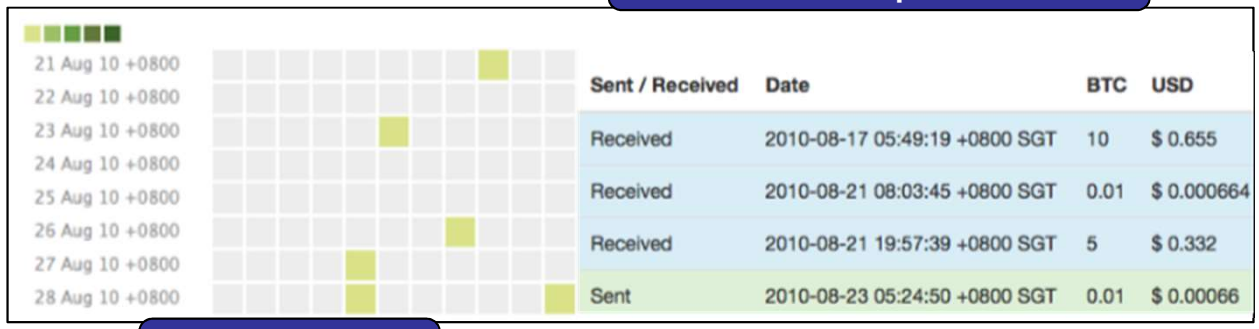


Conclusions of Transactions per Block and per Adress

- Sender / Receiver Addresses and, possibly, <u>known</u> Identities
- Date and Time for Blocks and Transactions
- Transfer Value

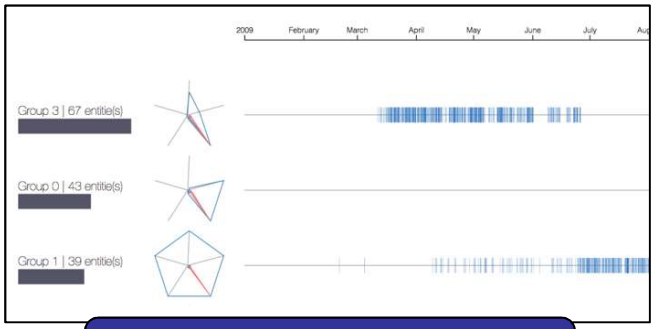
Kuzuno and Karam 2017

Transactions per Address



Heat Map

Kinkeldey et al. 2017



Clustering of Addreses

3.2. DISTRIBUTED LEDGER · ANALYSIS · MANUAL ANALYSIS EXAMPLE

Tool Used: Block Explorer Blockchain.info

1. Address 15yNZjR5CpdhEqojjiJAoYFBjCdtTjD341

Zusammenfassung		Transaktionen	
Adresse	15yNZjR5CpdhEqojjiJAoYFBjCdtTjD341	Anzahl der Transaktionen	2
Hash 160	3689cc495066ae3f444940141054002f07c3da16	Gesamtempfang	0.245 BTC
Tools	Kennzeichnungen - Unausgeglichene Ausgänge	Endgültige Balance	0 BTC

Zahlungsanfrage | Spenden-Button

2. Transaction 4707551f3cf507f42968ec3000eb48e05d51bea4ec51e13bdd0f8dccb98e65c1

4707551f3cf507f42968ec3000eb48e05d51bea4ec51e13bdd0f8dccb98e65c1

15yNZjR5CpdhEqojjiJAoYFBjCdtTjD341	1N1izs1ULXKDnipAuot4939CpJvoKD8JGw 16jsmyrFsA2M5QwLkTkfUyog5auyJrtMtN	0.1 BTC 0.14459 BTC

0.24459 BTC

3. Address 1N1izs1ULXKDnipAuot4939CpJvoKD8JGw

Zusammenfassung		Transaktionen	
Adresse	1N1izs1ULXKDnipAuot4939CpJvoKD8JGw	Anzahl der Transaktionen	4
Hash 160	e67db30604d177b46a9b0885c648f668ddfbd459	Gesamtempfang	0.25 BTC
Tools	Kennzeichnungen - Unausgeglichene Ausgänge	Endgültige Balance	0 BTC

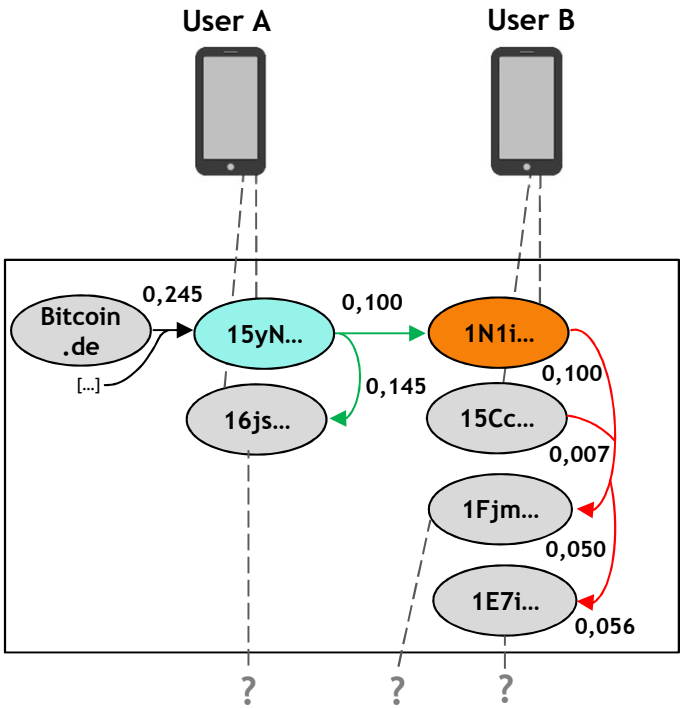
Zahlungsanfrage | Spenden-Button

4. Transaction b56b6ee03dfdb96b2cc402122cde72a52938b296d5242cf94efcb2041f601937

b56b6ee03dfdb96b2cc402122cde72a52938b296d5242cf94efcb2041f601937

15CcjpPcE77Ve5ub9aeKaM8wVT8bzGFy8Y 1N1izs1ULXKDnipAuot4939CpJvoKD8JGw	1FjmTJCkaVW1KK1c4TuCjTDBVaXNeBvftg 1E7iDXxWempNfSXPC8yQa3GBi6dRXPsMj3	0.05 BTC 0.05647308 BTC

