



Condividere  
informazioni  
in modo  
sicuro  
combinando  
Git e  
Blockchain

Studente:  
Paolo Speziali  
Relatore:  
Luca Grilli

Il Problema

Concetti  
preliminari

L'Obiettivo

Il Software  
PineSU

# Condividere informazioni in modo sicuro combinando Git e Blockchain

Studente: Paolo Speziali  
Relatore: Luca Grilli

Università degli Studi di Perugia - Dipartimento di Ingegneria  
Corso di laurea triennale in Ingegneria Informatica ed Elettronica



A.D. 1308  
**unipg**  
DIPARTIMENTO  
DI INGEGNERIA

A.A. 2020/2021



# Indice

Condividere  
informazioni  
in modo  
sicuro  
combinando  
Git e  
Blockchain

Studente:  
Paolo Speziali  
Relatore:  
Luca Grilli

Il Problema

Concetti  
preliminari

L'Obiettivo

Il Software  
PineSU

## 1 Il Problema

## 2 Concetti preliminari

## 3 L'Obiettivo

## 4 Il Software PineSU



# La digitalizzazione

Condividere  
informazioni  
in modo  
sicuro  
combinando  
Git e  
Blockchain

Studente:  
Paolo Speciali  
Relatore:  
Luca Grilli

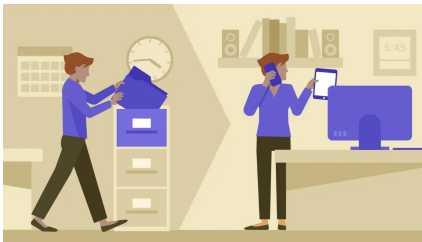
## Il Problema

Concetti  
preliminari

L'Obiettivo

Il Software  
PineSU

È in atto, negli ultimi anni, un piano di **digitalizzazione** delle PA. Esso mira all'evoluzione tecnologica di tutte le sue mansioni e alla creazione di portali web per il cittadino. L'esigenza di questa trasformazione si è fatta sentire anche da parte dell'**Unione Europea**, che con il **Recovery Fund** ci sta fornendo i fondi per attuarla, ben **11,75 milioni di euro**.





# Il problema della burocrazia

Condividere  
informazioni  
in modo  
sicuro  
combinando  
Git e  
Blockchain

Studente:  
Paolo Speciali  
Relatore:  
Luca Grilli

## Il Problema

Concetti  
preliminari

L'Obiettivo

Il Software  
PineSU

Il più grande avversario della digitalizzazione è la **burocrazia** italiana: i suoi processi sono **lenti** e **complessi** anche a causa dell'**importanza** dei documenti da gestire. È necessaria una **sburocratizzazione** grazie a degli strumenti digitali che permettano di **salvare**, **validare** e **condividere** documenti senza abbassare il **livello di sicurezza**.





# Gli strumenti attuali

Condividere  
informazioni  
in modo  
sicuro  
combinando  
Git e  
Blockchain

Studente:  
Paolo Speziali  
Relatore:  
Luca Grilli

## Il Problema

Concetti  
preliminari

L'Obiettivo

Il Software  
PineSU

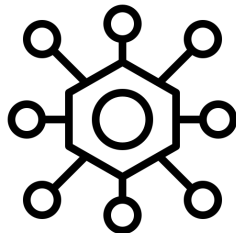
Uno strumento digitale solitamente segue uno di questi due paradigmi:

**centralizzato** e **distribuito**.

Nel primo un'entità centrale si occupa dell'**immagazzinamento** e della **verifica** dei dati degli utenti.

