Libertaria in Cyberspace: Vom Cyberpunk zum Cypherpunk

> It's the FBIs, NSAs, and Equifaxes of the world versus a swelling movement of Cypherpunks, civil libertarians, and millionaire hackers. At stake: Whether privacy will exist in the 21st century.[418]
> *(Steven Levy, Crypto Rebels, 1993)*

> ›The Net is an anarchy.‹ This truism is the core of crypto anarchy—no central control, no ruler, no leader (except by example or reputation), no ›laws‹. No single nation controls the Net, no administrative body sets policy.[419]
> *(Timothy May, Crypto Anarchy and Virtual Communities, 1994)*

> I'm with the Cypherpunks. We're the people that use cryptography or cryptotechnology to protect and preserve our privacy. The Cypherpunks are the elitist of the elite.[420]
> *(Captain Crunch im Interview mit Wes Thomas, Mondo 2000, 1993)*

Für die erste Ausgabe der *Boing Boing* (1988) steuerte der sich selbst als »libertarian Cyberpunk«[421] charakterisierende Chuck Hammill den Aufsatz *From Crossbows to Cryptography* bei, den er 1987 zuerst (in teilweise abgeänderter Form) als Vortrag an der libertären *Future of Freedom Conference*[422] hielt und der in libertären Cryptowährungs-Kreisen bis heute Verbreitung findet. Zu Beginn enthält der Text die bekannten Versprechen der technikoptimistischen Positionen. Beispielsweise wird der *Personal Computer* als *Equalizer* beworben. Wie schon bei David Bunnell ist Hammills Vergleich hierzu der Revolver der Frontier, der dem Volk eine Waffe in die Hand gab, ganz so wie der Computer die Bevölkerung ermächtigt:[423] »Not for nothing was the wild west's .45 revolver called the ›equalizer‹. It enabled the most petite dance-hall girl to defend herself against the burliest roughneck cowboy. […] The personal computer is today's equalizer in terms of information and idea processing, not brute force.«[424] Diese Kraft des Computers beleuchtet Hammill daraufhin mittels verschiedener weiterer historischer und kultureller Bezüge. Im Gegensatz zu den dystopischen Beispielen, wie Orwells *1984* oder Terry Gilliams *Brazil,* sei es beispielsweise falsch, den Computer nur als staatliches Unterdrückungsinstrument zu betrachten. Ganz im Gegenteil hiervon biete dieser, wie andere neue Technologien, ein potenzielles Gegenmittel gegenüber staatlicher Tyrannei. Der zentrale Mechanismus hierzu findet sich in der Verschlüsselungstechnologie. Auch dies führt Hammill

418 Levy, Steven: Crypto Rebels, in: Wired, 02.01.1993. Online: <https://www.wired.com/1993/02/crypto-rebels/>, Stand: 16.07.2021.

419 May, Timothy: Crypto Anarchy and Virtual Communities, in: Ludlow, Peter (Hg.): Crypto Anarchy, Cyberstates, and Pirate Utopias, Cambridge 2001, S. 69.

420 Wes, Thomas: Captain Crunch, Whistle Blower, in: Mondo 2000 (10), 1993, S. 40.

421 Hammill, Chuck: From Crossbows to Cryptography: Techno-Thwarting the State, in: Boing Boing 1 (1), 1988, S. 15.

422 Eine libertäre, sich jährlich wiederholende Konferenz, zu deren ersten SprecherInnen 1969 Ludwig von Mises gehörte.

423 Vgl. Bunnell, David: The Roots of Personal Computing, in: Mondo 2000 (1), 1989, S. 46–47.

424 Hammill: From Crossbows to Cryptography, 1988, S. 15.

mittels eines historischen Beispiels einer Waffe ein, die (angeblich) neue Freiheit mit sich brachte: Die Armbrust gab selbst einem ungeübten Bauern eine »personal Weapon«[425] in die Hände, mit der er bei Bedrohung einen sozial höhergestellten Ritter töten konnte. Analoges geschehe heute mit der Einführung von Verschlüsselungstechnologien. Diese schützten wie persönliche Waffen vor ungerechten Eingriffen auf die individuelle Freiheit. Bereits gegenwärtig brauche der Staat ein Jahr, um gut verschlüsselte Systeme zu knacken. In naher Zukunft werde der Staat bald gar keine Möglichkeit mehr zum unfreiwilligen Informationszugriff haben, so Hammills Prophezeiung. Und dies zöge weitreichende soziale Konsequenzen mit sich: Weil die Verschlüsselungsangebote das Informationsmonopol brechen, werde die Computerisierung »enhance the freedom of every man, woman and child on the planet«[426]. Dass in solchen Artikeln auch die amerikanische Liebe zum Waffengebrauch herausticht, zeigt ein Leser des *Wired*, der 1994 in einem wutentbrannten Leserbrief gegen den *Clipper Chip* den Vergleich zu persönlichen Waffen einbringt, indem er erläutert, dass »secure encryption, like firearms, represents an insurance policy for all citizens against future tyrants«[427]. Warum es nicht ganz Zufall ist, dass es zwischen den BefürworterInnen eines umfassenden Rechts auf Waffenbesitz und von Verschlüsselungstechnologien zu Überschneidungen kam, zeigt sich in den folgenden Ausführungen.

PGP

Die von Hammill beschriebene Verschlüsselungstechnologie hat ihren Ursprung in dem 1975 von Whitfield Diffie, dem »Prophet of Privacy«, dessen »politics are strongly libertarian«[428], so Steven Levys Porträt im *Wired*, und Martin Hellman theoretisch entwickelten Verschlüsselungsmechanismus, der das System von privaten und öffentlichen Schlüsseln einführte.[429] Ersteren behält man für die Verschlüsselung für sich, während Letzterer dem Kommunikationspartner gesendet wird. Dies ermöglicht das Verschlüsseln beziehungsweise Signieren einer Botschaft, ohne dass es zuvor einen sicheren Austausch der gleichen privaten Schlüssel braucht. Vereinfacht gesagt erleichtert dies die digitale Verschlüsselung, indem die sichere Kommunikation ermöglicht wird, selbst wenn dabei unsichere Verbindungen wie öffentliche Computernetzwerke verwendet werden, und indem der dezentralisierte Aufbau es ermöglicht, Schlüssel über Drittpersonen zu verifizieren und man so mit Menschen sicher kommunizieren kann, die man nie getroffen hat – in der *Mondo 2000* nahm man dies als Dehierarchisierung wahr, da die klassische

425 Ebd., S. 13.

426 Ebd., S. 15.

427 Rants & Raves, in: Wired, 09.01.1994. Online: <https://www.wired.com/1994/09/rants-raves-64/>, Stand: 01.07.2021. Vgl. den Hinweis auf das Zitat von Lockard: The Myth of Virtual Community, 1997, S. 223.

428 Levy, Steven: Prophet of Privacy, in: Wired, 01.09.1994. Online: <https://www.wired.com/1994/11/diffie/>, Stand: 05.04.2022.

429 Ein kurzer Überblick über die Entwicklung der Verschlüsselungstechnologie findet sich bei Hellegren, Z. Isadora: A History of Crypto-Discourse: Encryption as a Site of Struggles to Define Internet Freedom, in: Internet Histories 1 (4), 02.09.2017, S. 291ff.

Kryptografie auf einem hierarchischen Pyramidensystem beruhte, bei dem jede höhere Stelle diejenige unter sich zu verifizieren hatte.[430] Mit der im Juni 1991 veröffentlichten Verschlüsselungssoftware PGP (›*Pretty Good Privacy*‹) von Phil Zimmermann wurde die neue Verschlüsselungsmethode schließlich auch als zugängliche Massenanwendung angeboten.