0.10647308 BTC



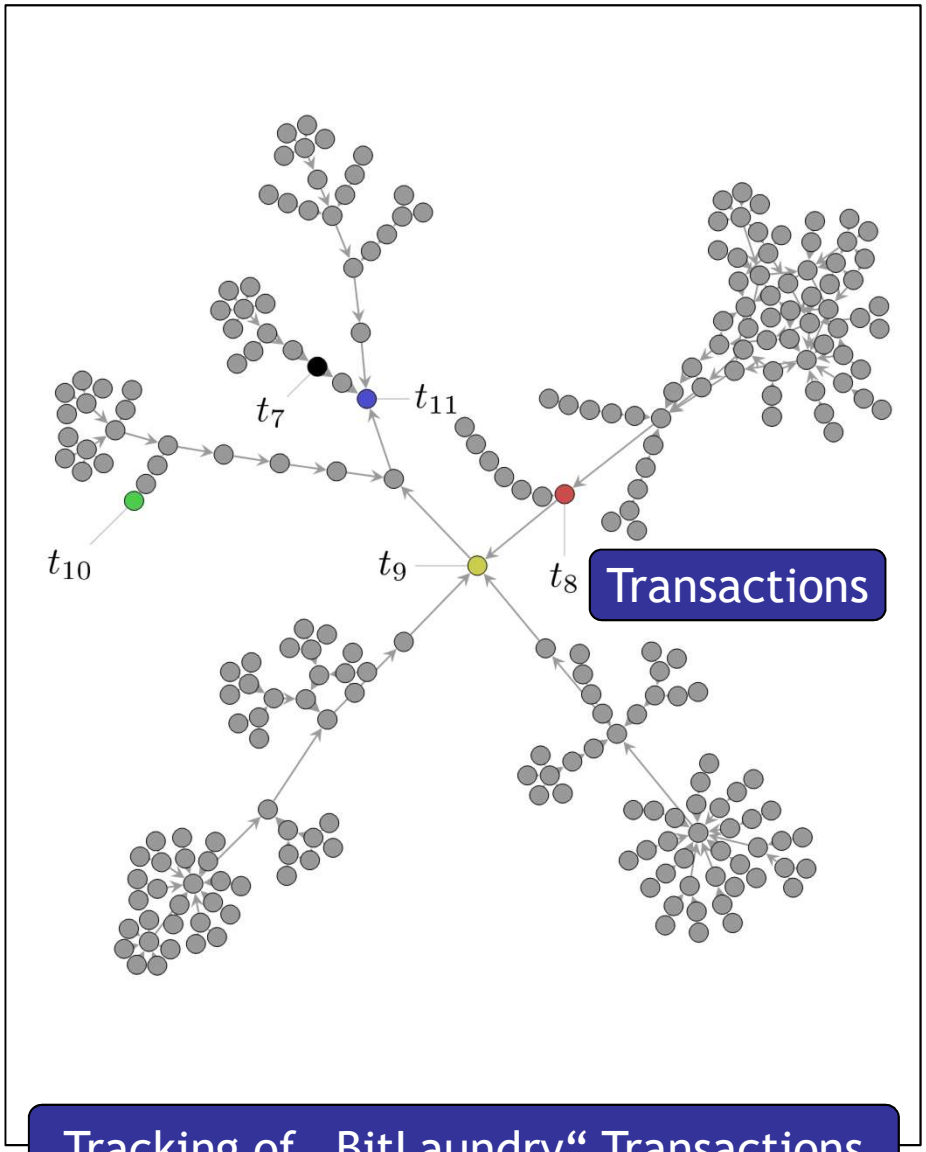
Transaction Graph

- **Node** *Address*
- **Edge** **Transaction**

  Value (per Input / Output) →

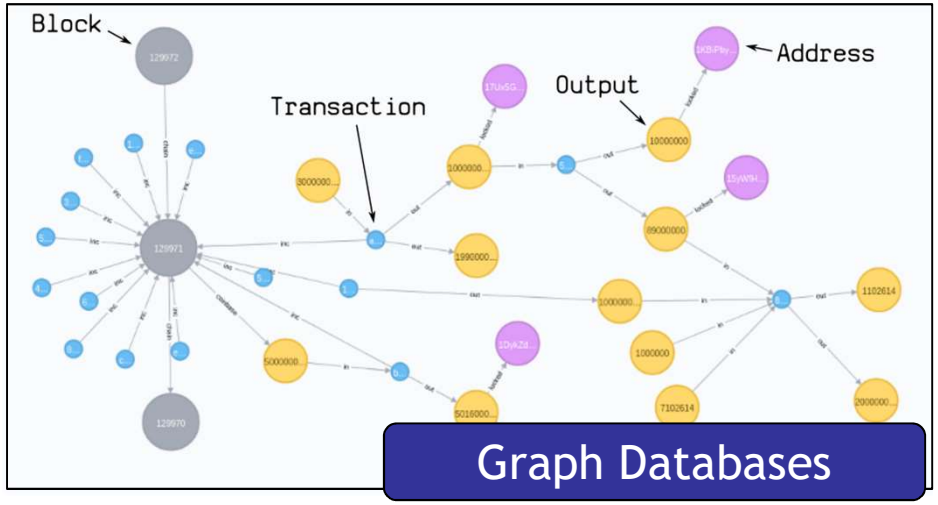
3.2. DISTRIBUTED LEDGER · ANALYSIS · TRANSACTION-GRAPH