Ciò ha diversi **svantaggi**:

- Potenziali attacchi all'entità
- Possibile uso malevolo dei nostri dati
- Alti costi d'intermediazione





# Strumenti distribuiti

Condividere  
informazioni  
in modo  
sicuro  
combinando  
Git e  
Blockchain

Studente:  
Paolo Speziali  
Relatore:  
Luca Grilli

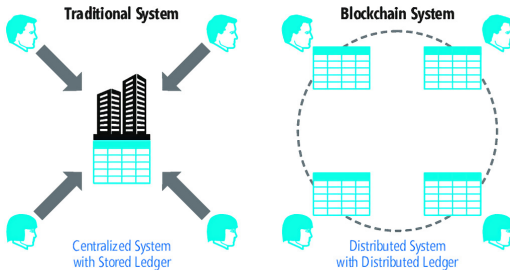
## II Problema

Concetti  
preliminari

L'Obiettivo

II Software  
PineSU

Usando invece **un'architettura distribuita**, sia per la gestione dei file, sia per la verifica delle informazioni, saremo in grado costruire uno strumento che può affidarsi alla parola di una moltitudine di entità, rendendo molto più complicati e rilevabili attacchi e manomissioni.





# Funzioni crittografiche di hashing

Condividere  
informazioni  
in modo  
sicuro  
combinando  
Git e  
Blockchain

Studente:  
Paolo Speziali  
Relatore:  
Luca Grilli

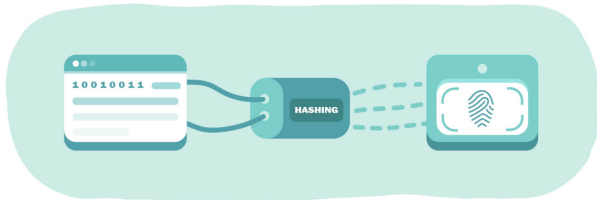
Il Problema

Concetti  
preliminari

L'Obiettivo

Il Software  
PineSU

Funzione che **associa**, a una qualsiasi sequenza  $m$  di lunghezza arbitraria in input, una sequenza in output  $h(m)$  di lunghezza costante, seguendo alcune proprietà che la rendono *crittograficamente sicura*. Ciò impedisce di risalire all'input originale e facilita i **controlli di integrità sui file**.





# Git

Condividere  
informazioni  
in modo  
sicuro  
combinando  
Git e  
Blockchain

Studente:  
Paolo Speciali  
Relatore:  
Luca Grilli

Il Problema

Concetti  
preliminari

L'Obiettivo

Il Software  
PineSU

**Git** è il sistema di controllo di versione (**VCS**) distribuito più diffuso al mondo.

Esso agevola la gestione **distribuita** di insiemi di file e directory. Un VCS considera tali insiemi unità chiamate **repository**.

Git ci permette di:

- **Tracciare** le modifiche in una repository.
- **Ripristinare** le repository ad uno stato precedente.
- **Condividere** le repository con il loro storico dei cambiamenti.

e molto altro...







# Blockchain

Condividere  
informazioni  
in modo  
sicuro  
combinando  
Git e  
Blockchain

Studente:  
Paolo Speziali  
Relatore:  
Luca Grilli

Il Problema

Concetti  
preliminari

L'Obiettivo

Il Software  
PineSU

La **blockchain** è un registro in continua crescita di record chiamati blocchi, collegati l'uno all'altro come in una catena grazie a metodi crittografici. Essa è:

- **Immutabile.**
- **Distribuita.**
- **Estremamente sicura.**





# Blockchain

Condividere  
informazioni  
in modo  
sicuro  
combinando  
Git e  
Blockchain

Studente:  
Paolo Speziali  
Relatore:  
Luca Grilli

Il Problema

Concetti  
preliminari

L'Obiettivo

Il Software  
PineSU

La **blockchain** è un registro in continua crescita di record chiamati blocchi, collegati l'uno all'altro come in una catena grazie a metodi crittografici. Essa è:

- **Immutabile.**
- **Distribuita.**
- **Estremamente sicura.**



È alla base delle reti di criptovalute, come **Ethereum**, su cui si possono anche costruire applicazioni decentralizzate con gli **Smart Contract**.



