Rollback

The student, whose name Gem did not know, blinked in surprise. "Why not?"

"I can't have you go research this. It isn't our department. Computer science, maybe."

"I thought for sure this would interest you. This course isn't about Technology and Society today. It's about tomorrow."

Gem turned her monitor around so that the student, inching closer to the desk, would sit back. "Do you see this? It's the number of citable works using Datalirium. It was a flash in the pan. Not a peep in the past six months. Not going anywhere tomorrow."

"No, that's not what I'm interested in at all." A pause. "I mean, Datalirium *started* there."

"What do you mean?"

"Well, no one knows the inventors for sure, and it started with citable works and research data. Then there's this guy online now, Jacob Lenton, who says it can be a new currency."

"I don't see how that could be."

"The original concept is to track your research data as it’s recorded and log it in this blockchain network, right? So research couldn't get forged or backdated, anyway. So hackercept adds this extra component, a 3D fractal. If someone finds patterns in the fractal, they get one Datalyra credit. And computers can't mine it; the geometry is too complicated for them to pick up on it so far."

Gem turned the screen around, typed a few words into Google and scrolled a bit. "Could you write me an abstract? By tomorrow, even? I don't want the project to get ahead of you, if you need to change topics."

"Thank you ma'am."

As the student stood to leave he admitted, "I’m surprised that you knew about Datalirium anyway. Where did you hear about it?"

Gem smiled. "Just a friend of a friend. Undergrad."

On the inside, she was panicking.

In Gem's sophomore year, the college campus had been completely different. There were still areas she had not yet explored, labs for higher-level students and their higher-level projects. The room which would become Gem's office was not yet constructed, a field of tall grass behind the chemistry hall.

It was a dewy January morning, Gem remembered, when she had heard about Datalirium. She remembered because her sneakers squeaked all the way down the main hall of the computer science building, because she'd walked straight across the quad, because she liked to see the grass after a cold winter break in Minnesota. Before the semester began, they had two weeks to join a class or not, to study a subject short-term or not. The flyer for this session had been only: "Hack. Bring laptops." The grad student organizer made sure the undergrads were in random groups and then, frustratingly, disappeared to her lab.

In the meetings that they held afterward, there was an unspoken rule that no one had come up with the idea. But in Gem's memory, it was Edward. He showed them them the article: "Prize-winning Lab Retracts Paper". He asked the question, "can we make a lab notebook that can't tell a lie?". It was not the group's favorite idea. But it was a good question. It stuck with them. When Nathan's idea failed to wow in its first demo, they met in the library's whiteboard-walled study room, and Edward asked it again.

"No," said Nathan. He and Paul, the last of the group, began listing reasons. A determined liar would give the lab computer false numbers. They could alter the recorded data, and electronic sensors, and test equipment, to fit what they wanted.

"What if they couldn't alter any of that?" Gem had asked. "The moment data is recorded, by sensor or by human, it gets sent out on a network. That's how Bitcoin transactions work, you know. Everyone has a copy of everyone's checkbook. We do that to the lab notebook. You can't tell everyone to rewrite your data if you change your mind later."

"They could still give the notebook false numbers," reminded Paul.

"Only if they knew from the beginning, each measurement, what they wanted the numbers to say. Fraud is usually an act of last-minute desperation."

"Gem, it either works against a determined liar or it doesn't work at all."

Edward cut in, "what if they don't know what they want the numbers to say?"

Paul and Gem processed this.

"Double blind experiments. An internet-connected instrument brings in a second factor, an offset into the output. If that offset number is off, it's fake. The liar won't know how to alter his numbers. The only way to get data and know what it means is to share it with the network and convince it that a human did the experiment at that moment, without knowing the result."

Nathan picked up a whiteboard marker. "Let’s look at what you’re saying mathematically, though..."