Möser 2013

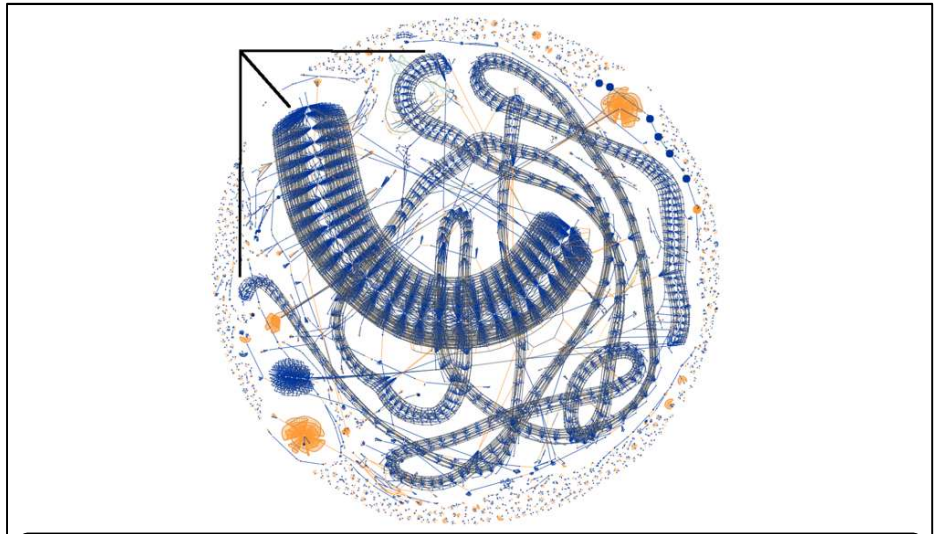


Tracking of „BitLaundry“ Transactions

Walker 2018 / Neo4J.com



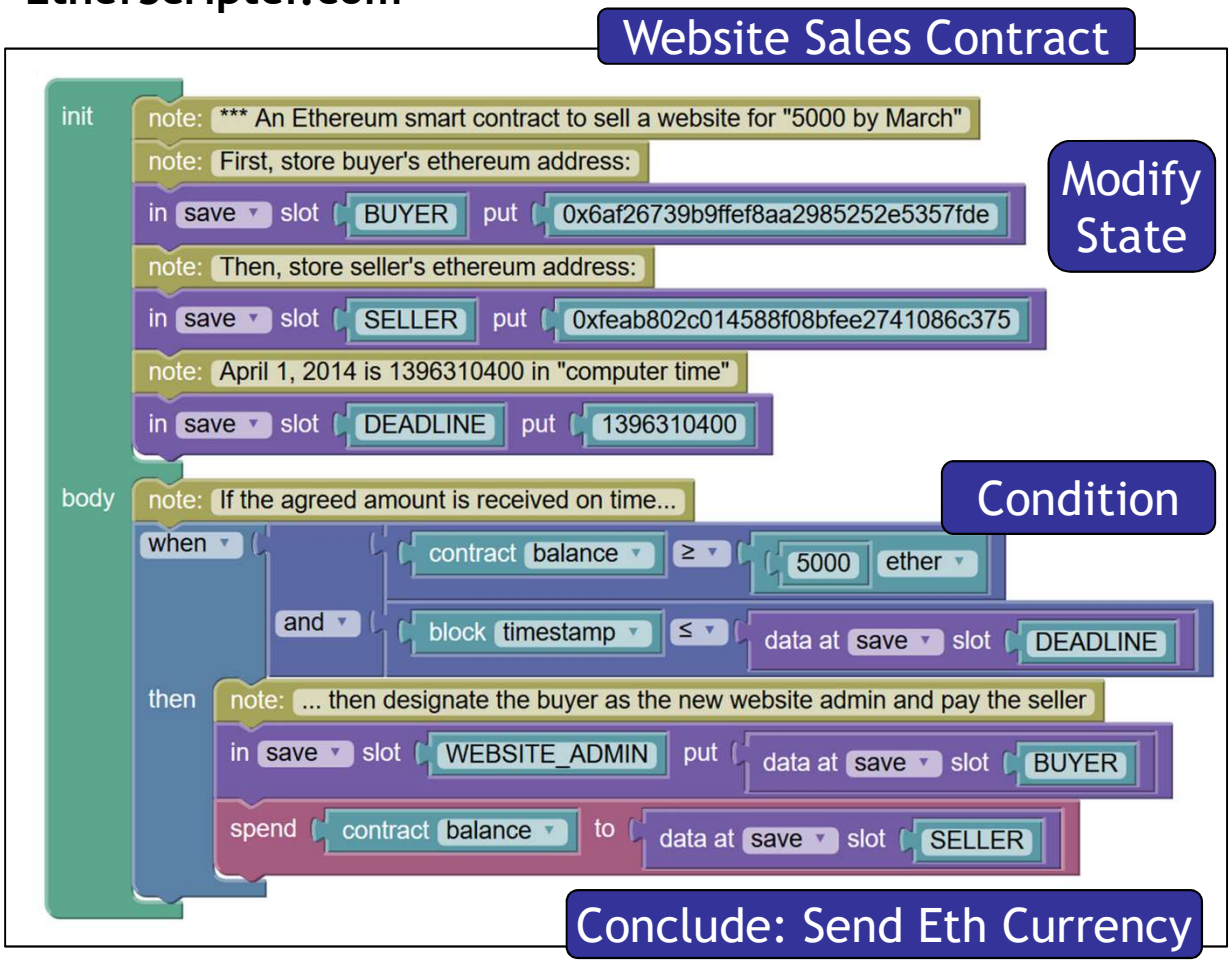
McGinn et al. 2018



Worm-Structure of Spam/DoS Transactions

3.2. SMART CONTRACT · DESIGN · VISUAL PROGRAMMING

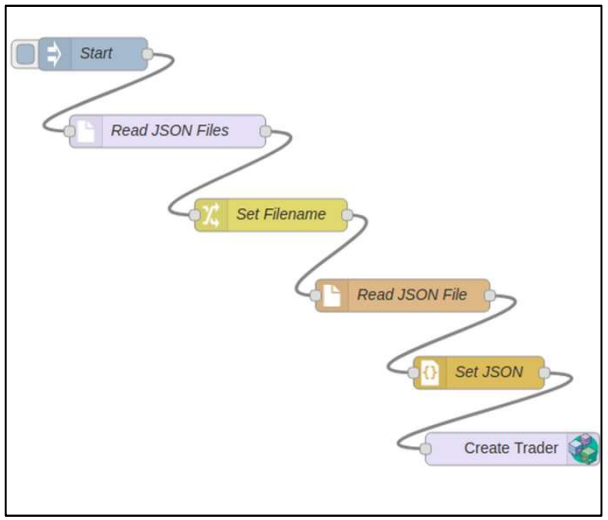
EtherScripter.com



Drawing up a Smart Contract

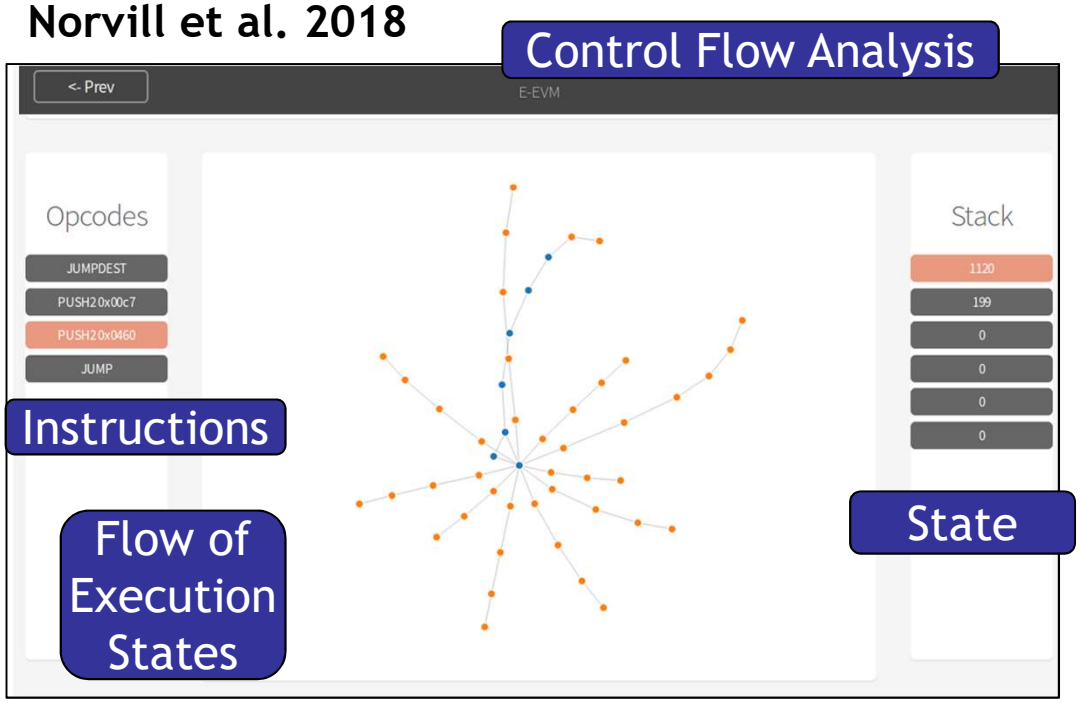
- Visual programming methods developed e.g. by MIT, Google, applied to Blockchains
- Block-structured languages: Blocks of nested instructions
- Flow-based languages: Connected Instruction Elements