# Perché blockchain?

Condividere  
informazioni  
in modo  
sicuro  
combinando  
Git e  
Blockchain

Studente:  
Paolo Speziali  
Relatore:  
Luca Grilli

Il Problema

Concetti  
preliminari

L'Obiettivo

Il Software  
PineSU

L'utilizzo della blockchain nel progetto è giustificato da:

- Immutabilità → Garantisce integrità dei dati
- Decentralizzazione → Resistenza allo **SPOF**<sup>1</sup>
- Disintermediazione → Eliminazione di *middle-men* e dei loro costi
- Validazione *peer-to-peer* → Potere distribuito

---

<sup>1</sup>Single Point Of Failure



# Il problema della blockchain

Condividere  
informazioni  
in modo  
sicuro  
combinando  
Git e  
Blockchain

Studente:  
Paolo Speziali  
Relatore:  
Luca Grilli

Il Problema

Concetti  
preliminari

L'Obiettivo

Il Software  
PineSU

Vogliamo usare la blockchain per **immagazzinare** informazioni, ciò è problematico: **più dati** vorremo registrare, **più dovremo pagare**. Occorre trovare una soluzione per registrare **pochi dati** ma utilizzabili per **numerosi controlli** in **breve tempo**. La soluzione è l'utilizzo di **accumulatori crittografici**.



# Accumulatori crittografici

Condividere  
informazioni  
in modo  
sicuro  
combinando  
Git e  
Blockchain

Studente:  
Paolo Speziali  
Relatore:  
Luca Grilli

Il Problema

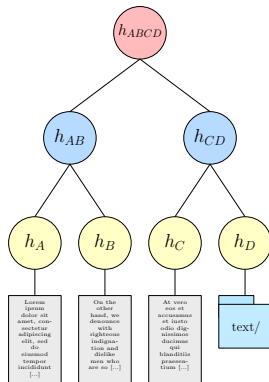
Concetti  
preliminari

L'Obiettivo

Il Software  
PineSU

Strumenti che **comprimono molte informazioni** in una **costante** di dimensione fissa.

Un esempio ne sono i **Merkle Tree**, alberi binari in cui ogni foglia corrisponde all'hash di un elemento. Risalendo ogni nodo interno calcolerà il proprio hash con gli hash dei nodi figli, l'hash della root sarà **univoco** a quelle foglie in quell'ordine.





# L'Obiettivo

Condividere  
informazioni  
in modo  
sicuro  
combinando  
Git e  
Blockchain

Studente:  
Paolo Speciali  
Relatore:  
Luca Grilli

Il Problema

Concetti  
preliminari

L'Obiettivo

Il Software  
PineSU

Realizzare uno **strumento digitale distribuito** in grado,  
tramite interazioni con **Git** e la **blockchain**, di:



**Salvare** hash di  
repository su  
blockchain



**Esportare**  
sottoinsiemi di  
repository verificabili



**Verificare** l'integrità  
di singoli file e  
repository



# Il Software PineSU

Condividere  
informazioni  
in modo  
sicuro  
combinando  
Git e  
Blockchain

Studente:  
Paolo Speziali  
Relatore:  
Luca Grilli

Il Problema

Concetti  
preliminari

L'Obiettivo

Il Software  
PineSU

**PineSU** è un software **Javascript** che sfrutta il runtime **Node.js**.

L'applicazione crea delle **strutture** sulle repository Git chiamate **Storage Unit (SU)** tramite metadati.

Queste SU sono le unità su cui effettueremo le singole operazioni, eccetto la registrazione su blockchain che si svolgerà collettivamente con l'ausilio di accumulatori crittografici.





