

# Der erste dezentrale Annuity-Pool auf Blockchain-Basis - Aspekte der aktuariellen und technischen Umsetzung

qx-Club, 5. September 2023, 17 Uhr

- 1 Rückblick
- 2 Blockchain und Blocksurance
- 3 Annuity Pools
- 4 Blockchain Annuity

- 1. Technische Umsetzung
- 2. Banny

- **5** Ausblick
- **6** Q&A

© 2023 HBA-Consulting AG



#### Vertrauen ...

J. Cryptology (1991) 3: 99-111

Journal of Cryptology
© 1991 International Association for
Cryptologic Research

# 23.8.2023 - Pressemeldung Blockchain statt Börse

https://www.hanseatischeversicherungsboerse.de/

#### How To Time-Stamp a Digital Document<sup>1</sup>

Stuart Haber and W. Scott Stornetta
Bellcore, 445 South Street,
Morristown, NJ 07960-1910, U.S.A.
stuart@bellcore.com
stornetta@bellcore.com

Abstract. The prospect of a world in which all text, audio, picture, and video documents are in digital form on easily modifiable media raises the issue of how to certify when a document was created or last changed. The problem is to

time-stamp the data, not the medium. We propose computationally practical procedures for digital time-stamping of such documents so that it is infeating to a user either to back-date or to forward-date his document, even with the discount of a time-stamping service. Our procedures maintain complete privacy of the

documents themselves, and require no record-keeping by the time-stamping

Key words. Time-stamp, Hash.

Satoshin@gmx.com www.bitcoin.org

Bitcoin: A Peer-to-Peer Electronic Cash System

2008

heute

@ ifo Institut

Um 1500...



\*Lutherhaus, Wittenberg/Germany

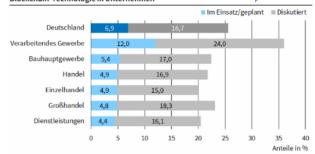
#### **Smart Contracts**

Copyright (c) 1994 by Nick Szabo permission to redistribute without alteration hereby granted

#### Glossary

A smart contract is a computerized transaction protocol that executes the terms of a contract, enforcement), minimize exceptions both malicious and accidental, and minimize the need for





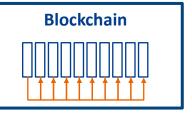
Quelle: ifo Konjunkturumfragen, Juni 2023.

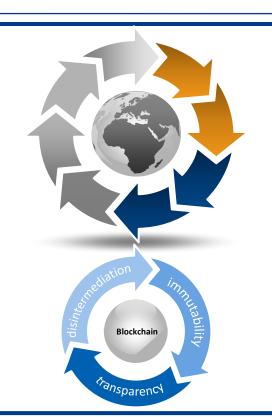
ujunkturumfragen, Juni 2023.

# Elemente der Digitalisierung und Automatisierung

- Abgestimmtes, elektronisches, unveränderliches gemeinsames
   Geschäftsbuch
- Ohne zentralen Ausfallpunkt
- Nachvollziehbare Transaktionen
- Leicht auditierbar
- (Daten)-Integrität im dezentralen System

System of transactions and records







# System of automation

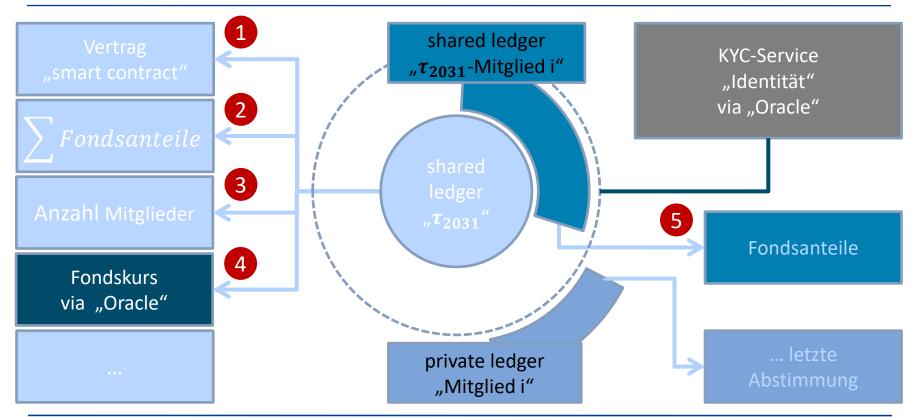
- Finheitliche Prozesse
- Hoher Automatisierungsgrad
- Echtzeit-Transaktionen
- Geringere Kosten
- Eingebautes Vertrauen
- (Prozess)-Integrität im dezentralen System

