decred

POLITEIA

Platform Launch Party

POLITEIA

Blockchain Applications for Compliance

Austin, TX

2017.12.01

Introduction

Marco Peereboom

- Decred New Systems Development
- CTO of Company 0 LLC

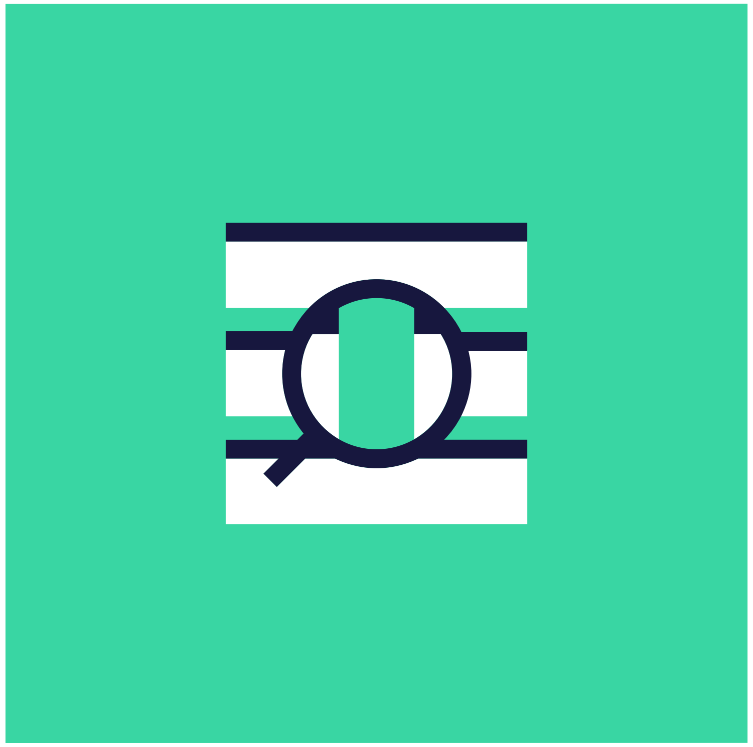
What is Decred?

- A crypto currency with a focus on community input
- Open governance
- Sustainable financing
- And continued development

Motivation

Why we developed it

We needed to create a permanent record of Decred’s governance discussions and decisions that was not vulnerable to history-rewriting and censorship.



What purpose it serves

By preventing manipulation of historical records and making censorship more transparent, we can do a better job with self-governance.

How it is a general solution

The main features of the system are attribution and time-ordering, which have high utility in various compliance and record-keeping contexts.

What is Politeia?

- Ancient Greek term meaning “a system of government”.
- Decred’s new public proposal system
- Stores governance related data off chain

Identity

Why we have identities

While dcrtime allows us to know some data existed on or before a given date, it is also important to know who is attesting to this data.

The utility of an identity for attestation

Without an identity, it’s difficult to assess the relevance of arbitrary data, e.g. is it Company X, as an organization, attesting to some data, or is it just someone with a Company X email address?

Public vs Private Data

How a single Politeia instance works

A single Politeia instance can be either public or private. All users of a particular instance can access all the data stored in that instance.

A “split horizon” configuration

For your application, it may make sense to have multiple sets of users with varying levels of access to the data stored in Politeia.

Politeia (Pi)

Politeia creates a **time-ordered cryptographically-accountable digital commons** where speech of various formats can be exchanged with **a transparent censorship mechanism.**

Politeia (Pi)