# Workflow

Condividere  
informazioni  
in modo  
sicuro  
combinando  
Git e  
Blockchain

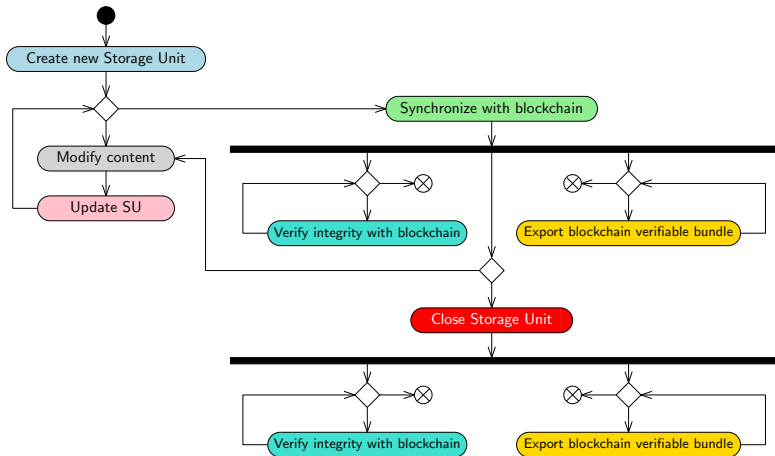
Studente:  
Paolo Speziali  
Relatore:  
Luca Grilli

II Problema

Concetti  
preliminari

L'Obiettivo

II Software  
PineSU







# Ciclo vitale di una Storage Unit

Condividere  
informazioni  
in modo  
sicuro  
combinando  
Git e  
Blockchain

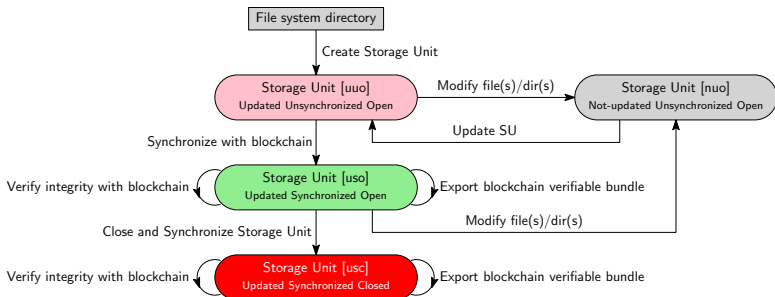
Studente:  
Paolo Speziali  
Relatore:  
Luca Grilli

Il Problema

Concetti  
preliminari

L'Obiettivo

Il Software  
PineSU





# Architettura

Condividere  
informazioni  
in modo  
sicuro  
combinando  
Git e  
Blockchain

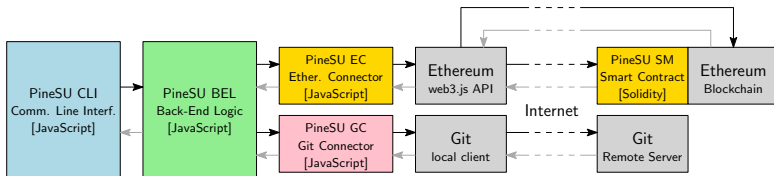
Studente:  
Paolo Speziali  
Relatore:  
Luca Grilli

II Problema

Concetti  
preliminari

L'Obiettivo

II Software  
PineSU





# Architettura (Cont.)

Condividere  
informazioni  
in modo  
sicuro  
combinando  
Git e  
Blockchain

Studente:  
Paolo Speziali  
Relatore:  
Luca Grilli

Il Problema

Concetti  
preliminari

L'Obiettivo

Il Software  
PineSU

- *PineSU CLI (Command Line Interface)*: **Crea l'interfaccia utente** con cui è possibile interagire e **richiama le funzioni** degli altri moduli all'occorrenza.
- *PineSU BEL (Back End Logic)*: Il **nucleo** di PineSU. **Gestisce le SU** e controlla la comunicazione con la **blockchain** e il client **Git** locale.
- *PineSU EC (Ethereum Connector)*: Si interfaccia con le **API della blockchain**.
- *PineSU GC (Git Connector)*: Si interfaccia con il client **Git**.
- *PineSU SM (Smart Contract)*: Permette **registrazioni permanenti** di singole SU nella blockchain.