Node Red Language



3.2. SMART CONTRACT · ANALYSIS · MANUAL ANALYSIS

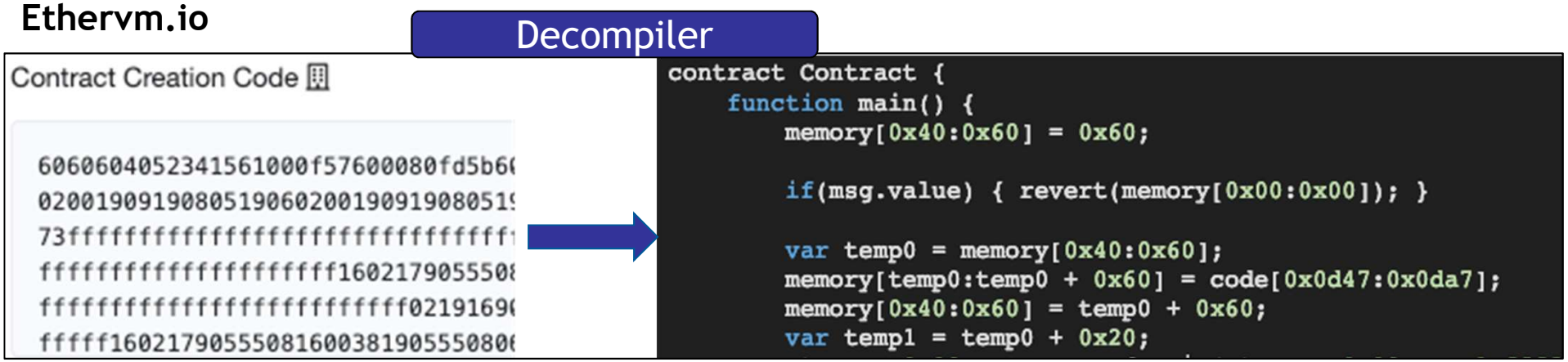
Norvill et al. 2018



Analysis of Contract Behaviour

- Contract Code stored in non-textual Bytecode
- Requires manual analysis
- Technical analysis of execution states
- Limitations due to missing semantics, e.g. no function and variable names

Ethervm.io



A Comparison of Approaches for Visualizing Blockchains and Smart Contracts

4. DISCUSSION OF RESULTS

How to Interact with Blockchains from a legal and not necessarily technical point of view?

- Approaches are limited regarding the design of legal contracts
  - Technically applicable, primarily for transfer of ownership
  - For targeted investigations, visualization provides some insight
- However, there are two prerequisites:
  Technical knowledge of blockchains and **underlaying programming techniques**
- **Key Reasons:**
  - **One-by-one substitution of technical elements with visual elements**
  - **Visual model and technical realization are on the same abstraction level**

Visualization by itself is, thus, insufficient

4. DISCUSSION OF RESULTS

❖ Three Main Requirements

R1 *Analysis or design must be expressible in the language of the domain.*

R2 *Domain concepts must establish their meaning in the context of the analysis or the design by themselves, using visualization techniques.*

R3 *For the design and analysis as part of complex systems, the level of abstraction must match the level of the domain and the level of knowledge of the user.*

5. Conclusion

Thank you for your attention!

Further Information:

http://www.knowledge-blockchain.org

felix.haerer@unifr.ch

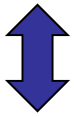
hans-georg.fill@unifr.ch

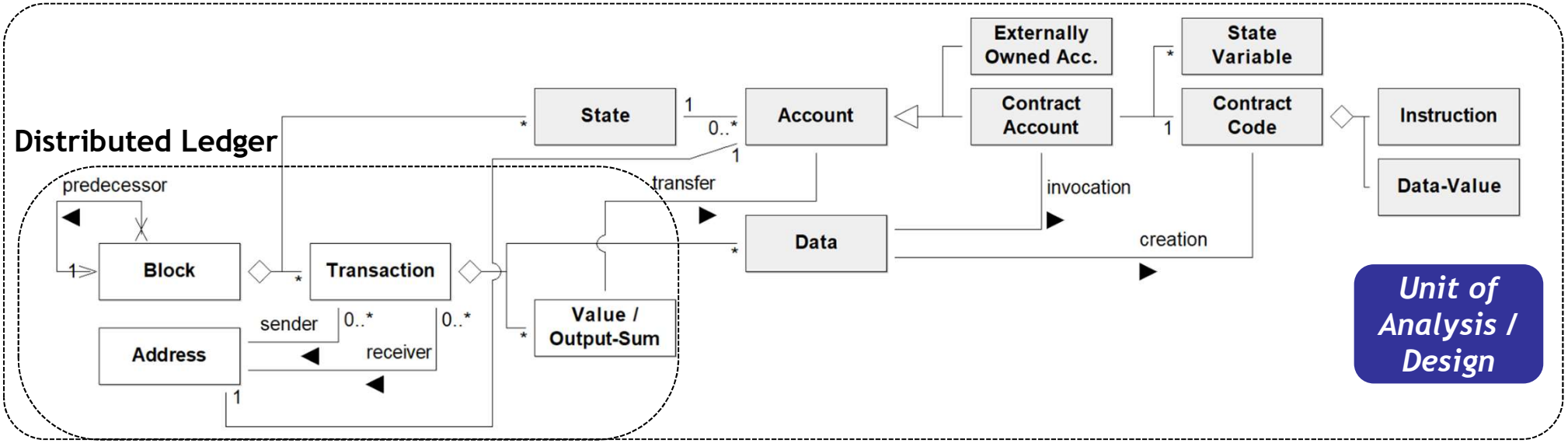
BACKUP SLIDES

3.1. Classification Framework

Visualization Approach

Distributed Ledger		Smart Contract	
Design	**Analyis**	**Design**	**Analysis**
• Model-Driven Design of Blockchain Applications • Modelling of Blockchain-based software applications • Wallet User-Interface-Design	• Chart-based Statistical Evaluation • Block-Transaction Visualization • Address-Transaction Visualization • Transaction Graph • Network Analysis • Network Node Map	• Visual Programming Languages • Declarative Logic for Smart Contracts • Domain Specific Modelling Languages	• Chart-based Statistical Evaluation • Contract-Transaction-Visualization • Smart Contract Decompiler • Control Flow Analysis