## Anwendungsfälle im Versicherungssektor

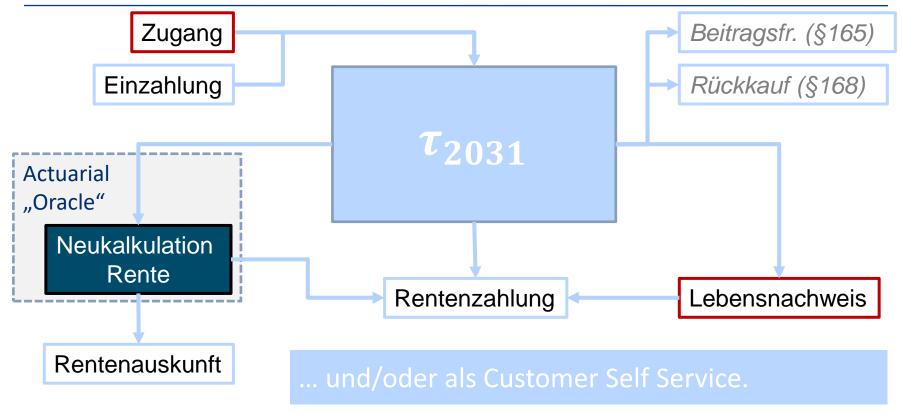
P2P-Versicherungen Geschäftsprozess Todesfallbearbeitung beneficiary hospital insurer blockchain register **Business-**Netzwerke Arbeitgeber VN insured Konsorte 1 claims payment trigger Neben-buch Kn insurer Parametrische Versicherungen Abrechnung zwischen Unternehmen

**BL®CKSURANCE** 

# Welche fünf Attribute braucht man unbedingt?



## Geschäftsvorfälle laufen automatisch ...



# **Banny-Team**













> ETHERISC

hba|consulting



## **Blockchain und Blocksurance**



# **BL6CKSURANCE**

## Blockchaintechnologie

2008: Veröffentlichung des Bitcoin Whitepaper Insbesondere ab 2015: Viele verschiedene Technologiestandards und Anwendungen

Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto satoshin@gmx.com www.bitcoin.org

Kryptowährungen waren für die Verbreitung von Blockchains tragend sind jedoch nicht die alleinige Nutzung

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

Löst zum ersten mal das Double Spend Problem und verbessert Lösungen z.B. für dezentralen Konsens

#### Was ist eine Blockchain?

Kombination aus bestehenden Technologien

Dezentrale, transaktionale Datenbank

Einheitliche Regeln werden verbindlich festgelegt, z.B. für:

- Lese- und Schreibrechte
- Gültige Transaktionen



#### Was ist eine Blockchain?

Eine Blockchain nutzt typischerweise 3 technische Konzepte:

- Hashing
  - Mathematische Einwegfunktion
  - Produziert einen stets Output mit fester Länge
- Public-Private-Key Encryption
  - Verschlüsselung auf Basis öffentlicher und privater Schlüssel
  - Kann zum Signieren von Nachrichten verwendet werden
- Merkle Trees
  - Methode zur schnellen Datenverifikation
  - Basiert auf Datenbäumen