By the end of the two-week class, they had only made an opaque cylinder that Tweeted when its volume changed. The protocol itself was never discussed in the classroom. In their follow-up meetings the four resolved to become a club. They never registered with the Activities Board, because they would need to accept freshman members and limit their library time. As far as the librarian knew, they were a study group.

But one night, deep inside one of the computer labs, they gathered around Paul's touchscreen tablet. It awoke with a chirp and the name DATALIRIUM appeared. Edward tapped at his phone to start the genesis block. "2014/03 Prize-winning Lab Retracts P" the first message read. They groaned at the bug.

"Keep it running," Paul insisted. "We'll put some data on it and see if it sticks."

Keeping the project a secret from friends, classmates, and parents was easy. No one in their network would understand the project, as far as they knew. There were a few times Edward would hint at a startup. The problem was that their protocol was too easy to reproduce, the hardware much easier for any established company to manufacture. Their mini start-up was bound to be overshadowed or acquired.

Edward and Nathan got offers from biochemistry labs in opposite parts of the country. One day Gem ran into them at the university center, lounging in front of the TV. She came up from behind them and saw slides flickering across their screens.

“You better not be selling out," Gem said.

They were startled but moved a futon over for her to sit. Edward was watching some sort of livestream and let Nathan do the talking. "There's a bigshot professor in Ukraine who's coming here to present at a conference. We're working with him."

"On the project?"

"On what happens when he claims asylum. He crossed the wrong guys back home. Big mess. Edward is organizing the event, so the university asked him to help keep it quiet."

"That's... wow I didn't know. It sounds like a big deal."

"Yes. All our communication's PGP-encrypted. Huge deal."

"Well, is he a computer scientist? Worth telling him about the project?"

"We're going to keep him on the dark. In fact, we're going to tell him not to give the talk."

"That's too bad."

"It's an opportunity, Gem. They're going to call out this professor's name, and anyone can walk up there and talk about their project. Any photo will tell them it wasn't the same guy. But if he has a good topic, people will listen."

Gem wrung her hands to try and lose some nerves. "They will see you! Don't fuck this up!"

"Oh, we thought of that! We're hiring an actor to read word-for-word off of the slides."

"Word-for-word?"

"I'm not about to call him up and give him a crash course on cryptography and Proof of Work. In fact, it's better if we don't speak to him directly at all."

Gem fidgeted in the auditorium. She could barely see the stage. The others must be in the audience somewhere, but she hadn't spoken to them since the previous day.

The provost was on the microphone. "Aleksander, welcome. Show us what you've been working on."

A tall blond man emerged from behind the side curtain. He strode out, shook hands, and grasped the podium tightly. "I am here today to talk about this fantastic project my students have been doing," the false Aleksander said. "I am talking about Datalibbum."

The false Aleksander was mobbed by people at the end of the talk. Students and greybeards alike. His insisting, "please, no questions!" was the last thing Gem heard as he left the hall.

Gem thought for a moment to thank him, to shaking his hand. But it would be too conspicuous. And she had to add new resources on her server. Datalirium was trending.

After the meeting with her student, Gem had driven out to Nathan’s new office.

Nathan was turning a thimble-sized model of a pH sensor over and over in his hands. He didn't look directly at Gem, but she remembered that was typical when he was lost in thought.

"You can't discount Datalirium, and what's come of it. A sensor like this could be in every lab in the country. Quite affordable." He returned the sensor to a set of new creations along the edge of his glass and aluminum desk. "Even without the hype, we've always been profitable."

"I don't have anything against what you've made of Datalirium since we graduated. We always thought... I mean when we were in school, we thought someone might make a profit from it." Gem had brought her student’s abstract in her bag, but wanted to get to the point directly and personally. "There's someone out there who's using it as a currency."

"What now?" Nathan stopped moving altogether for a second, then shook his head. "I don't see how that'd be. It's just numbers. There's no role for automatic computation like with Ethereum."