# PineSU CLI

Condividere  
informazioni  
in modo  
sicuro  
combinando  
Git e  
Blockchain

Studente:  
Paolo Speciali  
Relatore:  
Luca Grilli

Il Problema

Concetti  
preliminari

L'Obiettivo

Il Software  
PineSU

```
MINGW64:/d/Progetti/Tesi

PineSU

? Welcome to PineSU, choose the operation to perform (Use arrow keys)
> Create new SU / Recalculate open SU
  Stage Storage Unit for Synchronization
  Close current SU
  Register Staged SUS in the blockchain network
  Check SU integrity
  Export files from current SU
  Check files integrity
(Move up and down to reveal more choices)
```

La creazione di interfacce user-friendly è fatta tramite  
**Inquirer.js.**



Condividere  
informazioni  
in modo  
sicuro  
combinando  
Git e  
Blockchain

Studente:  
Paolo Speziali  
Relatore:  
Luca Grilli

Il Problema

Concetti  
preliminari

L'Obiettivo

Il Software  
PineSU

Il nucleo centrale che si occupa di:

- 1 **Gestione dei file descrittivi.**
- 2 **Gestione degli accumulatori crittografici.**
- 3 **Comunicazione con Git e blockchain.**



# Gli accumulatori di PineSU

Condividere  
informazioni  
in modo  
sicuro  
combinando  
Git e  
Blockchain

Studente:  
Paolo Speciali  
Relatore:  
Luca Grilli

Il Problema

Concetti  
preliminari

L'Obiettivo

Il Software  
PineSU

- *SU Merkle Tree*: Le sue **foglie** sono gli **hash dei file e directory** della SU. La sua **root** è l'**hash della SU** stessa.
- *Storage Group (SG)*: Le sue **foglie** sono le **SU da registrare** su blockchain nella prossima transazione.

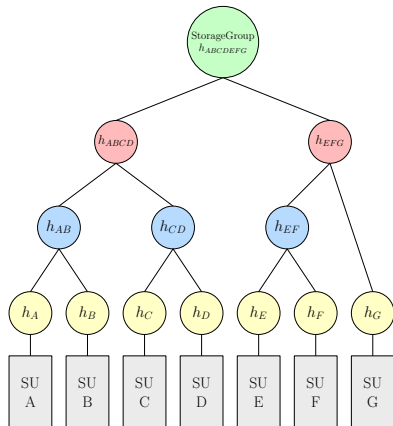


Figura: Uno Storage Group



# Gli accumulatori di PineSU (Cont.)

Condividere  
informazioni  
in modo  
sicuro  
combinando  
Git e  
Blockchain

Studente:  
Paolo Speciali  
Relatore:  
Luca Grilli

Il Problema

Concetti  
preliminari

L'Obiettivo

Il Software  
PineSU

- *Merkle Calendar (MC)*: Albero in cui le **foglie** sono i Blockchain Synchronization Point (**BSP**), istanze di Storage Group, a loro volta raggruppate in nodi rappresentanti **mesi e anni**, ciò rende i reperimenti di registrazioni passate più agevoli e veloci.