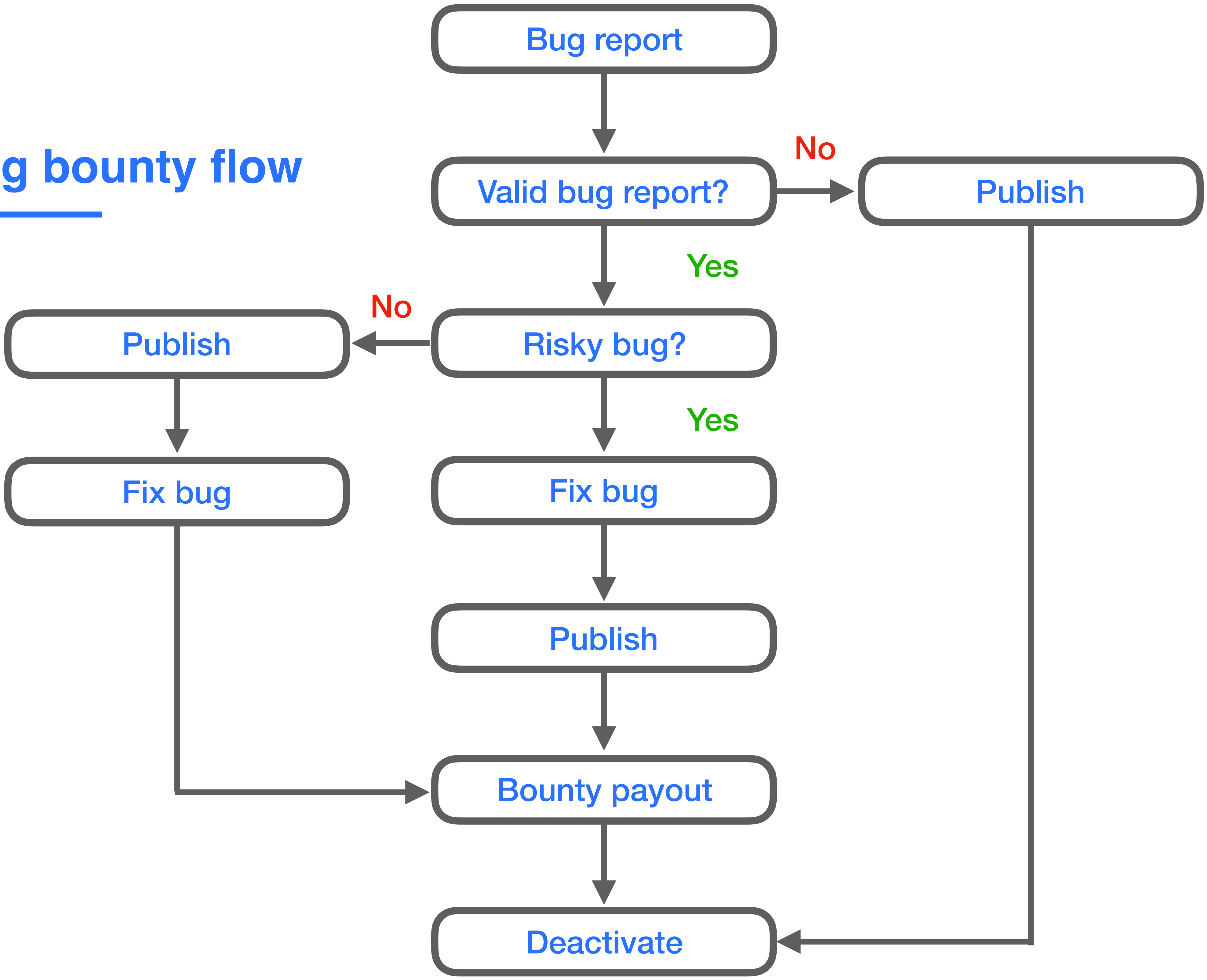
By creating cryptographic accountability for both users and administrators, censorship, other administrative actions and all user actions **can be demonstrated to have occurred.**

Politeia (Pi)

This heightened accountability and time-ordering of the data stored in Politeia makes it **ideal for use in scenarios where attribution matters and audit trails are either desired or required.**

Example: Bug bounty

Bug bounty flow



Bug report

Valid bug report?

No

Publish

Yes

Risky bug?

No

Publish

Fix bug

Yes

Fix bug

Publish

Bounty payout

Deactivate

Integration Format

Integrating Politeia for your application requires making several identifications:

- **Who are the users?**
- **Who are the administrators?**
- **What are the records?**
- **Will this be public, private or some combination thereof?**

Once these identifications are made for your application, you can determine what further customization, if any, is required for your use case.

Who are the users?

- Interested end users
- Security researchers
- Security professionals
- Project managers
- Developers

Who are the administrators?

- Project managers
- Accounts payable

What are the records?

- Externally generated bug reports.
- Bug bounty payout.