"The algorithm measures human work and measurement. So this guy - his name is Jacob Lenton - puts out a time-sensitive automata, one of those pattern generators from Wolfram's books. Even an advanced computer is going to have a hard time looking at the pattern and figuring out if it can folds on itself in the future. A person does pretty well, or so he says."

"So the person is just looking at patterns all day? There’s no value in that."

"Well suppose I solved a thousand patterns today. That means me or some poor soul working for me entered a thousand different combinations. Or maybe two people solved five hundred each."

"I don't see how it matters at all how many you solved. Looking at these sort of patterns is meaningless."

"The currency isn't about the patterns at all. It's measuring human capital. If I solved a million patterns and didn't miss one, it means I have a thousand workers at their desks with quality control backing them up. That sort of thing is incredibly valuable in the outsourcing business. You could even sell futures. There's some guy out there right now with an office in Bangalore asking staff to just click on patterns all day."

That idea took a long time to digest. Nathan wasn't going to change his mind anytime soon, Gem could tell. They needed more time to research this idea.

"You're going to find a problem with this, aren't you?"

"I'm sorry?"

"You're going to use this to tell me that Datalirium should never have been created. I've had many people storm in here and tell me the same. Researchers who've been undermined by their own measurements. I make sure they know that Liri Labs had nothing to do with its creation. We just built what came after."

"Well without a public inventor, there's no one responsible for it. There's no one to guide it, no one to throw a wrench in the gears if it goes astray."

"An inventor would only mean control, which any open system has to reject. There was no one telling me what to do with Datalirium, how to build on it, how to market it. How do we know that this Jacob guy isn't on the right track?"

"Because we know, Nathan. You were there."

Nathan put his hand up to wave away the suggestion, but then nodded. "Sorry, I have to distance myself from that. People make very close guesses sometimes. We're one of the few companies deep in this business, which puts me right in the center."

Looking past Nathan through floor-to-ceiling glass, Gem could see lines of cars starting to fill in the parking lot below. They would soon have company. "I'm glad you didn't run from it. You've done more than any of us to make Datalirium happen, whether anyone knows it or not."

Nathan beamed. "If you run into any trouble with this Jacob guy... you know what, I'll set up a meeting for you. Yes. He'll answer my call, I'm sure. And last thing, if this is real, if things get serious, if you ever need to get the band back together..."

"All of us?"

"Yes, all of us - I can book a secure room. Tickets can be arranged. I don't know about Paul, though. He's gone off the grid."

Now this, Gem hadn't heard. "Off the grid?"

"On a mountaintop. In the middle of nowhere, western Nepal. Poetic in a way."

On the way out the door Gem said to herself: "Getting his key is going to be a bitch."

“You see, professor, the first smart contract in Datalirium uses an interesting cryptographic signature."

"What do you mean by that?"

"Well, in this case it means the creator of Datalirium can publish messages to the users, but only if it gets signatures from multiple keys. Having a second key to avoid a hack makes sense. But this contract, when you decompile it from bytecode, looks like it takes four separate keys."

"Why do you think that is?"

"It isn't possible to tell. It could be one for each hacker, or different levels of security. If a message comes out signed by any other set of keys it could just turn out be a hoax. Or it could mean they got to one of them."

"They? Get to?"

"With any system that breaks up the old structure, you know there's a line of people trying to disrupt it. Look what the SEC did to all of the Bitcoin exchanges in the U.S."

"But whoever the inventors are, they have multiple keys."

"Yes."

"And if they lose track of any one, they'll never make a statement people will agree is from them."

"Right again."

"Well, let's hope no one is an asshat and loses their keys."

Gem stared up at the dark ceiling and found no sleep.
Let's hope no one is an asshat and loses their keys.
She kept picturing Paul, with shaggy hair and a lengthy beard, smashing his USB key with a rock. Or with his head shaven, in monks' robes, tossing the key into a ceremonial fire. Or just one day going into an internet cafe, opening up the file window, and clicking delete.