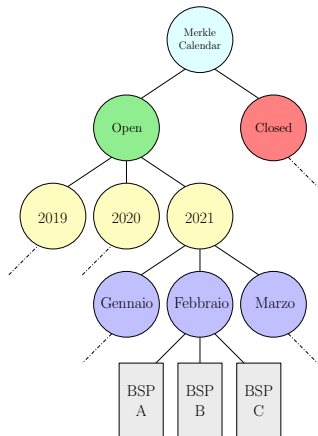


Figura: Un Merkle Calendar



# Merkle Calendar UML

Condividere  
informazioni  
in modo  
sicuro  
combinando  
Git e  
Blockchain

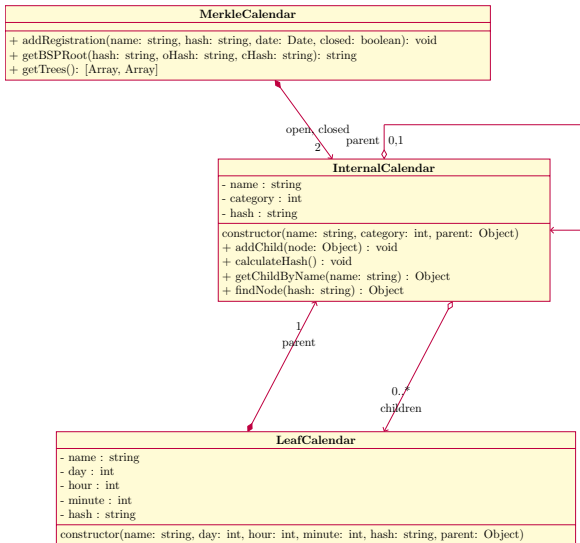
Studente:  
Paolo Speciali  
Relatore:  
Luca Grilli

II Problema

Concetti  
preliminari

L'Obiettivo

II Software  
PineSU







# Codice - Reperimento di una BSP Root

Condividere  
informazioni  
in modo  
sicuro  
combinando  
Git e  
Blockchain

Studente:  
Paolo Speziali  
Relatore:  
Luca Grilli

Il Problema

Concetti  
preliminari

L'Obiettivo

Il Software  
PineSU

```
for(let i = 0; i <= leafIndex; i++){
    leavesHash.push(monthNode.getChildByNum(i).getHash())
}
let newMonth = this.calculateHash(leavesHash);
let monthsHash = new Array();
for(let i = 0; i < monthIndex; i++){
    monthsHash.push(yearNode.getChildByNum(i).getHash())
}
monthsHash.push(newMonth);
let newYear = this.calculateHash(monthsHash);
let yearsHash = new Array();
for(let i = 0; i < yearIndex; i++){
    yearsHash.push(yearNode.getChildByNum(i).getHash())
}
yearsHash.push(newYear);
let newRoot = this.calculateHash(yearsHash)
```



## GitConnector

- git : SimpleGit

```
constructor(dir: string)
+ init() : void
+ add(arg: string) : void
+ commit(msg: string, enmsg: boolean) : void
+ getRepoFiles() : Array
+ push() : void
+ pull() : void
+ reset() : void
+ hasRemote() : Array
+ custom(commands: Array) : string
```



Condividere  
informazioni  
in modo  
sicuro  
combinando  
Git e  
Blockchain

Studente:  
Paolo Speziali  
Relatore:  
Luca Grilli

Il Problema

Concetti  
preliminari

L'Obiettivo

Il Software  
PineSU

## EthConnector

- web3 : Web3
- w1 : string
- w2 : string
- k : string

```
constructor(host: string, w1 : string, w2 : string, k : string)
+ deploy(hashRoot: string) : string
+ verifyHash(transHash: string, hash: string) : boolean
```



# Codice - Salvataggio di un hash su blockchain

Condividere  
informazioni  
in modo  
sicuro  
combinando  
Git e  
Blockchain

Studente:  
Paolo Speziali  
Relatore:  
Luca Grilli

Il Problema

Concetti  
preliminari

L'Obiettivo

Il Software  
PineSU

```
async deploy(hashRoot){  
  const ct = await this.web3.eth.accounts  
    .signTransaction({  
      from: this.w1,  
      to: this.w2,  
      data: hashRoot,  
      gas: 3000000,  
    },  
    this.k  
  );  
  const receipt = await this.web3.eth  
    .sendSignedTransaction(ct.rawTransaction);  
  return receipt.transactionHash;  
}
```



# PineSU SM

Condividere  
informazioni  
in modo  
sicuro  
combinando  
Git e  
Blockchain

Studente:  
Paolo Speziali  
Relatore:  
Luca Grilli

Il Problema

Concetti  
preliminari

L'Obiettivo

Il Software  
PineSU

```
contract SURegistry {  
  
    string StorageUnit;  
    mapping(uint => string) public registry;  
    uint public SUCount;  
  
    function addSU(string memory hashSU) public {  
        SUCount++;  
        registry[SUCount] = hashSU;  
    }  
}
```

Codice dello **Smart Contract** che gestisce il salvataggio su blockchain delle **single SU**.



