Pet3rpan
Cryptography enthusiast
Mar 24 · 17 min read

Before Bitcoin Pt.1—70s "Public Key Saga"

70s, 80s, 90s, 00s and the people behind the tech.

Part One's Notes

If you ask people where does Bitcoin or cryptocurrency come from? You will get many answers, and if they are right, they will likely be vague jabs at the truth. What many do not know is that Bitcoin was a creation born out the cypherpunk movement. Originated during the 70s but formed in the 90s, it fought the US government's injustices surrounding digital freedom and pioneered modern rights to personal privacy.

While you can try to understand the cypherpunks through a google search…You may struggle to deeply understand the full picture unless you understand the context of the movement itself. You have to zoom out and think bigger. Who seeded the movement of the cypherpunks? Where did all the ideas come from?

Before Bitcoin is a series which aims to give you a historical perspective of cryptocurrency's technology and philosophy.

To do this, I will be writing a 4 or 5 part series focusing on cryptography, the underlying mechanism of all cryptocurrencies along with the philosophies of privacy formed over time. This will be explore through the 70s, 80s, 90s and 2000s where in each decade. Overview of the series focus points:

Part One—70s: How cryptographic knowledge was democratised through the publication of public key cryptography.

Part Two—80s: The origins of decentralised services, anonymous communication networks and digital cash.

Part Three—90s: The origins of the cypherpunks.

Part Four— 00s: The technologies born out of the cypherpunk movement during the 2000s.

Part Five—Bitcoin: The original designs of bitcoin and early coin forks.

This series will be a long read. It won't be your typical 300 word pamphlet-disgusied-as-a-medium-article written a marketer or the usual short punchy stuff you find. To understand anything, historical context is important and the time in doing so is an investment. This aims to provide just that.

Introduction

So… We want to understand cryptocurrency and it's history.

Where do we start?

I want to kick this off by first talking about the 70s and the creation of public key cryptography. While you might groan at dusty, black and white image of the 70s just like I did when I first researched cryptography, I didn't realise how important this decade was…

Until the 70s cryptography was mostly used by the military to secure communications. Research was mostly conducted by intelligence agencies (GCHQ, NSA etc.) or licensed research labs operated by enterprises such as IBM. Cryptography was used for commercial purposes and the public had little access to the knowledge. This hold on modern day cryptography would be broken by the publication of **public cryptography**, released by three cryptographers known as Hellman, Diffie and Merkle. Their work would result in the first big public wave of interest into cryptography.

So what is public key cryptography?

Cryptography is the practice of securing and protecting information against 'enemies' or people who have no right to the information. It is the underlying mechanism that secures the authenticity and integrity of information, and also ultimately what makes blockchains and cryptocurrency possible.

Public key cryptography is a shift in the use of cryptography that now secures most cryptocurrency protocols.

How does it work?

Essentially, public key cryptography allows people to send encrypted information to a public address over unsecured channels. And only

people with access to the public address’s corresponding private key can decrypt the information. The private key is also used to sign off and authenticate information sent away to verify the legitimacy of its origin.

In the case of cryptocurrency, while people can send bitcoin to a public address and see how many bitcoins it holds, only the owner with its corresponding private key can use the bitcoins and sign off on transactions.

Easy video outline the concept of public key encryption

This was an extremely important concept for cryptography and would lead to the first big interest in cryptography…

Three cryptographers known as Martin Hellman, Whitfield Diffie and Ralph Merkle would be behind. And they have an very interest story…

So how did these three researchers defeat the government’s control on strong cryptographic knowledge?

First, lets follow the story of a cryptographer known as Martin Hellman.

Martin Hellman, a young ambitious man

Hellman grew up as a nerd where he was exposed to science at an early age by his father, a physics teacher at a local high school. He remembers that:

> “My Father had books on the bookshelf that I would pull down and read about things. Including one I remember, Ganot’s Physics, an old physics text from the 1890s that he bought. Obviously it was an antique

> even for him. And my seventh grade science fair project came out of that. So I was interested in science, but not particularly cryptography, and I loved math too."