3.2. SMART CONTRACT · ANALYSIS · CONTRACT-TRANSACTIONS

Bloxy.info

Contract Transactions

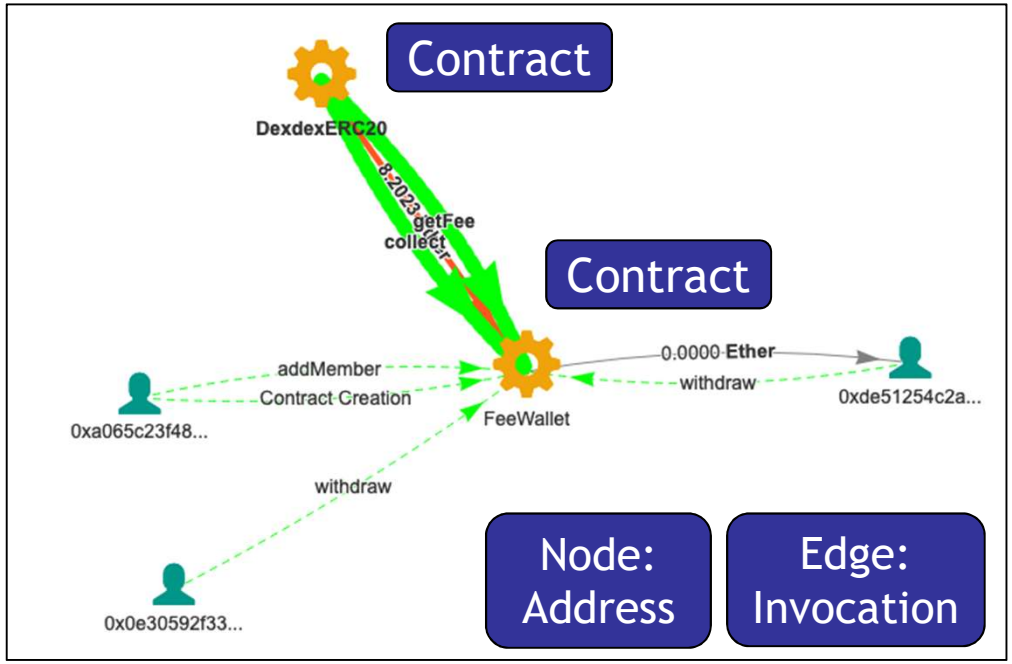
Smart Contract FeeWallet had 126 updates

Smart Contract **sent 0.15168292674850417 ETH** in 42 transactions

Too much data, only first 25 is shown. Look address page for details on all transactions

Time	From		Amount	Transaction
00:27:22 20/02/19	DexdexERC20	→	0.063321 ETH	0x3becdfef6f8aa0f...
05:08:46 20/02/19	DexdexERC20	→	0.005000m ETH	0xa401784379f807f...
05:30:10 20/02/19	DexdexERC20	→	0.089267m ETH	0x26ee28d0e919ab0...
13:57:28 19/02/19	DexdexERC20	→	0.050348m ETH	0xbaa3018c7074ce1...
14:24:07 19/02/19	DexdexERC20	→	0.010918m ETH	0x5a798d3c2e7b786...
14:56:08 19/02/19	DexdexERC20	→	0.071171m ETH	0xb1744318971ba6e...

Known Sender Addresses

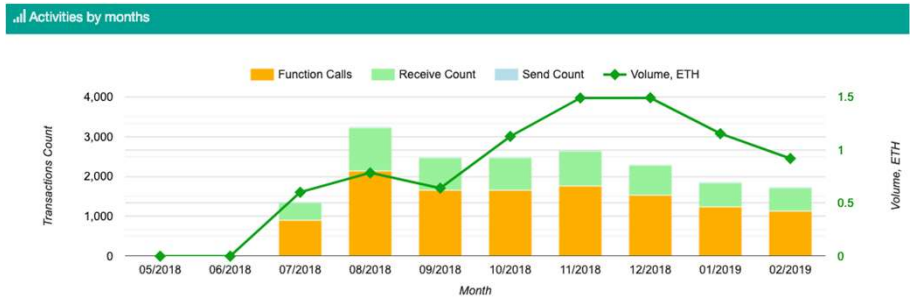


Conclusions of Contract

- Sender / Receiver Addresses and, possibly, known Contracts
- Date and Time for Blocks and Transactions
- Transfer Value

Contract Specific:

- Contract creation
- Function Invocation

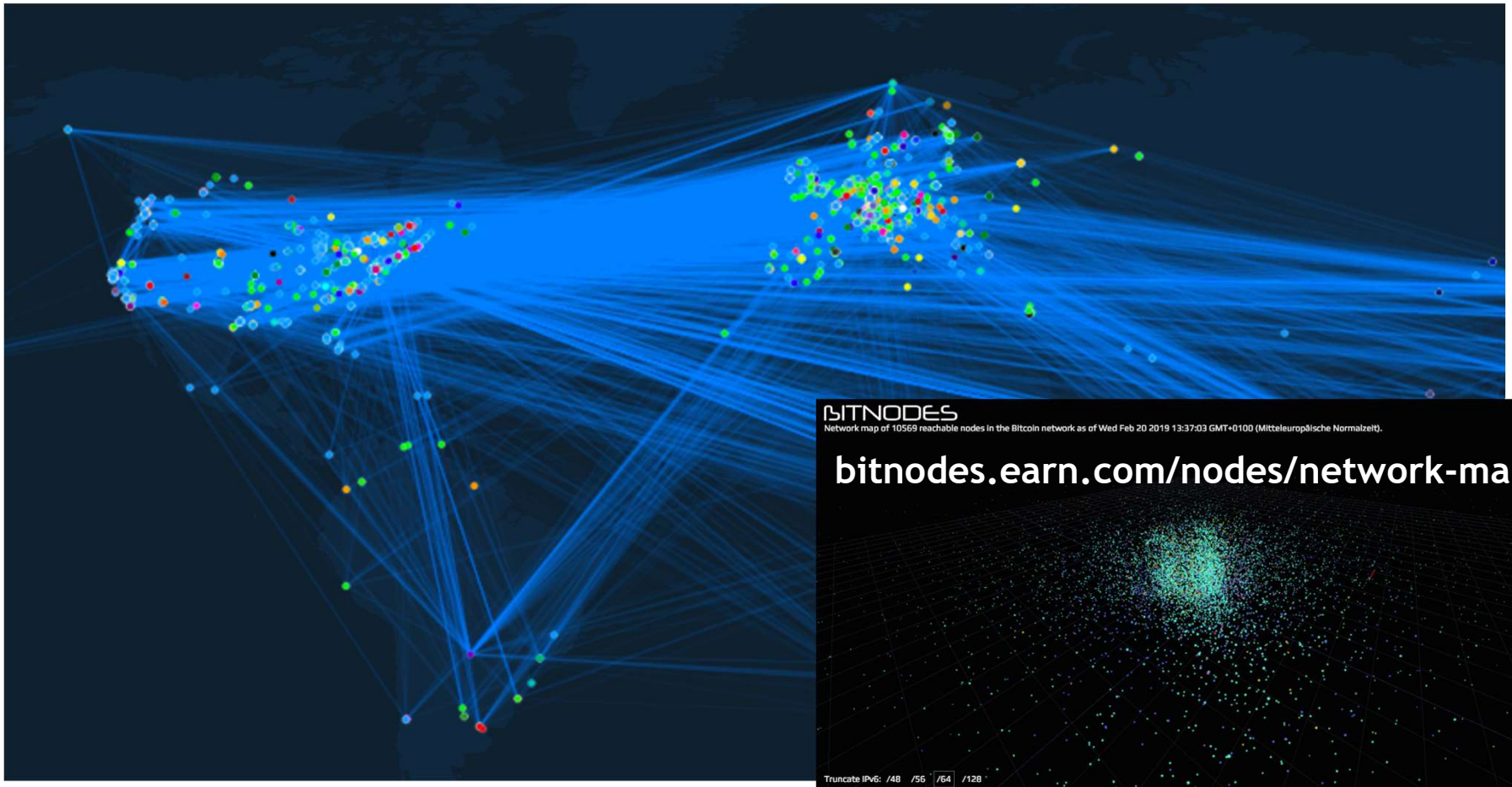


3.2. DISTRIBUTED LEDGER · ANALYSIS · NETWORK NODE MAP

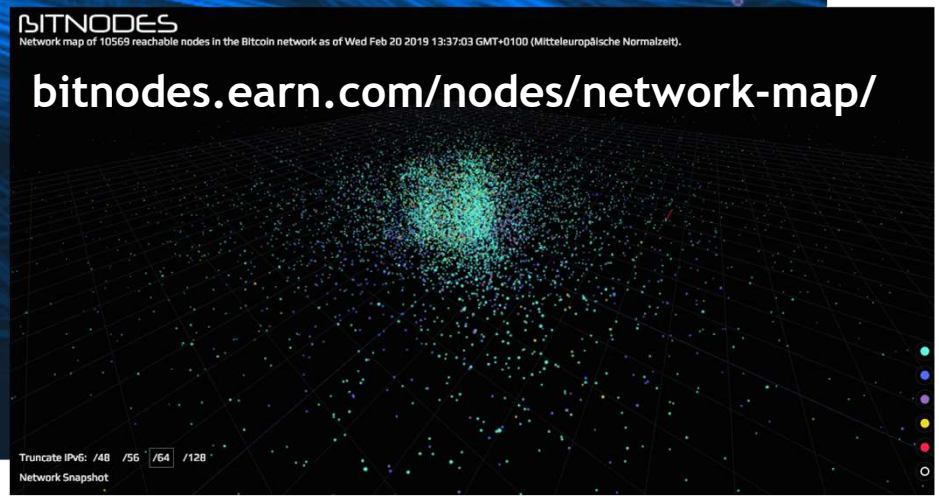
explorer.acinq.co

Node: Public Key / Address

Edge: Payment Channel



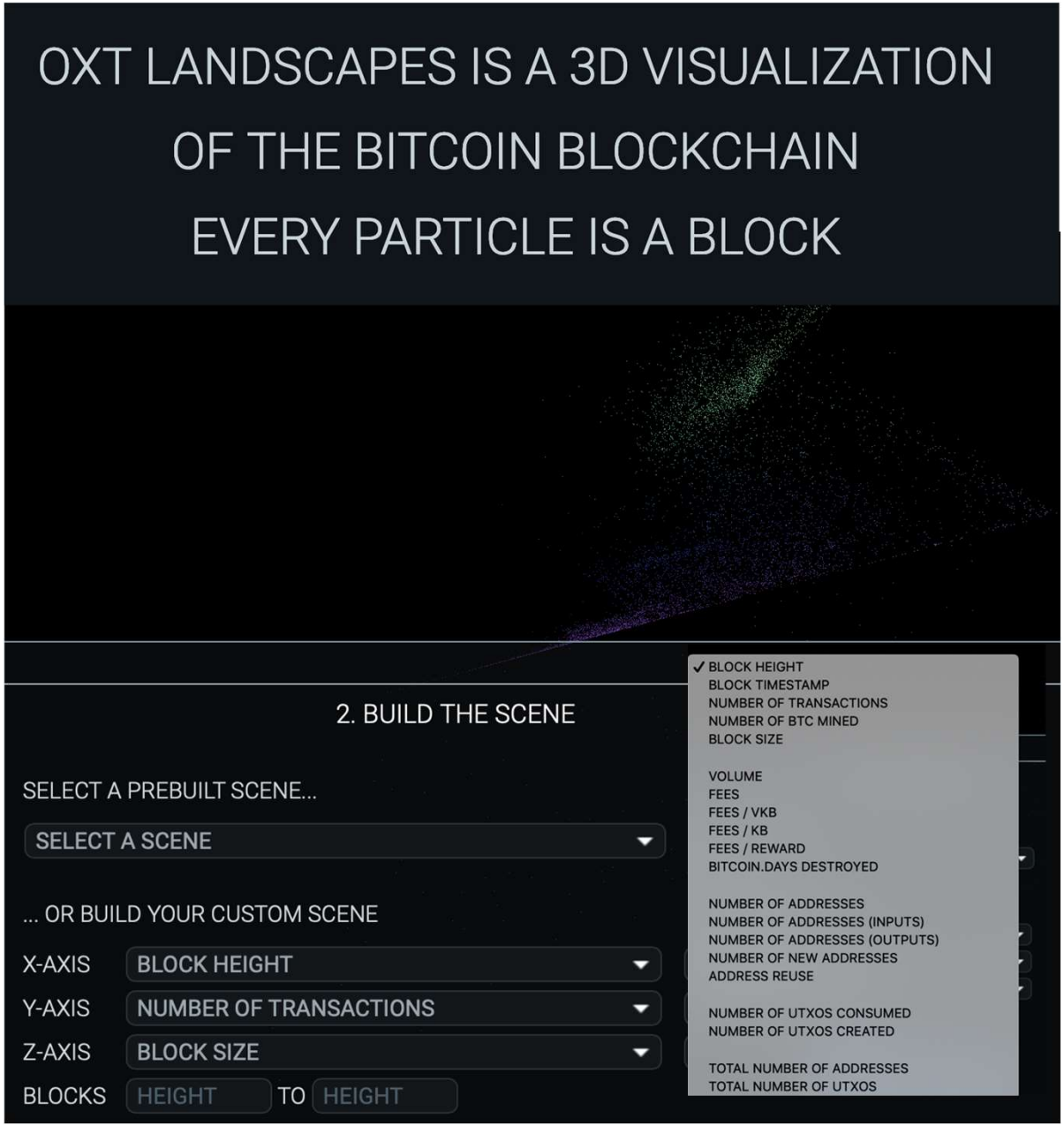
Bitcoin Lightning Network



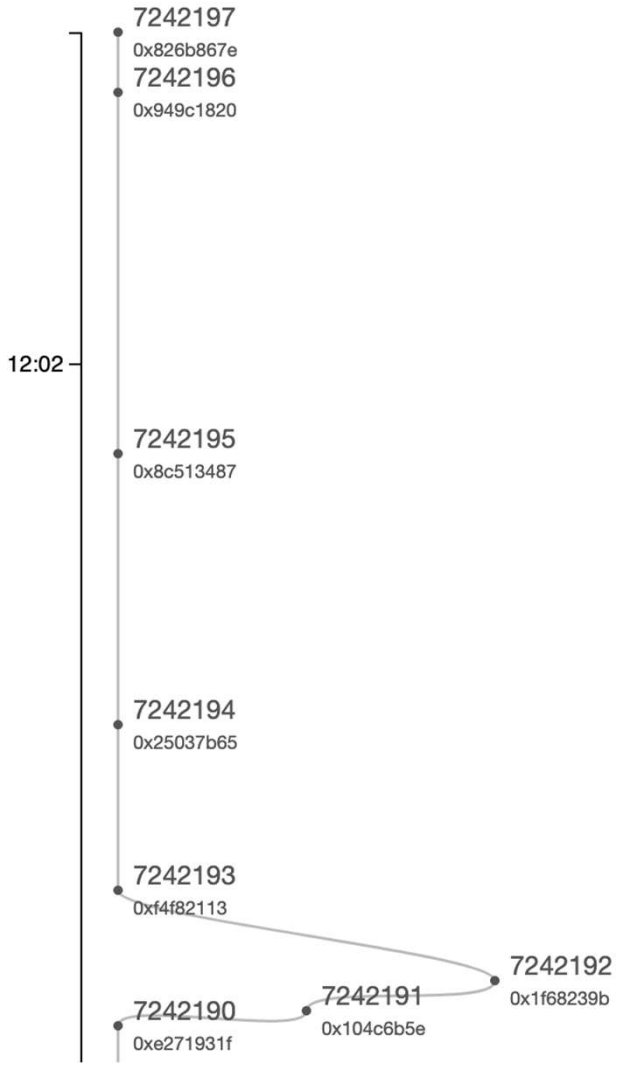
Bitcoin Network