# Le operazioni disponibili

Condividere  
informazioni  
in modo  
sicuro  
combinando  
Git e  
Blockchain

Studente:  
Paolo Speziali  
Relatore:  
Luca Grilli

Il Problema

Concetti  
preliminari

L'Obiettivo

Il Software  
PineSU

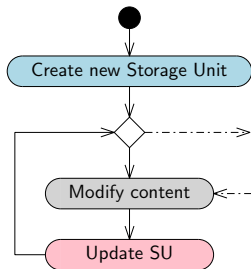
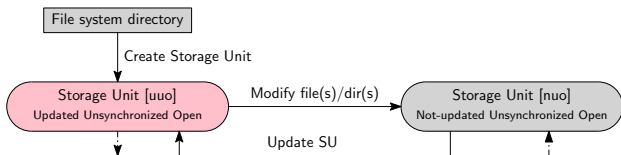
- 1 Creazione di una Storage Unit o Ricalcolo di una Storage Unit pre-esistente
- 2 Staging di una Storage Unit nello Storage Group
- 3 Registrazione dello Storage Group nella Blockchain
- 4 Chiusura di una Storage Unit
- 5 Esportazione di sottoinsiemi di file da una SU
- 6 Controllo di integrità di singoli file esportati da altre SU
- 7 Controllo di integrità su una SU



# Creazione di una Storage Unit

Condividere  
informazioni  
in modo  
sicuro  
combinando  
Git e  
Blockchain

Studente:  
Paolo Speziali  
Relatore:  
Luca Grilli



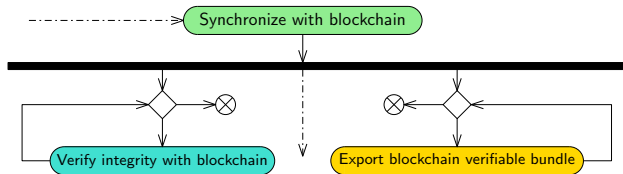
```
var merkleroot =  
  gitLogic.calculateTree(filelist);  
await inquirer.askSUDetails(  
  files.getCurrentDirectoryBase(),  
  remote).then((details) => {  
    details.owner = w1  
    details.hash = merkleroot  
    details.filelist = filelist  
    details.closed = false  
    files.saveJSON(details);  
  });
```



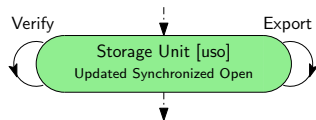
# Registrazione di uno Storage Group

Condividere informazioni in modo sicuro combinando Git e Blockchain

Studente:  
Paolo Speziati  
Relatore:  
Luca Grilli



```
var [doc, openRoot, closedRoot] =
  files.createSGTrees(sg);
ethLogic.
  addToTree(openRoot, mc, false);
ethLogic.
  addToTree(closedRoot, mc, true);
var [oHash, cHash, transHash] =
  await ethLogic.registerMC(mc);
for(var el of document){
  el.oHash = oHash;
  el.cHash = cHash;
  el.transHash = transHash;
  files.createReg(el);
}
```







# Visualizzazione post-registrazione

Condividere  
informazioni  
in modo  
sicuro  
combinando  
Git e  
Blockchain

Studente:  
Paolo Speciali  
Relatore:  
Luca Grilli

Il Problema

Concetti  
preliminari

L'Obiettivo

Il Software  
PineSU

BLOCK 94	MINED ON 2021-08-18 16:00:20	GAS USED 21320
BLOCK 93	MINED ON 2021-08-18 15:27:51	GAS USED 21320
BLOCK 92	MINED ON 2021-08-18 15:26:23	GAS USED 21320
BLOCK 91	MINED ON 2021-08-18 15:25:55	GAS USED 21320