#### Was bieten moderne Blockchains?

#### Cryptocurrencies und Tokens

- Digitale Repräsentation von Werten, die trotz der Dezentralität sicher "ausgegeben" werden können
- Können sowohl frei handelbare Werte sein (wie BTC, ETH) oder Token für eine bestimmte kontrollierte Nutzung innerhalb einer Anwendung/Ökosystem

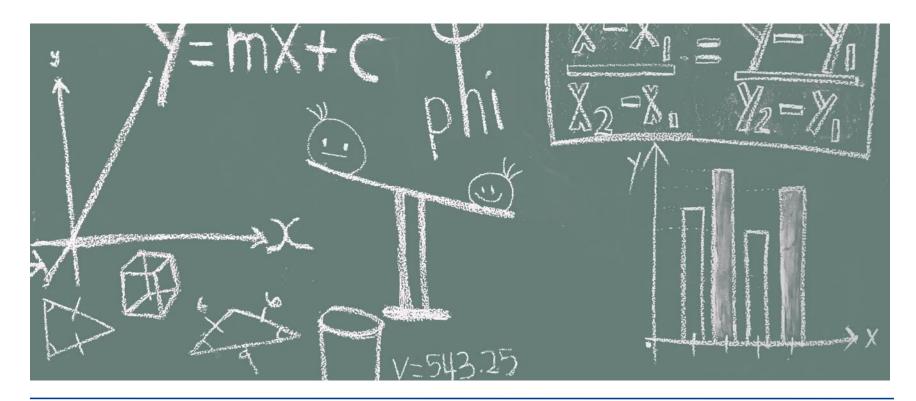


#### **Smart Contracts**

- Programmcode, der auf einer Blockchain gespeichert wird und mit dem jeder Nutzer interagieren kann
- Ist öffentlich auditierbar und läuft deterministisch ab, wenn die Bedingungen erreicht sind
- Kann durch Oracles Daten von außerhalb der Blockchain verwenden



# **Annuity Pools**

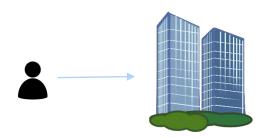


# Klassische Rente vs Annuity Pool

#### Klassische Rente:

Die Versicherungsnehmer geben ihr Risiko an ein Versicherungsunternehmen ab.

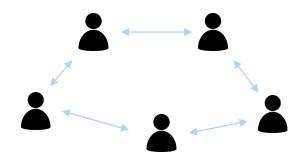
Risikomanagement: GGZ, vorsichtige Kalkulation mit Überschussbeteiligung, Pufferbildung



#### **Annuity Pool:**

Das Risiko wird zwischen den Versicherungsnehmern verteilt, aber nicht abgegeben.

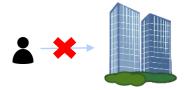
Risikomanagement: GGZ, Realistische Kalkulation, Verrechnung mit der Rentenhöhe



# **Mathematische Besonderheiten von Annuity Pools**

#### Keine Risikotransfer zum Versicherungsunternehmen

Realisierten Mortalität und Zins werden auf die Personen verteilt





#### Realistische Schätzwerte

Unrealistische/Vorsichtige Schätzwerte würden nicht für mehr Sicherheit sorgen, sondern junge und alte Versicherungsnehmer gegeneinander ausspielen

#### Äquivalenzprinzip und das "Alle Sterben"-Szenario

Annuity Pools zahlen nie mehr aus als Geld im Pool ist, aber können weniger auszahlen, wenn keine lebende Person mehr existiert.







#### Rechtlicher Rahmen in Deutschland

#### Betriebliche Altersvorsorge

Rechtlicher Rahmen seit 01.01.2018 durch das Betriebsrentenstärkungsgesetz.