Early Career

Following his interest, he studied electrical engineering from New York University and completed his masters degree in electrical engineering at Stanford University in 1967. **Fairly well suited to academia, he did well and enjoyed his time at school.**

While it might be intuitive to assume that he studied cryptography at some point, he never much associated with that side of computer science until later on. Instead, early on he was very career driven, having already planned his life at an early age.

He envisioned that he would be married at the age of 35 and until then, he would be travelling the world working in management for big businesses.

At the age of 22, he set out to complete a PhD in some esoteric way of thinking called 'decision logic'. Hellman saw a doctorate as an opportunity to 'counter' his youth in management based on the logic of:

> If I had the PhD. it would be a way to help quell questions like 'what can this kid do?'

Ironically in the first year of his PhD, he had gotten married. That did not slow him down and within 2 years of starting his PhD, at the age of 24, he achieved an early breakthrough. He released his dissertation: Learning with Finite Memory

Hanging on to his grand life plan, he followed his dreams to go work for IBM.

For a brief moment, he was juggling the decision to either teach or work in enterprise but guided by the allure of travelling the world and a lot more money, he decided: **"No thanks, I don't want to be poor."**

Early influences of Harry Feistel & Peter Elias

So off he went to go work for IBM at the Thomas J. Watson Research Centre in New York. Hellman worked in the Pattern Recognition Department building machines that tried to recognise numbers from photographs (captcha lol).

While Hellman's work had nothing to do with cryptography, IBM had it's own division focused on cryptographic research. From that division, he met a German researcher called **Horst Feistel**. Through their friendship, Feistel introduced Hellman to cryptography. They often had lunch discussing cryptographic systems and seemingly unsolvable problems. Hellman regards Feistel as one of his biggest early influences and would go on to later design the government's data encryption standard (DES).

As he mentally matured, and also when his wife was pregnant: he asked himself **"Do I really want to be traveling the world or do I want to have more time with my family?".** It was the timeless dilemma that we had to face throughout history: wife & child vs. money

Choosing family, he became an assistant professor at MIT's Department of Electronic Engineering. This was where he met **Peter Elias, MIT's Head of the Electronic Engineering, who collaborated on research with Claude Shannon** "the Father of information theory". If that means nothing to you, he essentially invented the modern day cryptography that was used in WWII.

After meeting, Peter gave Hellman a copy of Shannon's landmark paper: "A Mathematical Theory of Communication" (1948). This was another major influence of Hellman that shaped his mathematical understanding of cryptography.

He became pretty good friends with Elias which overtime deepened his fascination and knowledge of cryptography. Hellman regarded Elias as being another pivotal part of his education in cryptographic philosophy.

Pursuing research

In 1971, Hellman returned to Stanford. This time as an Assistant Professor. While he continued his worked on decision making research, by the end of 1971, he had started to pursue cryptographic research.

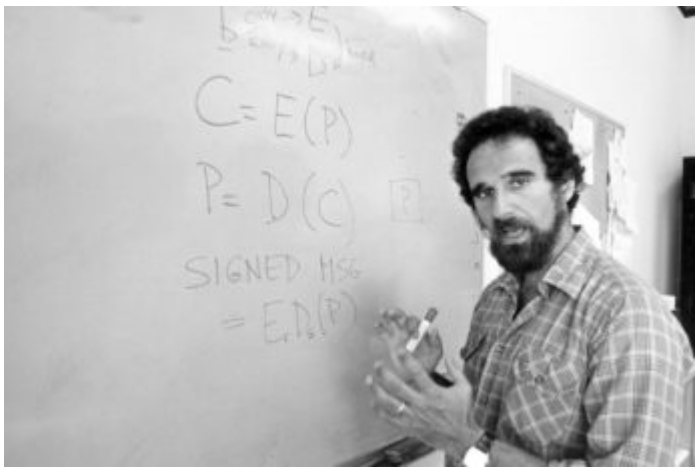
His colleagues and friends at Stanford did not support his decision to do so. "They told me I was crazy", Hellman said. Funny thing was, he didn't exactly disagree with their sentiment:

> "How could I hope to discover anything that the National Security Agency, which is the primary American code-making, code-breaking

> agency, didn’t already know? And they classified everything so highly that if we came up with anything good, they’d classify it.”

But driven by his intellectual fascination and previous experience with his influences at IBM and MIT, he believed that cryptography would be of commercial importance in the future.