Der amerikanische Computerwissenschaftler und Anti-Atomwaffen-Aktivist Zimmermann sah in seinem Programm ein Angebot, das, wie auch von Hammill beschrieben, einen Schutzmechanismus in die Hände der NutzerInnen geben sollte.[431] Dass sich dies bezüglich der digitalen Kommunikation zu einem gewissen Grad tatsächlich bewahrheiten sollte – zumindest ist PGP bis heute die gängige Verschlüsselungssoftware für AktivistInnen wie auch für Firmen – hat viel mit der nicht ganz freiwilligen Dekommodifizierung des Programmes zu tun. Zimmermann dachte zuerst daran, seine Software für eine Gebühr anzubieten, entschied sich dann aber aus Furcht vor Repression dafür, sie gratis ins Netz zu stellen beziehungsweise später auch den Quellcode zu veröffentlichen. »[L]ike thousands of dandelion seeds blowing in the wind«[432], so Zimmermanns poetischer Vergleich, verbreitete sich das Programm danach im Cyberspace. Damit ließ sich Zimmerman weder zum Ursprung der Verbreitung machen, noch konnte er wegen Exportbestimmungen angeklagt werden – dennoch kam es 1993 zu einer letztlich folgenlosen Untersuchung gegen Zimmermann wegen angeblicher Verstöße gegen das Waffenexportgesetz, unter das die starke Verschlüsselung fiel.

Zimmermanns Versprechen, die Privatsphäre durch Verschlüsselungssoftware zu schützen, fand auch innerhalb der Cyberkultur regen Anklang. Die Cyberpunk-Magazine, wie *Mondo 2000,* druckten Zimmermanns Texte ab oder bezogen sich positiv darauf. Norman French beispielsweise charakterisierte die erste Version von PGP ganz im Sinne des *Hands-on Imperative* der HackerInnenethik als ein »very American, home-grown act of guerilla techno-monkeywrenching«[433]. Levy selbst bestätigte diesen *Very-American*-Style in der *New York Times,* indem er Zimmermanns PGP mit einem weltweiten Freiheitskampf in Verbindung brachte. So habe Zimmermann beispielsweise erfahren, dass die »Burmese freedom fighters learn PGP in jungle training camps on portable computers, using it to keep documents hidden from their oppressive Government«[434], und eine Person aus Lettland habe ihm in einem Brief mitgeteilt, dass »his program was a favorite among one-time refuseniks in that former Soviet republic«[435]. Auch in der *Mondo 2000* betonte man den Freiheitskampf durch Verschlüsselung. Dundee Friedman beispielsweise warnte im Orwell'schen Diskurs vor den Gefahren der »thought police«[436], die sich nicht mehr dafür interessierte, ob man selbst tatsächlich Verbrechen begehe oder nicht, die sich allerdings durch die Verwendung von PGP überlisten lasse. Auch abseits

430 Vgl. French, Norman: Son of PGP, in: Mondo 2000 (9), 1993, S. 13–15.

431 . So antwortet Zimmermann beispielsweise in seinem ersten *GP User's Guide* auf die gestellte Frage, warum es PGP brauche, mit folgender Ansage: »PGP empowers people to take their privacy into their own hands.« (Zimmermann, Philip: Why do you need PGP?, in: Mondo 2000 (9), 1993, S. 15.)

432 Levy: Crypto Rebels, 1993.

433 French: Son of PGP, 1993, S. 13.

434 Zitiert nach Levy: Battle of the Clipper Chip, 1994.

435 Ebd.

436 Friedman, Dundee: Use a random number, go to jail, in: Mondo 2000 (10), 1993, S. 43.

der Cyberpunk-Magazine stieß die Verschlüsselungssoftware auf Interesse. William Gibson veröffentlichte beispielsweise 1992 in Zusammenarbeit mit dem Künstler Dennis Ashbaugh und dem Verleger Kevin Begos Jr. das experimentelle Buchprojekt *Agrippa (A Book of the Dead)*. Das Projekt enthielt ein Buch aus lichtempfindlichen Chemikalien, die dafür sorgten, dass die Wörter bei Lichteinwirkung zu verblassen begannen, und eine Floppy-Disk mit einem Gedicht von Gibson, das nach der ersten Verwendung für immer verschlüsselt werden sollte.[437] Anders als bei den VerschlüsselungsapologetInnen ging es bei Gibsons *Agrippa* thematisch nicht primär um die Stärkung der Privatsphäre – das Gedicht fand sich innerhalb kurzer Zeit als ›illegal‹ angefertigte Kopie auf verschiedenen BBS –, das Projekt sorgte dennoch dafür, dass das Interesse an Verschlüsselungssoftware wuchs – dass der Verschlüsselungscode erst gut zwanzig Jahre später geknackt wurde, sorgte zusätzlich für eine Art Aura, die die *Agrippa* umgab.

Cypherpunks

Unter dem Begriff ›Cypherpunks‹ entstand zu Beginn der 90er-Jahre eine eigene Bewegung, die die Kryptografie als zentrale Praxis propagierte und die sich, so Timothy May im *CYPHERNOMICON*, einem der wichtigen Dokumente der Bewegung, selbst als politisch und zugleich antidemokratisch verstand: »Many of us are explicity anti-democratic, and hope to use encryption to undermine the so-called democratic governments of the world.«[438] Was mit diesem antidemokratischen Bekenntnis letztlich genau gemeint war, bleibt bis heute umstritten. So verstand man darunter in manchen Fällen einen antiautoritären Kampf gegen jene Regierungen, die sich selbst als Demokratien bezeichneten, es aber im Verständnis der Cypherpunks nicht waren. Andere nahmen den antidemokratischen Aufruf wörtlicher, beispielsweise im Negieren kollektiver gesellschaftlicher Verantwortung oder im Widerstand gegen jegliche Form der Regulierung des Cyberspace, selbst wenn er demokratisch institutionalisiert und legitimiert war. Ein anderes Beispiel der antidemokratischen Haltung findet sich bei Chuck Hammill, der in der Vortragsversion von *Crossbows To Cryptography* (1987) in einer libertären Milchbüchleinrechnung die Defizite der Demokratie anhand der Sozialhilfe aufzuzeigen versuchte: »When those who sup at the public trough outnumber (and thus outvote) those whose taxes must replenish the trough, then what possible choice has a democracy but to perpetuate and expand the taking from the few for the unearned benefit of the many.«[439] Deshalb brauchen »those who love liberty«, so Hammills Argument, »an ›edge‹ of some sort«, wollten sie ihre individualistisch gedachten Freiheiten – und bezogen auf die Sozialhilfe und Steuern auch die »fruits of your life's labor« – nicht verlieren, und dafür ga-

437 Erst dachte man auch daran, einen Virus zu programmieren, der das Gedicht für immer löschen sollte, man kam allerdings aus verschiedenen rechtlichen wie auch aus politischen Gründen davon ab, unter anderem weil man die öffentliche Angst vor Viren nicht durch unvorhersehbare Konsequenzen des eigenen Programmes befeuern wollte.

438 May, Timothy: THE CYPHERNOMICON: Cypherpunks FAQ and More, 1994. Online: <https://nakamotoinstitute.org/static/docs/cyphernomicon.txt>, Stand: 21.06.2021.