If Paul's key was gone, then they no longer existed as verifiable founders. They could make a statement and be a curiosity to the press, and it could change all of their futures. But the Datalirium community and this new monetization project would ignore them. With an outcome like that, who would stand with her? What would be the point?

The future, then, was likely with Jacob and his money-making scheme. There was nothing Gem could say to him to stop it, but she'd agreed to a meeting anyhow. She couldn't prove to Jacob that she had created it. It would be foolish for her to try.

And then she had an another idea.

"... because we've found a bug in Datalirium". She was surprised to hear her voice echo aloud on the other end of their phone line. She changed her tone to a more hushed concern. "There's a bug... in Datalirium. You can't use it." He would need to hear it was real and dire. "We'll show the bug at a conference. Um. Next month."

And now she had a plan.

Gem's steps echoed through the all-marble lobby of DL Capital. Some Googling told her Jacob had acquired the space in downtown Phoenix from an investment bank. The lobby could have made the company look grandiose, but without a single person present or passing through, the effect was lost. At the counter where a receptionist would sit, a terminal came to life and flicked through several forms. Gem approached and selected her name from a list. There was a momentary loading screen, then a message that the CEO would arrive shortly. Gem thought through her script one more time. The right turn of phrase. The need for the words "we don't have much time" to show up somewhere.

Elevator doors opened with an unceremonious ping, and Jacob appeared with two uniformed employees. He smiled and reached out his hand.

Despite the oppressive heat, they found an outdoor table in a nearby cafe. When small talk was finished, Gem laid out a detailed description of how Datalirium was working, internally. How she understood the currency angle and its interaction with Datalirium's API. Jacob nodded, but once or twice asked his engineers if they had gotten the gist of it.

Now Gem acrobatically jumped through multiple topics: how different clients communicated in the protocol, how the clients found each other through DNS servers, how these servers told the clients when it was time to update. She'd purposely lost them, and before they could question it, she added, "and we've got research showing that exploit could be a problem. Not today, but for a payment network like this, you can't wait for an unsigned checkpoint that could get through to a thin client."

"We can't have that now, can we?" The engineers chuckled. Jacob turned out to be a bit of a joker, but he could understand the significance of what Gem was saying for his business. "The

bug is what happens after a rogue actor tries to break the blockchain, right? Is it like a 51 percent attack, when the majority of the computing power on the network is misinforming the others?"

"Yes, but when more of your users or even your own servers go online, when you respond to a 51 percent attack by increasing hash-power by activating thin clients, some of your own processing power would contribute to the problem."

Jacob shook his head. "Now I see why Nathan encouraged me to speak with you. I'm glad that you're doing a responsible disclosure of the bug; we actually see a number of hackers doing that in cryptocurrency. What I don't understand is how this affects us more than Nathan and his devices. We're using the same code, the same protocol."

"Maybe not. He could switch to an alternative." They looked surprised. “NDA, oops.”

"Regardless, the little handheld devices that Nathan's mad science experiments run on, those are all going to run thin clients. Most of what we have - the outsourcing markets, the Bangalore project - they're running full nodes on desktops. They're always connected. The only logic I can make out of this is that your team needs a grant to patch this bug."

Gem didn't know whether to take this angle or not.

Jacob continued, "we'd like to see it patched, to keep our users’ confidence, but I don't think the community is ready to accept our involvement just yet. Already we're doing the majority of the transactions on the network. Already we're dominating the press. The only way new code is going to get into production is if the whole thing breaks down. Unless, of course, a patch comes out with the blessing of the original developers."

"The original developers? Really?"

“If my market analyst weren't convinced the developers were a ring of professors in Mongolia... I would of course suspect you, Gem."

For now she said only, "you shouldn’t make wild guesses like that. It’s the least funny joke in crypto."

With Jacob undeterred, the best option was to call the others. Edward agreed right away, provided she could pull in the others. Gem decided not to tell him about Paul.