Use case

The idea is that bugs are submitted into the unvetted repository and then ultimately are promoted to the vetted repository once complete.

```
$ bash -x report_bug.sh
+ politeia -v -testnet -rpchost 127.0.0.1 new '{"name":"Marco", "description":"Bad bug #1"}'
badbug1.txt
00: 512cd8bc7980a6186fd36e7a095310f33b8cda1a696185bf77c6de97a7f2cfcb badbug1.txt text/plain;
charset=utf-8
Record submitted
  Censorship record:
    Merkle   : 512cd8bc7980a6186fd36e7a095310f33b8cda1a696185bf77c6de97a7f2cfcb
    Token    : 141aed9b800e49bb8db9b30d32994a1b56154bc3c64842e177ba80e0e1715883
    Signature:
643e142d24004883a824bb42c083622bfb0069de9659ae0dd3ee296bc20cc1a9d07c7dd6e97b6fb01d28240aaa344
05df42eec15febcdda57b98eb109f5bf30d
```

```
$ bash -x report_silly_bug.sh
+ politeia -v -testnet -rpchost 127.0.0.1 new '{"name":"Tr0llZ0rz", "description":"Silly bug
#1"}' notabug1.txt
00: 4c72e0b7bebb8f6a3a00ae622d80ab51aa93e044e62d37f69598ea078f4ea8c6 notabug1.txt text/plain;
charset=utf-8
Record submitted
  Censorship record:
    Merkle   : 4c72e0b7bebb8f6a3a00ae622d80ab51aa93e044e62d37f69598ea078f4ea8c6
    Token    : fe8cd0b805cab11e8b883316b8bc164370a3d2c7258859de6596999c6cad9c66
    Signature:
106747dafe27682be4c499803ef7ac82b661b6a55814f0a2f3be7b0f648346f6b894ac1b6475fad5c50871cc83e64
c96c9e7f6564552b0ddcfc1edaa93833d0b
```

```
$ bash -x admin_inventory.sh
+ politeia -v -testnet -rpchost 127.0.0.1 -rpcuser user -rpcpass pass inventory 1 1
Unvetted record:
  Status     : not reviewed
  Timestamp  : 2017-12-01 15:03:58 +0000 UTC
  Censorship record:
    Merkle   : 512cd8bc7980a6186fd36e7a095310f33b8cda1a696185bf77c6de97a7f2cfcb
    Token    : 141aed9b800e49bb8db9b30d32994a1b56154bc3c64842e177ba80e0e1715883
    Signature
643e142d24004883a824bb42c083622bfb0069de9659ae0dd3ee296bc20cc1a9d07c7dd6e97b6fb01d28240aaa3
4405df42eec15febcdda57b98eb109f5bf30d
  Metadata   : {"name":"Marco", "description":"Bad bug #1"}
Unvetted record:
  Status     : not reviewed
  Timestamp  : 2017-12-01 15:07:00 +0000 UTC
  Censorship record:
    Merkle   : 4c72e0b7bebb8f6a3a00ae622d80ab51aa93e044e62d37f69598ea078f4ea8c6
    Token    : fe8cd0b805cab11e8b883316b8bc164370a3d2c7258859de6596999c6cad9c66
    Signature:
106747dafe27682be4c499803ef7ac82b661b6a55814f0a2f3be7b0f648346f6b894ac1b6475fad5c50871cc83e
64c96c9e7f6564552b0ddcfc1edaa93833d0b
  Metadata   : {"name":"Tr0llZ0rz", "description":"Silly bug #1”}
```

```
$ bash -x admin_publish.sh 141aed9b800e49bb8db9b30d32994a1b56154bc3c64842e177ba80e0e1715883
+ politeia -v -testnet -rpchost 127.0.0.1 -rpcuser user -rpcpass pass setunvettedstatus
publish 141aed9b800e49bb8db9b30d32994a1b56154bc3c64842e177ba80e0e1715883
Set record status:
  Status   : public
```

```
$ bash -x admin_censor.sh fe8cd0b805cab11e8b883316b8bc164370a3d2c7258859de6596999c6cad9c66
+ politeia -v -testnet -rpchost 127.0.0.1 -rpcuser user -rpcpass pass setunvettedstatus
censor fe8cd0b805cab11e8b883316b8bc164370a3d2c7258859de6596999c6cad9c66
Set record status:
  Status   : censored
```

```
$ bash -x admin_inventory.sh
+ politeia -v -testnet -rpchost 127.0.0.1 -rpcuser user -rpcpass pass inventory 1 1
Vetted record:
  Status     : public
  Timestamp  : 2017-12-01 15:03:58 +0000 UTC
  Censorship record:
    Merkle   : 512cd8bc7980a6186fd36e7a095310f33b8cda1a696185bf77c6de97a7f2cfcb
    Token    : 141aed9b800e49bb8db9b30d32994a1b56154bc3c64842e177ba80e0e1715883
    Signature:
643e142d24004883a824bb42c083622bfb0069de9659ae0dd3ee296bc20cc1a9d07c7dd6e97b6fb01d28240aaa344
05df42eec15febcdda57b98eb109f5bf30d
  Metadata   : {"name":"Marco", "description":"Bad bug #1"}
Unvetted record:
  Status     : censored
  Timestamp  : 2017-12-01 15:07:00 +0000 UTC
  Censorship record:
    Merkle   : 4c72e0b7bebb8f6a3a00ae622d80ab51aa93e044e62d37f69598ea078f4ea8c6
    Token    : fe8cd0b805cab11e8b883316b8bc164370a3d2c7258859de6596999c6cad9c66
    Signature:
106747dafe27682be4c499803ef7ac82b661b6a55814f0a2f3be7b0f648346f6b894ac1b6475fad5c50871cc83e64
c96c9e7f6564552b0ddcfc1edaa93833d0b
  Metadata   : {"name":"Tr0llZ0rz", "description":"Silly bug #1"}
```