He gave his first talk and released his first technical report on cryptography in 1973. Hellman’s work soon spread and did not go unnoticed. In 1973, a researcher called Whitfield Diffie reached out to him.



Martin Hellman at Stanford (1973)

Whitfield Diffie, a very bored young man

In contrast to Hellman, Diffie was first introduced to cryptography early at the 10 year old, when his Father, a history professor, brought home cryptography books from a local library. He loved mathematics but hated school. **Diffie was described to have “performed competently” and how he “never did apply himself to the degree his Father hoped”.** Diffie barely graduated.

Despite his performance, he was smart enough to ace the entrance exams for MIT. Studying mathematics there, he remembers how he tried to teach himself how to program but thought of it as **“very low class work”**. Overall he was pretty bored and instead spent most of his time studying pure mathematics.

Skimming day jobs to work on AI & ’The Codebreakers’

Just when he graduated, the US government started to draft young men to fight in Vietnam. Machine guns and screaming Vietcong did not

particularly interest Diffie so instead, he took at job developing software and doing other "low class work". At the same time, he also started to work 'part time' at MIT's Project MAC's Artificial Intelligence Laboratory run by two pretty smart people: Marvin Minsky and **John McCarthy.**

Diffie had a very strong relationship with McCarthy and learnt a lot from him. Unknown to Diffie and many at that time, **McCarthy would go on later to be regarded as the father of artificial intelligence (coined the term: AI)**. Often quoted, McCarthy believed that "every aspect of learning or any other feature of intelligence can in principle be so precisely described that a machine can be made to simulate it.". He was incredibly focused on the future, believing that the conception of such intelligence will come in "five to 500 years". Under his guidance, Diffie was exposed to his computing philosophy and developed a deep understanding of networking, electronic keys and authentication. Diffie later followed McCarthy to Stanford to join his new AI Lab (SAIL: Stanford Artifical Intelligence Laboratory).

During his time at Stanford, Diffie read David Kahn's book: *'The Codebreakers: The Story of Secret Writing'.* It summarised the history of cryptography from ancient Egypt to the time of its writing and was described to have 'profoundly' influenced him in his beliefs surrounding privacy.

Compelled to pursue his own personal research of cryptography, he left SAIL in 1973, spending the next year jumping around the country to meet and discuss cryptography with different experts.

> *"I was doing one of the things I am good at, which is digging up rare manuscripts in libraries, driving around, visiting friends at universities."*

And in 1974, as part of his research, he visited the IBM Thomas J. Watson Laboratory at Yorktown Heights to meet with the cryptography research team. At that time it was led by **Horst Feistel,** the guy who introduced cryptography to Hellman.

When Diffie visited, he couldn't learn much as much of the work was classified by the NSA. Instead, he was referred to Martin Hellman, a professor at Stanford University who was working on similar cryptography.

IBM Thomas J. Watson Laboratory in Yorktown Heights

Hellman meets Diffie

> “In the fall of 1974 Whit shows up on my doorstop. I’ll never forget that day,”—Hellman (2011)

Through a referral, Hellman agreed to meet Diffie at his house in 1974.

Diffie came in the afternoon but stayed for dinner and left at 11 p.m. The short meeting expanded over hours of discussion. Hellman recounts how “Working in a vacuum had been taxing in a way, and finding a kindred spirit was really something,”. Soon after, Diffie took at job a local research group and like his first job, he would soon spend more time working with Hellman on cryptography than his actual job.

Early next year in 1975, they had something else to worry about: the DES.

Data Encryption Standard (DES)

In early 1975, the government published the DES. It was the first encryption cipher that was approved for public and commercial use. The NSA pushed for the adoption of the DES by financial services and other commercial sectors where strong encryption was needed (SIM cards, network devices, routers and modems).

Previous to the DES, the first amendment classified cryptography along with Munitions and other items that were military in character. You had to be licensed to handle any form of cryptography and all work related to it was classified by the NSA. This was the publicly approved use of such technology.

1970s Stock photos from the NSA!

How the DES was designed

The need for a national encryption cipher was realised after a study conducted in 1972 by the the National Bureau of Standards (now known as NIST, National Institute of Standards and Technology). Basically a shell of the NSA. They requested design proposals from research centres around the US in 1973 and 1974. After running up dry the first time, in 1974, IBM conceived a cipher called Lucifer.