439 Hammill, Chuck: From Crossbows to Cryptography: Techno-Thwarting The State | Satoshi Nakamoto Institute, Future of Freedom Conference, 11.1987. Online: <https://nakamotoinstitute.org/from-crossbows-to-cryptography/>, Stand: 05.05.2022.

rantierten zukünftig die Verschlüsselungstechnologien. Dass es ein Spektrum zwischen solchen tatsächlich antidemokratischen – und im Bild von SozialhilfeempfängerInnen, die sich vermehren und am Trog des Staates hängen, oft auch rassitisch untermauerten – und weitaus gemäßigteren Positionen gab, liegt auch daran, dass die Bewegung der Cypherpunks nicht homogen war und sie sich eher als informelle Gruppe beschreiben lässt, die sich um eine Mailinglist von Eric Hughes, Timothy C. May und John Gilmore scharte, wobei der Begriff ›Cypherpunk‹ wohl auf Jude Milhon zurückgeht, die zu Beginn auch an einigen Treffen teilnahm.[440]

Die Mailingliste erreichte bis 1994 gut 500 Mitglieder, darunter auch einige bekanntere Personen wie Julian Assange, Hal Finney oder Nick Szabo. Später wuchs die Liste auf maximal einige Tausend LeserInnen, bis sie zu Beginn der 2000er-Jahre nach internen Streitigkeiten abgeschaltet wurde[441] – zu Differenzen kam es allerdings schon zuvor, beispielsweise als John Gilmore 1997 ankündigte, dass er nach Diskussionen um Zensur (so die eine Seite) beziehungsweise um Moderationskriterien gegenüber Spam und inhaltslosen Botschaften (so die andere Seite) die Mailingliste nicht weiter selbst hosten wolle, was zu einem teilweisen Umzug auf Usenet beziehungsweise zu neuen Mailinglisten[442] und zu weiteren Polemiken gegenüber Gilmore und dem »Millionaire's club«[443] EFF führte. Zu den ›offiziellen‹ Cypherpunks hinzu kamen einige weitere, damit vergleichbare Initiativen. Kevin Kelly beispielsweise berichtet in *Out of Control*, dass es im Internet zahlreiche weitere Zusammenschlüsse gab, beispielsweise die Information Liberation Front, die wissenschaftliche Artikel zur Kryptografie scannte und verbreitete, die zuvor nur in teuren Zeitschriften zu finden waren.[444] Doch meist waren solche Gruppen mehr Mythos denn Realität. Die Cypherpunk-Bewegung war zwar diskursprägend, personell erschien sie in der öffentlichen Wahrnehmung aber weit größer, als sie es tatsächlich war. Dieses Ungleichgewicht hängt vor allem mit der großen medialen Aufmerksamkeit für die Bewegung und ihre ProtagonistInnen zusammen, was sich erneut auch auf Steven Levy zurückführen lässt. Der *Hackers*-Autor veröffentlichte in den 90er-Jahren in großen Publikationen, wie der *New York Times* oder dem *Wired*, mehrere Reportagen über die »techie-cum-civil libertarians«[445] – darunter die Titelstory der zweiten Ausgabe des *Wired* mit Timothy C. May, Eric Hughes und John Gilmore, maskiert mit der amerikanischen Flagge in der Hand auf dem Titelbild.[446] 2001 kam dann noch das bereits im Titel das

440 Vgl. Sirius, R. U.: Cypherpunk Rising: WikiLeaks, Encryption, and the Coming Surveillance Dystopia, in: The Verge, 07.03.2013. Online: <https://www.theverge.com/2013/3/7/4036040/cypherpunks-julian-assange-wikileaks-encryption-surveillance-dystopia>, Stand: 15.07.2021; May, Timothy: True Nyms and Crypto Anarchy, 1996, S. 28. Online: <https://www.gwern.net/docs/bitcoin/1996-may.pdf>, Stand: 16.07.2021.

441 Vgl. Hellegren: A History of Crypto-Discourse, 2017, S. 296.

442 Vgl. Frauenfelder, Mark: Homeless Cypherpunks Turn to Usenet, in: Wired, 17.02.1997. Online: <https://www.wired.com/1997/02/homeless-cypherpunks-turn-to-usenet/>, Stand: 03.11.2021.

443 Schultz, Pit; Garrin, Paul: Pit Schultz with Paul Garrin on Name.Space., <www.ljudmila.org/nettime/zkp4/19.htm>, Stand: 03.11.2021.

444 Vgl. Kelly, Kevin: Out of Control. The New Biology of Machines, Social Systems and the Economic World, 2008, S. 179. Online: <https://kk.org/kevinkelly/out-of-control-the-illustrated/>, Stand: 12.10.2024.

445 Levy: Crypto Rebels, 1993.

446 Vgl. Hellegren: A History of Crypto-Discourse, 2017.

Wohlwollen Levys anzeigende Buch *Crypto: How the Code Rebels Beat the Government Saving Privacy in the Digital Age* hinzu.

Für Levy selbst waren die Cypherpunks auch eine vor allem informell existierende Gruppe. Zwar traf man sich mitunter auch im engeren Kreis, doch hauptsächlich tauschte sich die »loose confederation of computer hackers, hardware engineers and high-tech rabble-rousers«[447] über die Mailingliste aus. Diesem informellen Netzwerk schreibt Levy aber eine große gesellschaftliche Bedeutung zu. Der Kampf um Verschlüsselungstechnologien erscheint beispielsweise als zentraler gesellschaftlicher Konflikt, dessen Ergebnis »may determine the amount of freedom our society will grant us in the 21st Century.«[448] Dieses Emporheben der eigenen Bedeutung zeigt sich auch in den von den Cypherpunks selbst publizierten Texten. In dem von Timothy May bereits 1988 verfassten, aber vor allem mit dem mit der Mailingliste der Cypherpunks Verbreitung findenden *Crypto Anarchist Manifesto* erscheinen die Cypherpunks in Anspielung auf das kommunistische Manifest als revolutionäres Subjekt des Computerzeitalters: »A specter is haunting the modern world, the specter of crypto anarchy«[449], so beginnt der Text, der mit einem Aufruf in Form einer zweiten Referenz auf Marx und Engels abschließt: »Arise, you have nothing to lose but your barbed wire fences!«[450] Dieses rhetorische Spiel mit den Sätzen des wohl bekanntesten Manifests der Menschheitsgeschichte täuscht über seine Botschaft hinweg. Nichts lag den Cypherpunks wie May ferner als die politischen Konzepte und Analysen von Marx und Engels. May, der als ehemaliger Intel-Mitarbeiter dank Firmenbeteiligung mit 35 in den Ruhestand ging, pochte darauf, in Porträts als ›Libertärer‹ charakterisiert zu werden.[451] Und, wie insbesondere in Mays Manifest deutlich wird, positionierten sich die Cypherpunks auch inhaltlich radikaler als die Cyberpunks oder die EFF als libertäre Kraft.[452]

Die Verschlüsselungstechnologie verändere die sozialen Zusammenhänge und schaffe einen andersartigen digitalen Raum, so die zentrale These in Mays Manifest. Zwar war der verbesserte Schutz der Privatsphäre prinzipiell schon seit einiger Zeit möglich, die massenhafte Anwendung und schnelleren Internetverbindungen erlaubten nun einen qualitativen Sprung, der die ›krypto-anarchistische‹ Vision Wirklichkeit werden ließ. Das Themenfeld, das May daran am meisten interessierte, war der Handel als Vorbild und Grundlage sozialer Interaktionen. Die Verschlüsselung werde beispielsweise die unterschiedliche »interference in economic transactions«[453] künftig mehr und mehr unterbinden. Damit zielt May zwar nicht nur auf den Staat, sondern auch

447 Levy: Battle of the Clipper Chip, 1994.

448 Levy: Crypto Rebels, 1993.

449 May, Timothy: A Crypto Anarchist Manifesto, in: Ludlow, Peter (Hg.): High Noon on the Electronic Frontier: Conceptual Issues in Cyberspace, Cambridge 1996, S. 237.

450 Ebd., S. 239.

451 Vgl. Levy: Crypto Rebels, 1993.

452 Eine gegenteilige These vertritt Enrico Beltramini, der den Libertarismus der Cypherpunks als offeneren Begriff las, weil sich darunter verschiedene Strömungen wiederfanden und sich in den Schriften auch Bezüge zu unterschiedlichen TheoretikerInnen finden, etwa zu Foucault. Vgl. Beltramini, Enrico: Against technocratic authoritarianism. A short intellectual history of the cypherpunk movement, in: Internet Histories 5 (2), 03.04.2021, S. 101–118.