- Steuer- und sozialversicherungsrechtliche Rahmenbedingungen
- Sozialpartnermodell f
   ür Arbeitgeber

#### Chronik:

- In den ersten Jahren keine Anbieter
- 2022 CHEMIE Pensionsfonds AG
- Andere Pensionsfonds/-kassen planen nach

#### Private Altersvorsorge (3. Schicht)

VAG Anlage 1/22

kann mit Genehmigung angeboten werden.

**Aber:** Kein "gleich bleibender oder steigender Bezug"

Keine Ertragsanteilsbesteuerung

Besteuerung nach § 20 (1) Nr. 6 EStG (wie Teilauszahlungen einer Kapitalversicherung

→ Lohnt sich deswegen aktuell nicht



## Übersicht bekannter mathematischer Modelle

# <u>Annuity Pools - Wackelrente oder</u> sinnvolle Produktinnovation?

Sandra Blome, Alexander Kling, and Jochen Ruß (2018)

- Korridor Methode
   → Nur bei starker Abweichung wird die Rentenhöhe angepasst
- Wird in der deutschen bAV verwendet

# The Simple Analytics of a Pooled Annuity Fund

Piggott, J., E. A. Valdez, and B. Detzel (2005)

- Regelmäßige Rentenanpassung
- Populär in ua den USA

Equitable retirement income tontines: Mixing cohorts without discriminating

Moshe Milevsky and Thomas Salisbury (2016)

- Mathematisch schön, da auch bei extremen Portfolios.
- In der Anwendbarkeit unpraktisch.

→ Für unsere Blockchain Anwendung am passendsten.



# The Simple Analytics of a Pooled Annuity Fund

Periodische Anpassung der Rente:

$$Rente(t) = Rente(t - 1) * MEA(t) * IRA(t)$$

Wobei

Interest Rate Adjustment

$$=\frac{realer\ Zins}{erwarteter\ Zins}$$

Mortality Experience Adjustment =  $\frac{erwartete "uberlebende" (gewichtet)"}{real "uberlebende" (gewichtet)}$ 

Alternative Darstellung: Vorhandenes Kapital anteilig an Lebende vererben

# Rechenbeispiel

Justus 50, Peter 50 und Bob 50 gründen einen Pooled Annuity Fund und zahlen jeweils 10 000€ ein.

In diesem Beispielszenario wird im ersten Jahr 5% Zinsen erwirtschaftet und niemand stirbt. Im zweiten Jahr werden -2% Zinsen erwirtschaftet und Bob stirbt.

Als Rechnungsgrundlagen wird die Sterbetafel "DAV 2004 R Selektionstafel 2. Ordnung" und der Rechnungszins 1,25% verwendet.

Policierung: 
$$Rentenh\"{o}he = \frac{Pr\"{a}mie}{a_x} = \frac{10\ 000€}{42.93855298} = 232,89 €$$
 (bei 1. Ordnung und 0,25% RZ: 163,56 €)

Jahr 1: 
$$Rente(1) = Rente(0) * MEA(1) * IRA(1) = 232,89 € * \frac{3*0,998531048}{3} * \frac{1,05}{1,0125} = 241,16 €$$

Jahr 2: 
$$Rente(2) = Rente(1) * MEA(2) * IRA(2) = 241,16 € * \frac{3*0,0,997977306}{2} * \frac{0,98}{1.0125} = 349,42 €$$

Beispielrechnung mit Altersverschiebung zu 2023



#### **Von der Theorie zur Praxis**

Blockchain Prozesse müssen exakt und vollständig definiert werden

- Kein nachträgliches rückgängig machen
- Kein Puffer für ungenaue Prozesse

Rentenauszahlung an Verstorbene kann nicht zurückgefordert oder aus Puffer ausgeglichen werden.

→ Rentenauszahlung müssen durch einen Lebensbescheinigung abgeholt werden.

Wird ein Lebensbescheinigung nicht innerhalb einer Karenzzeit eingereicht, so gilt die Person als verstorben und ihr Kapital wird vererbt.