Lucifer’s design was led by IBM’s very own **Horst Feistel.**

This cipher was an improvement on a previously developed cipher but fit the design request from the NSA. Lucifer underwent an extra stage of collaboration with the NSA where they wanted to reduce the key size from 64 bits to 48 bits (on a basic level, it means needing less processing power to encrypt and decrypt). Their final decision to reduce the key size to 56 bits would later come back to bite them.

Hellman and Diffie’s criticisms

Hellman and Diffie initially embraced the DES with open arms as they saw it as a huge step towards bringing cryptography into the public view. But as they looked closer, they foresaw how the shortened key length was vulnerable to brute force attacks.

But more importantly, amongst the researcher circles, the IBM team accused the NSA of tampering with the cipher. After the cipher was

sent to Washington for approval, it was returned with an altered S-box (the part of a cipher that turns plain text into cipher text).

During the 70s, there was a general sense of distrust about the government. This wariness stemmed from the period after WWII. Learning from the control of totalitarian governments (USSR, Nazi Germany), the public was vigilant against the intrusion by the government. The public’s fears were reflected in Orwell’s 1984 and other popular texts that explored government surveillance, control of society and personal freedom. This sentiment continued into the 60s where the decade was rocked by the assassination of JFK, the Cuban Missile Crisis and sociopolitical movements such as black rights and gay rights. In the 70s, this was exacerbated by the Watergate incident in 1972 which was a controversy surrounding President Nixon’s authorised bugging of the Democratic National Committee Headquarters in Washington DC. To the public, their fears were slowly but surely manifesting before their eyes.

People believed that the NSA had built a cipher which they could bypass themselves.

Merkle, the kid who knew nothing

Soon after the release of the DES, Hellman and Diffie released a technical paper called “Multi-User Cryptographic Techniques”, and they soon learnt of Ralph Merkle, a young 23 year old computer science student from Berkeley, (Hellman was 30 years old at the time and Diffie was only one year older).

Merkle’s Puzzles

Before meeting Hellman and Diffie, Merkle had already been working on his own early concept of public key encryption, which would be later known as Merkle’s puzzles. He started working on his ideas during his computer science course CS244 where he stumbled across the riddle: how do you reestablish secure communications when a hostile enemy already knows everything? He needed to complete a personal project for the course and this seemed perfect for him to develop his ideas.

> *When I thought about how can you possibly establish security when everything is known to the eavesdropper, and the eavesdropper can listen in on communications, how can you possibly establish security?*

> *So my first thought was: it doesn’t look like you can, so I’ll try and prove that it’s impossible. So I tried to prove that you couldn’t establish security, and I tried and I tried and I tried and I failed miserably.*

> *Then I thought about it some more and I said, “Well, if I can’t prove that you can’t do it I’ll turn around and try and figure out a method to do it.” And when I tried to come up with a method for doing it, having just tried to prove you can’t do it, I knew where the cracks in my proof were, so to speak, and I knew where I could try and slide through. So I worked on those places and lo and behold it turned out it was possible. I could use the cracks in my proof to come up with a method for actually doing it, and when I figured out how to do it there was this, well, the traditional “aha moment” where I said, “Oh, yeah, that works. I can do it.”*

> *That happened very rapidly. It was all one night of staying up late and thinking and then realizing “Oh, my gosh, I can do this thing. It seems very counterintuitive but I can actually figure out a key. I can establish a cryptographic key over an open communications line even if the enemy, the interloper, the eavesdropper knows everything”.*

With no theoretical or historical knowledge about cryptography, he was unaware of how the problem was considered to be unsolveable.

He put everything into a paper and shared it around. **The Head Teacher of the security course couldn’t understand his work and told Merkle to bugger off.** And when he submitted his work to the CACM, a well respected computer science journal, he was rejected. But this time, not because it was nonsense, but because the Editor thought the contents of his work was…

> *“…not in the main stream of present cryptography thinking….”*

Covers of 1970s CACM editions

However he had also shared it with a computer scientist called Peter Blatman, who immediately noticed the value of the his work. Unbeknown to Merkle, Blatman was friends with Diffie, who invited him out to a cryptography meetup in Stanford. During a car ride, Blatman briefly outlined the problem Merkle was working on.