453 May: A Crypto Anarchist Manifesto, 1996, S. 238.

auf Unternehmen, doch die daraus abgeleitete Vision besteht aus einem libertären Cyberspace, in dem jeder selbst als UnternehmerIn und HandelspartnerIn agieren kann, ohne mit irgendwelchen Einschränkungen konfrontiert zu werden: »Combined with emerging information markets, crypto anarchy will create a liquid market for any and all material which can be put into words and pictures.«[454] Diese ›Anarchie‹ definiert May an anderer Stelle in expliziter Abgrenzung zu Proudhon, dem Anarchosyndikalismus, den ›BombenlegerInnen‹ und der ArbeiterInnenbewegung des 19. Jahrhunderts als »absence of government«[455], die einer Definition der »anarchy used in anarchocapitalism, the libertarian free-market ideology«[456] entspreche. Als theoretische Vorbilder hierfür erschienen beispielsweise Ayn Rand, so May in seinem 1994 veröffentlichten *Cypherpunk FAQ*, als »one of the prime motivators of crypto anarchy«[457], oder auch Hayek und David D. Friedman, Milton Friedmans libertärer Sohn.

Die einzige damalige ›linke‹ (und sich heute ebenfalls als problematisch herausstellende)[458] Kraft, der May eine legitime anarchistische Position zusprach, war Hakim Bey (Peter Lamborn Wilson). Der schon von den Cyberpunks bewunderte amerikanische Anarchist bezog sich in seiner meistrezipierten Schrift *Temporary Autonomous Zone* (TAZ) positiv auf neue (Telekommunikations-)Technologien. Diesen schrieb er zwar ein repressives Potenzial zu, doch zugleich erschienen sie als potenzielle Basis für eine »entire world of autonomous zones«[459]. So sei das offizielle ›Net‹ durch Hierarchien geprägt, aber dieses werde nie fähig sein, das ›Counter-Net‹ beziehungsweise das ›Web‹, so Beys Gegenbegriff zum Netz, zu zerstören. Im Web fließen die Informationen frei, beispielsweise in Form von ›Datenpiraterie‹ oder des unzensurierten Austausches in den BBS, was zur Entstehung von temporären[460] Freiräumen beitragen würde – was wiederum auch von der Cyberkultur aufgenommen und umgesetzt wurde: Die beiden Berkeley-Doktoranden Ian Goldberg und David Wagner schlugen beispielsweise 1998 als Teil ihrer Forschung für die ISAAC Research Group (›*Internet Security, Applications, Authentication and Cryptography*‹) an der University of California einen ›*TAZ Server*‹ vor, der, mit Namensbezug auf Bey, Teil einer »anonymous WWW publishing infrastructure«[461] werden sollte. Beys positive Vision des Web stand unter dem Einfluss der Cyberpunk-Romane. Bey beschrieb sich selbst als Cyberpunk-Fan, bezog sich unter anderem auf Sterlings *Island in*

454 Ebd.

455 May: Crypto Anarchy and Virtual Communities, 2001, S. 69.

456 Ebd.

457 May: THE CYPHERNOMICON: Cypherpunks FAQ and More, 1994.

458 Zur Problematik bezüglich Bey vgl. z.B. Helms, Robert: Paedophilia and American anarchism – the other side of Hakim Bey, libcom.org, 10.11.2006, <http://libcom.org/library/paedophilia-and-american-anarchism-the-other-side-of-hakim-bey>, Stand: 22.06.2021.

459 Bey, Hakim: The Temporary Autonomous Zone, in: Ludlow, Peter (Hg.): Crypto Anarchy, Cyberstates, and Pirate Utopias, Cambridge 2001, S. 402.

460 Beys Verweis auf den temporären Charakter spielt zum einen mit der fragmentierten Netz-Zeit, unterwirft sich dieser allerdings unfreiwillig, indem der Bruch über die Kontinuität gestellt wird und der temporäre Charakter zur Legitimation werden kann, den potenziellen Freiraum je nach Lust und Laune aufzugeben – ganz so wie man sich auch im Internet ein- und ausloggt.

461 Goldberg, Ian; Wagner, David: TAZ servers and the rewebber network: Enabling anonymous publishing on the world wide web, in: First Monday, 06.04.1998. Online: <https://doi.org/10.5210/fm.v3i4.586>, Stand: 26.04.2022.

the Net oder Gibsons *Neuromancer* und verstand ›*Reality Hacking*‹ als wichtige Funktion in der Erschaffung einer digitalen TAZ.[462] In späteren Interviews warnte Bey allerdings zugleich in marxistischer Terminologie vor einer falschen Verdinglichung, die Technologie fälschlicherweise als »autonomous thing«[463] erscheinen ließe, und vor falschen Transzendierungswünschen, bei denen der köperlose Übergang des Bewusstseins in den Cyberspace kurz bevorstehe, als auch davor, dass das Netz nicht als von der Realität isolierte Insel funktioniere: »[T]here's no such thing as a T.A.Z. that's only on the Net«[464]. So bezog sich Bay in seinen Visionen der TAZ stets auf kollektive politische Praktiken, wie beispielsweise Hausbesetzungen. Konträr dazu verstanden sich die Cypherpunks zwar als politische Kraft, die durch ihre Praxis intervenierte, doch implizit enthielten ihre libertären Cyberspaceimaginationen zugleich einmal mehr eine Abkehr von politischen Aushandlungsprozessen. Die regulierende Kraft, die künftig entscheiden sollte, was in der virtuellen Welt als Inhalt und Verhaltensnorm angemessen erscheint und was nicht, die aber auch umfassende gesellschaftliche Beziehungen prägen sollte, war einmal mehr der freie Markt, und dies letztlich nicht nur im Cyberspace selbst: In Kombination mit »strong cypto« und »cheap telecoms« sollten »free markets« die »organizing basis for a workable society«[465] bilden, so Duncan Frissell, ein amerikanischer Anwalt und Cypherpunk, in einer von Timothy May wiedergegebenen Weisheit.

Etwas weniger deutlich, aber doch vorhanden sind die libertäre Positionierung und die Betonung des freien Handels als Vorbild für alle Interaktionsformen im zweiten bekannten Manifest der Cypherpunks, Eric Hughes' 1993 online veröffentlichtes *Cypherpunk's Manifesto*. Der Text des amerikanischen Programmierers und Mathematikers wurde vor allem bezüglich seines Satzes »Cypherpunks write code«[466] bekannt, der später auch als pointiert antipolitische Parole durch die Cypherpunks-Mailinglisten geisterte: »If you want to change the world, don't protest. Write code!«[467] Mit seiner Definition zielte Hughes auf die Praxis ab, Verschlüsselungssoftware (gratis) bereitzustellen. Zugleich warnt Hughes wie May vor den Staaten und bürokratischen Unternehmen, die aufgrund ihrer eigenen Interessen unweigerlich die Privatsphäre der Menschen untergraben. Dagegen kämpfen die Cypherpunks mit ihrem Angebot an Verschlüsselungstechnologien: »We the Cypherpunks are dedicated to building anonymous systems. We are defending our privacy with cryptography, with anonymous mail forwarding systems, with digital

462 Vgl. Bey: The Temporary Autonomous Zone, 2001, S. 410ff.

463 Vgl. Hakim Bey; Sugár, János: Interview of Peter Lamborn Wilson (Hakim Bey), <https://www.nettime.org/nettime/DOCS/1/wilson.html>, Stand: 14.10.2021.

464 Hakim Bey interviewed by geekgirl, Nettime, 1997, <https://www.nettime.org/nettime/DOCS/2/04(2).html>, Stand: 02.11.2021.