Zu lange Karenzzeit → Spätes Vererben



Kurze Karenzzeit → Geringer Kundenkomfort

#### **Von der Theorie zur Praxis**

Rente(t) = Rente(t-1) \* MEA(t) \* IRA(t)

Exakte Berechnung benötigt Lebens-/Todesinfo aller Teilnehmer → erst nach Karenzzeit möglich → zu spät

Aufteilung der Rentenhöhe in direkt und später berechenbar:

$$\mathit{MEA}(t) = \min\bigl(\mathit{MEA}(t)\bigr) + \mathit{variabel}\bigl(\mathit{MEA}(t)\bigr)$$

Wobei: 
$$min(MEA(t)) = \frac{erwartete "uberlebende" (gewichtet)}{real "uberlebende" ALLE" (gewichtet)}$$

$$variabel(MEA(t)) = MEA(t) - min(MEA(t))$$

#### Von der Theorie zur Praxis

$$Rente(t) = Rente(t-1) * MEA(t) * IRA(t)$$

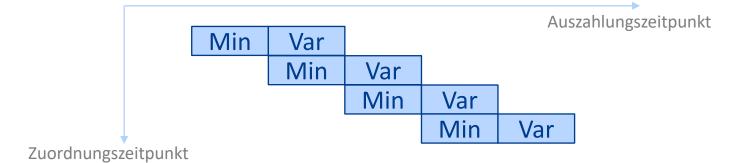
$$= Rente(t-1) * min(MEA(t)) * IRA(t) + Rente(t-1) * variabel(MEA(t)) * IRA(t)$$

Variablen Teil später auszahlen

$$= Rente(t-1) * min(MEA(t)) * IRA(t) + Rente(t-1) * variabel(MEA(t)) * IRA(t) * IRA(t+1)$$

Auszahlungszeitpunkt t

Auszahlungszeitpunkt t+1



# **Technische Umsetzung**



## **Exkurs: Etherisc & Generic Insurance Framework**

Führende Anbieter von blockchainbasierten und parametrischen Versicherungen

#### Bekannte Produkte:

- Flugverspätungsversichern
- Ernteausfallversicherung

Entwickler des Open Source Generic Insurance Frameworks

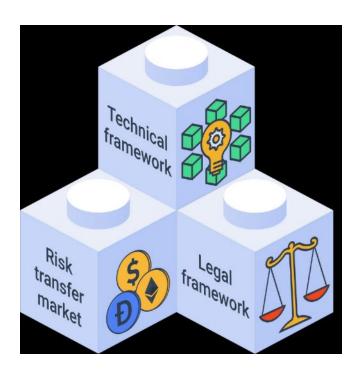


## **Exkurs: Etherisc & Generic Insurance Framework**

Das Generic Insurance Framework bietet die Möglichkeit individuelle Versicherungsprodukte standardisiert auf Basis von Blockchaintechnologie zu deployen

Besteht im wesentlichen aus den Komponenten:

- 1. Versicherungsprodukte
- 2. Oracles
- 3. Risikopools



# **Kooperation mit Etherisc**



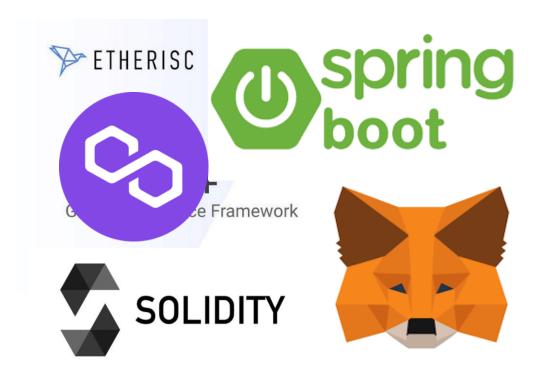
Seit ca. 1 Jahr kooperieren wir offiziell mit Etherisc