Apparently, Diffie had been obsessing over the same problem for years and upon hearing about how some young computer science student had potentially solved the problem, he dismissed such a possibility, erupting into an outburst. **But once Diffie was calm again, he became excited about the possibility of such a solution.**

Hellman and Diffie had recently submitted a paper which explored the applications of public key encryption under the assumption that it was possible. Diffie gave Blatman a copy to give to Merkle.

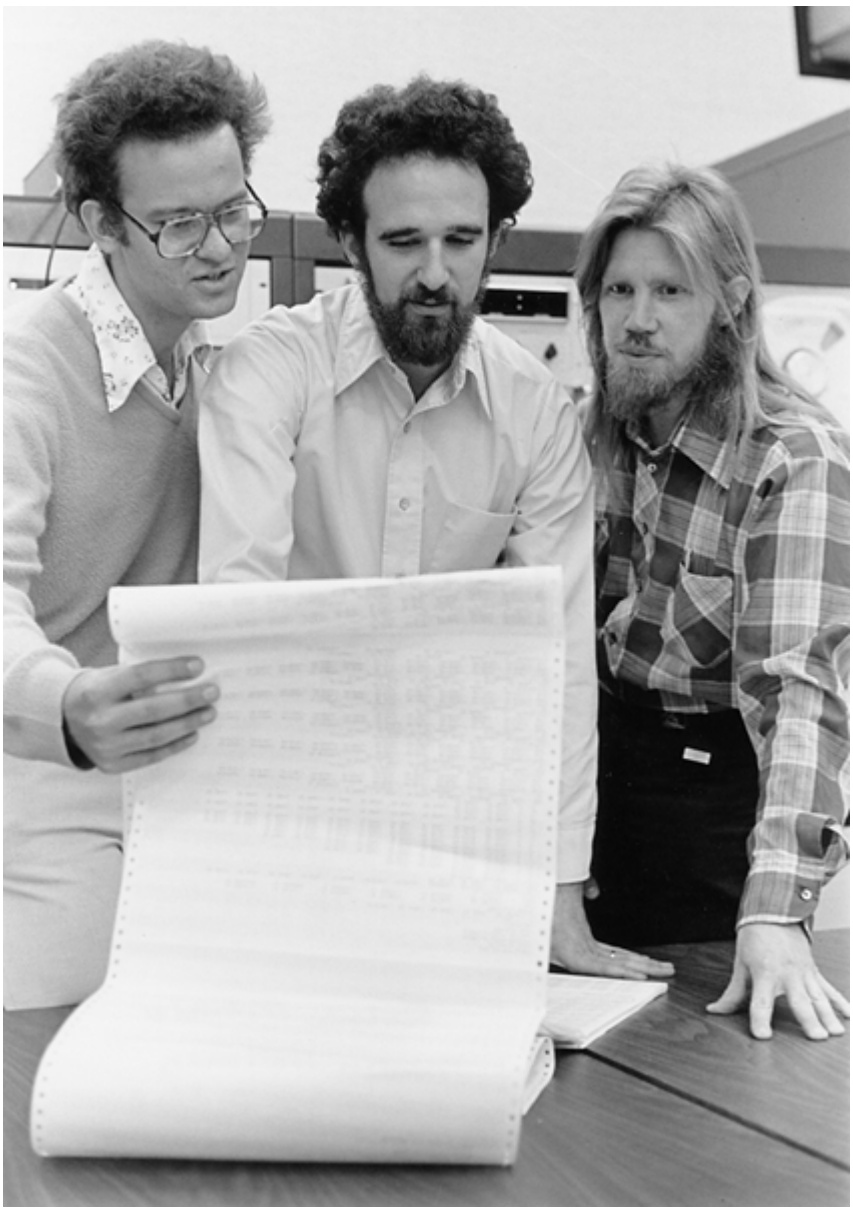
> *"There are these guys at Stanford who talk just like you."*

After reading their work, Merkle sent over his paper. When the other two had read it, they had completely shifted their way of thinking. Despite Merkle's youth and complete lack of cryptographic knowledge, his creativity had solved the public key distribution problem. **This**

young 23 year old managed to achieve what academics had strived to do for years.