Other Examples

Other Examples

Financial Record Keeping

Makes it substantially harder to commit fraud when the records cannot be altered after the fact, both for public and private applications

Insurance Policies

When individuals or organizations present insurance coverage, it could be verified with the issuer directly

Asset Tracking

Maintaining chain of custody on certain assets can be either a legal requirement or a very good idea, especially in the case of high-value assets, e.g. nuclear weapons, precious metals, scientific equipment

Other Examples

Medical Records

Patients, doctors and medical insurers could benefit from timestamped and attested to medical records

Government Records Storage

Citizens and their governments can benefit from storing various public and private records, e.g. recorders of deeds, secretaries of state, treasurers, citations, courts, identity documents

Social Media

Users and administrators can interact in a more honest fashion without opaque censorship

The Politeia Challenge Contest

- Designed to discover alternate uses for Politeia codebase
- Competitors will use Politeia source code to address alternate use cases besides a public proposal system
- Prizes will be awarded for 1st, 2nd, and 3rd place

The Politeia Challenge Contest

- Competitors are encouraged to work in teams
- Teams will demonstrate projects live at the contest event in February.
- National competitors will present their projects remotely

The Politeia Challenge Contest

- Submissions must focus on some combination of changes to the backend and/or the frontend.

- If Ideas require a different workflow than Politeia, you will need to make some modifications to the backend.   Ideas that require user interface, you will need to modify the frontend.

- Presentations for submissions should focus on what use cases are addressed and how the backend was changed to accommodate those cases.

- Demonstrating frontend changes is optional - User interface mockups is suggested in lieu of having a working frontend for the submission

The Politeia Challenge Contest

- Submissions can be open sourced or not

- Confirmation that submissions have working proof-of-concept level code will be needed prior to the contest event date

- You must make the source code for the proof-of-concept available for evaluation, but not necessarily open source it publicly

- If code is open source, Decred may choose to fund further work on the submission after the competition is completed.

The Politeia Challenge Contest

- 1st Place = USD$10K
- 2nd Place = USD $5K
- 3rd Place = USD $2k
- Prizes are equivalent to USD and are payable in Decred
- Winners will be selected by a panel of judges

The Politeia Challenge Contest

- Payments shall be made in Decred after the contest event is completed using a exchange rate averaged over the month of January 2018.

- The average is determined by averaging the DCR/USDT exchange rate, calculated by taking the DCR/BTC and BTC/USDT data from Poloniex, weighted averages over 15 minute intervals, multiplying them, and then averaging over the month of January 2018.

The Challenge Contest

- Interested parties should write a brief description of intended project and email to **pi2017@decred.org**

- Working code must be submitted on or before January 26th, 2018 with all instructions on how to make it work.