Was it going to work? Gem pondered it through the meeting with her department head to get emergency leave, unexplained, the day-long flight through Qatar, and the six hour long bus ride, squeezed between Czech backpackers, on the road from Kathmandu to Pokhara.

Watching the GPS dot trace the curves on the road, Gem knew they were last at her stop. She signalled the driver, and she emerged, exhausted, choking on dust. From her backpack, she withdrew a pair of binoculars, and spied the monastery on the other side of the river.

After paying a local man 500 rupees, Gem began to scale the path up to the building. Ahead she heard the ringing of bells, fading into nothing, interrupted by the occasional horn from the road.

At the final flight of steps, a monk up ahead noticed her. “No pictures,” he said, moving his hands frantically.

Gem called out to him: “You got anyone named Paul up there?”

Another monk appeared and jumped back. “Jesus Christ! Hey, I’ll have to call you back.” As he pocketed the phone in his robes, Gem at last she recognized Paul, skinnier and somehow more youthful before. “

“You could have just called me. But I know I’ve been bad about keeping in touch.” Paul gestured for them both to sit down at a tea table with plastic chairs. He recovered a tablet where he showed her a Financial Times article. "Nathan set up a partnership with this Jacob guy. Looks like Datalirium is in their hands."

I covered my eyes, let out an exasperated sigh, and then remembered that yes - yes, losing Nathan would end the chance of doing the announcement cryptographically, via smart contract. I closed my laptop.

Paul resumed scrolling through the story. "He uses some very strong wording to endorse the project."

"You think that meeting him spooked him into picking a side?"

"Can't say. Something like this would take time to set up. Here it says-"

"You know what? I can't even look at it. I can't even think about it. You can laugh at me now, for trying."

Paul got up, and gestured for me to stand, too. We embraced. "I'm glad that you found me. We do need to do something about this, to fix what is wrong in the world. I can't be going back here, meditating with the others, while I know my creation is being used for evil."

"Good morning."

"Welcome back, professor!" One of the students called.

Aside from someone who I recognized from the student newspaper and classes, the others were new to me. The video window on my laptop indicated that two cryptocurrency blogs and MIT Technology Review were livestreaming us.

"Most of you signed up for this class to test and document a vulnerability in blockchain technology. Unfortunately I have to say that we don't have one today. I have an announcement regarding Datalirium, which I am proud to deliver on campus here today. Probably we should have done it this way, years ago."

I waved and the other two came on stage.

"The three of us - plus the founder of Liri Labs, are the original inventors of Datalirium. Everyone onstage today has signed a sworn affidavit to this effect. We would have liked for everyone to make a joint statement, but as you can see, Nathan has declined to appear."

"Didn't Liri Labs have a spokesman deny any connection to the original Datalirium platform last week?"

Paul answered: "Yes. I spoke to Nathan again this morning and he refused to join us in this effort."

"Which company are you from?"

"I was part of the original project team. Until recently I was encamped outside a Buddhist monastery, and..."

"That's not really important," Gem waved on. "We have come to an agreement - us here today - that Datalirium must be shut down, and its miners should discontinue using the program. Our invention is being used to dehumanize and commodify workers in a way which I cannot - in a way which only a cruel mind would contrive and understand."

A VoIP question queued in - "Professor - though your story is interesting, what is your best proof that you were one of the inventors? Is there a strictly cryptographic proof of it?"

"I can move some early tokens," I offered, "but not the original ones. If we had one more signature, we could have issued a statement through the original smart contract."

"But how can you possibly shut down Datalirium? It's a decentralized network used by thousands of people who you've never met."

"We're the inventors, and... you're right, in a successfully decentralized system, who has the authority to speak to who uses the network and how it works? The only ones with credibility are the people with the greatest share of mining hash-rate, or the inventors themselves. And here we are."