Erste blockchainbasierte Personenversicherung gemeinsam entwickelt und kurz vor der Veröffentlichung

Weiterentwicklung des GIFs für Personenversicherungen

## **Verwendet Technologien**

- Nutzung von
   Standardtechnologien
- Komplexe Mathematik Off-Chain berechnen
- Niederschwellige Nutzbarkeit
- Höchstmögliche Transparenz liefern
- Zukunftssichere Komponenten
- Wissensgewinn für das HBA-Lab



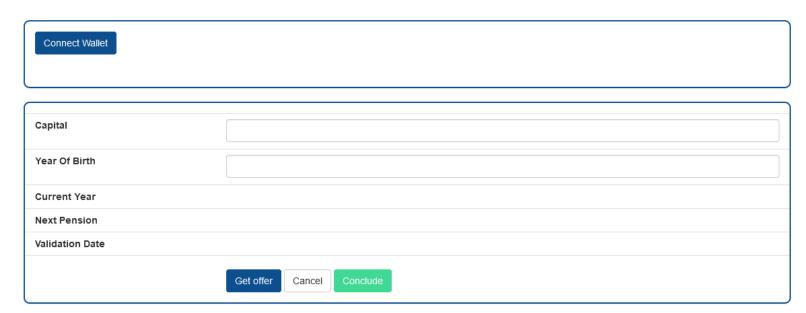
# **Banny – Blockchain Annuity**



BL&CKSURANCE

# **Banny - Lebenszyklus**

#### Blockchain Annuity



# **Banny - Lebenszyklus**

BL&CKSURANCE

# **Banny - Lebenszyklus**

## **Blockchain Annuity**

Connected with Wallet	
Address	0x69a5f9f5f281534fa57844130eb48e52ab24b9a6
Matic	1.190418460286769328
Stable	393804.929363

Capital	
Year Of Birth	
Current Year	
Next Pension	
Validation Date	
	Get offer Cancel Conclude

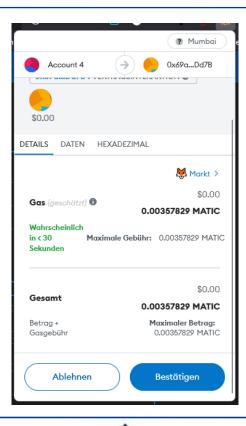
BL&CKSURANCE

© 2023 HBA-Consulting AG

Capital	10000		
Year Of Birth	1989		
Current Year	2035		
Next Pension	195.59		
Validation Date	04.09.2023		
	Get offer Cancel Conclude		

© 2023 HBA-Consulting AG

# **Banny - Lebenszyklus**



# **Banny - Lebenszyklus**



Capital	Year Of Birth	Next Pension	Validation Date	Process Id	
96195.07	1989	1919.06	18.08.2023	0x77dc0d4c	Collect pension
9808.01	1989	195.59	30.08.2023	0xcf2328ef	Collect pension
10000.00	1989	195.59	04.09.2023	0xbabbb05e	Collect pension



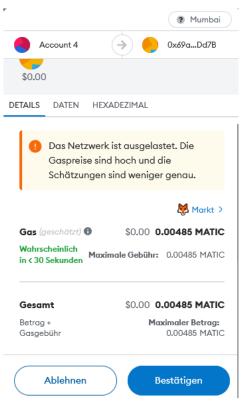


Capital	Year Of Birth	Next Pension	Validation Date	Process Id	
96195.07	1989	1919.06	18.08.2023	0x77dc0d4c	Collect pension
10000.00	1989	191.99	30.08.2023	0xcf2328ef	Collect pension
10000.00	1989	195.59	04.09.2023	0xbabbb05e	Collect pension

## **Banny - Lebenszyklus**



BL&CKSURANCE



-	hhΑ	new	
	, waa		

Capital	Year Of Birth	Next Pension	Validation Date	Process Id	
96195.07	1989	1919.06	18.08.2023	0x77dc0d4c	Collect pension
9808.01	1989	195.59	30.08.2023	0xcf2328ef	Collect pension
10000.00	1989	195.59	04.09.2023	0xbabbb05e	Collect pension