VALUE 0.00 ETH	GAS USED 21320
TX DATA 0xe67006f15ecd3fa2719d148be68d3a3242e1be8b	

## EVENTS

BLOCK 94	
GAS USED 21320	GAS LIMIT: MINED ON: BLOCK HASH: 5 0:20 0+baa08b6b640accbb9648ff313929998ced4a1abel 4d6769756c
TX HASH 0xc563030328e652d427cd00707d7a0e2ce0bcf6c76b23482469eb497e2dc87d2e	
FROM ADDRESS 0xc21544bfc002905532b086bF647754A8A 0x3a0999caE86a35a402210504c090DEF6490 21320 732960	TO CONTRACT ADDRESS 8A0029
GAS USED 21320	VALUE 0

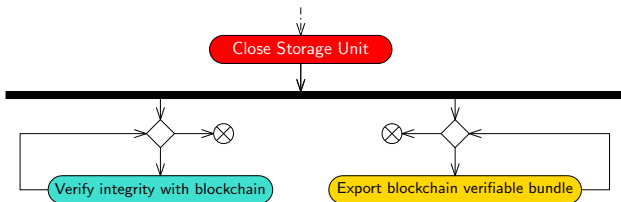
```
{
  "path":
    "D:/Progetti/Tirocinio/
    sample",
  "root":
    "e67006f15ecd3[...]
    e68d3a3242e1be8b",
  "transHash":
    "0xc563030328e[...]69
    eb497e2dc87d2e"
}
```



# Chiusura di una Storage Unit

Condividere  
informazioni  
in modo  
sicuro  
combinando  
Git e  
Blockchain

Studente:  
Paolo Speziali  
Relatore:  
Luca Grilli

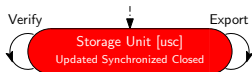


Il Problema

Concetti  
preliminari

L'Obiettivo

Il Software  
PineSU



```
if(fs.existsSync(".pinesu.json")){  
  var data =  
    fs.readFileSync(".pinesu.json")  
  var myObj = JSON.parse(data);  
  myObj.closed = true;  
  fs.writeFileSync(".pinesu.json",  
    JSON.stringify(myObj));  
  return myObj;  
}
```



# Esportazione di sottoinsiemi di Storage Unit

Condividere  
informazioni  
in modo  
sicuro  
combinando  
Git e  
Blockchain

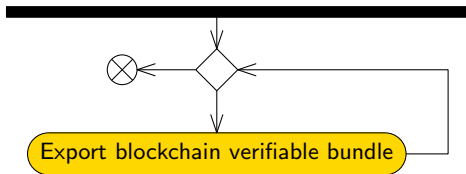
Studente:  
Paolo Speziali  
Relatore:  
Luca Grilli

Il Problema

Concetti  
preliminari

L'Obiettivo

Il Software  
PineSU



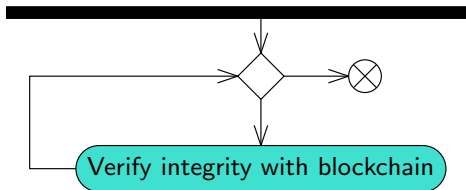
```
var zip = new AdmZip()
var fl = JSON.stringify(json)
zip.addFile(".pifiles.json", Buffer.alloc(fl.length, fl))
for(var el of list){
    zip.addLocalFile(path)
}
zip.writeZip("../pinesuExport.zip")
```



# Controllo d'integrità su una Storage Unit

Condividere  
informazioni  
in modo  
sicuro  
combinando  
Git e  
Blockchain

Studente:  
Paolo Speciali  
Relatore:  
Luca Grilli



Il Problema

Concetti  
preliminari

L'Obiettivo

Il Software  
PineSU

```
async verifyHash(transHash, hash){
  const res =
    await this.web3.eth.getTransaction(transHash)
  if(res.input == "0x"+hash){
    return true;
  } else {
    return false;
  }
}
```