- Competitors can post questions about the competition or Politeia codebase on:
    1. Matrix chat matrix.decred.org "DCR Development" channel
    2. Decred Rocket Chat #dev channel
    3. IRC #decred-dev channel

Interrogative

Questions?

Thanks!

Decred Project

December 1, 2017

decred

POLITEIA

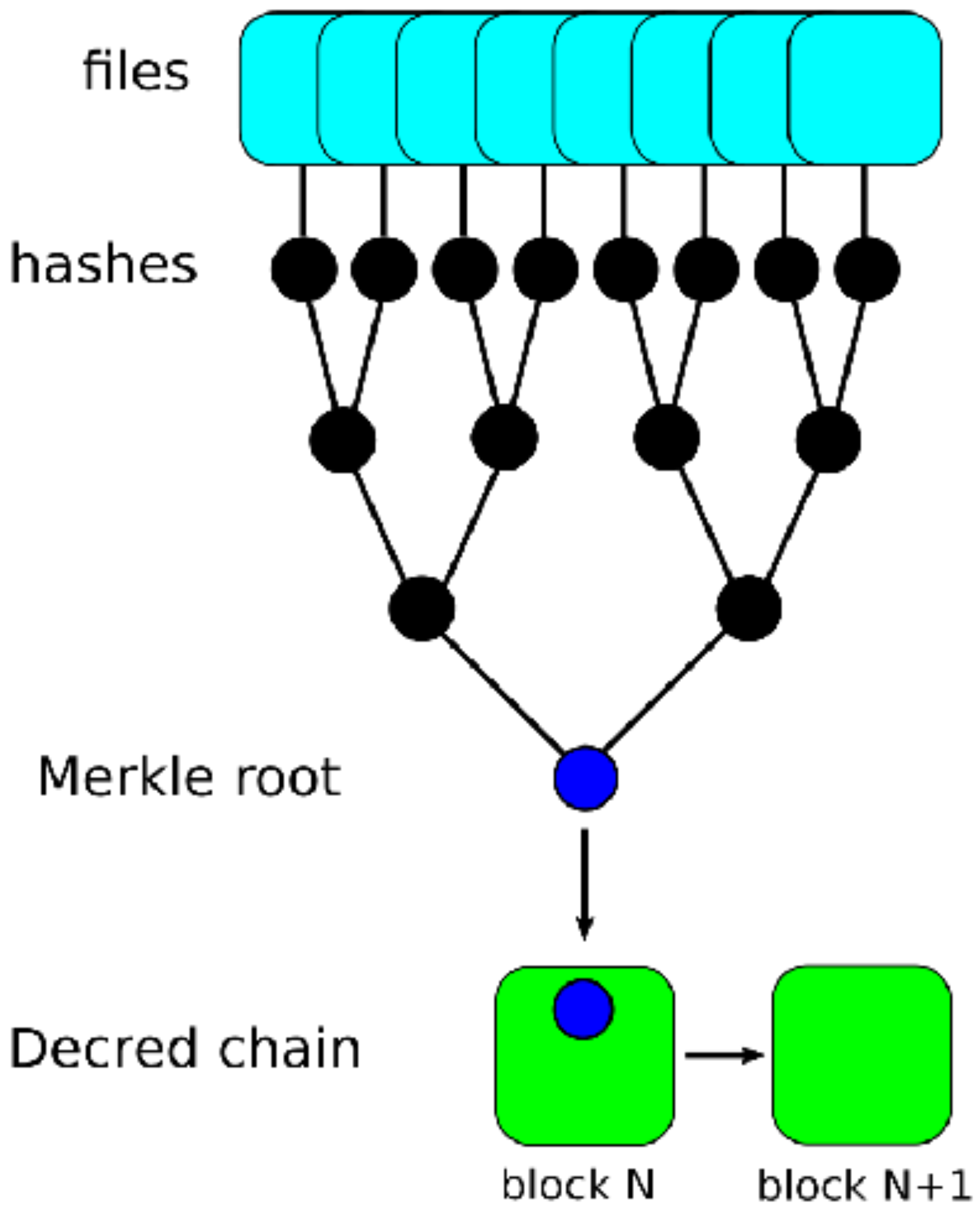
Platform Launch Party

Technical summary: dcrtime

- Decred provides timestamps via its blockchain for transactions which can be leveraged to timestamp external data