#### **Statistics**

# of Policies		15	Oldes	st Person	113	
# of Active Policies		13	Youn	gest Person	10	
# of Closed	l Policies	2	Avera	ige Age	61	
Capital		655320.10	Bigge	est Pension	18457.98	
Average Ca	apital	50409.24	Lowe	st Pension	0.00	
Unique Add	dresses	4	4 Averag		2111.86	
Current Year		2033	2033 Total Pensio		NaN	
Year	Sum of Pensions	Active Policies	Total Capital	Inherited Capital	Inheritance Rate	
2023	0.00	3	20000.01	0.00	0 %	
2024	516.14	4	29483.87	0.00	0 %	
2025	793.58	4	28690.29	0.00	0 %	
2026	799.89	4	27890.40	0.00	0 %	
2027	798.78	4	27091.62	0.00	0 %	
2028	797.37	6	46294.25	0.00	0 %	
2029	0.00	7	77709.25	0.00	0 %	
2030	516.73	7	77192.52	0.00	0 %	
2031	525.15	11	322777.38	0.00	0 %	
2032	21457.28	13	455320.10	200000.00	43.92514193124272 %	
2033	0.00	0	0.00	0.00	0 %	

## **Banny - Kollektivstatistiken**

# of Policies	15	Oldest Person	113
# of Active Policies	13	Youngest Person	10
# of Closed Policies	2	Average Age	61
Capital	655320.10	Biggest Pension	18457.98
Average Capital	50409.24	Lowest Pension	0.00
Unique Addresses	4	Average Pension	2111.86
Current Year	2033	Total Pension	NaN

## **Banny - Kollektivstatistiken**

Year	Sum of Pensions	Active Policies	Total Capital	Inherited Capital	Inheritance Rate
2023	0.00	3	20000.01	0.00	0 %
2024	516.14	4	29483.87	0.00	0 %
2025	793.58	4	28690.29	0.00	0 %
2026	799.89	4	27890.40	0.00	0 %
2027	798.78	4	27091.62	0.00	0 %
2028	797.37	6	46294.25	0.00	0 %
2029	0.00	7	77709.25	0.00	0 %
2030	516.73	7	77192.52	0.00	0 %
2031	525.15	11	322777.38	0.00	0 %
2032	21457.28	13	455320.10	200000.00	43.92514193124272 %
2033	0.00	0	0.00	0.00	0 %

### **Abschluss und Ausblick**



### **Ausblick**

- Interne Beta (14.09.2023-31.10.2023)
- Anmeldung zur öffentlichen Beta
- d1conf (16.11.2023)
- Start der öffentlichen Beta (20.11.2023)



## **Fragen und Antworten**



### **HBA-Consulting AG – Ihr Ansprechpartner**







Mathias Ott	Maximilian Sourisseau	Timo Stoll
mathias.ott@hba- consulting.de	m.sourisseau@hba- consulting.de	t.stoll@hba-consulting.de
0163 702 98 25	0170 635 1443	0 171 332 8312
https://www.linkedin.com/in/mathias-ott- 0b796110/	https://www.linkedin.com/in/maximiliansourisseau/	https://www.linkedin.com/in/timo-stoll- 5a02061b2/

Vervielfältigung und Weitergabe nur mit ausdrücklicher Genehmigung der HBA-Consulting AG

Standort 65510 Idstein, Tel. +49 (6126) 9566-0, E-Mail: <a href="mail@hba-consulting.de">mail@hba-consulting.de</a>, <a href="mail@hba-consulting.de">www.hba-consulting.de</a>, <a href="mail@www.hba-consulting.de">www.hba-consulting.de</a>, <a href="mail

Folie 48 05.09.2023