But Hellman and Diffie found his solution inefficient. With their cryptographic understanding, they had found a far more compact solution to the key distribution problem and came up with a new iteration of public key cryptography. Soon their concepts would be formulated into a paper that would be known as: ‘New Directions in Cryptography’.

Following their collaboration, Merkle left for Stanford, taking up Hellman’s invitation to work under him as a PhD student.



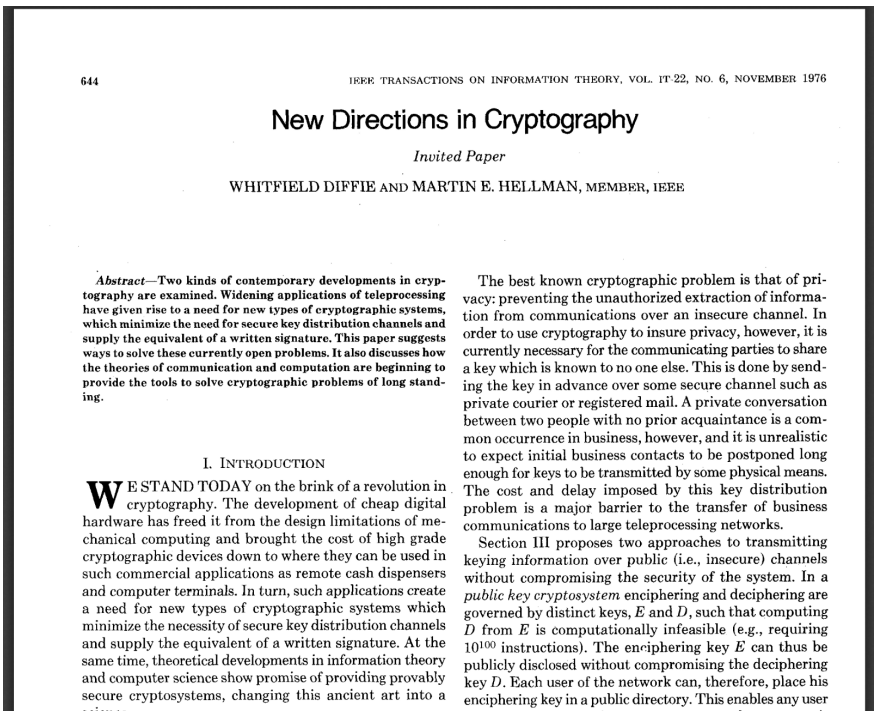
Merkle on the left, Hellman in the middle, Diffie on the right (1977)

New Directions in Cryptography

In November 1976, the paper: ‘New Directions in Cryptography’ was released. It discussed fundamental problems of cryptography, public key cryptography and protocols that facilitated authenticated communication.

Merkle was credited for his independent work but in the end the communication protocol was named: the Diffie-Hellman key exchange. However despite this, in 1977 when public key encryption was patented, Merkle was credited as one of the three inventors. Diffie reflected on Merkle as “possibly the most inventive character in the public-key saga,.

> The system has since become known as Diffie–Hellman key exchange. While that system was first described in a paper by Diffie and me, it is a public key distribution system, a concept developed by Merkle, and hence should be called ‘Diffie–Hellman–Merkle key exchange’ if names are to be associated with it. I hope this small pulpit might help in that endeavour to recognise Merkle’s equal contribution to the invention of public key cryptography.
> *- Martin Hellman (2002)*



644 IEEE TRANSACTIONS ON INFORMATION THEORY, VOL. IT-22, NO. 6, NOVEMBER 1976

New Directions in Cryptography

Invited Paper

WHITFIELD DIFFIE AND MARTIN E. HELLMAN, MEMBER, IEEE

Abstract—**Two kinds of contemporary developments in cryptography are examined. Widening applications of teleprocessing have given rise to a need for new types of cryptographic systems, which minimize the need for secure key distribution channels and supply the equivalent of a written signature. This paper suggests ways to solve these currently open problems. It also discusses how the theories of communication and computation are beginning to provide the tools to solve cryptographic problems of long standing.**