- Users submit hashes of files to dcrtime

- dcrtime puts these hashes in a Merkle tree and includes its Merkle root in a block every hour

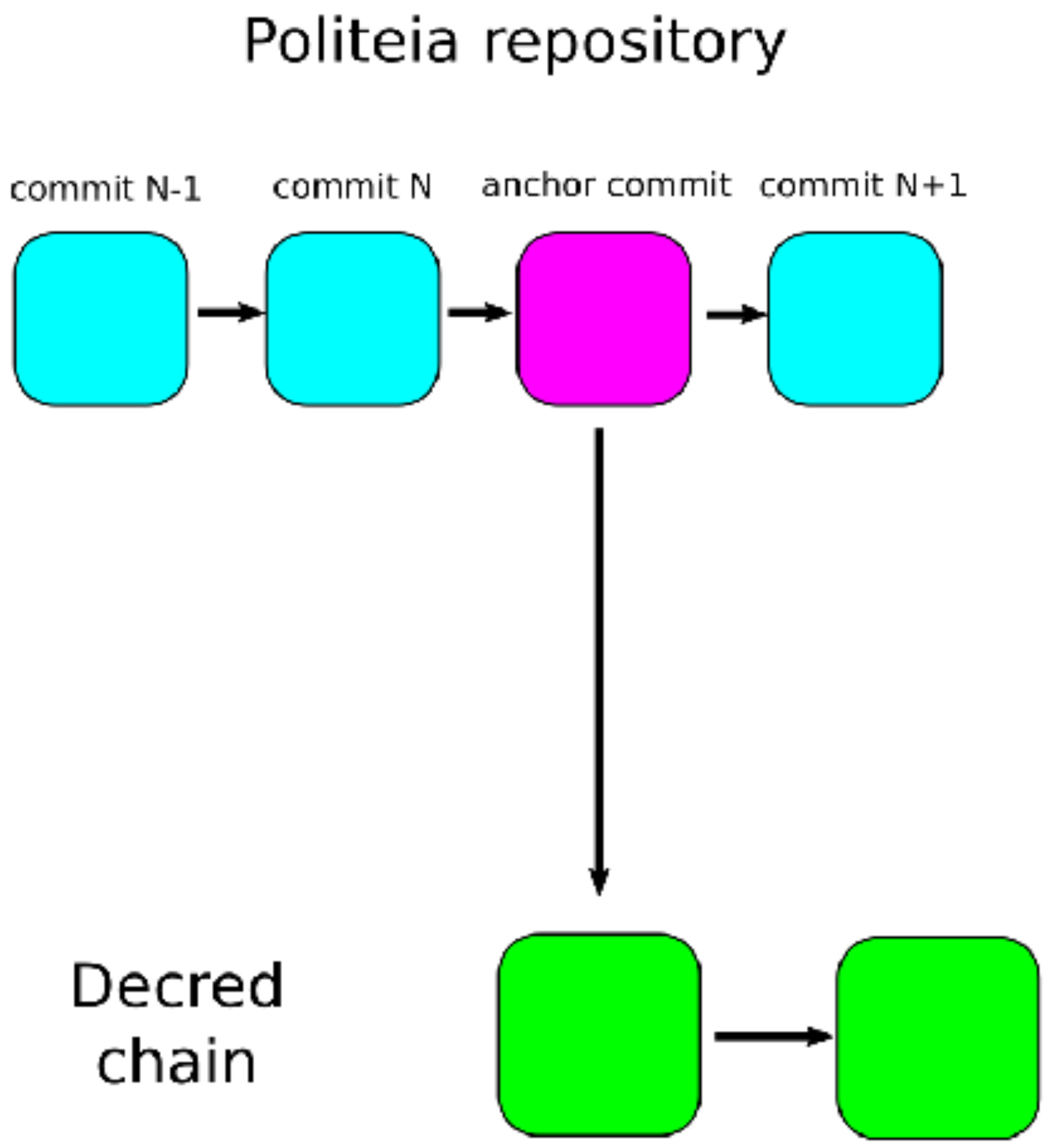


Technical summary: politeia

- Politeia is a repository of data that is episodically anchored via dcrtime

- It adds an identity layer to the data being stored

- The data being stored is logically grouped into one or more repositories


Politeia repository
commit N-1
commit N
anchor commit
commit N+1
Decred chain