Gem's announcement - and a future bug disclosure - were ignored. Soon she was suspended by the university. Forced to share an apartment with Paul, the wayward computer scientist turned conflicted monk. Pestered on social media with questions and accusations.

Gem found only misery in being an unverifiable founder, and knowing that the DL Capital people were getting away with it. Then came the call, a flight to DC, and an introduction to people at DARPA who believed her, and offered her a job. It was a revelation.

Gem followed her supervisor into the conference room, where several people were checking in on video screens.

"Oak Ridge, are you fully online?"

"Yes, and hearing you load and clear."

"We're going to send the professor's drawing over to your board for your experts to review."

"Excellent."

"This will take a while. Professor, maybe you would like to meet the director while we wait?"

"Sure." Gem got up and followed the woman down the corridor to an executive office. We were still underground, but the office was lit with a warm glow, the style was decidedly more ornate than the government-issue office furniture in the conference center.

"Ah, here you are!" An aging Japanese man got up from his chair and stretched out his hand.

I went in to shake his hand lightly, and he bowed instinctively.

"Pleasure to meet you-"

"Dr. Nakamoto, Director."

"Are you-"

"Yes, of course. Would you like some Danish cookies?"

My thoughts were racing as I settled onto the man's couch. "I have so many questions, you know? I mean..."

"Unfortunately we won't be able to answer those today. It is, I suppose, a bit of a revelation to find me working here." Nakamoto passed a blue tray of cookies. I took one.

"It's commonly known that I stopped coding and sending e-mails in the Bitcoin project shortly after it became of interest to the WikiLeaks and then, in turn, the CIA."

"Yes."

"The Agency has never liked the type of freelance projects that we have in our own team. It was a conflict of interest, they said, for us to create Bitcoin at the same time that we were tasked with embedding hardware for anti-leaking and anti-laundering. The National Security Council asked me to do whatever I could, short of exposing my identity, to kill the project. So I quit and never spent the coins."

"But people kept using it, and making currencies of their own. It was too late for you to stop it."

"Yes. That's why I've taken such an interest in your case, Professor, in your project, and what could be the first successful rollback."

"I'm honored, Dr. Nakamoto, but the vulnerability in Datalirium... if it is possible to exploit, which I'm not sure we have the compute power for, it doesn't exist in Bitcoin."

"Oak Ridge has near limitless compute power, by industry standards. Teraflops, petaflops, yottaflops..."

"Then why not use that and take over the Bitcoin network?"

"At this point, there is an understandable fear about exposing the intel community involvement in the Bitcoin world, and our capabilities. It's a political issue. We did make one attempt early on, and for a few hours in March 2013 we thought it was over, but everyone updated their clients to

avoid a contentious fork. Fortunately this time around, we are dealing with different technologies, and their response measures, with thin clients, could be advantageous."

"Okay, so we use this compute power to mislead and burn out the Datalirium network?"

"Even here, too much hash-power would make our meddling obvious and tip the info-sec community off to our processing power. Then as soon as we stopped intervening with hash-power, people would pick up from when we last started. Our goal must be to fork the blockchain and get DL Capital official bots to contribute to both chains, permanently discrediting the currency with a minimum amount of manipulation."

The plan made sense. "It would be a pleasure working with you, Dr. Nakamoto."

Gem stepped back into the control room.

"Good evening, Dr. Nakamoto." The old man nodded and then left.

A technician stepped up. "We're ready, Professor. On your mark."

Gem wished Satoshi Nakamoto could have stayed for support, but didn't want to question him. Too late now. "Oak Ridge, you have my permission to close my civilian research project. Initiate the blockchain fork."

"Thank you, Professor. We have confirmed your cryptographic signature on the codebase. We are queueing up 40% AWS, 40% GCS, and 20% local for a start."

"When you move to the second spike, put more of that into local so that DL Capital responds with their thin wallet images on AWS."

"Got it."

The graph started to trace itself on the screen, and a second, shallow line showed the increase in hash-power in response.