465 May: THE CYPHERNOMICON: Cypherpunks FAQ and More, 1994.

466 Hughes, Eric: A Cypherpunk's Manifesto, 1993. Online: <https://www.activism.net/cypherpunk/manifesto.html>, Stand: 17.06.2021.

467 Zitiert nach Finney, Hal: Politics vs Technology, 02.01.1994, <http://web.archive.org/web/20130513043046/http://finney.org/~hal/pol_v_tech.html>, Stand: 05.05.2022. Hal Finney, der in seinem kurzen Essay *Politics vs Technology* mit dem Zitat beginnt, kritisiert die Vorstellung und den Rückzug aus der Politik als naiv und falsch, zeigte sich doch gerade in der Auseinandersetzung um den *Clipper Chip*, dass Technologie allein nicht automatisch zum Ziel führt.

signatures, and with electronic money.«[468] Dass Hughes ebenfalls digitales Geld als Mittel der künftigen Anonymität aufführt, hängt ähnlich wie bei May damit zusammen, dass er Transaktionen als zentrale Basis des sozialen Handelns betrachtete. So wird etwa Bargeld bei ihm in der damaligen Verwendung zum Vorbild für ein System anonymer (und nicht geheimer) Transaktionen. Kaufe ich beispielsweise an einem Kiosk ein Magazin, so Hughes' Beispiel, brauche ich dafür dem Kioskverkäufer nicht meine Identität preiszugeben. Analog dazu ermögliche der verschlüsselte Austausch im Netz, seine Identität nur dann zu veröffentlichen, wenn man es auch will.

Die anonyme Transaktion wird zum Vorbild des sozialen Austausches im Cyberspace, der, so May in seiner libertären Vision *Libertaria in Cyberspace* (1992), denjenigen Raum bildet, der »is more hospitable than physical locations for the kind of ›crypto anarchy‹ libertarian system I've been describing«[469]. Mit ›Libertaria‹ spielt May auf die libertären Ideen der 70er-Jahre an, sich eine Insel zu kaufen, um dort das eigene Paradies zu entwickeln – dass die meisten von May genannten Vorbilder dazu, »Vanuatu, Minerva, Mike Oliver, Tonga«[470], allesamt schon bewohnt waren, spielte in der libertären Kolonialfantasie bezeichnenderweise nie eine Rolle. Im Gegensatz zu diesen pazifischen Südseeinseln erscheint der Cyberspace »more promising. There is more ›space‹ in cyberspace, thus allowing more security and more colonizable space.«[471] Wiederum verweist May dabei auf die Verschlüsselungstechnologie und die dezentralisierten Zugänge, die im Gegensatz zur lokalisierbaren Insel verhindern sollen, dass mächtige Staaten das libertäre Paradies kaputtmachen – eine Erfahrung, die Mike Oliver mit seiner libertären ›*Republic of Minerva*‹ erleiden musste: Nachdem der amerikanische Millionär 1972 auf dem pazifischen Atoll eine Republik ausgerufen hatte, die er mit Sand auffüllen wollte, um sie bewohnbar zu machen, und auf der es keine Steuern, staatliche Wohlfahrt oder ökonomische Intervention geben sollte, nahm das anliegende Tonga das Gebiet kurzerhand ein.[472] So weit Mays digitaler Raum von diesen neokolonialen Experimenten entfernt war, so verwandt war seine Cyberspaceimagination mit den früheren libertären Kolonialfantasien. May träumte von einem digitalen Raum, in dem jeder seine eigene Existenz aufbauen kann und in dem, von jeder staatlichen Intervention befreit, nur noch Selbstregulation und das Privatrecht (als im Austausch selbst abgemachtes flexibles Recht zwischen zwei HandelspartnerInnen) gilt, da es keine höhere Instanz als den freien Austausch zweier anonymer HandelspartnerInnen gibt: »Alice and Bob[473], our favorite cryptographic stand-ins, can communicate and transact business without ever meeting or even knowing who the other is. This can be extended to create virtual communities subject only to rules they themselves reach agreement on […]. Private law

468 Hughes: A Cypherpunk's Manifesto, 1993.

469 May, Timothy: Libertaria in Cyberspace, 1992. Online: <https://nakamotoinstitute.org/libertaria-in-cyberspace/#selection-3.32-3.172>, Stand: 21.06.2021.

470 Ebd.

471 Ebd.

472 Vgl. Budds, Diana: This failed utopia from the 1970s sparked an international dispute, in: Curbed, 12.07.2019. Online: <https://archive.curbed.com/2019/7/12/20690898/republic-of-minerva-south-pacific-michael-oliver>, Stand: 21.06.2021.

473 Zwei fiktive Figuren, die oft als Platzhalterinnen in kryptografischen Diskussionen und Anschauungsbeispielen dienen.

is the only law, as there is no appeal to some higher authority like the Pope or police.«[474] Diese Vision, eine virtuelle Ordnung zu erschaffen, in der jeder Lebensbereich durch Marktbeziehungen geregelt ist und in der jeder zum gleichberechtigten Marktteilnehmer werden kann, um so seine Entfaltungsmöglichkeiten zu verbessern, wurde von anderen Cypherpunks geteilt, wie sich im Folgenden zeigt – auch in literarischen Beiträgen.[475]

Cypherpunk Fiction

Wie schon im Non-Fiction-Cyberpunk spielten die literarischen Vorbilder für die Visionen der Cypherpunks eine wichtige Rolle. Levy nennt beispielsweise drei Science-Fiction-Romane, die von den Cypherpunks intensiv gelesen und die NeueinsteigerInnen empfohlen wurden: Orson Scott Cards *Ender's Game*, in dem digitale Pseudonyme Verwendung finden, John Brunners *Shock-Wave Rider*, das zeige, was passiert, wenn eine vernetzte Gesellschaft die Privatsphäre unterdrückt, und Vinges *True Names*, das die mitunter problematische Verbindung zwischen elektronischer und physischer Identität herstelle.[476] May selbst verweist (neben Bruce Schneiers *Applied Cryptography* und Hakim Beys *TAZ*)[477] zusätzlich zu *True Names*, *Ender's Game* und *Neuromancer* auf Sterlings *Islands in the Net* und Stephensons *Snow Crash*.[478] Die Begeisterung für diese Romane basierte vor allem auf der Bedeutung der Anonymität, der neuen Wirtschaftsräume (zum Beispiel Sterlings Datenhäfen) und des Kampfes gegen den Überwachungsstaat. So konnte May beispielsweise *True Names* einiges an Realitätssinn abgewinnen: »Arguably, Mr. Slippery is already here and, as Vernor predicted, the Feds are already trying to track him down.«[479] Unter diesem Eindruck entstand, so zumindest die nachträgliche Reflexion Mays, dann auch das *Crypto Anarchist Manifesto.*[480] Gleichzeitig wurden allerdings

474 May: Libertaria in Cyberspace, 1992.

475 Auch in Essays finden sich Versionen solcher Vorstellungen. Duncan Frissell erläuterte beispielsweise auf der Cypherpunk-Mailliste als Antwort auf einen Artikel von Dorothy Denning, die konservativ und staatstragend die libertäre Vision der Abschaffung staatlicher Institutionen kritisierte, wie Crypto-AnarchistInnen einzig aufzeigen wollten, dass der zukünftige Markt im Cyberspace nicht mehr länger in den Händen verschiedener höhergestellter Autoritäten sei, »but rather in the hands of those trading on the markets«. (Frissell, Duncan: Re: Denning's Crypto Anarchy, in: Ludlow, Peter (Hg.): Crypto Anarchy, Cyberstates, and Pirate Utopias, Cambridge, Massachusetts 2001 (Digital communication), S. 106. Vgl. Denning, Dorothy: The Future of Cryptography, in: Ludlow, Peter [Hg.]: Crypto Anarchy, Cyberstates, and Pirate Utopias, Cambridge, Massachusetts 2001 [Digital communication], S. 85–101.)