PARTICLE VISUALIZATION

oxt.me/
landscapes



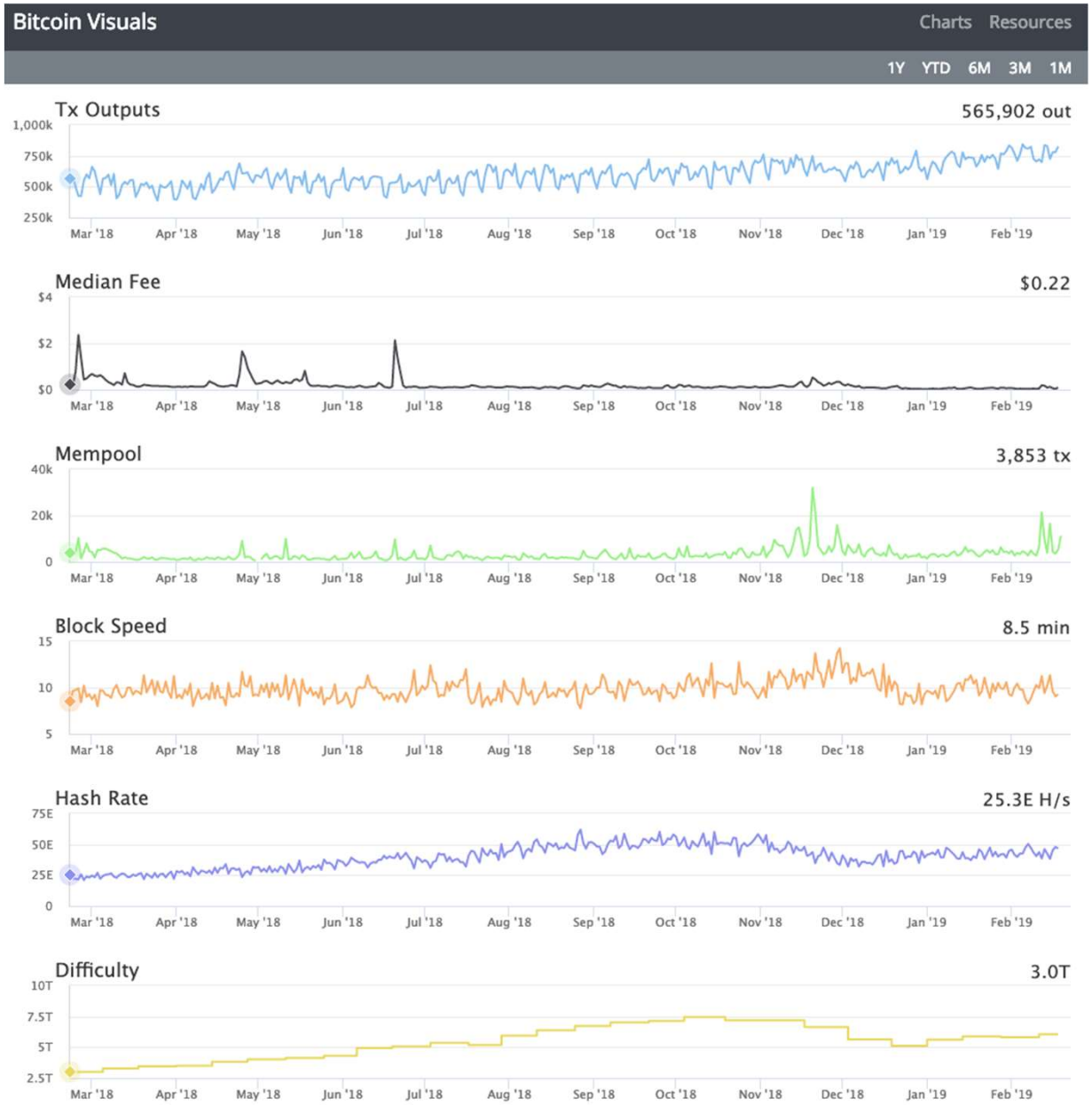
ETHEREUM FORK MONITOR



http://forkmon.ethdevops.io/

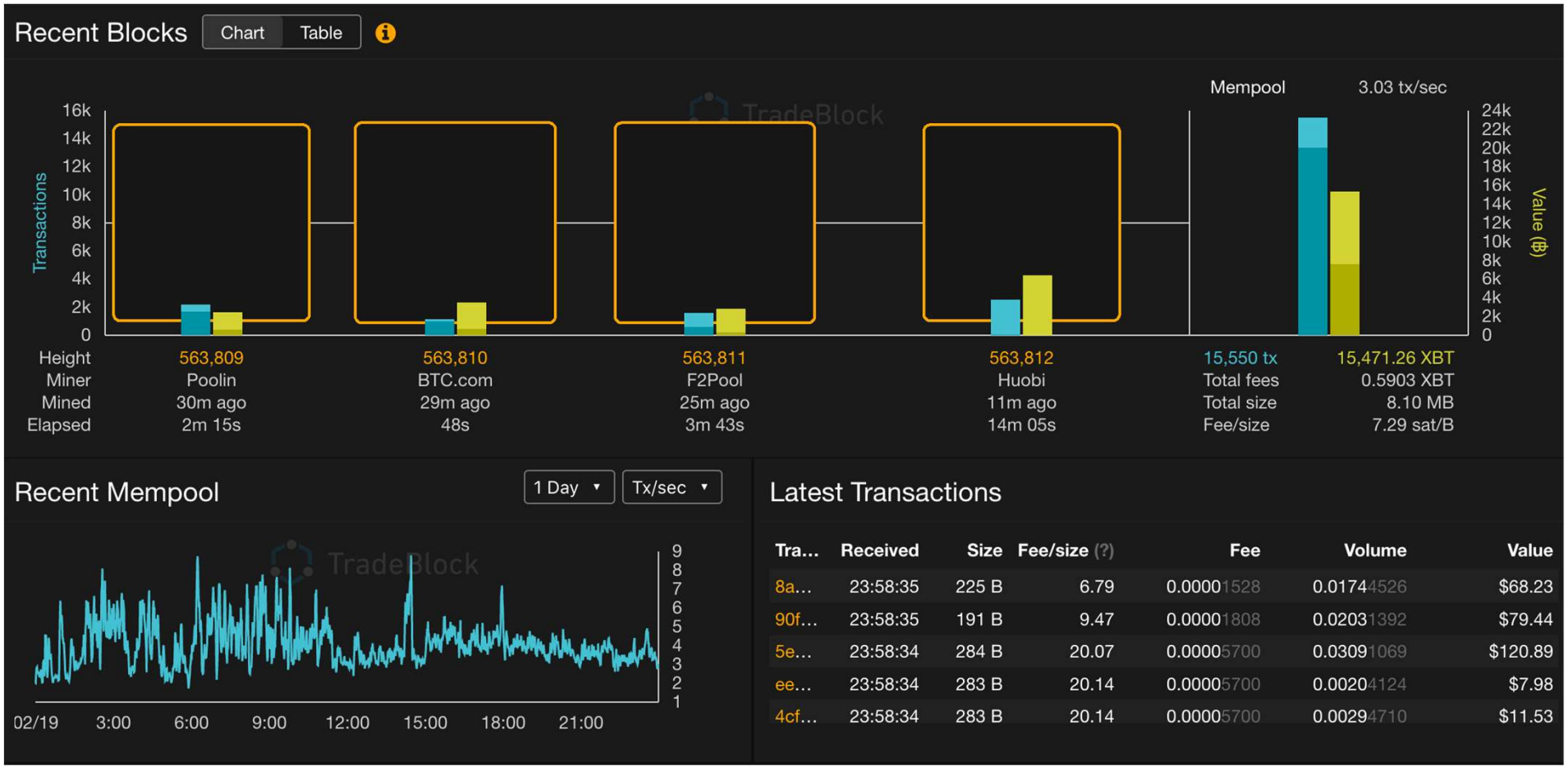
DATA ANALYTICS

Bitcoinvisuals.com



BLOCK SIZE IN BITCOIN

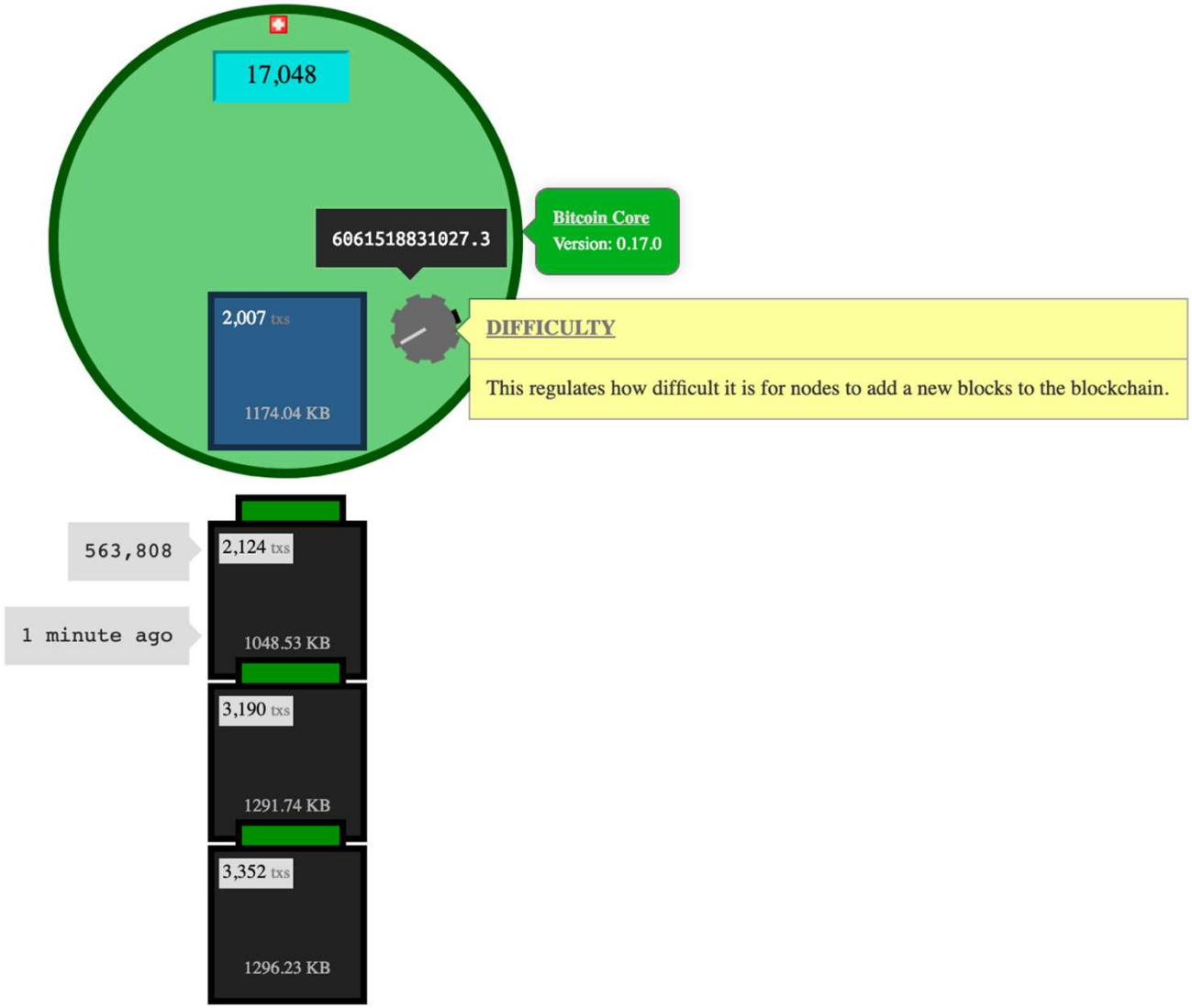
Tradeblock.com/bitcoin



Tra...	Received	Size	Fee/size (?)	Fee	Volume	Value
8a...	23:58:35	225 B	6.79	0.00001528	0.01744526	$68.23
90f...	23:58:35	191 B	9.47	0.00001808	0.02031392	$79.44
5e...	23:58:34	284 B	20.07	0.00005700	0.03091069	$120.89
ee...	23:58:34	283 B	20.14	0.00005700	0.00204124	$7.98
4cf...	23:58:34	283 B	20.14	0.00005700	0.00294710	$11.53

BLOCKCHAIN SIMULATION

learnmeabitcoin.com/browser/node/



ETHEREUM TRANSACTION VISUALIZATION

www.ethviewer.live