I. INTRODUCTION

WE STAND TODAY on the brink of a revolution in cryptography. The development of cheap digital hardware has freed it from the design limitations of mechanical computing and brought the cost of high grade cryptographic devices down to where they can be used in such commercial applications as remote cash dispensers and computer terminals. In turn, such applications create a need for new types of cryptographic systems which minimize the necessity of secure key distribution channels and supply the equivalent of a written signature. At the same time, theoretical developments in information theory and computer science show promise of providing provably secure cryptosystems, changing this ancient art into a

The best known cryptographic problem is that of privacy: preventing the unauthorized extraction of information from communications over an insecure channel. In order to use cryptography to insure privacy, however, it is currently necessary for the communicating parties to share a key which is known to no one else. This is done by sending the key in advance over some secure channel such as private courier or registered mail. A private conversation between two people with no prior acquaintance is a common occurrence in business, however, and it is unrealistic to expect initial business contacts to be postponed long enough for keys to be transmitted by some physical means. The cost and delay imposed by this key distribution problem is a major barrier to the transfer of business communications to large teleprocessing networks.

Section III proposes two approaches to transmitting keying information over public (i.e., insecure) channels without compromising the security of the system. In a *public key cryptosystem* enciphering and deciphering are governed by distinct keys, E and D, such that computing D from E is computationally infeasible (e.g., requiring 10^{100} instructions). The enciphering key E can thus be publicly disclosed without compromising the deciphering key D. Each user of the network can, therefore, place his enciphering key in a public directory. This enables any user

The concepts discussed in the paper are used to design and secure blockchains we use today. One of their purposes of the paper, noted at the end, was to:

> Inspire others to work in this fascinating area in which participation has been discouraged in the recent past by a nearly total government monopoly—New Directions in Cryptography

For the first time, the public had access to powerful encryption technology. Their work broke the control on cryptographic knowledge. Fuelled by the growing distrust of the government's DES cipher, the technology in the paper enabled the first big wave of public interest in cryptography and encryption.

It was later revealed that Hellman, Diffie and Merkle were not the first conceivers of public key cryptography. A form of it was initially created and applied to an algorithm by researchers from Great Britain's intelligence agency (GCHQ). And while the NSA had access to this, it was all classified and remained in the dark untouched.

Now, imagine if these three never published public key encryption. Our world potentially might be very different.

Hellman, Diffie and Merkle's publication managed to incite a new wave of innovation that would last for decades whereas governmental agencies kept their findings behind closed doors. This contrast very much highlights the importance of open collaborative work within cryptography and but also other sciences.

Fittingly, in the first line of the paper, it had begun with:
"We stand today on the brink of a revolution in cryptography"

While Hellman and Diffie continued working on cryptography, Merkle was the one that continued to excel. Spending the rest of the 70s as a student of Hellman and Diffie, Merkle continued to impact cryptography in the 80s; ***later going on to invent cryptographic hashing.***

. . .

Closing statement

These three cryptographers would break down the barrier for cryptography. A cryptography in the 80s, known as David Chaum, would go on to directly build upon their work and conceptualise the need for anonymous communications, payments and ultimately the need for decentralised services. Chaum's work however would only be made possible through the dedication of Hellman, Diffie and Merkel.

Continue to Part Two: https://medium.com/@pet3rpan/history-of-things-before-bitcoin-cryptocurrency-part-two-94c4576005

Some trends that I found really cool:

- A late start: Hellman knew little about cryptography until much later after his PhD / academic education but through his influences, managed to form a sophisticated understanding of the field. Merkle was a studen.
- Exposure to greatness: Hellman and Diffie were mentored by some of the most smartest people in computer science history (Feistel who designed the DES, Elias who worked with Claude Shannon and McCarthy who invented artificial intelligence).
- Merkle had absolutely little knowledge of cryptography but managed to solve the unsolvable riddle.

. . .

Credit to the people who helped make this legible: DK, Terrado Technologies, Mr Luke Schoen, Radek, Mark “UX” Pereira

Continue to Part Two: https://medium.com/@pet3rpan/history-of-things-before-bitcoin-cryptocurrency-part-two-94c4576005

I would appreciate it if you shared any thoughts or feedback that you had while reading through this. Thank you.