476 Vgl. Levy: Crypto Rebels, 1993.

477 Vgl. May: True Nyms and Crypto Anarchy, 1996, S. 28.

478 Vgl. May: Libertaria in Cyberspace, 1992; May: THE CYPHERNOMICON: Cypherpunks FAQ and More, 1994.

479 May: True Nyms and Crypto Anarchy, 1996, S. 27.

480 Besonders viel vertiefte Forschung zum Verhältnis zwischen den literarischen Vorbildern und den Cyberpunks gibt es nicht. Eine Ausnahme bildet Enrico Beltramini, für den hinter diesem literarischen Einfluss zugleich eine Transformation des Menschenbildes steht. Während der Mensch beziehungsweise die Masse in den dystopischen Cyberpunk-Welten dazu prädestiniert sind, manipuliert zu werden, besitzt das menschliche Wesen bei den Cyberpunks die positive Grundlage, die neue Technologie stärker als Empowerment zu verwenden. Ob das Bild bei den Cyberpunks

die technologischen und politischen Zukunftsvisionen der Science-Fiction-Geschichten angezweifelt. May beispielsweise warf den Cyberpunk-Autoren in seinem, neben dem Manifest, zweiten bekannten Essay *Crypto Anarchy and Virtual Communities* (1994) vor, dass in deren Zukunftsvisionen Megakonzerne als parastaatliche Gebilde agieren.[481] Doch wenn man sich die Zukunft des Netzes anschaue, dann seien Unternehmen nur eine von mehreren Einheiten, die im Cyberspace künftig mit dem Staat in Konkurrenz treten würden. Dabei, so der zweite Vorwurf, blieb der Cyberspace kein metaphysischer Traum. Im Gegensatz zu *Snow Crash*, so May, dessen Protagonist im Cyberspace ein Held und reich an Reputation, in der Realität jedoch (zumindest bis kurz vor Schluss) arm ist, sei der Wohlstandstransfer vom Netz in die Realität durchaus möglich[482] – und, wie der erfolgreiche Handel im Cyberspace zeige, auch bereits an der Tagesordnung. So ging es May weniger um eine »virtual reality-photorealistic images-Jaron Lanier sort of thing«[483] oder andere Science-Fiction-Visionen – wenn auch er an anderer Stelle davon ausgeht, dass 3D-VR und textbasierte Systeme miteinander verschmelzen werden[484] –, sondern um einen real zu verwirklichenden libertären Netztraum. Bereits textbasierte Systeme, wie etwa die Mailinglisten, erscheinen da als potenzielle Grundlage libertärer Communitys im Cyberspace.

Die Cypherpunks konnten auch auf literarische Neuerscheinungen zurückgreifen. 1999 veröffentlichte Neal Stephenson mit *Cryptonomicon* (bereits rückwirkend) das ›Epos‹ der Cypherpunks, das viele von May angesprochene Themen aufnimmt und sie, anders als die Cyberpunk-Romane, in der Gegenwart beziehungsweise in der Vergangenheit verortet – Stephenson betonte, dass der Titel ein Wortspiel aus H. P. Lovecrafts *Necronomicon* sei und nicht etwa aus Mays *Cyphernomicon* abgeleitet sei. In zwei parallelen und indirekt miteinander verknüpften Handlungssträngen beschäftigt sich der gut 900 Seiten umfassende Roman erstens mit Verschlüsselungstechnologien während des Zweiten Weltkrieges. Die spätere Entwicklung, so einer der damit zusammenhängenden Gedanken, lässt sich nicht ohne die informationstheoretische und kryptografische Forschung denken, die in dieser Zeit entstand. Zugleich lässt sich die alte Technik in zeitgenössischeren Situationen nutzen, in denen man den Staat oder persönliche Feinde vom Zuhören abhalten will, beispielsweise wenn man im Gefängnis sitzt und nicht will, dass die Kommunikation abgehört wird. Der zweite Strang handelt von den Möglichkeiten neuer digitaler Verschlüsselungstechnologien. Das Start-up Epiphyte Corporation will in einem fiktiven Königreich zwischen den Philippinen und Malaysia einen sicheren Datenhafen errichten. Dieser soll künftig nicht nur als Cloud für Firmen dienen, sondern auch, frei von staatlicher Zensur und Interessen, die Menschheit schützende Informationen speichern. Dazu verspricht der Sultan der Insel wie »a scruffy hacker talking to a

---

allerdings tatsächlich derart dystopisch angelegt ist, gerade was die Nutzungsmöglichkeiten neuer Technologien betrifft, kann angezweifelt werden. (Vgl. Beltramini, Enrico: True Names, True Nyms. The Power of Technology and the Future of Identity., in: Messages, Sages and Ages 7 (1), 2019, S. 12–23.).

481 Vgl. May: Crypto Anarchy and Virtual Communities, 2001, S. 67.

482 Vgl. ebd., S. 73.

483 May: Libertaria in Cyberspace, 1992.

484 Vgl. May: Crypto Anarchy and Virtual Communities, 2001, S. 67.

room full of crypto-anarchists«[485] »total freedom of information«[486]. Aus Offshore-Banking wird Offshore-Datenspeicherung, und die HackerInnen sind die zentralen AkteurInnen dieser Entwicklung. Parallel dazu kündigt *Cryptonomicon* die Gründung einer verschlüsselten digitalen Währung an, die die Macht der Staaten ebenfalls unterläuft – die Vision lag auch hier mitunter nahe an der Realität beziehungsweise an deren Wünschen und Visionen: 1997 berichtete beispielsweise das *Wired* über die von Vincent Cate mitinitiierte *First International Conference on Financial Cryptography*, ein Treffen von achtzig Cypherpunks – »mostly anarchists and libertarians«[487] –, die sich in Anguilla über die Zukunft des digitalen Finanzwesens unterhielten. Dass man dabei das karibische Steuerparadies als Konferenzort wählte, macht gemäß dem Autor Charles Platt auch deswegen Sinn, weil sich darin eine Parallele zu den eigenen Cyberspaceimaginationen eröffnete: »It's undeveloped territory, like the Net. It's uncommercialized, virtually crime-free, informal, untaxed, and unregulated. Best of all, the local government is so small and unobtrusive, it creates a utopian feeling of freedom.«[488] Und dieser Zustand sollte mit den verschlüsselten ›Kryptowährungen‹ auch zukünftig erhalten bleiben.

Stephensons Roman vermittelt die Einführung der digitalen Währung ebenfalls als logische Fortführung der entstaatlichten und dezentralisierten Verschlüsselungstechnologien. Unterläuft man damit erst einmal die Macht des Staates, gibt es auch keinen Grund mehr, auf dessen Zentralbanken beziehungsweise dessen Monopol zur Geldschöpfung Rücksicht zu nehmen[489] – dank eines gigantischen, von Japan am Ende des Zweiten Weltkrieges vergrabenen Goldschatzes, der im zweiten Handlungsstrang dank Entschlüsselung alter verschlüsselter Funksprüche wieder hervorgehoben wird, lässt sich dafür auch noch ein neuer Goldstandard hervorzaubern, der die Stabilität unabhängig abzusichern vermag. Der Roman ist sich einiger Ambivalenzen seiner porträtierten Entwürfe durchaus bewusst.[490] Kryptogeld dient beispielsweise auch der Geldwäsche oder der persönlichen Bereicherung, je mehr der Bau des Datenhafens fortschreitet, desto größer werden die Verstrickungen und Interessen verschiedener mafiöser oder parastaatlicher Strukturen, und das Sultanat ist letztlich ebenso ein Staat, auf dessen *Goodwill* man angewiesen ist. Letztlich hofft der Roman allerdings, mit seinen Erfindungen eine neue Stabilität in die durch Finanzkrisen und Korruption gescholtenen Regionen zu bringen, indem die Macht der bisherigen Autoritäten gebrochen

485 Stephenson, Neal: Cryptonomicon, London 2000, S. 317.

486 Ebd., S. 319.

487 Platt: Plotting Away in Margaritaville, 1997.

488 Ebd.

489 Michael Tratner verbindet Stephensons Kryptowährung unter anderem deswegen mit Milton Friedmans Verständnis von entmaterialisiertem Geld als codierte Ordnungsinstanz (vgl. Tratner, Michael: Crypto-Economics: Neal Stephenson, Milton Friedman, and Post-Modernism, in: Lewis, Jon [Hg.]: Tomorrow through the Past. Neal Stephenson and the Project of Global Modernization, Cambridge 2006, S. 98–113.). Dies liest sich entgegen der positiven Referenz auf den Goldstandard als notwendige Grundlage monetärer Stabilität, die Friedman ablehnt, die allerdings bei neueren libertären DenkerInnen durchaus auf Anklang stieß, da man sich daraus weniger politischen Einfluss auf den Geldfluss erhoffte.

490 Vgl. Youngquist, Paul: Cyberpunk, War, and Money: Neal Stephenson's »Cryptonomicon«, in: Contemporary Literature 53 (2), 2012, JSTOR, S. 349.

wird.[491] Dies gilt auch für den Datenhafen und die moderne Verschlüsselungstechnologie. Beides leitet sich aus einer grundlegenden Kritik an der Internetstruktur ab, die in ihrem gegenwärtigen Zustand für ungleiche Machtverhältnisse sorgt. Wenn Daten durch »a small number of choke-points«[492] fließen, die »are controlled and monitored by local governments«[493], »then, any Internet application that wants to stand free of governmental interference is undermined, from the very beginning, by a fundamental structure problem«[494]. Verschlüsselungstechnologien liefern die notwendige Korrektur für dieses Problem, indem sie sowohl den sicheren Austausch zwischen zwei oder mehr KommunikationsteilnehmerInnen ermöglichen, als auch einen sicheren Speicherplatz für abrufbare Informationen bieten. Bedingung hierfür ist eine Privatisierung der Informationen und Plattformen, wie sie in *Cryptonomicon* durch den Bau des Datenhafens vorangetrieben wird.

Als dessen eigentliches Ziel wird der Schutz der Menschheit vor ihrem größten Verbrechen deklariert.[495] So dient die Cloud als Speicherort für den *Holocaust Education and Avoidance Pod* (HEAP), ein Informationspaket, das auf alle Ewigkeiten hin sicher gespeichert und über den Datenhafen verteilt werden soll und das alle notwendigen Informationen enthält, wie die Menschheit künftig Genozide verhindern soll, beispielsweise durch Taktiken, wie man sich gegen eine autoritäre Regierung wehren kann.[496] HEAP wird zugleich zum Zweck der Betreiberfirma des Datenhafens, die mit ihrem Profit das Informationsprojekt verbreiten soll. Ausgerüstet mit einem egalitäreren Kommunikationsnetzwerk abseits staatlicher Einmischung wird der freie Markt zum Retter seiner eigenen Verfehlungen. Stephensons Vision ist ein reinerer Kapitalismus ohne regulierende Einflüsse.[497] Für dieses Ziel kehren sich selbst die größten Verbrechen um, so die Lektüre von Paul Youngquist.[498] Das japanische Gold etwa, das der brutalen kolonialen Enteignungspraxis entspringt, wird zur Grundlage einer neuen Welt, in der eine private Firma und ihre Plattform mehr Freiheit bieten als staatliche Institutionen.

Während *Cryptonomicon* eine zumindest literarisch elaborierte Version der kryptoanarchistischen Vision darstellt, schrieb Stephenson mit *The Great Simoleon Caper* (1995) für die *Time*-Ausgabe zum Cyberspace auch eine agitativere Variante, die sich heute wie eine schlechte Werbung für Kryptowährungen liest.[499] Die Kurzgeschichte spielt in der Welt des Metaverse, das einer Synthese von Internet, Glasfaserverbindungen, HDTV und digitalem Bargeld entspricht, so Stephensons im Vergleich zu *Snow Crash* vereinfachte

491 Vgl. ebd., S. 342.

492 Stephenson: Cryptonomicon, 2000, S. 317.

493 Ebd.

494 Ebd.

495 Vgl. Youngquist: Cyberpunk, War, and Money: Neal Stephenson's »Cryptonomicon«, 2012, S. 342.

496 Dieses (naive) Ideal, mittels frei zugänglicher und unzensierter Informationen die Welt schützen zu können, ist vielleicht auch der Grund dafür, dass Julian Assange *Cryptonomicon* einst als eines der für ihn einflussreichsten Bücher beschrieb.

497 Vgl. Tratner: Crypto-Economics: Neal Stephenson, Milton Friedman, and Post-Modernism, 2006, S. 99.

498 Vgl. Youngquist: Cyberpunk, War, and Money: Neal Stephenson's »Cryptonomicon«, 2012, S. 342ff.

499 Vgl. Stephenson, Neal: The Great Simoleon Caper, in: Time, 01.03.1995. Online: <http://content.time.com/time/subscriber/article/0,33009,982610,00.html>, Stand: 29.07.2021.

Definition. Darin wurden die ›Simoleons‹ entwickelt, eine freie digitale Währung, die Menschen, so das Versprechen der Hersteller, einen Ausweg aus der Inflation und dem schlechten Haushalten der Regierung bieten soll. Diesen Angriff auf sich selbst will die amerikanische Regierung allerdings nicht hinnehmen. Als Gegenmaßnahme plant sie, den Gründungsanlass der ›Simoleons‹, bei dem diese durch einen Wettbewerb verteilt werden sollen, zu sabotieren. Dieser Plan läuft jedoch schief, da er von einer Gruppe von ›*Cryptoanarchists*‹ oder ›*Panarchists*‹, so die beiden verwendeten Bezeichnungen, verhindert wird. Die KryptoanarchistInnen haben dank eines Informanten nicht nur Zugang zu Staatsgeheimnissen, die sie verschlüsselt weitergeben können, sondern bieten auch eine Perspektive, die über die Simoleons hinausgeht. Im Metaverse haben sie *The First Distributed Republic* gegründet, einen »virtual nation-state«[500], dessen Währung die verschlüsselten »CryptoCredits«[501] bilden. Dass die AnarchistInnen als erste Amtshandlung einen neuen Staat gründen, ist bereits komisch genug. Wenn Stephenson dann noch auf die Vorzüge des digitalen Staates hinweist, wird seine Kurzgeschichte endgültig zur simplen libertären Parabel: Die Stärke des neuen Staates und seiner Währung besteht nämlich einzig darin, dass man die Steuern umgehen kann. Davon wird schließlich auch der CEO der Simoleons überzeugt. In seinem ersten Treffen mit einem Kryptoanarchisten fragt er ihn unglaubwürdig: »You can rig it so that people who use E-money don't have to pay taxes to any government? Ever?« Die Antwort darauf und damit auch die Botschaft von Stephenson ist einfach: »›You got it,‹ the big panarchist says.«[502] So führt der Anarchist den CEO in die libertäre Welt des freien Marktes des Cyberspace ein, in dem die Regierung nichts zu suchen hat.

›Kryptowährungen‹ und *Digital Cash*

Stephensons literarische Idee eines digitalen und verschlüsselten Geldes existierte bereits seit Längerem. Der amerikanische Computerwissenschaftler David Chaum veröffentlichte 1983 Vorschläge zu einem verschlüsselten und anonymen Geldsystem[503] und wiederholte diese Vision auch in verschiedenen späteren Essays.[504] 1990 gründete er mit DigiCash gar eine eigene Firma, die anonymere Transaktionen im Netz ermöglichen sollte – das Unternehmen ging 1998 noch vor dem Höhepunkt der Dot-Com-Blase pleite. Verschiedene VertreterInnen der libertären Cyberkultur waren von Chaums Ideen angetan und entwickelten sie mit direktem oder indirektem Bezug weiter. Einen Schritt weiter ging beispielsweise Wei Dai mit seinem ›B-Money‹, einem 1998 erschienenen Vorschlag für eine Kryptowährung beziehungsweise einem dafür notwendigen Protokoll, der sich als Mischung von May, Stephenson und Cyberpunk-Romantik liest. Dai beginnt seinen kurzen Aufsatz dazu mit seiner Bewunderung für »Tim May's crypto-anarchy«[505],

500 Ebd.

501 Ebd.

502 Ebd.

503 Vgl. Chaum, David: Blind Signatures for Untraceable Payments, in: Chaum, David; Rivest, Ronald; Sherman, Alan (Hg.): Advances in Cryptology, Boston, MA 1983, S. 199–203.

504 Vgl. Chaum, David: Achieving Electronic Privacy, in: Scientific American 267 (2), 08.1992, S. 96–101.

505 Dai, Wei: b-money, 11.1998. Online: <www.weidai.com/bmoney.txt>, Stand: 05.05.2022.

in der Regierungen, nicht wie im klassischen Anarchismus, nur temporär zerstört, sondern »permanently forbidden and permanently unnecessary«[506] werden. Bis anhin sei weder praktisch noch theoretisch klar gewesen, wie sich dieses Ziel erreichen lässt, insbesondere deshalb nicht, weil eine ›Community‹ durch die Zusammenarbeit der TeilnehmerInnen definiert sei, was wiederum ein Tauschmittel benötige, in dessen gängigster Form das Geld nur durch Regierungen beziehungsweise Regierungsformen ausgegeben beziehungsweise legitimiert werden konnte. Dank der vorgeschlagenen digitalen und verschlüsselten Währung, deren Wert, wie in heutigen Kryptowährungen, im direkten Handeln ermittelt wird und deren Ausgabe periodisch in einem Zusatzprotokoll vorherbestimmt sein könnte, sollte diese staatliche Aufgabe nun aber überflüssig werden, wodurch gleich auch die Bedingungen erschaffen werden würden, die den Staat selbst überflüssig machen.

Solche wiederkehrenden Ankündigungen weckten Hoffnungen. Kevin Kelly widmete dem elektronischen (und verschlüsselten) Geld mit Bezug auf Chaum, May und die Cypherpunks in *Out of Control* beispielsweise ein ganzes Kapitel über das »key element« der »anticipated information economy«[507], worin er dem »encrypted e-money« dasselbe Potenzial für die Transformation der ökonomischen Strukturen zusprach wie »personal computers did for overhauling management and communication structure«[508]. Wie genau dies geschehen sollte, blieb jedoch im Dunkeln, zumidest abseits der Hinweise auf das per E-Mail versendbare Geld, die angedeuteten Möglichkeiten der anonymisierten Kommodifizierung von Informationen oder die automatisierten Zahlungssysteme für den Nahverkehr, wie sie vor allem in europäischen, staatlich finanzierten Systemen auf Interesse stießen. John Barlow sinnierte ebenfalls über verschlüsseltes digitales Geld, das bald schon zum wichtigen Wirtschaftsfaktor werden könnte: »It is imaginable that, with the widespread use of digital cash and encrypted monetary exchange on the Global Net, economies the size of America's could appear as nothing but oceans of alphabet soup.«[509] Stärker als Kelly verknüpfte Barlow damit offen libertäre Hoffnungen. So sollte beispielsweise der Staat und insbesondere seine (Steuer-)Institutionen mit dem digitalen Geld hinfällig werden: »The payment of taxes might become more or less voluntary.«[510]

Auch die Cypherpunks wurden durch Chaum beeinflusst.[511] Timothy May konkretisierte die Ideen dahinter beispielsweise, wie später Dai, selbst weiter. So veröffentlichte er 1993 (erst anonym) die *Introduction to BlackNet*. Das BlackNet sollte eine über eine per PGP verschlüsselte Remailer-Mailingliste funktionierende Handelsplattform werden – ein Angebot im ›Darknet‹, wie man das heute wohl nennen würde, dessen Handelsanfragen per anonymisierten Mitteilungen gesendet werden konnten, das aber in seiner

506 Ebd.

507 Kelly: Out of Control, 2008, S. 189.

508 Ebd., S. 194.

509 Barlow: A Plain Text on Crypto Policy, 1993, S. 22.

510 Ebd.

511 Diese Begeisterung galt auch für andere Vorschläge von Chaum. Vgl. May: Crypto Anarchy and Virtual Communities, 2001, S. 66.

Anzeige des Angebots auf öffentliche Systeme wie das Usenet zurückgreifen konnte. Anonymisiert sollten darauf von Waffenplänen bis Firmengeheimnissen Informationen jeder Art gehandelt werden. Wie in vergleichbaren Projekten entstand dabei auch rasch die Frage, wie weit man gehen würde, zum Beispiel bezüglich der Frage, was passiert, wenn jemand Mordpläne in Auftrag gab. May antwortete auf dieses Problem stets mit denselben, für den amerikanischen Diskurs typischen Argumenten. Erstens zeige sich, dass, nur weil man eine Plattform oder Technologie für etwas nutzen könne, dies nicht bedeutet, dass man es auch tut. Sonst müsse man auch andere Technologien verbieten und das *First Amendment*, das heißt die Meinungsfreiheit, einschränken. Zweitens hätten die Staaten und Diktatoren in den vergangenen Jahrhunderten weitaus mehr Menschen getötet, als man online jemals in Auftrag geben könnte.[512] Die moralische Frage hinter dem Auftragsmord blieb allerdings eine hypothetische Frage, denn *BlackNet* war vor allem ein libertäres Gedankenexperiment, wie sich die im *Crypto Anarchist Manifesto* vorgestellten Visionen konkretisieren könnten und was dies für Folgen hätte. In Mays Cyberspaceimagination würde »the beauty of the free market«[513] beispielsweise alte und bürokratische Hindernisse überwinden. »Export laws, patent laws, national security considerations and the like«[514] erscheinen für May nur noch als »relics of the pre-cyberspace era«[515] und »national borders are just speed bumps on the information highway.«[516]. Das war prinzipiell nicht neu und glich den Cyberspace-Hoffnungen von Barlow. Radikaler als bei diesem verschmilzt in Mays Vision aber der politische Gestus der eigenen Bewegung mit einem latenten Wunsch nach Profit. Das BlackNet beziehungsweise der verschlüsselte Cyberspace-Markt wäre nämlich nicht nur ein revolutionäres Projekt, so die am Ende der ersten Ankündigung folgende Parole – die ebenso aus Stephensons *Cryptonomicon* stammen könnte –, sondern zugleich ein profitables Unternehmen: »Join us in this revolutionary – and profitable – venture.«[517]

512 Vgl. ebd., S. 77.

513 May, Timothy: BlackNet Worries, in: Ludlow, Peter (Hg.): High Noon on the Electronic Frontier: Conceptual Issues in Cyberspace, Cambridge 1996, S. 246.

514 May, Timothy: Introduction to BlackNet, in: Ludlow, Peter (Hg.): High Noon on the Electronic Frontier: Conceptual Issues in Cyberspace, Cambridge 1996, S. 241.

515 Ebd.

516 May: BlackNet Worries, 1996, S. 249.

517 May: Introduction to BlackNet, 1996, S. 242.